MP Agro- Security Test report

invicti

12/8/2023 5:08:52 PM (UTC+05:30)

Detailed Scan Report

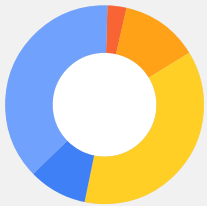
http://mpagroerp.tserver.co.in/mis/Login.aspx

Scan Time	: 12/8/2023 4:52:15 PM (UTC+05:30)
Scan Duration	: 00:00:14:39
Total Requests	: 7,904
Average Speed	: 9.0 r/s

Risk Level:
HIGH

32 IDENTIFIED	11 CONFIRMED	0 CRITICAL
1 HIGH	4 MEDIUM	12 LOW
	3 BEST PRACTICE	12 INFORMATION

Identified Vulnerabilities



Critical	0
High	1
Medium	4
Low	12
Best Practice	3
Information	12
TOTAL	**32**

Confirmed Vulnerabilities

Critical	0
High	1
Medium	2
Low	3
Best Practice	2
Information	3
TOTAL	**11**

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	Password Transmitted over HTTP	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	Out-of-date Version (jQuery)	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/assets/js/jquery-3.2.1.min.js	No Parameters	No Parameter Types
	SSL Certificate Name Hostname Mismatch	GET	https://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	Weak Ciphers Enabled	GET	https://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	[Possible] Cross-site Request Forgery in Login Form	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	Docker Cloud Stack File Detected	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/docker-cloud.yml	No Parameters	No Parameter Types
	Missing X-Frame-Options Header	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx/(%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)%3f(%23wr%3d%23context%5b%23parameters.obj%5b0%5d%5d.getWriter(),%23rs%3d@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec(%23parameters.command[0]).getInputStream()),%23wr.println(%23rs),%23wr.flush(),%23wr.close()):xx.toString.json?&obj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=cmd.exe%2...	No Parameters	No Parameter Types
	Programming Error Message	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/trace.axd	No Parameters	No Parameter Types

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	Stack Trace Disclosure (ASP.NET)	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx?nsextt=INJECTIONSTART889676%27%22*%2f%0d%0a%20%3c%3fphpINJECTIONEND	No Parameters	No Parameter Types
	Version Disclosure (ASP.NET)	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	Version Disclosure (IIS)	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	Version Disclosure (Jquery)	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/assets/js/jquery-3.2.1.min.js	No Parameters	No Parameter Types
	ViewState is not Encrypted	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	Autocomplete is Enabled	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	Internal Server Error	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx?nsextt=INJECTIONSTART889676%27%22*%2f%0d%0a%20%3c%3fphpINJECTIONEND	No Parameters	No Parameter Types
	Missing X-XSS-Protection Header	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx/(%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)%3f(%23wr%3d%23context%5b%23parameters.obj%5b0%5d%5d.getWriter(),%23rs%3d@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec(%23parameters.command[0]).getInputStream()),%23wr.println(%23rs),%23wr.flush(),%23wr.close()):xx.toString.json?&obj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=cmd.exe%2...	No Parameters	No Parameter Types
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	Subresource Integrity (SRI) Not Implemented	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	[Possible] Administration Page Detected	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/administrator/	No Parameters	No Parameter Types
	[Possible] Login Page Identified	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	data: Used in a Content Security Policy (CSP) Directive	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	default-src Used in Content Security Policy (CSP)	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	Email Address Disclosure	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/jquery.appear.min.js@r87.com	No Parameters	No Parameter Types
	HTTP Strict Transport Security (HSTS) via HTTP	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	IIS Identified	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	jQuery Identified	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/assets/js/jquery-3.2.1.min.js	No Parameters	No Parameter Types
	Autocomplete Enabled (Password Field)	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx	No Parameters	No Parameter Types
	Forbidden Resource	GET	http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/trace.axd	No Parameters	No Parameter Types

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	OPTIONS Method Enabled	OPTIONS	http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/	No Parameters	No Parameter Types

1. Password Transmitted over HTTP

HIGH 1 | CONFIRMED 1

Invicti Standard detected that password data is being transmitted over HTTP.

Impact

If an attacker can intercept network traffic, he/she can steal users' credentials.

Vulnerabilities

1.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

CONFIRMED

Input Name

- ctl00$ContentPlaceHolder1$txtUserPassword

Form target action

- http://mpagroerp.tserver.co.in/mis/Login.aspx

Form name

- aspnetForm

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Con
…
laceholder="User Name" />
<span class="glyphicon glyphicon-user form-control-feedback"></span>
</div>
<div class="form-group has-feedback">
<input name="ctl00$ContentPlaceHolder1$txtUserPassword" type="password" maxlength="50"
id="ctl00_ContentPlaceHolder1_txtUserPassword" class="form-control" placeholder="Password" />
<span class="glyphicon glyphicon-lock form-control-feedback"></span>
</div>
<div class="form-group has-feedback">
<div id="ctl00_ContentPla
…
```

Actions to Take

1. See the remedy for solution.
2. Move all of your critical forms and pages to HTTPS and do not serve them over HTTP.

Remedy

All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over HTTPS. All aspects of the application that accept user input, starting from the login process, should only be served over HTTPS.

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	319
CAPEC	65
WASC	4
ASVS 4.0	2.2.5
NIST SP 800-53	SC-8
DISA STIG	V-16796
ISO27001	A.14.1.3
ISO27001 2022	A.8.5
ISO27001 2022	A.8.24
ISO27001 2022	A.8.27
ISO27001 2022	A.8.3
OWASP Top Ten 2021	A02

CVSS 3.0 SCORE

CVSS 3.0 SCORE	
Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)

CVSS Vector String
CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE	
Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)

CVSS Vector String
CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

2. HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM | 1

Invicti Standard identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Vulnerabilities

2.1. https://mpagroerp.tserver.co.in/mis/Login.aspx

Certainty

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 82.533
Total Bytes Received : 492
Body Length : 315
Is Compressed : No

```
HTTP/1.1 404 Not Found
Server: Microsoft-HTTPAPI/2.0
Connection: close
Content-Length: 315
Content-Type: text/html; charset=us-ascii
Date: Fri, 08 Dec 2023 11:22:52 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
       ServerAlias *
       RewriteEngine On
       RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

External References

- Wikipedia - HTTP Strict Transport Security

- Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx
- HTTP Strict Transport Security (HSTS) HTTP Header
- Mozilla SSL Configuration Generator

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ASVS 4.0	14.4.5
NIST SP 800-53	SC-8
DISA STIG	V-6136
ISO27001	A.14.1.2
ISO27001 2022	A.8.24
OWASP Top Ten 2021	A02

CVSS 3.0 SCORE

Base	7.7 (High)
Temporal	7.7 (High)
Environmental	7.7 (High)

CVSS Vector String

CVSS Vector String
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L

CVSS 3.1 SCORE	
Base	7.7 (High)
Temporal	7.7 (High)
Environmental	7.7 (High)

CVSS Vector String
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L

3. Out-of-date Version (jQuery)

MEDIUM | 1

Invicti Standard identified the target web site is using jQuery and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Cross Site Scripting vulnerability in jQuery 2.2.0 through 3.x before 3.5.0 allows a remote attacker to execute arbitrary code via the <options> element.

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2020-23064

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2020-11023

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2020-11022

JQuery Prototype Pollution Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Affected Versions

1.0 to

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2019-11358

Vulnerabilities

3.1. http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/assets/js/jquery-3.2.1.min.js

Identified Version
- 3.2.1

Latest Version
- 3.7.1

Vulnerability Database
- Result is based on 12/05/2023 20:30:00 vulnerability database content.

Certainty

Request | Response

Request

```
GET /mis/Login.aspx/assets/assets/js/jquery-3.2.1.min.js HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/c%3a%5cboot.ini
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 46.8713
Total Bytes Received : 18831
Body Length : 18111
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6506
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:34:53 GMT
Content-Encoding:
```

```
<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta charset="utf-8" /><meta http-equiv="x-ua-compatible" content="ie=edge" /><title>
MP AGRO - Official Website
</title><link rel="icon" href="../../../../../assets/images/logo1.png" /><meta name="description" />
<meta http-equiv="cache-control" content="no-cache" /><meta http-equiv="expires" content="0" /><meta
http-equiv="pragma" content="no-cache" /><meta name="viewport" content="width=device-width, initial-
scale=1, shrink-to-fit=no" /><link href="https://fonts.googleapis.com/css?
family=Poppins:300,300i,400,400i,500,500i,600,600i,700,700i,800,800i,900,900i" rel="stylesheet" /><link
href="https://fonts.googleapis.com/css?family=Open+Sans:400,400i,600,600i,700,700i,800,800i"
rel="stylesheet" /><link href="https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-
awesome.min.css" rel="stylesheet" /><link rel="icon" type="image/png" href="../../../../favicon.html"
/>
<!-- Place favicon.ico in the root directory -->
<link rel="apple-touch-icon" href="../../../../apple-touch-icon.html" /><link
href="../../../../../assets/css/fontawesome-min.css" rel="stylesheet" /><link rel="stylesheet"
href="../../../../../assets/css/bootstrap.min.css" /><link rel="stylesheet" href="../.
…
```

Remedy

Please upgrade your installation of jQuery to the latest stable version.

Remedy References

- Downloading jQuery

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	1035 , 937
CAPEC	310
HIPAA	164.308(a)(1)(i)
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	V-16836
OWASP Proactive Controls	C1
ISO27001	A.14.1.2
ISO27001 2022	A.8.19
OWASP Top Ten 2021	A06

4. SSL Certificate Name Hostname Mismatch

MEDIUM 1 | CONFIRMED 1

Invicti Standard detected a hostname mismatch in the SSL certificate. This happens when the common name to which an SSL Certificate is issued (e.g., www.example.com) doesn't exactly match the name displayed in the URL bar.

Impact

It can impact both website and the users:

- Warning error messages displayed by browsers when visiting the site
- Personal information at risk from man-in-the-middle attacks
- Reduction in trust as the site becomes insecure
- Ability for an attacker to create identical phishing website

Vulnerabilities

4.1. https://mpagroerp.tserver.co.in/mis/Login.aspx

CONFIRMED

Subject Name

- CN=payroll.tserver.co.in

Remedy

The process of fixing name-hostname mismatch issues varies depending on the host or the certificate authority used. Please refer to the corresponding documentation.

External References

- What Is an SSL Common Name Mismatch Error and How Do I Fix It?

CLASSIFICATION

OWASP 2017	A3
CWE	295
ASVS 4.0	1.9.2
NIST SP 800-53	SC-8
DISA STIG	V-6136
ISO27001 2022	A.8.24
OWASP Top Ten 2021	A02

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)

CVSS 3.1 SCORE	
Environmental	5.3 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

5. Weak Ciphers Enabled

MEDIUM | 1 | CONFIRMED | 1

Invicti Standard detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

5.1. https://mpagroerp.tserver.co.in/mis/Login.aspx

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009D)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009C)

Request | Response

Request

```
[SSL Connection]
```

Response

Response Time (ms) : 1
Total Bytes Received : 16
Body Length : 0
Is Compressed : No

```
[SSL Connection]
```

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

   a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
   b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- Zombie Poodle - Golden Doodle (CBC)
- Mozilla SSL Configuration Generator
- Strong Ciphers for Apache, Nginx and Lighttpd

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ASVS 4.0	6.2.5
NIST SP 800-53	SC-8
DISA STIG	V-6136
ISO27001	A.14.1.3
ISO27001 2022	A.8.24
OWASP Top Ten 2021	A02

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE	
Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

6. [Possible] Cross-site Request Forgery in Login Form

LOW | 1

Invicti Standard identified a possible Cross-Site Request Forgery in Login Form.

In a login CSRF attack, the attacker forges a login request to an honest site using the attacker's user name and password at that site. If the forgery succeeds, the honest server responds with a Set-Cookie header that instructs the browser to mutate its state by storing a session cookie, logging the user into the honest site as the attacker. This session cookie is used to bind subsequent requests to the user's session and hence to the attacker's authentication credentials. The attacker can later log into the site with his legitimate credentials and view private information like activity history that has been saved in the account.

Impact

In this particular case CSRF affects the login form in which the impact of this vulnerability is decreased significantly. Unlike normal CSRF vulnerabilities this will only allow an attacker to exploit some complex XSS vulnerabilities otherwise it can't be exploited.

For example;

If there is a page that's different for every user (such as "edit my profile") and vulnerable to XSS (Cross-site Scripting) then normally it cannot be exploited. However if the login form is vulnerable, an attacker can prepare a special profile, force victim to login as that user which will trigger the XSS exploit. Again attacker is still quite limited with this XSS as there is no active session. However the attacker can leverage this XSS in many ways such as showing the same login form again but this time capturing and sending the entered username/password to the attacker.

In this kind of attack, attacker will send a link containing html as simple as the following in which attacker's user name and password is attached.

```
<form method="POST" action="http://honest.site/login">
  <input type="text" name="user" value="h4ck3r" />
  <input type="password" name="pass" value="passw0rd" />
</form>
<script>
    document.forms[0].submit();
</script>
```

When the victim clicks the link then form will be submitted automatically to the honest site and exploitation is successful, victim will be logged in as the attacker and consequences will depend on the website behavior.

- **Search History**
  Many sites allow their users to opt-in to saving their search history and provide an interface for a user to review his or her personal search history. Search queries contain sensitive details about the user's interests and activities and could be used by the attacker to embarrass the user, to steal the user's identity, or to spy on the user. Since the victim logs in as the attacker, the victim's search queries are then stored in the attacker's search history, and the attacker can retrieve the queries by logging into his or her own account.

- **Shopping**
  Merchant sites might save the credit card details in user's profile. In login CSRF attack, when user funds a purchase and enrolls the credit card, the credit card details might be added to the attacker's account.

Vulnerabilities

6.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

Form Name(s)

- aspnetForm

Certainty

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Con
…
/css/colors/color-1.css" /> -->

<link href="css/AdminLTE.css" rel="stylesheet" />
</head>
<body id="fontSize" style="background-image: url('../assets/images/123.jpg');">
<form name="aspnetForm" method="post" action="./Login.aspx" id="aspnetForm">
<div>
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwUINTAzMTA0NzMPZBYCZg9kFgICAw9kFgoCAQ8WAh4LXyFJdGVtQ291bnQCARYCZg9kF
…
```

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
    - For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();
xhr.setRequestHeader('custom-header', 'valueNULL');
```

For JQuery, if you want to add a custom header (or set of headers) to
a. **individual request**

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

b. **every request**

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

External References

- OWASP Cross-Site Request Forgery (CSRF)
- Robust Defenses for Cross-Site Request Forgery
- Identifying Robust Defenses for Login CSRF

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

CLASSIFICATION

PCI DSS v3.2	6.5.9
OWASP 2013	A8
OWASP 2017	A5
CWE	352
CAPEC	62
WASC	9
HIPAA	164.306(a)
ASVS 4.0	4.2.2
NIST SP 800-53	SC-23
DISA STIG	V-21500
ISO27001	A.14.2.5
ISO27001 2022	A.8.26
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A01

7. Autocomplete is Enabled

LOW | 1 | CONFIRMED | 1

Invicti Standard detected that Autocomplete is Enabled in one or more of the form fields which might contain sensitive information like "username", "credit card" or "CVV".

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

Vulnerabilities

7.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

CONFIRMED

Identified Field Name

- ctl00$ContentPlaceHolder1$txtUserName

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Con
…
<br />
<span id="ctl00_ContentPlaceHolder1_LblMsg" style="color:Red;"></span>
</div>


<div class="form-group has-feedback">
<input name="ctl00$ContentPlaceHolder1$txtUserName" type="text" maxlength="50"
id="ctl00_ContentPlaceHolder1_txtUserName" class="form-control" placeholder="User Name" />
<span class="glyphicon glyphicon-user form-control-feedback"></span>
</div>
<div class="form-group has-feedback">
<input name="ctl00$Conten
…
```

Actions to Take

1. Add the attribute `autocomplete="new-password"` to the form tag or to individual "input" fields. Please note that modern browsers might ignore the previously recommended `autocomplete="off"` instruction, due to their integrated password management mechanism.
2. Find all instances of inputs that store private data and disable autocomplete. Fields which contain data such as "Credit Card" or "CCV" type data should not be cached. You can allow the application to cache usernames and remember passwords; however, in most cases this is not recommended.

3. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	2.10.3
NIST SP 800-53	AC-16
DISA STIG	V-16786
ISO27001	A.14.1.2
ISO27001 2022	A.5.34
ISO27001 2022	A.8.3
OWASP Top Ten 2021	A05

8. Docker Cloud Stack File Detected

LOW | 1

Invicti Standard detected the Docker Cloud Stack file.

Impact

Docker configuration file. Docker is an open platform for developers and sysadmins to build, ship, and run distributed applications.

Vulnerabilities

8.1. http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/docker-cloud.yml

Method	Parameter	Parameter Type	Value
GET	URI-BASED	FullUrl	docker-cloud.yml

Certainty

Request | Response

Request

```
GET /mis/Login.aspx/assets/js/docker-cloud.yml HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 30.6842
Total Bytes Received : 18777
Body Length : 18057
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6498
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:27:16 GMT
Con
…
link rel="stylesheet" type="text/css" href="../../../assets/css/colors/color-1.css" /> -->

<link href="css/AdminLTE.css" rel="stylesheet" />
</head>
<body id="fontSize" style="background-image: url('../assets/images/123.jpg');">
<form name="aspnetForm" method="post" action="./docker-cloud.yml" id="aspnetForm">
<div>
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEP
…
```

Remedy

Do not leave Docker Cloud Stack file on production environments.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A96
CWE	527
CAPEC	118
WASC	13
ASVS 4.0	1.10.1
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Top Ten 2021	A05

CVSS 3.0 SCORE

Base	4 (Medium)
Temporal	4 (Medium)
Environmental	4 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N

CVSS 3.1 SCORE	
Base	4 (Medium)
Temporal	4 (Medium)
Environmental	4 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N

9. Insecure Transportation Security Protocol Supported (TLS 1.0)

LOW 1 | CONFIRMED 1

Invicti Standard detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 are considered non-compliant by PCI since 30 June 2018.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Vulnerabilities

9.1. https://mpagroerp.tserver.co.in/mis/Login.aspx

CONFIRMED

Request | Response

Request

```
[SSL Connection]
```

Response

Response Time (ms) : 1
Total Bytes Received : 16
Body Length : 0
Is Compressed : No

```
[SSL Connection]
```

Actions to Take

We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf` file and remove `TLSv1`.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
    1. Click on Start and then Run, type `regedt32` or `regedit`, and then click OK.
    2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\
```

    3. Locate a key named `Server` or create if it doesn't exist.
    4. Under the `Server` key, locate a DWORD value named `Enabled` or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

External References

- How to Disable TLS v1.0 on Windows Server 2019 and Windows Server 2016
- How to Disable TLS v1.0 on Windows Server 2012 and Windows Server 2008
- OWASP - Insecure Configuration Management
- OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
- How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services
- IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012
- Date Change for Migrating from SSL and Early TLS
- Browser Exploit Against SSL/TLS Attack (BEAST)
- Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	326
CAPEC	217
WASC	4
HIPAA	164.306
ASVS 4.0	9.1.2
NIST SP 800-53	SC-8
DISA STIG	V-6136
ISO27001	A.14.1.3
ISO27001 2022	A.8.24
OWASP Top Ten 2021	A02

10. Internal Server Error

LOW | 1 | CONFIRMED | 1

Invicti Standard identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Invicti Standard is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Invicti Standard will check for other possible issues and report them separately.

Vulnerabilities

10.1. http://mpagroerp.tserver.co.in/mis/Login.aspx?nsextt=INJECTIONSTART889676%27%22*%2f%0d%0a%20%3c%3fphpINJECTIONEND

CONFIRMED

Method	Parameter	Parameter Type	Value
GET	nsextt	Querystring	INJECTIONSTART889676'"*/ <?phpINJECTIONEND

Request | Response

Request

```
GET /mis/Login.aspx?nsextt=INJECTIONSTART889676%27%22*%2f%0d%0a%20%3c%3fphpINJECTIONEND HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 5063.6777
Total Bytes Received : 6832
Body Length : 6136
Is Compressed : No

```
HTTP/1.1 500 Internal Server Error
X-Content-Type-Options: nosniff
Server: Microsoft-IIS/10.0
Referrer-Policy: no-referrer
Access-Control-Allow-Origin: domain
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
X-Frame-Options: SAMEORIGIN
Date: Fri, 08 Dec 2023 11:23:42 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Expect-CT: enforce, max-age=43200
Content-Type: text/html; charset=utf-8
Permissions-Policy: fullscreen=()
Content-Length: 6136
X-XSS-Protection: 1; HTTP/1.1 500 Internal Server Error

X-Content-Type-Options: nosniff
Server: Microsoft-IIS/10.0
Referrer-Policy: no-referrer
Access-Control-Allow-Origin: domain
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; st
…
```

Remedy

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.

CLASSIFICATION

CWE	550
WASC	13
NIST SP 800-53	SI-11
DISA STIG	V-6166
ISO27001	A.14.1.2
ISO27001 2022	A.8.15
ISO27001 2022	A.8.26
ISO27001 2022	A.8.27

11. Missing X-Frame-Options Header

LOW | 1

Invicti Standard detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

11.1. http://mpagroerp.tserver.co.in/mis/Login.aspx/(%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)%3f(%23wr%3d%23context%5b%23parameters.obj%5b0%5d%5d.getWriter(),%23rs%3d@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec(%23parameters.command[0]).getInputStream()),%23wr.println(%23rs),%23wr.flush(),%23wr.close()):xx.toString.json?&obj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=cmd.exe%20/c%20set%20/a%20268409241%20-%2072847

Method	Parameter	Parameter Type	Value
GET	URI-BASED	FullUrl	`/(%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)%3f(%23wr%3d%23context%5b%23parameters....`

Certainty

Request | Response

Request

```
GET
/mis/Login.aspx/(%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)%3f(%23wr%3d%23context%5b%2
3parameters.obj%5b0%5d%5d.getWriter(),%23rs%3d@org.apache.commons.io.IOUtils@toString(@java.lang.Runtim
e@getRuntime().exec(%23parameters.command[0]).getInputStream()),%23wr.println(%23rs),%23wr.flush(),%23w
r.close()):xx.toString.json?
&obj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=cmd.exe%20/c%20set%20/a%20268409241
%20-%2072847 HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 8.5814
Total Bytes Received : 503
Body Length : 324
Is Compressed : No

```
HTTP/1.1 400 Bad Request
Server: Microsoft-HTTPAPI/2.0
Connection: close
Content-Length: 324
Content-Type: text/html; charset=us-ascii
Date: Fri, 08 Dec 2023 11:23:33 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request - Invalid URL</h2>
<hr><p>HTTP Error 400. The request URL is invalid.</p>
</BODY></HTML>
```

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
    - `X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.
    - `X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.
    - `X-Frame-Options: ALLOW-FROM` *URL* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

- Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

- Clickjacking
- Can I Use X-Frame-Options
- X-Frame-Options HTTP Header

Remedy References

- Clickjacking Defense Cheat Sheet

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ASVS 4.0	14.4.7
NIST SP 800-53	CM-6
DISA STIG	V-16786
OWASP API Top Ten 2019	API7
ISO27001	A.14.2.5
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A05

12. Programming Error Message

LOW | 1

Invicti Standard identified a Programming Error Message.

Impact

The error message may disclose sensitive information and this information can be used by an attacker to mount new attacks or to enlarge the attack surface. Source code, stack trace, etc. data may be disclosed. Most of these issues will be identified and reported separately by Invicti Standard.

Vulnerabilities

12.1. http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/trace.axd

Method	Parameter	Parameter Type	Value
GET	URI-BASED	FullUrl	trace.axd

Identified Error Message

- Exception of type 'System.Web.HttpException' was thrown.

Certainty

Request | Response

Request

```
GET /mis/Login.aspx/assets/js/trace.axd HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 14.1522
Total Bytes Received : 4109
Body Length : 3425
Is Compressed : No

```
HTTP/1.1 403 Forbidden
X-Content-Type-Options: nosniff
Server: Microsoft-IIS/10.0
Referrer-Policy: no-referrer
Access-Control-Allow-Origin: domain
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
X-Frame-Options: SAMEORIGIN
Date: Fri, 08 Dec 2023 11:26:36 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Expect-CT: enforce, max-age=43200
Content-Type: text/html; charset=utf-8
Permissions-Policy: fullscreen=()
Content-Length: 3425
X-XSS-Protection: 1; mode=block

…
=silver>

<b>Version Information:</b> Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.9206.0

</font>

</body>
</html>
<!--
[HttpException]: Exception of type &#39;System.Web.HttpException&#39; was thrown.
at System.Web.Handlers.TraceHandler.System.Web.IHttpHandler.ProcessRequest(HttpContext context)
at System.Web.HttpApplication.CallHandlerExecutionStep.System.Web.HttpApplication.IExecutionSte
…
```

Remedy

Do not provide error messages on production environments. Save error messages with a reference number to a backend storage such as a log, text file or database, then show this number and a static user-friendly error message to the user.

CLASSIFICATION

PCI DSS v3.2	6.5.5
OWASP 2013	A5
OWASP 2017	A6
CWE	210
CAPEC	118
WASC	13
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	7.4.1
NIST SP 800-53	SI-11
DISA STIG	V-6166
OWASP API Top Ten 2019	API7
ISO27001	A.18.1.3
ISO27001 2022	A.8.15
ISO27001 2022	A.8.9
OWASP Top Ten 2021	A05

13. Stack Trace Disclosure (ASP.NET)

LOW | 1

Invicti Standard identified a stack trace disclosure (ASP.NET) in the target web server's HTTP response.

Impact

An attacker can obtain information such as:

- ASP.NET version.
- Physical file path of temporary ASP.NET files.
- Information about the generated exception and possibly source code, SQL queries, etc.

This information might help an attacker gain more information and potentially focus on the development of further attacks for the target system.

Vulnerabilities

13.1. http://mpagroerp.tserver.co.in/mis/Login.aspx?nsextt=INJECTIONSTART889676%27%22*%2f%0d%0a%20%3c%3fphpINJECTIONEND

Method	Parameter	Parameter Type	Value
GET	nsextt	Querystring	INJECTIONSTART889676'"*/ <?phpINJECTIONEND

Certainty

Request | Response

Request

```
GET /mis/Login.aspx?nsextt=INJECTIONSTART889676%27%22*%2f%0d%0a%20%3c%3fphpINJECTIONEND HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 5063.6777
Total Bytes Received : 6832
Body Length : 6136
Is Compressed : No

```
HTTP/1.1 500 Internal Server Error
X-Content-Type-Options: nosniff
Server: Microsoft-IIS/10.0
Referrer-Policy: no-referrer
Access-Control-Allow-Origin: domain
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
X-Frame-Options: SAMEORIGIN
Date: Fri, 08 Dec 2023 11:23:42 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Expect-CT: enforce, max-age=43200
Content-Type: text/html; charset=utf-8
Permissions-Policy: fullscreen=()
Content-Length: 6136
X-XSS-Protection: 1;
…
ception can be identified using the exception stack trace below. </code>

</td>
</tr>
</table>

<br>

<b>Stack Trace:</b> <br><br>

<table width=100% bgcolor="#ffffcc">
<tr>
<td>
<code><pre>

[HttpRequestValidationException (0x80004005): A potentially dangerous Request.QueryString value was
detected from the client (nsextt=&amp;quot;...676&amp;#39;&amp;quot;*/
&amp;lt;?phpINJECTIONEND&amp;quot;).]
S
…
```

Remedy

Apply following changes on your `web.config` file to prevent information leakage by applying custom error pages.

```
<System.Web>
     <customErrors mode="On" defaultRedirect="~/error/GeneralError.aspx">
          <error statusCode="403" redirect="~/error/Forbidden.aspx" />
          <error statusCode="404" redirect="~/error/PageNotFound.aspx" />
          <error statusCode="500" redirect="~/error/InternalError.aspx" />
     </customErrors>
</System.Web>
```

Remedy References

- Error Handling in ASP.NET Pages and Applications

CLASSIFICATION

PCI DSS v3.2	6.5.5
OWASP 2013	A5
OWASP 2017	A6
CWE	248
CAPEC	214
WASC	14
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	7.4.1
NIST SP 800-53	SI-11
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
ISO27001	A.9.2.3
ISO27001 2022	A.8.15
ISO27001 2022	A.8.9
OWASP Top Ten 2021	A05

14. Version Disclosure (ASP.NET)

LOW | 1

Invicti Standard identified a version disclosure (ASP.NET) in the target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of ASP.NET.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

14.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

Extracted Version

- 4.0.30319

Certainty

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Con
…
tion: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319

Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:
…
```

Remedy

Apply the following changes to your `web.config` file to prevent information leakage by using custom error pages and removing `X-AspNet-Version` from HTTP responses.

```
<System.Web>
     <httpRuntime enableVersionHeader="false" />
     <customErrors mode="On" defaultRedirect="~/error/GeneralError.aspx">
```

```
          <error statusCode="403" redirect="~/error/Forbidden.aspx" />
          <error statusCode="404" redirect="~/error/PageNotFound.aspx" />
          <error statusCode="500" redirect="~/error/InternalError.aspx" />
     </customErrors>
</System.Web>
```

Remedy References

- Error Handling in ASP.NET Pages and Applications
- Remove Unwanted HTTP Response Headers

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	13
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
ISO27001	A.18.1.3
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A05

15. Version Disclosure (IIS)

LOW | 1

Invicti Standard identified a version disclosure (IIS) in the target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of IIS.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

15.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

Extracted Version

- 10.0

Certainty

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
ConHTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0

X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length:
…
```

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	13
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Proactive Controls	N/A
ISO27001	A.18.1.3
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A05

16. Version Disclosure (Jquery)

LOW | 1

Invicti Standard identified a version disclosure (Jquery) in the target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Jquery.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

16.1. http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/assets/js/jquery-3.2.1.min.js

Identified Version

- 3.2.1.min

Certainty

Request | Response

Request

```
GET /mis/Login.aspx/assets/assets/js/jquery-3.2.1.min.js HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/c%3a%5cboot.ini
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 46.8713
Total Bytes Received : 18831
Body Length : 18111
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6506
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:34:53 GMT
Content-Encoding:
```

```
<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta charset="utf-8" /><meta http-equiv="x-ua-compatible" content="ie=edge" /><title>
MP AGRO - Official Website
</title><link rel="icon" href="../../../../../assets/images/logo1.png" /><meta name="description" />
<meta http-equiv="cache-control" content="no-cache" /><meta http-equiv="expires" content="0" /><meta
http-equiv="pragma" content="no-cache" /><meta name="viewport" content="width=device-width, initial-
scale=1, shrink-to-fit=no" /><link href="https://fonts.googleapis.com/css?
family=Poppins:300,300i,400,400i,500,500i,600,600i,700,700i,800,800i,900,900i" rel="stylesheet" /><link
href="https://fonts.googleapis.com/css?family=Open+Sans:400,400i,600,600i,700,700i,800,800i"
rel="stylesheet" /><link href="https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-
awesome.min.css" rel="stylesheet" /><link rel="icon" type="image/png" href="../../../../favicon.html"
/>
<!-- Place favicon.ico in the root directory -->
<link rel="apple-touch-icon" href="../../../../apple-touch-icon.html" /><link
href="../../../../../assets/css/fontawesome-min.css" rel="stylesheet" /><link rel="stylesheet"
href="../../../../../assets/css/bootstrap.min.css" /><link rel="stylesheet" href="../.
…
```

Remedy

Configure your web server to prevent information leakage.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	13
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
ISO27001	A.18.1.3
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A05

17. ViewState is not Encrypted

LOW | 1

Invicti Standard detected that ViewState Encryption is disabled.

Impact

An attacker can study the application's state management logic for possible vulnerabilities; if your application stores application-critical information in the ViewState, it will also be revealed.

Vulnerabilities

17.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

ViewState Version

- .NET Framework 2.x

Certainty

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Con
…
rel="stylesheet" />
</head>
<body id="fontSize" style="background-image: url('../assets/images/123.jpg');">
<form name="aspnetForm" method="post" action="./Login.aspx" id="aspnetForm">
<div>
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwUINTAzMTA0NzMPZBYCZg9kFgICAw9kFgoCAQ8WAh4LXyFJdGVtQ291bnQCARYCZg9kFgJmDxUBbOCkquCkguCkmuCk
vuCkqOCkqCDgpK3gpLXgpKgs4KSk4KWD4KSk4KWA4KSvIOCkpOCksiAsIOCkreCli+CkquCkvuCksiDgpIfgpILgpKHgpL/gpK/gpL4
gLOCkquCkv+CkqCAtIDQ2MjAwM2QCAw8WAh8AAgEWAmYPZBYCZg8VAyhiMWYzZTkxMy01MmMzLTRhZjgtYWZlMC1hNmNiNDJiNWM0YT
kucG5nKGViYjA3ZWJjLTk5NWEtNDU4Zi1hNDkzLTgwMTgzMzIwZWI4YS5wbmcoMzlmMDJhMWMtNmY4ZS00NWI1LWI3MzAtM2U3N2EwN
mFhOTVjLnBuZ2QCBQ8WAh8AAgEWAmYPZBYCZg8VASg0YjQ1OGNjNS1jN2YzLTQ2MTAtOGY4My03YTQzZTEyOGJkYjYucG5nZAIHDxYC
Hglpbm5lcmh0bWwF0g88dWwgY2xhc3M9J25hdi1tZW51Jz48bGkgY2xhc3M9Jyc+PGEgaHJlZj0nLi4vaW5kZXguYXNweCc+4KSu4KW
B4KSW4KWN4KSvIOCkquClg+Ckt+CljeCkoDwvYT48L2xpPjxsaSBjbGFzcz0nJz48YSBocmVmPScuLi9EZXB0U3RydWN0dXJlLmFzcH
gnPuCkteCkv+CkreCkvuCkl+ClgOCkryDgpLjgpILgpLDgpJrgpKjgpL48L2E+PC9saT48bGkgY2xhc3M9Jyc+PGEgaHJlZj0nLi4vQ
m9hcmREaXJlY3Rvci5hc3B4Jz7gpLjgpILgpJrgpL7gpLLgpJUg4KSu4KSC4KSh4KSyPC9hPjwvbGk+PGxpIGNsYXNzPScnPjxhIGhy
ZWY9Jy4uL0J1c2lu...
</div>

<div>

<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="BEEA8346" />
<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/wEdA
…
```

Remedy

ASP.NET provides encryption for ViewState parameters.

For page based protection, place the following directive at the top of affected page.

```
<%@Page ViewStateEncryptionMode="Always" %>
```

You can also set this option for the whole application by using `web.config` files. Apply the following configuration for your application's `web.config` file.

```
<System.Web>
    <pages viewStateEncryptionMode="Always">
</System.Web>
```

Remedy References

- ASP.NET View State Security

CLASSIFICATION

OWASP 2017	A6
CWE	16
WASC	15
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	6.2.7
NIST SP 800-53	CM-6
DISA STIG	V-16787
ISO27001	A.14.2.5
ISO27001 2022	A.8.9
OWASP Top Ten 2021	A05

18. Insecure Transportation Security Protocol Supported (TLS 1.1)

BEST PRACTICE | 1 | CONFIRMED | 1

Invicti Standard detected that a deprecated, insecure transportation security protocol (TLS 1.1) is supported by your web server.

TLS 1.1 will be considered as deprecated by major web browsers (i.e. Chrome, Firefox, Safari, Edge, Internet Explorer) starting in 2020.

Impact

Your website will be inaccessible due to web browser deprecation.

Vulnerabilities

18.1. https://mpagroerp.tserver.co.in/mis/Login.aspx

CONFIRMED

Request | Response

Request

```
[SSL Connection]
```

Response

Response Time (ms) : 1
Total Bytes Received : 16
Body Length : 0
Is Compressed : No

```
[SSL Connection]
```

Actions to Take

We recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf` file and remove `TLSv1.1`.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
    1. Click on Start and then Run, type `regedt32` or `regedit`, and then click OK.
    2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\
```

    3. Locate a key named `Server` or create if it doesn't exist.
    4. Under the `Server` key, locate a DWORD value named `Enabled` or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

External References

- Deprecating TLSv1.0 and TLSv1.1 draft-ietf-tls-oldversions-deprecate-00
- Google Security Blog: Modernizing Transport Security
- OWASP - Insecure Configuration Management
- OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
- IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012
- Date Change for Migrating from SSL and Early TLS

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	326
CAPEC	217
WASC	4
HIPAA	164.306
ASVS 4.0	9.1.2
NIST SP 800-53	SC-8
DISA STIG	V-6136
ISO27001	A.14.1.3
ISO27001 2022	A.8.24
OWASP Top Ten 2021	A02

19. Missing X-XSS-Protection Header

BEST PRACTICE | 1

Invicti Standard detected a missing `X-XSS-Protection` header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

19.1. http://mpagroerp.tserver.co.in/mis/Login.aspx/(%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)%3f(%23wr%3d%23context%5b%23parameters.obj%5b0%5d%5d.getWriter(),%23rs%3d@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec(%23parameters.command[0]).getInputStream()),%23wr.println(%23rs),%23wr.flush(),%23wr.close()):xx.toString.json?&obj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=cmd.exe%20/c%20set%20/a%20268409241%20-%2072847

Method	Parameter	Parameter Type	Value
GET	URI-BASED	FullUrl	/(%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)%3f(%23wr%3d%23context%5b%23parameters....

Certainty

Request | Response

Request

```
GET
/mis/Login.aspx/(%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)%3f(%23wr%3d%23context%5b%2
3parameters.obj%5b0%5d%5d.getWriter(),%23rs%3d@org.apache.commons.io.IOUtils@toString(@java.lang.Runtim
e@getRuntime().exec(%23parameters.command[0]).getInputStream()),%23wr.println(%23rs),%23wr.flush(),%23w
r.close()):xx.toString.json?
&obj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=cmd.exe%20/c%20set%20/a%20268409241
%20-%2072847 HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 8.5814
Total Bytes Received : 503
Body Length : 324
Is Compressed : No

```
HTTP/1.1 400 Bad Request
Server: Microsoft-HTTPAPI/2.0
Connection: close
Content-Length: 324
Content-Type: text/html; charset=us-ascii
Date: Fri, 08 Dec 2023 11:23:33 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request - Invalid URL</h2>
<hr><p>HTTP Error 400. The request URL is invalid.</p>
</BODY></HTML>
```

Remedy

Add the X-XSS-Protection header with a value of "1; mode= block".

- `X-XSS-Protection: 1; mode=block`

Please also be advised that in some specific cases enabling XSS filter can be abused by attackers. However, in most cases, it provides basic protection for users against XSS attacks.

External References

- Internet Explorer 8 Security Features - MSDN
- X-XSS-Protection HTTP Header
- X-XSS-Protection
- XSS Auditors - Abuses, Updates and Protection

CLASSIFICATION

CWE	16
WASC	15
HIPAA	164.308(a)
NIST SP 800-53	CM-6
DISA STIG	V-16787
ISO27001	A.14.2.5
ISO27001 2022	A.8.27

20. Subresource Integrity (SRI) Not Implemented

BEST PRACTICE | 1 | CONFIRMED | 1

Subresource Integrity (SRI) provides a mechanism to check integrity of the resource hosted by third parties like Content Delivery Networks (CDNs) and verifies that the fetched resource has been delivered without unexpected manipulation.

SRI does this using hash comparison mechanism. In this way, hash value declared in HTML elements (for now only script and link elements are supported) will be compared with the hash value of the resource hosted by third party.

Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

Vulnerabilities

20.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

CONFIRMED

Identified Sub Resource(s)

- https://fonts.googleapis.com/css?family=Poppins:300,300i,400,400i,500,500i,600,600i,700,700i,800,800i,900,900i
- https://fonts.googleapis.com/css?family=Open Sans:400,400i,600,600i,700,700i,800,800i
- https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Con
…
l" content="no-cache" /><meta http-equiv="expires" content="0" /><meta http-equiv="pragma" content="no-
cache" /><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><link
href="https://fonts.googleapis.com/css?
family=Poppins:300,300i,400,400i,500,500i,600,600i,700,700i,800,800i,900,900i" rel="stylesheet" /><link
href="https://fonts.googleapis.com/css?family=Open+Sans:400,400i,600,600i,700,700i,800,800i"
rel="stylesheet" /><link href="https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-
awesome.min.css" rel="stylesheet" /><link rel="icon" type="image/png" href="favicon.html" />
<!-- Place favicon.ico in the root directory -->
<link rel="apple-touch-icon" href="apple-touch-icon.html" /><link href="../assets/
…
```

Remedy

Using Subresource Integrity is simply to add *integrity* attribute to the *script* tag along with a base64 encoded cryptographic hash value.

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js" integrity="sha384-
R4/ztc4ZlRqWjqIuvf6RX5yb/v90qNGx6fS48N0tRxiGkqveZETq72KgDVJCp2TC" crossorigin="anonymous"></script>
```

The hash algorithm must be one of **sha256**, **sha384** or **sha512**, followed by a '-' character.

External References

- Subresource Integrity
- Do not let your CDN betray you: Use Subresource Integrity
- Web Application Security with Subresource Integrity
- SRI Hash Generator

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	10.3.2 , 14.2.3
NIST SP 800-53	CM-6
DISA STIG	V-16786
ISO27001	A.14.2.5
ISO27001 2022	A.5.14
ISO27001 2022	A.8.27

21. [Possible] Administration Page Detected

INFORMATION | 1

Invicti Standard detected a possible administration page.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

21.1. http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/administrator/

Method	Parameter	Parameter Type	Value
GET	URI-BASED	FullUrl	/administrator/

Certainty

Request | Response

Request

```
GET /mis/Login.aspx/assets/js/administrator/ HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 22.5062
Total Bytes Received : 18812
Body Length : 18092
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6488
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:27:10 GMT
Con
…
glyphicon glyphicon-user form-control-feedback"></span>
</div>
<div class="form-group has-feedback">
<input name="ctl00$ContentPlaceHolder1$txtUserPassword" type="password" maxlength="50"
id="ctl00_ContentPlaceHolder1_txtUserPassword" class="form-control" placeholder="Password" />
<span class="glyphicon glyphicon-lock form-control-feedback"></span>

…
```

Remedy

You should manually investigate the found URL.

CLASSIFICATION

PCI DSS v3.2	6.5.8
OWASP 2013	A7
OWASP 2017	A5
CWE	425
CAPEC	87
WASC	34
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP Proactive Controls	C6
ISO27001	A.9.4.1
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A01

CVSS 3.0 SCORE

Base	5.3 (Medium)

CVSS 3.0 SCORE	
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE	
Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

22. [Possible] Login Page Identified

INFORMATION | 1

Invicti Standard identified a login page on the target website.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

22.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

form.action

- ./Login.aspx

window.location.pathname

- /mis/Login.aspx

input.id

- ctl00_ContentPlaceHolder1_txtUserName

Certainty

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Con
…
href="assets/css/colors/color-1.css" /> -->

<link href="css/AdminLTE.css" rel="stylesheet" />
</head>
<body id="fontSize" style="background-image: url('../assets/images/123.jpg');">
<form name="aspnetForm" method="post" action="./Login.aspx" id="aspnetForm"><form name="aspnetForm"
method="post" action="./Login.aspx" id="aspnetForm"><form name="aspnetForm" method="post"
action="./Login.aspx" id="aspnetForm">
<div>
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwUINTAzMTA0NzMPZBYCZg9kFgICAw9kFgoCAQ8WAh4LXyFJdGVtQ291bnQCARYCZg9kFgJmDxUBbOCkquCkguCkmuCk
vuCkqOCkqCDgpK3gpLXgpKgs4KSk4KW
…
```

CLASSIFICATION

OWASP Proactive Controls	C6

23. An Unsafe Content Security Policy (CSP) Directive in Use

INFORMATION | 1

Invicti Standard detected that one of following CSP directives is used:

- unsafe-eval
- unsafe-inline

By using `unsafe-eval`, you allow the use of string evaluation functions like `eval`.

By using `unsafe-inline`, you allow the execution of inline scripts, which almost defeats the purpose of CSP. When this is allowed, it's very easy to successfully exploit a Cross-site Scripting vulnerability on your website.

Impact

An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully.

Vulnerabilities

23.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

Unsafe Directive(s) Used In Csp

- unsafe-inline, unsafe-eval

Certainty

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Con
…
tions: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Content-Encoding:



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta charset="utf-8" /><meta ht
…
```

Remedy

If possible remove `unsafe-eval` and `unsafe-inline` from your CSP directives.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP) HTTP Header
- Content Security Policy (CSP)

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	14.4.3
NIST SP 800-53	CM-6
DISA STIG	V-16786
ISO27001	A.14.2.5
ISO27001 2022	A.8.27

24. Autocomplete Enabled (Password Field)

INFORMATION 1 | CONFIRMED 1

Invicti Standard detected that autocomplete is enabled in one or more of the password fields.

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

Vulnerabilities

24.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

CONFIRMED

Identified Field Name

- ctl00$ContentPlaceHolder1$txtUserPassword

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Con
…
laceholder="User Name" />
<span class="glyphicon glyphicon-user form-control-feedback"></span>
</div>
<div class="form-group has-feedback">
<input name="ctl00$ContentPlaceHolder1$txtUserPassword" type="password" maxlength="50"
id="ctl00_ContentPlaceHolder1_txtUserPassword" class="form-control" placeholder="Password" />
<span class="glyphicon glyphicon-lock form-control-feedback"></span>
</div>
<div class="form-group has-feedback">
<div id="ctl00_ContentPla
…
```

Actions to Take

1. Add the attribute `autocomplete="off"` to the form tag or to individual "input" fields. However, since early 2014, major browsers don't respect this instruction, due to their integrated password management mechanism, and offer to users to store password internally.
2. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the

data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

External References

- How to turn off form autocompletion

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	2.10.3
NIST SP 800-53	CM-6
DISA STIG	V-16786
ISO27001	A.14.1.2
ISO27001 2022	A.8.3
OWASP Top Ten 2021	A05

CVSS 3.0 SCORE

Base	4.6 (Medium)
Temporal	4.6 (Medium)
Environmental	4.6 (Medium)

CVSS Vector String

CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE	
Base	4.6 (Medium)
Temporal	4.6 (Medium)
Environmental	4.6 (Medium)

CVSS Vector String
CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

25. data: Used in a Content Security Policy (CSP) Directive

INFORMATION | 1

Invicti Standard detected `data:` use in a CSP directive.

Impact

An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully by using `data:` protocol.

Vulnerabilities

25.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

Data Directive Used

- data:

Certainty

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Con
…
tf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Content-Encoding:



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta charset="utf-8" /><meta http-equiv="x-ua-compatible" conte
…
```

Remedy

Remove `data:` sources from your CSP directives.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP)
- Content Security Policy (CSP) HTTP Header

CLASSIFICATION

ASVS 4.0	14.4.3
NIST SP 800-53	CM-6
DISA STIG	V-16786
ISO27001	A.14.2.5
ISO27001 2022	A.8.27

26. default-src Used in Content Security Policy (CSP)

INFORMATION | 1

Invicti Standard detected that you used *default-src* in CSP directive. It is important to know that *default-src* cannot be used as a fallback for the functions below:

```
base-uri

form-action

frame-ancestors

plugin-types

report-uri

sandbox
```

Vulnerabilities

26.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

Certainty

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Con
…
missions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
Content-Encoding:




…
```

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP)
- Content Security Policy (CSP) HTTP Header

CLASSIFICATION

ASVS 4.0	14.4.3
NIST SP 800-53	CM-6
DISA STIG	V-16787
OWASP Proactive Controls	C9
ISO27001	A.14.2.5
ISO27001 2022	A.8.27

27. Email Address Disclosure

INFORMATION | 1

Invicti Standard identified an Email Address Disclosure.

Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Vulnerabilities

27.1. http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/jquery.appear.min.js@r87.com

Method	Parameter	Parameter Type	Value
GET	URI-BASED	FullUrl	@r87.com

Email Address(es)

- jquery.appear.min.js@r87.com

Certainty

Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

External References

- Wikipedia - Email Spam

CLASSIFICATION

CWE	200
CAPEC	118
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP Proactive Controls	C7
ISO27001	A.9.4.1
ISO27001 2022	A.8.3

CVSS 3.0 SCORE

Base	0 (None)
Temporal	0 (None)
Environmental	0 (None)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

CVSS 3.1 SCORE	
Base	0 (None)
Temporal	0 (None)
Environmental	0 (None)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

28. Forbidden Resource

INFORMATION 1 | CONFIRMED 1

Invicti Standard identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

28.1. http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/trace.axd

CONFIRMED

Method	Parameter	Parameter Type	Value
GET	URI-BASED	FullUrl	trace.axd

Request | Response

Request

```
GET /mis/Login.aspx/assets/js/trace.axd HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 14.1522
Total Bytes Received : 4109
Body Length : 3425
Is Compressed : No

```
HTTP/1.1 403 Forbidden
X-Content-Type-Options: nosniff
Server: Microsoft-IIS/10.0
Referrer-Policy: no-referrer
Access-Control-Allow-Origin: domain
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
X-Frame-Options: SAMEORIGIN
Date: Fri, 08 Dec 2023 11:26:36 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Expect-CT: enforce, max-age=43200
Content-Type: text/html; charset=utf-8
Permissions-Policy: fullscreen=()
Content-Length: 3425
X-XSS-Protection: 1; mode=block
HTTP/1.1 403 Forbidden

X-Content-Type-Options: nosniff
Server: Microsoft-IIS/10.0
Referrer-Policy: no-referrer
Access-Control-Allow-Origin: domain
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; st
…
```

CLASSIFICATION

OWASP Proactive Controls	C8
ISO27001	A.8.1.1

29. HTTP Strict Transport Security (HSTS) via HTTP

INFORMATION | 1

HTTP Strict Transport Security header is sent via an HTTP response which must be sent in HTTPS responses instead.

Impact

Web browsers will ignore the HSTS implementation and the users will not be able to take advantage of HSTS. This renders the HSTS implementation useless. Not having HSTS will make MITM attacks easier for attackers.

Vulnerabilities

29.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

Certainty

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 26.958
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:51 GMT
Content-Encoding:



<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta charset="utf-8" /><meta http-equiv="x-ua-compatible" content="ie=edge" /><title>
MP AGRO - Official Website
</title><link rel="icon" href="../assets/images/logo1.png" /><meta name="description" /><meta http-
equiv="cache-control" content="no-cache" /><meta http-equiv="expires" content="0" /><meta http-
equiv="pragma" content="no-cache" /><meta name="viewport" content="width=device-width, initial-scale=1,
shrink-to-fit=no" /><link href="https://fonts.googleapis.com/css?
family=Poppins:300,300i,400,400i,500,500i,600,600i,700,700i,800,800i,900,900i" rel="stylesheet" /><link
href="https://fonts.googleapis.com/css?family=Open+Sans:400,400i,600,600i,700,700i,800,800i"
rel="stylesheet" /><link href="https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-
awesome.min.css" rel="stylesheet" /><link rel="icon" type="image/png" href="favicon.html" />
<!-- Place favicon.ico in the root directory -->
<link rel="apple-touch-icon" href="apple-touch-icon.html" /><link href="../assets/css/fontawesome-
min.css" rel="stylesheet" /><link rel="stylesheet" href="../assets/css/bootstrap.min.css" /><link
rel="stylesheet" href="../assets/css/xsIcon.css" /><link rel="stylesheet" href="../asse
…
```

External References

- HTTP Strict Transport Security (HSTS) HTTP Header
- Wikipedia - HTTP Strict Transport Security Implementation

CLASSIFICATION

OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	14.4.5
NIST SP 800-53	SC-8
DISA STIG	V-6136
OWASP API Top Ten 2019	API7
OWASP Proactive Controls	C10
ISO27001	A.14.1.2
ISO27001 2022	A.8.24
OWASP Top Ten 2021	A05

30. IIS Identified

INFORMATION | 1

Invicti Standard identified a web server (IIS) in the target web server's HTTP response.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

30.1. http://mpagroerp.tserver.co.in/mis/Login.aspx

Certainty

Request | Response

Request

```
GET /mis/Login.aspx HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=pcpx0mh1hzckfuvlcstkjxzi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 109.3767
Total Bytes Received : 18618
Body Length : 17898
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6489
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:22:42 GMT
ConHTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0

X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length:
…
```

External References

- IIS Official Website

CLASSIFICATION

OWASP 2017	A6
CWE	205
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Proactive Controls	C7
ISO27001	A.14.2.5
OWASP Top Ten 2021	A05

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE	
Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

31. jQuery Identified

INFORMATION | 1

Invicti Standard identified the usage of Jquery in the target web server's HTTP response.

This issue is reported as extra information only.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

31.1. http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/assets/js/jquery-3.2.1.min.js

Certainty

Request | Response

Request

```
GET /mis/Login.aspx/assets/assets/js/jquery-3.2.1.min.js HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/c%3a%5cboot.ini
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 46.8713
Total Bytes Received : 18831
Body Length : 18111
Is Compressed : Yes

```
HTTP/1.1 200 OK
Expect-CT: enforce, max-age=43200
Cache-Control: private
Access-Control-Allow-Origin: domain
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
Permissions-Policy: fullscreen=()
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 6506
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
Date: Fri, 08 Dec 2023 11:34:53 GMT
Content-Encoding:
```

```
<!DOCTYPE html>

<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta charset="utf-8" /><meta http-equiv="x-ua-compatible" content="ie=edge" /><title>
MP AGRO - Official Website
</title><link rel="icon" href="../../../../../assets/images/logo1.png" /><meta name="description" />
<meta http-equiv="cache-control" content="no-cache" /><meta http-equiv="expires" content="0" /><meta
http-equiv="pragma" content="no-cache" /><meta name="viewport" content="width=device-width, initial-
scale=1, shrink-to-fit=no" /><link href="https://fonts.googleapis.com/css?
family=Poppins:300,300i,400,400i,500,500i,600,600i,700,700i,800,800i,900,900i" rel="stylesheet" /><link
href="https://fonts.googleapis.com/css?family=Open+Sans:400,400i,600,600i,700,700i,800,800i"
rel="stylesheet" /><link href="https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-
awesome.min.css" rel="stylesheet" /><link rel="icon" type="image/png" href="../../../../favicon.html"
/>
<!-- Place favicon.ico in the root directory -->
<link rel="apple-touch-icon" href="../../../../apple-touch-icon.html" /><link
href="../../../../../assets/css/fontawesome-min.css" rel="stylesheet" /><link rel="stylesheet"
href="../../../../../assets/css/bootstrap.min.css" /><link rel="stylesheet" href="../.
…
```

CLASSIFICATION

OWASP 2017	A6
CWE	205
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Proactive Controls	C7
ISO27001	A.14.2.5
OWASP Top Ten 2021	A05

32. OPTIONS Method Enabled

INFORMATION 1 | CONFIRMED 1

Invicti Standard detected that `OPTIONS` method is allowed. This issue is reported as extra information.

Impact

Information disclosed from this page can be used to gain additional information about the target system.

Vulnerabilities

32.1. http://mpagroerp.tserver.co.in/mis/Login.aspx/assets/js/

CONFIRMED

Allowed methods

- OPTIONS, TRACE, GET, HEAD, POST

Request | Response

Request

```
OPTIONS /mis/Login.aspx/assets/js/ HTTP/1.1
Host: mpagroerp.tserver.co.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 6.7394
Total Bytes Received : 662
Body Length : 0
Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Type-Options: nosniff
Server: Microsoft-IIS/10.0
Referrer-Policy: no-referrer
Allow: OPTIONS, TRACE, GET, HEAD, POST
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src *; style-src 'self' http://* 'unsafe-inline'; script-src 'self'
http://* 'unsafe-inline' 'unsafe-eval'; img-src 'self' http://* data:;
X-Frame-Options: SAMEORIGIN
Public: OPTIONS, TRACE, GET, HEAD, POST
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Expect-CT: enforce, max-age=43200
Date: Fri, 08 Dec 2023 11:26:33 GMT
Permissions-Policy: fullscreen=()
Content-Length: 0
Access-Control-Allow-Origin: domain
```

Remedy

Disable `OPTIONS` method in all production systems.

External References

- Testing for HTTP Methods and XST (OWASP-CM-008)
- HTTP/1.1: Method Definitions

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
CAPEC	107
WASC	14
ASVS 4.0	14.5.1
NIST SP 800-53	CM-6
DISA STIG	V-16786
OWASP API Top Ten 2019	API7
ISO27001	A.14.1.2
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A05

Show Scan Detail

Enabled Security Checks	:	Arbitrary Files (IAST), BREACH Attack, Code Evaluation, Code Evaluation (IAST), Code Evaluation (Out of Band),

Command Injection,
Command Injection (Blind),
Command Injection (IAST),
Configuration Analyzer (IAST),
Content Security Policy,
Content-Type Sniffing,
Cookie,
Cross Frame Options Security,
Cross-Origin Resource Sharing (CORS),
Cross-Site Request Forgery,
Cross-site Scripting,
Cross-site Scripting (Blind),
Custom Script Checks (Active),
Custom Script Checks (Passive),
Custom Script Checks (Per Directory),
Custom Script Checks (Singular),
File Upload,
GraphQL Library Detection,
Header Analyzer,
HSTS,
HTML Content,
HTTP Header Injection,
HTTP Header Injection (IAST),
HTTP Methods,
HTTP Status,
HTTP.sys (CVE-2015-1635),
IFrame Security,
Insecure JSONP Endpoint,
Insecure Reflected Content,
JavaScript Libraries,
JSON Web Token,
LDAP Injection (IAST),
Local File Inclusion,
Local File Inclusion (IAST),
Log4j Code Evaluation (Out of Band),
Login Page Identifier,
Mail Header Injection (IAST),
Malware Analyzer,
Mixed Content,
MongoDB Injection (Boolean),
MongoDB Injection (IAST),
MongoDB Injection (Operator),
Open Redirection,
Referrer Policy,
Reflected File Download,
Remote File Inclusion,
Reverse Proxy Detection,
Security Assertion Markup Language (SAML),
Sensitive Data,
Server-Side Request Forgery (DNS),
Server-Side Request Forgery (Pattern Based),
Server-Side Template Injection,
Server-Side Template Injection (IAST),

		Signatures, **Software Composition Analysis (SCA),** **Spring4Shell Remote Code Execution,** **SQL Injection (Blind),** **SQL Injection (Boolean),** **SQL Injection (Error Based),** **SQL Injection (IAST),** **SQL Injection (Out of Band),** **SSL,** **Static Resources (All Paths),** **Static Resources (Only Root Path),** **Unicode Transformation (Best-Fit Mapping),** **WAF Identifier,** **Web App Fingerprint,** **Web Cache Deception,** **WebDAV,** **Windows Short Filename,** **Wordpress Plugin Detection,** **Wordpress Theme Detection,** **XML External Entity,** **XML External Entity (Out of Band),** **XML External Entity Injection (IAST),** **XPath Injection (IAST)**
URL Rewrite Mode	:	**Heuristic**
Detected URL Rewrite Rule(s)	:	**None**
Included URL Patterns	:	**gtm\.js** **WebResource\.axd** **ScriptResource\.axd**
Authentication	:	**Form Authentication**
Authentication Profile	:	**None**
Scheduled	:	**No**
Additional Website(s)	:	**None**

This report created with 23.8.0.41720-release_is-23.8.0-a9dc73c
https://www.invicti.com

SFA Technologies