21.08.2022 21:02:10 (UTC+03:00)

Detailed Scan Report

https://www.mustso.org.tr/

Scan Time	: 21.08.2022 13:16:50 (UTC+03:00)
Scan Duration	: 00:07:35:15
Total Requests	: 122.858
Average Speed	: 4,5r/s

Risk Level:
MEDIUM

30 IDENTIFIED	**11** CONFIRMED	**0** CRITICAL
0 HIGH	6 MEDIUM	11 LOW
	7 BEST PRACTICE	6 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	6
Low	11
Best Practice	7
Information	6
TOTAL	**30**

Confirmed Vulnerabilities

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

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	[Possible] BREACH Attack Detected	POST	https://www.mustso.org.tr/default.aspx	No Parameters	No Parameter Types
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Out-of-date Version (IIS)	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Out-of-date Version (jQuery)	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Active Mixed Content over HTTPS	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Weak Ciphers Enabled	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	[Possible] Backup File Disclosure	GET	https://www.mustso.org.tr/%C4%B0leti%C5%9Fim/tabid/17212/Copy%20of%20Default.aspx	No Parameters	No Parameter Types
	[Possible] Cross-site Request Forgery	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Missing X-Frame-Options Header	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Stack Trace Disclosure (ASP.NET)	GET	https://www.mustso.org.tr/trace.axd	No Parameters	No Parameter Types
	Version Disclosure (ASP.NET)	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Version Disclosure (IIS)	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	ViewState is not Encrypted	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Cookie Not Marked as Secure	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Insecure Frame (External)	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Internal Server Error	GET	https://www.mustso.org.tr/trace.axd	No Parameters	No Parameter Types
	Expect-CT Not Enabled	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Missing X-XSS-Protection Header	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	Referrer-Policy Not Implemented	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	SameSite Cookie Not Implemented	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Content Security Policy (CSP) Not Implemented	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Subresource Integrity (SRI) Not Implemented	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Email Address Disclosure	GET	https://www.mustso.org.tr/%C4%B0leti%C5%9Fim/tabid/17212/Default.aspx	No Parameters	No Parameter Types
	IIS Identified	GET	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Unexpected Redirect Response Body (Too Large)	GET	https://www.mustso.org.tr/Bas%C4%B1ndaBiz/Haber/tabid/17222/articleType/ArticleView/articleId/	No Parameters	No Parameter Types
	Forbidden Resource	GET	https://www.mustso.org.tr/DesktopModules/ProModules/Templates/	No Parameters	No Parameter Types
	OPTIONS Method Enabled	OPTIONS	https://www.mustso.org.tr/	No Parameters	No Parameter Types
	Robots.txt Detected	GET	https://www.mustso.org.tr/robots.txt	No Parameters	No Parameter Types

1. [Possible] BREACH Attack Detected

MEDIUM | 1

Invicti Standard detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.

Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

Impact

Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

- Inject partial plaintext they have uncovered into a victim's requests
- Measure the size of encrypted traffic

Vulnerabilities

1.1. https://www.mustso.org.tr/default.aspx

Method	Parameter	Parameter Type	Value
POST	__VIEWSTATE	Post	/wEPDwUKLTUxODU2MjE2OQ9kFgICAQ9kFgICAQ9kFgICAw9kFgJmD2QWQgIFDxYCHgdWaXNpYmxlZ2QCBw9kFgICAQ9kFgRmDw8W...
POST	__dnnVariable	Post	3
POST	__VIEWSTATEGENERATOR	Post	CA0B0334
POST	ScrollTop	Post	3

Reflected Parameter(s)

- __dnnVariable,ScrollTop

Sensitive Keyword(s)

- nonce

Certainty

Request | Response

Request

```
POST /default.aspx HTTP/1.1
Host: www.mustso.org.tr
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
Content-Length: 1837
Content-Type: multipart/form-data; boundary=0521d4e7125641c083c3703602b79361
Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; Article51578=1; Article51511=1; Article51372=1; Article51353=1;
Article43758=1; Article51173=1; Article41669=1; Article41518=1; Article40695=1; Article40563=1; Article40739=1; Article41471=1; Article40414=1;
Article40092=1; Article39975=1; language=en-US
Referer: https://www.mustso.org.tr/default.aspx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36

--0521d4e7125641c083c3703602b79361
Content-Disposition: form-data; name="__VIEWSTATE"

/wEPDwUKLTUxODU2MjE2OQ9kFgICAQ9kFgICAQ9kFgICAw9kFgJmD2QWQgIFDxYCHgdWaXNpYmxlZ2QCBw9kFgICAQ9kFgRmDw8WAh8AaGRkAgEPZBYCAgIPFgIfAGhkAgkPZBYCAgEPZBYEZg8PFgIfAG
hkZAIBD2QWAgICDxYCHwBoZAILDxYCHwBnFgICAQ9kFgRmDw8WAh8AaGRkAgEPZBYCAgIPFgIfAGhkAg0PFgIeBWNsYXNzBRNjb2wtMjIgRE5ORW1wdHlQYW5lZAIPDxYCHwEFFWNvbC11cnVuIEROTkVt
cHR5UGFuZWQCEQ8WAh8BBRJjb2wtMiBETk5FbXB0eVBhbmVkAhMPFgIfAQUSY29sLTkgRE5ORW1wdHlQYW5lZAIVDxYCHwEFE2NvbC0xMyBETk5FbXB0eVBhbmVkAhcPFgIfAQUMRE5ORW1wdHlQYW5lZA
IZD2QWAgIBD2QWBGYPDxYCHwBoZGQCAQ9kFgICAg8WAh8AaGQCGw9kFgICAQ9kFgRmDw8WAh8AaGRkAgEPZBYCAgIPFgIfAGhkZAIBD2QWAgICDxYCHwBoZAIfD2QW
AgIBD2QWBGYPDxYCHwBoZGQCAQ9kFgICAg8WAh8AaGQCIQ8WAh8BBRJjb2wtNCBETk5FbXB0eVBhbmVkAiMPFgIfAQUSY29sLTQgRE5ORW1wdHlQYW5lZAIlDxYCHwEFEmNvbC00IEROTkVtcHR5UGFuZW
QCJw8WAh8BBRJjb2wtNCBETk5FbXB0eVBhbmVkAikPFgIfAQUSY29sLTQgRE5ORW1wdHlQYW5lZAIrDxYCHwEFEmNvbC00IEROTkVtcHR5UGFuZWQCLQ8WAh8BBRJjb2wtNCBETk5FbXB0eVBhbmVkAi8P
FgIfAGcWAgIBD2QWBGYPDxYCHwBoZGQCAQ9kFgICAg8WAh8AaGQCMQ8WAh8BBQxETk5FbXB0eVBhbmVkAjMPFgIfAQUMRE5ORW1wdHlQYW5lZAI1DxYCHwEFEmNvbC00IEROTkVtcHR5UGFuZWQCNw8WAh
8BBRJjb2wtNCBETk5FbXB0eVBhbmVkAjkPFgIfAQUSY29sLTQgRE5ORW1wdHlQYW5lZAI7DxYCHwEFEmNvbC00IEROTkVtcHR5UGFuZWQCPQ8WAh8BBQxETk5FbXB0eVBhbmVkAj8PFgIfAQUTY29sLTEy
IEROTkVtcHR5UGFuZWQCQQ8WAh8BBRJjb2wtayBETk5FbXB0eVBhbmVkAkMPFgIfAQUTY29sLWtrIEROTkVtcHR5UGFuZWQCRQ8WAh8AZxYCAgEPZBYEZg8PFgIfAGhkZAIBD2QWAgICDxYCHwBoZGSMhz
RAP8nWj45u+yIzsPBANYr9WA==
--0521d4e7125641c083c3703602b79361
Content-Disposition: form-data; name="__dnnVariable"

3
--0521d4e7125641c083c3703602b79361
Content-Disposition: form-data; name="__VIEWSTATEGENERATOR"

CA0B0334
--0521d4e7125641c083c3703602b79361
Content-Disposition: form-data; name="ScrollTop"

3
--0521d4e7125641c083c3703602b79361--
```

Response

Response Time (ms) : 7515,0489
Total Bytes Received : 51790
Body Length : 51502
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13274
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:21:23 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş
TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası ©
| Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE"
content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1
DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style
id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" />
<link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet"
type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css"
href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link
href="/Portals/348/Skins/mustso/favicon.ico" rel="shortcut icon" /><meta name="viewport" content="width=device-width,initial-scale=1" /><title>
Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi > Ana Sayfa
</title></head>
<body id="Body">
<noscript></noscript>
<form method="post" action="/default.aspx" id="Form" enctype="mu
…
```

Remedy

Invicti Standard reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:

- Served from a server that uses HTTP-level compression (ie. gzip)
- Reflects user-input in the HTTP response bodies
- Contains sensitive information (such as a CSRF token) in HTTP response bodies

To mitigate the issue, we recommend the following solutions:

1. If possible, disable HTTP level compression
2. Separate sensitive information from user input
3. Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
4. Hide the length of the traffic by adding a random number of bytes to the responses.
5. Add in a rate limit, so that the page maximum is reached five times per minute.

External References

- Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext
- Using the Same-Site Cookie Attribute to Prevent CSRF Attacks

CLASSIFICATION

OWASP 2013	A9
OWASP 2017	A9
CWE	310
ASVS 4.0	6.2.1
NIST SP 800-53	SC-8
DISA STIG	3.6.2
OWASP API Top Ten 2019	API7
OWASP Top Ten 2021	A02

CVSS 3.0 SCORE

Base	6,5 (Medium)
Temporal	6,5 (Medium)
Environmental	6,5 (Medium)

CVSS Vector String

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

CVSS 3.1 SCORE

Base	6,5 (Medium)
Temporal	6,5 (Medium)
Environmental	6,5 (Medium)

CVSS Vector String

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

2. Active Mixed Content over HTTPS

MEDIUM | 1 | CONFIRMED | 1

Invicti Standard detected that an active content loaded over HTTP within an HTTPS page.

Impact

Active Content is a resource which can run in the context of your page and moreover can alter the entire page. If the HTTPS page includes active content like scripts or stylesheets retrieved through regular, cleartext HTTP, then the connection is only partially encrypted. The unencrypted content is accessible to sniffers.

A man-in-the-middle attacker can intercept the request for the HTTP content and also rewrite the response to include malicious codes. Malicious active content can steal the user's credentials, acquire sensitive data about the user, or attempt to install malware on the user's system (by leveraging vulnerabilities in the browser or its plugins, for example), and therefore the connection is not safeguarded anymore.

Vulnerabilities

2.1. https://www.mustso.org.tr/

CONFIRMED

Resources Loaded from Insecure Origin (HTTP)

```
http://code.jquery.com/jquery-2.2.4.min.js
http://paracevirici.com/servis/widget/widget.js
```

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş
TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası ©
| Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE"
content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1
DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style
id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" />
<link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet"
type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css"
href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link
href="/Portals/348/Skins/mustso/fa
…
```

Remedy

There are two technologies to defense against the mixed content issues:

1. HTTP Strict Transport Security (HSTS) is a mechanism that enforces secure resource retrieval, even in the face of user mistakes (attempting to access your web site on port 80) and implementation errors (your developers place an insecure link into a secure page)
2. Content Security Policy (CSP) can be used to block insecure resource retrieval from third-party web sites
3. Last but not least, you can use "protocol relative URLs" to have the user's browser automatically choose HTTP or HTTPS as appropriate, depending on which protocol the user is connected with. For example:

A protocol relative URL to load an style would look like `<link rel="stylesheet" href="//example.com/style.css"/>`.

Same for scripts `<script type="text/javascript" src="//example.com/code.js"></script>`

The browser will automatically add either "http:" or "https:" to the start of the URL, whichever is appropriate.

External References

- Mixed Content

Remedy References

- Wikipedia - HTTP Strict Transport Security
- Wikipedia - Content Security Policy

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	319
ASVS 4.0	9.2.2
NIST SP 800-53	SC-8
DISA STIG	3.7.4
ISO27001	A.14.1.3
OWASP Top Ten 2021	A02

3. 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

3.1. https://www.mustso.org.tr/

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 319,7919
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=JwwaQ9nr2AEkAAAANTdhM2NjNGEtM2NhMy00NWQxLTkwODEtNWE5NWNjNjIxNjJh0; expires=Sat, 29-Oct-2022 20:58:57 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=JwwaQ9nr2AEkAAAANTdhM2NjNGEtM2NhMy00NWQxLTkwODEtNWE5NWNjNjIxNjJh0; expires=Sat, 29-Oct-2022 20:58:57 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:18:57 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" />
<link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link href="/Portals/348/Skins/mustso/fa
…
```

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	3.7.4
ISO27001	A.14.1.2
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: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)

CVSS 3.1 SCORE	
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

4. Out-of-date Version (IIS)

MEDIUM | 1

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

Impact

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

Internet Information Services Permissions, Privileges, and Access Controls Vulnerability

The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."

Affected Versions

8.0 to 8.5

CVSS

AV:N/AC:H/Au:N/C:P/I:P/A:P

External References

- CVE-2014-4078

Vulnerabilities

4.1. https://www.mustso.org.tr/

Identified Version

- 8.5

Latest Version

- 10.0

Vulnerability Database

- Result is based on 08/18/2022 18:00:00 vulnerability database content.

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" /><link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link href="/Portals/348/Skins/mustso/fa
…
```

Remedy

Upgrading IIS to a higher version is not a standalone operation. The IIS version depends heavily on the Windows OS version that you use on your server machine.

If it is not possible to upgrade IIS to a higher version for this type of reason, we strongly recommend that you track and apply the patches that are published by the vendor.

Please note that all updates and patches for IIS come as Windows Updates. Also, you can select which update package(s) will be applied.

External References

- The Official Microsoft IIS Site

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	6.6.2
OWASP Proactive Controls	C1
ISO27001	A.14.1.2
OWASP Top Ten 2021	A06

5. 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 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 3.3.1

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

5.1. https://www.mustso.org.tr/

Identified Version

- 1.7

Latest Version

- 1.12.4 (in this branch)

Overall Latest Version

- 3.6.0

Vulnerability Database

- Result is based on 08/18/2022 18:00:00 vulnerability database content.

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" /><link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link href="/Portals/348/Skins/mustso/fa
…
```

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	6.6.2
OWASP Proactive Controls	C1
ISO27001	A.14.1.2
OWASP Top Ten 2021	A06

6. 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

6.1. https://www.mustso.org.tr/

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)

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	3.6.2
ISO27001	A.14.1.3
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

7. [Possible] Backup File Disclosure

LOW | 1

Invicti Standard identified a possible backup file disclosure on the web server.

Impact

Backup files can contain old or current versions of a file on the web server. This could include sensitive data such as password files or even the application's source code. This form of issue normally leads to further vulnerabilities or, at worst, sensitive information disclosure.

Vulnerabilities

7.1. https://www.mustso.org.tr/%C4%B0leti%C5%9Fim/tabid/17212/Copy%20of%20Default.aspx

Certainty

Request | Response

Request

```
GET /%C4%B0leti%C5%9Fim/tabid/17212/Copy%20of%20Default.aspx HTTP/1.1
Host: www.mustso.org.tr
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: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; Article51578=1; Article51511=1; Article51372=1; Article51353=1;
Article43758=1; Article51173=1; Article41669=1; Article41518=1; Article40695=1; Article40563=1; Article40739=1; Article41471=1; Article40414=1;
Article40092=1; Article39975=1; Article51002=1; Article49295=1; Article51172=1; Article48507=1; Article48748=1; language=en-US
Referer: https://www.mustso.org.tr/%C4%B0leti%C5%9Fim/tabid/17212/Copy%20of%20Default.aspx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 873,3111
Total Bytes Received : 17244
Body Length : 16957
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 5729
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:25:40 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="İletişim" /><meta id="MetaKeywords" name="KEYWORDS" content="İletişim" /><meta
id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR"
content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" />
<meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-
equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_"
rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" /><link id="_Portals_348_" rel="stylesheet" type="text/css"
href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><!
[endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link
rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link href="/Portals/348/Skins/mustso/favicon.ico" rel="shortcut icon" />
<meta name="viewport" content="width=device-width,initial-scale=1" /><title>
İletişim
</title></head>
<body id="Body">
<noscript></noscript>
<form method="post" action="/İletişim/tabid/17212/Copy of Default.aspx" id="Form" enctype="multipart/form-data" autocomplete="off">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE
…
```

Remedy

Do not store backup files on production servers.

CLASSIFICATION

PCI DSS v3.2	6.5.8
OWASP 2013	A7
OWASP 2017	A5
CWE	530
CAPEC	87
WASC	34
HIPAA	164.306(a), 164.308(a)
ASVS 4.0	8.1.6
NIST SP 800-53	AC-22
DISA STIG	3.13
ISO27001	A.18.1.3
OWASP Top Ten 2021	A01

8. [Possible] Cross-site Request Forgery

LOW | 1

Invicti Standard identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

Vulnerabilities

8.1. https://www.mustso.org.tr/

Form Action(s)

- /

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" /><link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link href="/Portals/348/Skins/mustso/fa
…
```

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)

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	3.10.6
ISO27001	A.14.2.5
OWASP Top Ten 2021	A01

9. [Possible] Phishing by Navigating Browser Tabs

LOW | 1

Invicti Standard identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"` can modify *window.opener.location* and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"` attribute, a third party site can change the URL of the source tab using *window.opener.location.assign* and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

Vulnerabilities

9.1. https://www.mustso.org.tr/

External Links

- https://uye.tobb.org.tr/organizasyon/firma-index.jsp
- https://uye.tobb.org.tr/organizasyon/firma-index.jsp
- https://mersis.gtb.gov.tr/
- https://youtu.be/sjf6AzBvico
- http://www.tobb.org.tr
- http://www.resmigazete.gov.tr
- http://www.balo.tc
- http://www.gtias.com.tr
- http://tv.tobb.org.tr
- http://www.tepav.org.tr/tr
- http://www.turkiye100.org
- http://www.tobb.org.tr/FuarlarMudurlugu/Sayfalar/AnaSayfa.php
- http://www.tobb.org.tr/Sayfalar/TOBBIstatistikleri.php
- http://www.kosgeb.gov.tr
- http://www.rekabet.gov.tr/
- http://www.ilan.gov.tr/
- http://www.mus.bel.tr/
- http://www.alparslan.edu.tr/
- http://www.mus.gov.tr/
- http://www.daka.org.tr/
- http://www.kosgeb.gov.tr/site
- http://www.iskur.gov.tr/
- https://www.ombudsman.gov.tr/
- http://icc.tobb.org.tr/
- https://www.deik.org.tr/
- https://www.cimer.gov.tr/
- http://meybem.com.tr/
- http://tv.tobb.org.tr/
- https://www.tobb.org.tr/FuarlarMudurlugu/Sayfalar/AnaSayfa.php
- http://www.eximbank.gov.tr/
- https://www.tobb.org.tr/Sayfalar/TOBBIstatistikleri.php
- https://www.tuik.gov.tr/
- https://www.tobb.org.tr/BilgiErisimMudurlugu/Sayfalar/KurulanKapananSirketistatistikleri.php
- https://www.tobb.org.tr/BilgiErisimMudurlugu/Sayfalar/sanayi-kapasite-raporu-istatistikleri.php
- https://tobb.org.tr/MaliveSosyalPolitikalar/Sayfalar/EkonomikRapor.php
- https://www.tobb.org.tr/KamuPolitikalariMudurlugu/Sayfalar/ggnot.php
- https://www.tuik.gov.tr/Kurumsal/Veri_Takvimi
- http://www.resmigazete.gov.tr/default.aspx
- https://www.tobb.org.tr/HukukMusavirligi/Sayfalar/MevzuatBulteni.php
- https://www.tobb.org.tr/HukukMusavirligi/Sayfalar/Mevzuat.php
- https://www.tobb.org.tr/HukukMusavirligi/Sayfalar/TOBBTahkimiveTahkimSozlesmesi.php
- http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.6102&MevzuatIliski=0&sourceXmlSearch=&Tur=1&Tertip=5&No=6102
- http://www.ekonomi.gov.tr/portal/faces/home/yatirim/yatirimTesvik/yatirimTesvik-YatirimTesvikMevzuati?_afrLoop=891193306660909&_afrWindowMode=0&_afrWindowId=null#!%40%40%3F_afrWindowId%3Dnull%26_afrLoop%3D891193306660909%26_afrWindowMode%3D0%26_adf.ctrl-st
- http://www.mirsoft.com.tr

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug
…
r</a></div>
<div class="btn-col"><a href="https://uye.tobb.org.tr/hizliaidatodeme.jsp" class="CommandButton" style="background-color: #c94d64;">
Hızlı Ödeme</a></div>
<div class="btn-col"><a href="https://uye.tobb.org.tr/organizasyon/firma-index.jsp" class="CommandButton" style="background-color: #29619d;">
Online Belge</a></div>
</div>
<div class="sosyal mobile-hide" style="top: 110px;position: absolute;height: 32px;right: -114px;/* backgrou
…
iz</span></a></li><li><a href="https://www.mustso.org.tr/TicaretSicil/tabid/17408/Default.aspx"><span class="l"></span><span class="r"></span><span
class="t">Ticaret Sicil</span></a></li><li><a href="https://www.tobb.org.tr/HukukMusavirligi/Sayfalar/Mevzuat.php"><span class="l"></span><span class="r">
</span><span class="t">Mevzuat</span></a></li><li><a href="https://www.mustso.org.tr/Üyelerimiz/tabid/17226/Default.aspx"><span class="l"></span><span
class="r
…
lockcontent-body">

<div id="dnn_ctr24192_ContentPane" class="DNNAlignleft"><!-- Start_Module_24192 --><div id="dnn_ctr24192_ModuleContent">
<div>
<div class="anasayfa-brans-menu">
<div><a href="https://uye.tobb.org.tr/organizasyon/firma-index.jsp" target="_blank">
<div><img src="/Portals/309/skins/bintso/images/buton/card.PNG" width="100%" alt="" /></div>
<span>Online Ödeme</span></a></div>
<div><a href="https://uye.tobb.org.tr/organizasyon/firma-index.jsp" target="_blank">
<div><img src="/Portals/309/skins/bintso/images/buton/belge.png" width="100%" alt="" /></div>
<span>Online Belge</span></a></div>
<div><a href="#" target="_blank">
<div><img src
…
div>
<div><a href="/Anketler/tabid/17407/Default.aspx">
<div><img src="/Portals/309/skins/bintso/images/buton/anket.PNG" width="100%" alt="" /></div>
<span>Anketler</span></a></div>
<div><a href="https://mersis.gtb.gov.tr/" target="_blank">
<div><img src="/Portals/309/skins/bintso/images/buton/mersis.png" width="100%" alt="" /></div>
<span>MERSİS</span></a></div>
<div><a href="#">
<div><img src="/Portals/309/skins/
…
.fancybox_biz.css?v=2.1.4" type="text/css" rel="stylesheet" /> <script type="text/javascript" src="/webhelper/fancyBox/helpers/jquery.fancybox-media.js?
v=1.0.5"></script></p>
<p><a href="https://youtu.be/sjf6AzBvico" target="_blank"><img width="100%" border="0" src="/Portals/348/mustanıtım.PNG" alt="" /></a></p>
<script type="text/javascript"> jQuery(document).ready(function() { jQuery(".fancybox").
…
ox"></div>
<div id="referans" class="tso">
<div id="referansWrap">
<ul id="referansCarousel" class="jcarousel-skin-referans">
<li>
<div class="refaransItem">
<div class="refaransResim"><a href="http://www.tobb.org.tr" target="_blank"><img alt="1" src="/Portals/269/referans/tobb.jpg " /></a></div>
<div class="referansBaslik">TOBB </div>
</div>
</li><li>
<div class="refaransItem">
<div class="refaransResim"><a href="http://www.resmigazete.gov.tr" target="_blank"><img alt="1" src="/Portals/269/referans/resmigazete.png " /></a></div>
<div class="referansBaslik">RESMİ GAZETE </div>
</div>
</li><li>
<div class="refaransItem">
<div class="refaransResim"><a href="http://www.balo.tc" target="_blank"><img alt="1" src="/Portals/269/referans/balo.png " /></a></div>
<div class="referansBaslik">BALO </div>
</div>
</li><li>
<div class="refaransItem">
<div class="refaransResim"><a href="http://www.gtias.com.tr" target="_blank"><img alt="1" src="/Portals/269/referans/gti.png " /></a></div>
```

```
<div class="referansBaslik">GÜMRÜK VE T. </div>
</div>
</li><li>
<div class="refaransItem">
<div class="refaransResim"><a href="http://tv.tobb.org.tr" target="_blank"><img alt="1" src=" /Portals/269/referans/tobb-tv.jpg " /></a></div>
<div class="referansBaslik">TOBB TV</div>
</div>
</li><li>
<div class="refaransItem">
<div class="refaransResim"><a href="http://www.tepav.org.tr/tr" target="_blank"><img alt="1" src="/Portals/269/referans/tepav.jpg " /></a></div>
<div class="referansBaslik">TEPAV </div>
</div>
</li><li>
<div class="refaransItem">
<div class="refaransResim"><a href="http://www.turkiye100.org" target="_blank"><img alt="1" src=" /Portals/269/referans/hizli100.jpg " /></a></div>
<div class="referansBaslik">TÜRKİYE 100</div>
</div>
</li><li>
<div class="refaransItem">
<div class="refaransResim"><a href="http://www.tobb.org.tr/FuarlarMudurlugu/Sayfalar/AnaSayfa.php" target="_blank"><img alt="1"
src="/Portals/269/referans/fuar.jpg " /></a></div>
<div class="referansBaslik">FUAR REHBERİ </div>
</div>
</li><li>
<div class="refaransItem">
<div class="refaransResim"><a href="http://www.tobb.org.tr/Sayfalar/TOBBIstatistikleri.php" target="_blank"><img alt="1"
src="/Portals/269/referans/tobbistatistikleri.png " /></a></div>
<div class="referansBaslik">TOBB İSTATİSTİK </div>
</div>
</li><li>
<div class="refaransItem">
<div class="refaransResim"><a href="http://www.kosgeb.gov.tr" target="_blank"><img alt="1" src="/Portals/269/referans/kosgeb.png " /></a></div>
<div class="referansBaslik">KOSGEB </div>
</div>
</li><li>
<div class="refaransItem">
<div class="refaransResim"><a href="http://www.rekabet.gov.tr/" target="_blank"><img alt="1" src="/Portals/269/referans/rekabet.jpg " /></a></div>
<div class="referansBaslik">REKABET KURUMU </div>
</div>
</li><li>
<div class="refaransItem">
<div class="refaransResim"><a href="http://www.ilan.gov.tr/" target="_blank"><img alt="1" src="/Portals/348/Skins/mustso/images/ilan-1.png" /></a></div>
<div class="referansBaslik">İlan Portalı</div>
</div>
</li></ul></div></div>
<div class="cleared reset
…
pan_8_of_12">
<div style="height: 160px;">
<div class="yazifont">
<ul>
<li><span style="color: rgb(255, 255, 255);"><u><strong>Yerel Faydalı Linkler</strong></u></span></li>
<li><a href="http://www.mus.bel.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› Muş Belediyesi</span></a></li>
<li><a href="http://www.alparslan.edu.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› Muş Üniversitesi</span></a></li>
<li><a href="http://www.mus.gov.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› Muş Valiliği</span></a></li>
<li><a href="http://www.daka.org.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› Daka Kalkınma Ajansı</span></a></li>
<li><a href="http://www.kosgeb.gov.tr/site" target="_blank"><span style="color: rgb(255, 255, 255);">› KOSGEB</span></a></li>
<li><a href="http://www.iskur.gov.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› İŞKUR</span></a></li>
</ul>
</div>
<div style="width: 230px;" class="yazifont">
<ul>
<li><span style="color: rgb(255, 255, 255);"><u><strong>Ulusal Faydalı Linkler</strong></u></span></li>
<li><a href="https://www.ombudsman.gov.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› Kamu Denetçiliği Kurumu</span></a></li>
<li><a href="http://icc.tobb.org.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› ICC Milletlerarası Ticaret Odası</span></a></li>
<li><a href="https://www.deik.org.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› DEİK Dış Ekonomik İlişkiler Kurulu</span></a></li>
<li><a href="https://www.cimer.gov.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› CİMER</span></a></li>
<li><a href="http://meybem.com.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› MEYBEM</span></a></li>
<li><a href="http://tv.tobb.org.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› TOBB TV</span></a></li>
<li><a href="https://www.tobb.org.tr/FuarlarMudurlugu/Sayfalar/AnaSayfa.php" target="_blank"><span style="color: rgb(255, 255, 255);">› TOBB Fuarlar
Müdürlüğü</span></a></li>
<li><a href="http://www.eximbank.gov.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› EXIMBANK</span></a></li>
</ul>
</div>
<div class="yazifont">
<ul>
<li><span style="color: rgb(255, 255, 255);"><u><strong>İstatistikler</strong></u></span></li>
<li><a href="https://www.tobb.org.tr/Sayfalar/TOBBIstatistikleri.php" target="_blank"><span style="color: rgb(255, 255, 255);">› TOBB
İstatistikleri</span></a></li>
<li><a href="https://www.tuik.gov.tr/" target="_blank"><span style="color: rgb(255, 255, 255);">› TUİK</span></a></li>
<li><a href="https://www.tobb.org.tr/BilgiErisimMudurlugu/Sayfalar/KurulanKapananSirketistatistikleri.php" target="_blank"><span style="color: rgb(255,
255, 255);">› Kurulan/Kapanan Şirket İstatistikleri</span></a></li>
<li><a href="https://www.tobb.org.tr/BilgiErisimMudurlugu/Sayfalar/sanayi-kapasite-raporu-istatistikleri.php" target="_blank"><span style="color: rgb(255,
255, 255);">› Sanayi Kapasite Rapor İstatistikleri</span></a></li>
<li><a href="https://tobb.org.tr/MaliveSosyalPolitikalar/Sayfalar/EkonomikRapor.php" target="_blank"><span style="color: rgb(255, 255, 255);">› Ekonomik
```

```
Raporlar</span></a></li>
<li><a href="https://www.tobb.org.tr/KamuPolitikalariMudurlugu/Sayfalar/ggnot.php" target="_blank"><span style="color: rgb(255, 255, 255);">› Yönetici
Özetleri ve Bilgi Notları</span></a></li>
<li><a href="https://www.tuik.gov.tr/Kurumsal/Veri_Takvimi" target="_blank"><span style="color: rgb(255, 255, 255);">› Veri Takvimi</span></a></li>
</ul>
</div>
<div style="border-right: none;" class="yazifont">
<ul>
<li><span style="color: rgb(255, 255, 255);"><u><strong>Mevzuatlar</strong></u></span></li>
<li><a href="http://www.resmigazete.gov.tr/default.aspx" target="_blank"><span style="color: rgb(255, 255, 255);">› T.C. Resmi Gazete</span></a></li>
<li><a href="https://www.tobb.org.tr/HukukMusavirligi/Sayfalar/MevzuatBulteni.php" target="_blank"><span style="color: rgb(255, 255, 255);">› Mevzuat
Bülteni</span></a></li>
<li><a href="https://www.tobb.org.tr/HukukMusavirligi/Sayfalar/Mevzuat.php" target="_blank"><span style="color: rgb(255, 255, 255);">› TOBB Hukuk
Müşavirliği</span></a></li>
<li><a href="https://www.tobb.org.tr/HukukMusavirligi/Sayfalar/TOBBTahkimiveTahkimSozlesmesi.php" target="_blank"><span style="color: rgb(255, 255,
255);">› TOBB Tahkim Kurulu</span></a></li>
<li><a href="http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.6102&amp;MevzuatIliski=0&amp;sourceXmlSearch=&amp;Tur=1&amp;Tertip=5&amp;No=6102"
target="_blank"><span style="color: rgb(255, 255, 255);">› Türk Ticaret Kanunu</span></a></li>
<li><a href="http://www.ekonomi.gov.tr/portal/faces/home/yatirim/yatirimTesvik/yatirimTesvik-YatirimTesvikMevzuati?
_afrLoop=891193306660909&amp;_afrWindowMode=0&amp;_afrWindowId=null#!%40%40%3F_afrWindowId%3Dnull%26_afrLoop%3D891193306660909%26_afrWindowMode%3D0%26_adf
.ctrl-st" target="_blank"><span style="color: rgb(255, 255, 255);">› Yatırım Teşvik Mevzuatı</span></a></li>
</ul>
</div>
</div>
</div>
</div>
</div> <!-- End_Module_23962 -->
</div></span>
</div>


…
ss="col span_5_of_12" style="color: #fff;font-size: 14px;margin-top: 5px;">
<div class="mirsoftlogo">
<div class="mirsoft">
<a title="Mirsoft Bilişim Teknolojileri" target="_blank" href="http://www.mirsoft.com.tr"><div class="mirsofthov"> </div></a>
</div>
</div>
</div>
</div>




</div>
</div>
</div>
<div class="cleared"></div>



<script type="text/javascript">
collapseS
…
```

Remedy

- Add `rel=noopener` to the links to prevent pages from abusing *window.opener*. This ensures that the page cannot access the *window.opener* property in Chrome and Opera browsers.
- For older browsers and in Firefox, you can add `rel=noreferrer` which additionally disables the Referer header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

External References

- Reverse Tabnabbing
- Blankshield & Reverse Tabnabbing Attacks
- Target="_blank" - the most underestimated vulnerability ever

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16

WASC	15
ASVS 4.0	14.1.3
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.1.2
OWASP Top Ten 2021	A05

10. Cookie Not Marked as Secure

LOW | 1 | CONFIRMED | 1

Invicti Standard identified a cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

Impact

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (*such as a session cookie*), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

Vulnerabilities

10.1. https://www.mustso.org.tr/

CONFIRMED

Identified Cookie(s)

- .ASPXANONYMOUS
- language

Cookie Source

- HTTP Header

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly

Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly

Set-Cookie: language=en-US; path=/; HttpOnly

Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT

…
```

Actions to Take

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

Remedy

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to be understand layer 2, have physical access to systems either as waypoints for the traffic, or have locally gained access to to a system between the victim and the web server.

External References

- Invicti Standard - Security Cookies - Secure Flag
- .NET Cookie.Secure Property
- How to Create Totally Secure Cookies

CLASSIFICATION

PCI DSS v3.2	6.5.10
OWASP 2013	A6
OWASP 2017	A3
CWE	614
CAPEC	102
WASC	15
ASVS 4.0	3.4.1
NIST SP 800-53	AC-16
DISA STIG	3.5.1
ISO27001	A.14.1.2
OWASP Top Ten 2021	A02

CVSS 3.0 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String

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

CVSS 3.1 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String

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

11. Insecure Frame (External)

LOW | 1 | CONFIRMED | 1

Invicti Standard identified an external insecure or misconfigured iframe.

Impact

IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly.

Here is an example, the URLs below all belong to the same origin as *http://site.com*:

http://site.com
http://site.com/
http://site.com/my/page.html

Whereas the URLs mentioned below aren't from the same origin as *http://site.com*:

http://www.site.com (a sub domain)
http://site.org (different top level domain)
https://site.com (different protocol)
http://site.com:8080 (different port)

When the `sandbox`attribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
- Forms are disabled. The hosted content is not allowed to make forms post back to any target.
- Scripts are disabled. JavaScript is disabled and will not execute.
- Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
- Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the `sandbox`attribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

- It might trick the user into supplying a username and password to the site loaded inside the iframe.
- It might navigate the parent window to a phishing page.
- It might execute untrusted code.
- It could show a popup, appearing to come from the parent site.

Sandboxcontaining a value of :

- `allow-same-origin`will not treat it as a unique origin.
- `allow-top-navigation`will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.
- `allow-forms`will allow form submissions from inside the iframe.
- `allow-popups`will allow popups.
- `allow-scripts`will allow malicious script execution however it won't allow to create popups.

Vulnerabilities

11.1. https://www.mustso.org.tr/

CONFIRMED

Frame Source(s)
- https://www.trthaber.com/sitene-ekle/ekonomi-7/?haberSay=3&renk=a
- https://calendar.google.com/calendar/embed?src=mustso1968%40gmail.com&ctz=Europe%2Fistanbul

Parsing Source
- DOM Parser

Frame Name(s)
- fce16e481136e4

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" /><link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link href="/Portals/348/Skins/mustso/fa
…
```

Remedy

- Apply sandboxing in inline frame

```
<iframe sandbox src="framed-page-url"></iframe>
```

- For untrusted content, avoid the usage of `seamless`attribute and `allow-top-navigation`, `allow-popups`and `allow-scripts`in sandbox attribute.

External References

- HTML5 Security Cheat Sheet

Remedy References

- How to Safeguard your Site with HTML5 Sandbox
- Play safely in sandboxed IFrames

CLASSIFICATION

OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	14.3.2
NIST SP 800-53	CM-6

DISA STIG	3.5.1
ISO27001	A.14.1.2
OWASP Top Ten 2021	A05

12. 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

12.1. https://www.mustso.org.tr/trace.axd

CONFIRMED

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

Request | Response

Request

```
GET /trace.axd HTTP/1.1
Host: www.mustso.org.tr
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: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; language=en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 451,8608
Total Bytes Received : 3523
Body Length : 3306
Is Compressed : No

```
HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
Content-Length: 3306
Content-Type: text/html; charset=utf-8
Date: Sun, 21 Aug 2022 10HTTP/1.1 500 Internal Server Error

Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
Content-Length: 3306
Content-Type: text/html; charset=utf-8
Date: Sun, 21 Aug 2022 10:19:25 GMT
Cache-Control: private

<!DOCTYPE html>
<
…
```

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
ISO27001	A.14.1.2

13. 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

13.1. https://www.mustso.org.tr/

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş
TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası ©
| Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE"
content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1
DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style
id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" />
<link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet"
type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css"
href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link
href="/Portals/348/Skins/mustso/fa
…
```

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	3.5.1
OWASP API Top Ten 2019	API7
ISO27001	A.14.2.5
OWASP Top Ten 2021	A05

14. 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

14.1. https://www.mustso.org.tr/trace.axd

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

Certainty

Request | Response

Request

```
GET /trace.axd HTTP/1.1
Host: www.mustso.org.tr
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: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; language=en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 451,8608
Total Bytes Received : 3523
Body Length : 3306
Is Compressed : No

```
HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
Content-Length: 3306
Content-Type: text/html; charset=utf-8
Date: Sun, 21 Aug 2022 10:19:25 GMT
Cache-Control: private

<!DOCTYPE html>
<html>
<head>
<title>Trace Error</title>
<meta name="viewport" content="width=device-width" />
<style>
body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;}
p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px}
b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px}
H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red }
H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon }
pre {font-family:"Consolas","Lucida Console",Monospace;font-size:11pt;margin:0;padding:0.5em;line-height:14pt}
.marker {font-weight: bold; color: black;text-decoration: none;}
.version {color: gray;}
.error {margin-bottom: 10px;}
.expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:hand; }
@media screen and (max-width: 639px) {
pre { width: 440px; overflow: auto; white-space: pre-wrap; word-wrap: break-word; }
}
@media screen and (max-width: 479px) {
pre { width: 280px; }
}
</style>
</head>

<body bgcolor="white">

<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

<h2> <i>Trace Error</i> </h2></span>

<font face="Arial, Helvetica, Geneva, SunSans-Regular, sans-serif ">

<b> Description: </b>Trace.axd is not enabled in the configuration file for this application. Note: Trace is never enabled when &lt;deployment retail=true
/&gt;
<br><br>

<b>Details:</b> To enable trace.axd, please create a &lt;trace&gt; tag within the c
…
```

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	3.13
OWASP API Top Ten 2019	API7
ISO27001	A.9.2.3
OWASP Top Ten 2021	A05

15. 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

15.1. https://www.mustso.org.tr/

Extracted Version

- 4.0.30319

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş
TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası ©
| Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE"
content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1
DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style
id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" />
<link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet"
type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css"
href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link
href="/Portals/348/Skins/mustso/fa
…
```

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	3.13
OWASP API Top Ten 2019	API7
ISO27001	A.18.1.3
OWASP Top Ten 2021	A05

16. 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

16.1. https://www.mustso.org.tr/

Extracted Version

- 8.5

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş
TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası ©
| Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE"
content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1
DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style
id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" />
<link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet"
type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css"
href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link
href="/Portals/348/Skins/mustso/fa
…
```

Remedy

Configure your web server to prevent information leakage from the SERVERheader 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	3.13
OWASP API Top Ten 2019	API7
OWASP Proactive Controls	N/A
ISO27001	A.18.1.3
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. https://www.mustso.org.tr/

ViewState Version

- .NET Framework 2.x

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug
…
> Ana Sayfa
</title></head>
<body id="Body">
<noscript></noscript>
<form method="post" action="/" id="Form" enctype="multipart/form-data" autocomplete="off">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwUKLTUxODU2MjE2OQ9kFgICAQ9kFgICAQ9kFgICAw9kFgJmD2QWQgIFDxYCHgdWaXNpYmxlZ2QCBw9kFgICAQ9kFgRmDw8WAh8AaGRkAgEPZBYCAgIPFgIfAGhkAgkPZBYCAgEPZBYEZg8
PFgIfAGhkZAIBD2QWAgICDxYCHwBoZAILDxYCHwBnFgICAQ9kFgRmDw8WAh8AaGRkAgEPZBYCAgIPFgIfAGhkAg0PFgIeBWNsYXNzBRNjb2wtMjIgRE5ORW1wdHlQYW5lZAIPDxYCHwEFFWNvbC11cnVuI
EROTkVtcHR5UGFuZWQCEQ8WAh8BBRJjb2wtMiBETk5FbXB0eVBhbmVkAhMPFgIfAQUSY29sLTkgRE5ORW1wdHlQYW5lZAIVDxYCHwEFE2NvbC0xMyBETk5FbXB0eVBhbmVkAhcPFgIfAQUMRE5ORW1wdHl
QYW5lZAIZD2QWAgIBD2QWBGYPDxYCHwBoZGQCAQ9kFgICAg8WAh8AaGQCGw9kFgICAQ9kFgRmDw8WAh8AaGRkAgEPZBYCAgIPFgIfAGhkAh0PZBYCAgEPZBYEZg8PFgIfAGhkZAIBD2QWAgICDxYCHwBoZ
AIfD2QWAgIBD2QWBGYPDxYCHwBoZGQCAQ9kFgICAg8WAh8AaGQCIQ8WAh8BBRJjb2wtNCBETk5FbXB0eVBhbmVkAiMPFgIfAQUSY29sLTQgRE5ORW1wdHlQYW5lZAIlDxYCHwEFEmNvbC00IEROTkVtcHR
5UGFuZWQCJw8WAh8BBRJjb2wtNCBETk5FbXB0eVBhbmVkAikPFgIfAQUSY29sLTQgRE5ORW1wdHlQYW5lZAIrDxYCHwEFEmNvbC00IEROTkVtcHR5UGFuZWQCLQ8WAh8BBRJjb2wtNCBETk5FbXB0eVBhb
mVkAi8PFgIfAGcWAgIB...
</div>


<script src="/js/dnncore.js?v2" type="text/javascript"></script>
<script src="/Portals/348/Skins/mustso/jquery.js" type="text/javascript"></script>
<script src="/Portals/348/Skins/must
…
```

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	3.6
ISO27001	A.14.2.5
OWASP Top Ten 2021	A05

18. Content Security Policy (CSP) Not Implemented

BEST PRACTICE | 1 | CONFIRMED | 1

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src:**Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
- **base-uri:**The base element is used to resolve a relative URL to an absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to the base-href attribute of the document.
- **frame-ancestors**: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- **frame-src / child-src**: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe on the page. (Please note that frame-src was brought back in CSP 3)
- **object-src**: Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- **default-src**: It is a fallback for the directives that mostly end with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
  - child-src
  - connect-src
  - font-src
  - img-src
  - manifest-src
  - media-src
  - object-src
  - script-src
  - style-src

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self** : Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as eval().

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://*.example.com;
Content-Security-Policy: script-src https://example.com:*;
Content-Security-Policy: script-src https:;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out on this extra layer of security.

Vulnerabilities

18.1. https://www.mustso.org.tr/

CONFIRMED

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" /><link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link href="/Portals/348/Skins/mustso/fa
…
```

Actions to Take

- Enable CSP on your website by sending the `Content-Security-Policy`in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Invicti Standard identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the `Content-Security-Policy`in HTTP response headers that instruct the browser to apply the policies you specified.

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	3.5.1
ISO27001	A.14.2.5

19. Expect-CT Not Enabled

BEST PRACTICE | 1

Invicti Standard identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissused certificates to be used.

Vulnerabilities

19.1. https://www.mustso.org.tr/

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" /><link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link href="/Portals/348/Skins/mustso/fa
…
```

Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode**first. If everything goes well and your certificate is ready, go with the Expect-CT enforcemode. To use **report-only mode**first, omit **enforce**flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

External References

- Expect-CT Extension for HTTP
- Expect-CT HTTP Header
- Expect-CT Header

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	9.2.4
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.1.2

20. 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

20.1. https://www.mustso.org.tr/

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	3.6.2
ISO27001	A.14.1.3
OWASP Top Ten 2021	A02

21. 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

21.1. https://www.mustso.org.tr/

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" /><link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link href="/Portals/348/Skins/mustso/fa
…
```

Remedy

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

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

External References

- Internet Explorer 8 Security Features - MSDN
- X-XSS-Protection HTTP Header
- Internet Explorer 8 XSS Filter

CLASSIFICATION

CWE	16
WASC	15
HIPAA	164.308(a)
ISO27001	A.14.2.5

22. Referrer-Policy Not Implemented

BEST PRACTICE | 1

Invicti Standard detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Vulnerabilities

22.1. https://www.mustso.org.tr/

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" /><link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link href="/Portals/348/Skins/mustso/fa
…
```

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the rel attribute.

External References

- Referrer Policy
- Referrer Policy - MDN
- Referrer Policy HTTP Header
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	200
ASVS 4.0	14.4.6
NIST SP 800-53	AC-22
DISA STIG	3.13
ISO27001	A.14.2.5

23. SameSite Cookie Not Implemented

BEST PRACTICE | 1

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite*was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

Vulnerabilities

23.1. https://www.mustso.org.tr/

Identified Cookie(s)

- .ASPXANONYMOUS
- language

Cookie Source

- HTTP Header

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly

Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly

Set-Cookie: language=en-US; path=/; HttpOnly

Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT

...
```

Remedy

The server can set a same-site cookie by adding the `SameSite=...`attribute to the `Set-Cookie`header. There are three possible values for the `SameSite`attribute:

- Lax:In this mode, the cookie will only be sent with a top-level get request.

```
Set-Cookie: key=value; SameSite=Lax
```

- Strict: In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

```
Set-Cookie: key=value; SameSite=Strict
```

- None: In this mode, the cookie will be sent with the cross-site requests. Cookies with `SameSite=None`must also specify the `Secure`attribute to transfer them via a secure context. Setting a `SameSite=None`cookie without the `Secure`attribute will be rejected by the browsers.

```
Set-Cookie: key=value; SameSite=None; Secure
```

External References

- Security Cookies - SameSite Attribute - Invicti Standard
- Using the Same-Site Cookies Attribute to Prevent CSRF Attacks
- Same-site Cookies
- Preventing CSRF with the same-site cookie attribute
- SameSite cookies explained
- Get Ready for New SameSite=None; Secure Cookie Settings

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	3.4.3
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.2.5

24. 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

24.1. https://www.mustso.org.tr/

CONFIRMED

Identified Sub Resource(s)

- https://connect.facebook.net/tr_TR/sdk.js#xfbml=1&version=v9.0
- https://www.googletagmanager.com/gtag/js?id=UA-113784354-1

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug
…
<div class="art-box-body art-blockcontent-body">

<div id="dnn_ctr24235_ContentPane" class="DNNAlignleft"><!-- Start_Module_24235 --><div id="dnn_ctr24235_ModuleContent">
<div id="fb-root"></div>
<script async defer crossorigin="anonymous" src="https://connect.facebook.net/tr_TR/sdk.js#xfbml=1&version=v9.0" nonce="tUEeNzfw"></script>
<divclass="fb-page" data-href="https://www.facebook.com/mustso49/" data-tabs="timeline" data-width="251" data-height="361" data-small-header="false" data-
adapt-container-width="true" data-hide-cover="fal
…
i < links.length; i++) { if (links[i].href == window.location.href) { jQuery(links[i]).parent().addClass('aktif'); break; } } }); </script>


<!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-113784354-1"></script>
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());

gtag('config', 'UA-113784354-1');
</script>



<input
…
```

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	3.5.1
ISO27001	A.14.2.5

25. 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

25.1. https://www.mustso.org.tr/%C4%B0leti%C5%9Fim/tabid/17212/Default.aspx

Email Address(es)

- mustso@tobb.org.tr

Certainty

Request | Response

Request

```
GET /%C4%B0leti%C5%9Fim/tabid/17212/Default.aspx HTTP/1.1
Host: www.mustso.org.tr
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: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; language=en-US
Referer: https://www.mustso.org.tr/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 1796,0042
Total Bytes Received : 17236
Body Length : 16949
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 5721
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:19:21 GMT
Cache-C
…
opel Cad. Kat: 1 No:3 Merkez / MUS</i></p>
<p><label>TELEFON</label> <i> +90(436) 212 1195 </i></p>
<p><label>FAKS</label> <i>+90(436) 212 9993</i></p>
<p><label>E-POSTA</label> <i><a href="mailto:mustso@tobb.org.tr" style="font-size: 15px;">mustso@tobb.org.tr</a></i></p>
</div> <!-- End_Module_23946 -->
</div></div>


<div class="cleared"></div>
</div>
</div>

<div align="right">


…
```

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	3.13
OWASP Proactive Controls	C7
ISO27001	A.9.4.1

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: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

26. 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

26.1. https://www.mustso.org.tr/DesktopModules/ProModules/Templates/

CONFIRMED

Request | Response

Request

```
GET /DesktopModules/ProModules/Templates/ HTTP/1.1
Host: www.mustso.org.tr
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: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; language=en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 901,6467
Total Bytes Received : 1370
Body Length : 1233
Is Compressed : No

```
HTTP/1.1 403 Forbidden

Server: Microsoft-IIS/8.5
Content-Length: 1233
Content-Type: text/html
Date: Sun, 21 Aug 2022 10:18:28 GMT

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
<div class="content-container"><fieldset>
<h2>403 - Forbidden: Access is denied.</h2>
<h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>
</fieldset></div>
</div>
</body>
</html>
```

CLASSIFICATION

OWASP Proactive Controls	C8
ISO27001	A.8.1.1

27. 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

27.1. https://www.mustso.org.tr/

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: www.mustso.org.tr
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/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 2657,4095
Total Bytes Received : 51989
Body Length : 51399
Is Compressed : Yes

```
HTTP/1.1 200 OK
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; expires=Sat, 29-Oct-2022 20:56:49 GMT; path=/; HttpOnly
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
Content-Length: 13238
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 21 Aug 2022 10:16:48 GMT
Cache-Control: private

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş TSO, Muş Ticaret ve Sanayi Odası, Muş , Muş Ticaret ,Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" /><link id="_Portals_348_" rel="stylesheet" type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><link rel="stylesheet" type="text/css" href="/Portals/348/Skins/mustso/tema.css?v=4" /><link href="/Portals/348/Skins/mustso/fa
…
```

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	3.13
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

28. OPTIONS Method Enabled

INFORMATION 1 | CONFIRMED 1

Invicti Standard detected that OPTIONSmethod 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

28.1. https://www.mustso.org.tr/

CONFIRMED

Allowed methods

- OPTIONS, TRACE, GET, HEAD, POST

Request | Response

Request

```
OPTIONS / HTTP/1.1
Host: www.mustso.org.tr
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: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; language=en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 722,5436
Total Bytes Received : 183
Body Length : 0
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Allow: OPTIONS, TRACE, GET, HEAD, POST
Content-Length: 0
Public: OPTIONS, TRACE, GET, HEAD, POST
Date: Sun, 21 Aug 2022 10:18:59 GMT
```

Remedy

Disable OPTIONSmethod 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	3.5.1
OWASP API Top Ten 2019	API7
ISO27001	A.14.1.2
OWASP Top Ten 2021	A05

29. Robots.txt Detected

INFORMATION | 1 | CONFIRMED | 1

Invicti Standard detected a `Robots.txt` file with potentially sensitive content.

Impact

Depending on the content of the file, an attacker might discover hidden directories and files.

Vulnerabilities

29.1. https://www.mustso.org.tr/robots.txt

CONFIRMED

Interesting Robots.txt Entries

- Disallow: /DesktopModules/Gallery/Viewer.aspx # This is an infinite virtual URL space
- Disallow: /DesktopModules/
- Disallow: /DesktopModules/*
- Disallow: /*?ctl=profile
- Disallow: /*/ctl/
- Disallow: /LinkClick.aspx?*
- Disallow: /*rss.aspx
- Disallow: /

Request | Response

Request

```
GET /robots.txt HTTP/1.1
Host: www.mustso.org.tr
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: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; Article51578=1; Article51511=1; Article51372=1; Article51353=1;
Article43758=1; Article51173=1; Article41669=1; language=en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 22619,9698
Total Bytes Received : 948
Body Length : 649
Is Compressed : Yes

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
Content-Length: 342
Last-Modified: Tue, 16 Mar 2021 07:18:12 GMT
Accept-Ranges: bytes
ETag: "c3e36186341ad71:0"
Content-Type: text/plain
Content-Encoding:
Date: Sun, 21 Aug 2022 10:20:28 GMT
Cache-Control: max-age=604800

User-agent:*
Disallow:/DesktopModules/Gallery/Viewer.aspx # This is an infinite virtual URL space
Disallow:/DesktopModules/
Disallow:/DesktopModules/*
Disallow:/*?ctl=profile
Disallow:/*/ctl/
Disallow:/LinkClick.aspx?*
Disallow:/*rss.aspx

User-agent:AhrefsBot
Disallow:/

User-agent:HubSpot
Disallow:/

User-agent:HubSpot Crawler 1.0
Disallow:/

User-agent:HubSpot Webcrawler
Disallow:/

User-agent:Linguee
Disallow:/

User-agent:dotbot
Disallow:/

User-agent:SemrushBot
Disallow:/

User-agent:SemrushBot-SA
Disallow:/

User-agent:MJ12bot
Disallow:/

User-agent:PetalBot
Disallow:/
```

Remedy

Ensure you have nothing sensitive exposed within this file, such as the path of an administration panel. If disallowed paths are sensitive and you want to keep it from unauthorized access, do not write them in the `Robots.txt`, and ensure they are correctly protected by means of authentication.
`Robots.txt`is only used to instruct search robots which resources should be indexed and which ones are not.

The following block can be used to tell the crawler to index files under /web/ and **ignore the rest**:

```
User-Agent: *
Allow: /web/
Disallow: /
```

Please note that when you use the instructions above, **search engines will not index your website** except for the specified directories.

If you want to hide certain section of the website from the search engines `X-Robots-Tag`can be set in the response header to tell crawlers whether the file should be indexed or not:

```
X-Robots-Tag: googlebot: nofollow
X-Robots-Tag: otherbot: noindex, nofollow
```

By using `X-Robots-Tag`you don't have to list the these files in your `Robots.txt`.

It is also not possible to prevent media files from being indexed by putting using Robots Meta Tags. `X-Robots-Tag`resolves this issue as well.

For Apache, the following snippet can be put into `httpd.conf`or an `.htaccess`file to restrict crawlers to index multimedia files without exposing them in `Robots.txt`

```
<Files ~ "\.pdf$">
# Don't index PDF files.
Header set X-Robots-Tag "noindex, nofollow"
</Files>
```

```
<Files ~ "\.(png|jpe?g|gif)$">
#Don't index image files.
Header set X-Robots-Tag "noindex"
</Files>
```

External References

- What Content Is Not Crawled? - Google
- How Search organizes information
- X-Robots-Tag: A Simple Alternate For Robots .txt and Meta Tag

CLASSIFICATION

OWASP Proactive Controls	C7
ISO27001	A.18.1.3

30. Unexpected Redirect Response Body (Too Large)

INFORMATION | 1

Invicti Standard identified an unexpected redirect response body (too large).

This generally indicates that after redirect the page did not finish the response as it was supposed to.

Impact

This can lead to serious issues such as authentication bypass in authentication required pages. In other pages it generally indicates a programming error.

Vulnerabilities

30.1. https://www.mustso.org.tr/Bas%C4%B1ndaBiz/Haber/tabid/17222/articleType/ArticleView/articleId/

Certainty

Request | Response

Request

```
GET /Bas%C4%B1ndaBiz/Haber/tabid/17222/articleType/ArticleView/articleId/ HTTP/1.1
Host: www.mustso.org.tr
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: .ASPXANONYMOUS=xVOo9tjr2AEkAAAAMDk2ZmI3YmItYTI2Mi00MGRmLTkyZjktMDgzM2U3YTE4NzFl0; language=en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
```

Response

Response Time (ms) : 783,6224
Total Bytes Received : 18243
Body Length : 17911
Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: language=en-US; path=/; HttpOnly
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
Content-Length: 17911
Content-Type: text/html; charset=utf-8
Location: https://www.mustso.org.tr/Bas%C4%B1ndaBiz/Haber/tabid/17222/Default.aspx
Date: Sun, 21 Aug 2022 10:19:28 GMT
Cache-Control: private

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="https://www.mustso.org.tr/Bas%C4%B1ndaBiz/Haber/tabid/17222/Default.aspx">here</a>.</h2>
</body></html>
<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Haber" /><meta id="MetaKeywords" name="KEYWORDS" content="Haber" /><meta
id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR"
content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" />
<meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-
equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="Template_23961"
rel="stylesheet" type="text/css" href="/DesktopModules/DnnForge - NewsArticles/Templates/Standard/Template.css" /><link
id="_DesktopModules_DnnForge___NewsArticles" rel="stylesheet" type="text/css" href="/DesktopModules/DnnForge - NewsArticles/module.css" /><link
id="_Portals__default_" rel="stylesheet" type="text/css" href="/Portals/_default/default.min.css" /><link id="_Portals_348_" rel="stylesheet"
type="text/css" href="/Portals/348/portal.css" /><!--[if IE 6]><link id="styleIE6" rel="stylesheet" type="text/css"
href="/Portals/348/Skins/mustso/style.ie6.css" /><![endif]--><!--[if IE 7]><link id="styleIE7" rel="stylesheet" type="text/css"
href="/Portals/348/Skins/mustso/style.ie7.css" /><![endif]--><l
…
```

Remedy

1. Finish the HTTP response after you redirect the user.
2. In ASP.NET, use `Response.Redirect("redirected-page.aspx", true)`instead of `Response.Redirect("redirected-page.aspx", false)`.
3. In PHP applications, call `exit()`after you redirect the user.

CLASSIFICATION

CWE	698
WASC	40
ASVS 4.0	14.1.3
NIST SP 800-53	SI-15
DISA STIG	3.13
OWASP Proactive Controls	C6
ISO27001	A.14.2.5

Show Scan Detail

Enabled Security Checks : Apache Struts S2-045 RCE,
Apache Struts S2-046 RCE,
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),
Drupal Remote Code Execution,
Expect Certificate Transparency (Expect-CT),
Expression Language Injection,
File Upload,
Header Analyzer,
Heartbleed,
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,
Local File Inclusion,
Local File Inclusion (IAST),
Log4j Code Evaluation (Out of Band),
Login Page Identifier,
Mixed Content,
Open Redirection,
Oracle WebLogic Remote Code Execution,
Referrer Policy,
Reflected File Download,
Remote File Inclusion,
Remote File Inclusion (Out of Band),
Reverse Proxy Detection,
RoR Code Execution,
Server-Side Request Forgery (DNS),

		Server-Side Request Forgery (Pattern Based), Server-Side Template Injection, Signatures, Software Composition Analysis (SCA), 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, XML External Entity, XML External Entity (Out of Band)
URL Rewrite Mode	:	Heuristic
Detected URL Rewrite Rule(s)	:	/BasındaBiz/Haber/tabid/{param1}/articleType/ArchiveView/currentpage/{param2}, /BasındaBiz/Haber/tabid/{param1}/articleType/ArticleView/articleId/{param2}, /BasındaBiz/Haber/tabid/{param1}/articleType/ArticleView/articleId/{param2}/api, /BasındaBiz/Haber/tabid/{param1}/articleType/ArticleView/articleId/{param2}/etc, /BasındaBiz/Haber/tabid/{param1}/articleType/ArticleView/articleId/{param2}/ndaBiz, /Portals/{param1}/HaberFoto/{param2}
Excluded URL Patterns	:	gtm\.js WebResource\.axd ScriptResource\.axd
Authentication	:	None
Authentication Profile	:	None
Scheduled	:	No
Additional Website(s)	:	None