21/07/2023 11:47 AM (UTC+05:30)

Detailed Scan Report

Go to the report on Invicti Enterprise.

https://sfs.turkiyeshell.com/

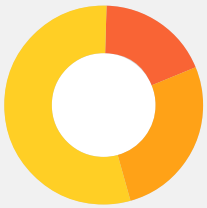
Scan Time	: 01/07/2023 04:00 AM
Scan Duration	: 00:02:10:36
Total Requests	: 74,501
Average Speed	: 9.5 r/s
Tags	DSSOM, Mobility, Mobility

Risk Level:
HIGH

IDENTIFIED	CONFIRMED	CRITICAL
11	2	0

HIGH	MEDIUM	LOW	BEST PRACTICE	INFORMATION
2	3	6	0	0

Identified Vulnerabilities



Critical	0
High	2
Medium	3
Low	6
Best Practice	0
Information	0
TOTAL	**11**

Confirmed Vulnerabilities

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

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	Out-of-date Version (jQuery Validation)	GET	https://sfs.turkiyeshell.com/lib/jquery-validation/dist/jquery.validate.js	No Parameters	No Parameter Types
	Out-of-date Version (Moment.js)	GET	https://sfs.turkiyeshell.com/	No Parameters	No Parameter Types
	[Possible] Cross-site Scripting	POST	https://sfs.turkiyeshell.com/account/loginsfs	UserName	Querystring
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://sfs.turkiyeshell.com/	No Parameters	No Parameter Types
	Weak Ciphers Enabled	GET	https://sfs.turkiyeshell.com/	No Parameters	No Parameter Types
	[Possible] Phishing by Navigating Browser Tabs	GET	https://sfs.turkiyeshell.com/	No Parameters	No Parameter Types
	Missing X-Frame-Options Header	GET	https://sfs.turkiyeshell.com/(%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)%3f(%23wr%3d%23context%5b%23parameters.obj%5b0%5d%5d.getWriter(),%23rs%3d@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec(%23parameters.command[0]).getInputStream()),%23wr.println(%23rs),%23wr.flush(),%23wr.close()):xx.toString.json?&obj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=expr%20268409241%20-%20993...	URI-BASED	Querystring
	Version Disclosure (Jquery)	GET	https://sfs.turkiyeshell.com/	No Parameters	No Parameter Types
	Version Disclosure (JqueryValidation)	GET	https://sfs.turkiyeshell.com/lib/jquery-validation/dist/jquery.validate.js	No Parameters	No Parameter Types
	Version Disclosure (Momentjs)	GET	https://sfs.turkiyeshell.com/	No Parameters	No Parameter Types
	Autocomplete is Enabled	GET	https://sfs.turkiyeshell.com/	No Parameters	No Parameter Types

1. Out-of-date Version (jQuery Validation)

HIGH | 1

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

Impact

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

Vulnerabilities

1.1. https://sfs.turkiyeshell.com/lib/jquery-validation/dist/jquery.validate.js

Identified Version

- 1.19.3

Latest Version

- 1.19.5

Vulnerability Database

- Result is based on 06/27/2023 15:00:00 vulnerability database content.

Certainty

Request | Response

Request

```
GET /lib/jquery-validation/dist/jquery.validate.js HTTP/1.1
Host: sfs.turkiyeshell.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: .AspNetCore.Antiforgery.IOH2qP4C9lk=CfDJ8I4hPoQOtxJNkFdlxKdQaaj61YWL07fDpF-ClCDhm_pPgj-
67UZX3w2uryZeXKR60HZMGynGssWi2luhrYfHAfcWHsRTa05TQKE8z2Idgvlgxkc9jNi6X22oqjJCv68RzFXOJ2p3NAe3AlBLw06
LPIE;
.AspNetCore.Session=CfDJ8I4hPoQOtxJNkFdlxKdQaahdraxoML2YikJMr5CtJegWDjJBB4cc7DLrVuZbE1SQ47e%2Bp2rv3A
6QidMg6Qpd4ExEJ2QwFKjm8Lus2I%2Ft3WUvje5SqvKtsGb5dMAIoAtHXJsYsqgSX5V2XPdaNKDY9ghWS6payV%2BcBIOSr2dOFV
qP
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 2698.1322
Total Bytes Received : 275
Body Length : 0
Is Compressed : No

```
…
GMT
Accept-Ranges: bytes
Strict-Transport-Security: max-age=2592000
Content-Type: text/javascript
Transfer-Encoding: chunked
Date: Fri, 30 Jun 2023 22:39:36 GMT
ETag: "1d858b11d3643f7"

/*!
* jQuery Validation Plugin v1.19.3
*
* https://jqueryvalidation.org/
*
* Copyright (c) 2021 Jörn Zaefferer
* Released under the MIT license
*/
(function( factory ) {
if ( typeof define === "function" && define.amd ) {

…
```

Remedy

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

Remedy References

- Downloading jQuery Validation

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	1035 , 937

CAPEC	310
HIPAA	164.308(a)(1)(i)
OWASP Proactive Controls	C1
ISO27001	ISO 27001-A.14.1.2
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	V-16836
OWASP Top Ten 2021	A06

2. Out-of-date Version (Moment.js)

HIGH | 1

Invicti Enterprise identified that the target web site is using Moment.js and detected that it is out of date.

Impact

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

Moment.js Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability

Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js.

Affected Versions

1.0.1 to 2.29.1

External References

- CVE-2022-24785

Exploits

Vulnerabilities

2.1. https://sfs.turkiyeshell.com/

Identified Version

- 2.29.1

Latest Version

- 2.29.4

Vulnerability Database

- Result is based on 06/27/2023 15:00:00 vulnerability database content.

Certainty

Request | Response

Request

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

Response

Response Time (ms) : 1007.3124
Total Bytes Received : 874
Body Length : 0
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: .AspNetCore.Antiforgery.IOH2qP4C9lk=CfDJ8I4hPoQOtxJNkFdlxKdQaaj61YWL07fDpF-ClCDhm_pPgj-
67UZX3w2uryZeXKR60HZMGynGssWi2luhrYfHAfcWHsRTa05TQKE8z2Idgvlgxkc9jNi6X22oqjJCv68RzFXOJ2p3NAe3AlBLw06
LPIE; path=/; secure; samesite=strict; httponly
Set-Cookie:
.AspNetCore.Session=CfDJ8I4hPoQOtxJNkFdlxKdQaahdraxoML2YikJMr5CtJegWDjJBB4cc7DLrVuZbE1SQ47e%2Bp2rv3A
6QidMg6Qpd4ExEJ2QwFKjm8Lus2I%2Ft3WUvje5SqvKtsGb5dMAIoAtHXJsYsqgSX5V2XPdaNKDY9ghWS6payV%2BcBIOSr2dOFV
qP; path=/; secure; samesite=lax; httponly
Referrer-Policy: no-referrer
X-Content-Type-Options: nosniff
Expires: -1
Pragma: no-cache
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=2592000
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Date: Fri, 30 Jun 2023 22:37:53 GMT
Cache-Control: no-store, no-cache

<!DOCTYPE html>
<html lang="en">
<head>
<base href="">
<meta charset="utf-8" />
<title>Giri&#x15F; | SFS Portal&#x131;</title>
<meta name="description" content="Shell Filo &#xC7;&#xF6;z&#xFC;mleri SFS Portal&#x131;" />
<meta property="og:title" content="Shell Filo Çözümleri Portalı" />
<meta name="description" content="Filo yönetiminde ihtiyaç duyduğunuz Shell TTS, Partner Card,
Kurumsal HGS ve Pratik Kart ürünlerine buradan ulaşabilir, filonuzu ofisinizden çıkmadan tek
merkezden kolayca yönetebilirsiniz.">
<meta property="og:description" content="Filo yönetiminde ihtiyaç duyduğunuz Shell TTS, Partner
Card, Kurumsal HGS ve Pratik Kart ürünlerine buradan ulaşabilir, filonuzu ofisinizden çıkmadan tek
merkezden kolayca yönetebilirsiniz." />
<meta property="og:site_name" content="Shell Filo Çözümleri Portalı">
<meta name="viewport" content="width=device-width, initial-scale=1.0, shrink-to-fit=no" />

<meta property="og:image" content="~/assets/shell-ographimg.png">
<meta property="og:type" content="website" />
<script>
var tim
…
```

Remedy

Please upgrade your installation of Moment.js to the latest stable version.

Remedy References

- Downloading Moment.js

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	1035 , 937
CAPEC	310
HIPAA	164.308(a)(1)(i)
OWASP Proactive Controls	C1
ISO27001	ISO 27001-A.14.1.2
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	V-16836
OWASP Top Ten 2021	A06

3. [Possible] Cross-site Scripting

MEDIUM | 1

Invicti Enterprise detected Possible Cross-site Scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Although Invicti Enterprise believes there is a cross-site scripting in here, it could **not confirm it**. We strongly recommend investigating the issue manually to ensure it is cross-site scripting and needs to be addressed.

Impact

There are many different attacks that can be leveraged through the use of XSS, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Vulnerabilities

3.1. https://sfs.turkiyeshell.com/account/loginsfs

Method	Parameter	Parameter Type	Value
POST	DNTCaptchaInputText	Querystring	
POST	__RequestVerificationToken	Querystring	CfDJ8I4hPoQOtxJNkFdlxKdQaahYpdwQb7VpknvM2ZfIouWfiOPdqpMIAGQ3QpuTnNVMVeGQkX6Bvkdp-dqqIJJGk2FcJM1z4Led...
POST	DNTCaptchaText	Querystring	otbJvQc_G3y-pjeWNRWNCQ
POST	Password	Querystring	Inv1@cti
POST	CustomerCode	Querystring	3
POST	DNTCaptchaToken	Querystring	xu-YbN1u0rwILG53YWIuOvQZu33O8lWeJ-II3jZDSxjLzcoxZa_eOS9Zrn5ZNePQhvifQNMq7V4vl1_ZG6Eg923KATWiSiYy7RSL...
POST	UserName	Querystring	'"--></style></scRipt><scRipt>netsparker(0x005BCF)</scRipt>

Notes

- Due to the Content-type header of the response, exploitation of this vulnerability might not be possible because of the browser used or because of the presence of certain web tools. We recommend that you fix this even if it is not an exploitable XSS vulnerability because it can allow an attacker to introduce other attacks to exploit it. But, these issues are not confirmed; you will need to manually confirm them yourself. In general, lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with built-in mime sniffing (such as Internet Explorer).

Certainty

Request | Response

Request

```
POST /account/loginsfs HTTP/1.1
Host: sfs.turkiyeshell.com
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 469
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
X-Requested-With: XMLHttpRequest

DNTCaptchaInputText=&__RequestVerificationToken=CfDJ8I4hPoQOtxJNkFdlxKdQaahYpdwQb7VpknvM2ZfIouWfiOPd
qpMIAGQ3QpuTnNVMVeGQkX6Bvkdp-
dqqIJJGk2FcJM1z4Led4q4xDrgIvF0Z_V_pRA6A6wVyiSAqScOvh8XK3BpIYfJzw5EvvsgB1rY&DNTCaptchaText=otbJvQc_G3
y-pjeWNRWNCQ&Password=Inv1%40cti&CustomerCode=3&DNTCaptchaToken=xu-YbN1u0rwILG53YWIuOvQZu33O8lWeJ-
II3jZDSxjLzcoxZa_eOS9Zrn5ZNePQhvifQNMq7V4vl1_ZG6Eg923KATWiSiYy7RSLNIfKFjs&UserName='"--></style>
</scRipt><scRipt>netsparker(0x005BCF)</scRipt>
```

Response

Response Time (ms) : 252.8771
Total Bytes Received : 622
Body Length : 0
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie:
.AspNetCore.Session=CfDJ8I4hPoQOtxJNkFdlxKdQaaglrKW%2B%2FKfZdntSx1xH3bBs0xrU7YjQg9%2F6%2F1AmcFaHrUGB
HcWLcDaIqwz%2Bs8eQrFh0z49vyASB7cjr19T%2BPJTZUe5aSV%2FNAZqxRyi%2FPL9Dnti7IkmlFoQ0fAenBkhAg3XS7tPYdApW
ha%2FLE9mK7FPo; path=/; secure; samesite=lax; httponly
Expires: -1
X-Content-Type-Options: nosniff
Pragma: no-cache
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=2592000
Referrer-Policy: no-referrer
Content-Type: application/json; charset=utf-8
Transfer-Encoding: chunked
Date: Sat, 01 Jul 2023 00:16:32 GMT
Cache-Control: no-store, no-cache

{"result":false,"message":"Value cannot be null. (Parameter 'user is NULL. '\"--></style></scRipt>
<scRipt>netsparker(0x005BCF)</scRipt>-3-0.0.0.1 Kullanıcısı İçin Hesap
Bulunamadı.')","maxFailedAttempts":1}
```

Remedy

This issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered / encoded. Output should be filtered / encoded according to the output format and location.

There are a number of pre-defined, well structured whitelist libraries available for many different environments. Good examples of these include OWASP Reform and Microsoft Anti-Cross-site Scripting libraries.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

- OWASP - Cross-site Scripting
- Cross-site Scripting Web Application Vulnerability
- XSS Shell
- XSS Tunnelling

Remedy References

- Content Security Policy (CSP) Explained
- Negative Impact of Incorrect CSP Implementations
- [ASP.NET] - Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet

CLASSIFICATION

PCI DSS v3.2	6.5.7
OWASP 2013	A3
OWASP 2017	A7
CWE	79
CAPEC	19
WASC	8
HIPAA	164.308(a)
ISO27001	ISO 27001-A.14.2.5
ASVS 4.0	5.3.3
NIST SP 800-53	SI-15
DISA STIG	V-16811
OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)

CVSS 3.0 SCORE	
Environmental	7.4 (High)

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

CVSS 3.1 SCORE	
Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

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

4. Weak Ciphers Enabled

MEDIUM 1 | CONFIRMED 1

Invicti Enterprise 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

4.1. https://sfs.turkiyeshell.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_RC4_128_MD5 (0x0004)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009D)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009C)

Request | Response

Request

```
[SSL Connection]
```

Response

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

```
[SSL Connection]
```

Actions to Take

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

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

2. Lighttpd:

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

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

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

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

Remedy

Configure your web server to disallow using weak ciphers.

External References

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

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6

OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ISO27001	ISO 27001-A.14.1.3
ASVS 4.0	6.2.5
NIST SP 800-53	SC-8
DISA STIG	V-6136
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

5. HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM | 1

Invicti Enterprise detected errors during parsing of Strict-Transport-Security header.

Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Vulnerabilities

5.1. https://sfs.turkiyeshell.com/

Error	Resolution
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

Certainty

Request | Response

Request

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

Response

Response Time (ms) : 1147.9115
Total Bytes Received : 874
Body Length : 0
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: .AspNetCore.Antiforgery.IOH2qP4C9lk=CfDJ8I4hPoQOtxJNkFdlxKdQaahEu14mIyMuE7H-
Dvubhlw75BG7PGHLbEXV-F5RR0sm3ZyhJSY8EpI1XIThGF-
n_KeBHc2LhVkBhc0ZTFKd0s844fsXkUT_Encbw2FH9bZZavOPcTv20Duq3-Z_jrEJAkM; path=/; secure;
samesite=strict; httponly
Set-Cookie:
.AspNetCore.Session=CfDJ8I4hPoQOtxJNkFdlxKdQaagIkQCjNPoSW8S4PCLKwFxBv4HZm56HoaT0eYLuUp%2BpJLHBICFbFX
LvbrHsmHCSRvZqRjEC4Oq8aA0CJf1%2BgOFSrGZ7nQRqSu%2FylNk6DcOL6sJx7U8vtgoWQRzBgsQ7b0kZLzDHe28iaFJQR811io
K0; path=/; secure; samesite=lax; httponly
Referrer-Policy: no-referrer
X-Content-Type-Options: nosniff
Expires: -1
Pragma: no-cache
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=2592000
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Date: Fri, 30 Jun 2023 22:38:17 GMT
Cache-Control: no-store, no-cache

<!DOCTYPE html>
<html lang="en">
<head>
<base href="">
<meta charset="utf-8" />
<title>Giri&#x15F; | SFS Portal&#x131;</title>
<meta name="description" content="Shell Filo &#xC7;&#xF6;z&#xFC;mleri SFS Portal&#x131;" />
<meta property="og:title" content="Shell Filo Çözümleri Portalı" />
<meta name="description" content="Filo yönetiminde ihtiyaç duyduğunuz Shell TTS, Partner Card,
Kurumsal HGS ve Pratik Kart ürünlerine buradan ulaşabilir, filonuzu ofisinizden çıkmadan tek
merkezden kolayca yönetebilirsiniz.">
<meta property="og:description" content="Filo yönetiminde ihtiyaç duyduğunuz Shell TTS, Partner
Card, Kurumsal HGS ve Pratik Kart ürünlerine buradan ulaşabilir, filonuzu ofisinizden çıkmadan tek
merkezden kolayca yönetebilirsiniz." />
<meta property="og:site_name" content="Shell Filo Çözümleri Portalı">
<meta name="viewport" content="width=device-width, initial-scale=1.0, shrink-to-fit=no" />

<meta property="og:image" content="~/assets/shell-ographimg.png">
<meta property="og:type" content="website" />
<script>
var tim
…
```

Remedy

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
    - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
    - The `max-age` must be at least 31536000 seconds (1 year)
    - The `includeSubDomains` directive must be specified
    - The `preload` directive must be specified
    - If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

External References

- HTTP Strict Transport Security (HSTS) HTTP Header
- Wikipedia - HTTP Strict Transport Security Implementation
- Check HSTS Preload status and eligibility

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ISO27001	ISO 27001-A.14.1.2
ASVS 4.0	14.4.5
NIST SP 800-53	SC-8
DISA STIG	V-6136
OWASP API Top Ten 2019	API7
	A05

OWASP Top Ten 2021

6. Autocomplete is Enabled

LOW 1 | CONFIRMED 1

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

Impact

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

Vulnerabilities

6.1. https://sfs.turkiyeshell.com/

CONFIRMED

Identified Field Name

- UserName

Request | Response

Request

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

Response

Response Time (ms) : 1007.3124
Total Bytes Received : 874
Body Length : 0
Is Compressed : No

```
…
"font-size-h6 font-weight-bolder text-dark" data-placement="right" data-toggle="tooltip"
title="Kullanıcı adı giriniz">
Kullanıcı Adı *
</label>
<input class="form-control form-control-solid h-auto py-4 px-6 rounded-lg border border-info" data-
val="true" data-val-required="Kullan&#x131;c&#x131; ad&#x131; bo&#x15F; olamaz" id="UserName"
name="UserName" required="required" type="text" value="" />
<span class="field-validation-valid" data-valmsg-for="UserName" data-valmsg-replace="true"></span>
</div>

<div class="form-group">
<label
…
```

Actions to Take

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

Required Skills for Successful Exploitation

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

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16

WASC	15
ISO27001	ISO 27001-A.14.1.2
ASVS 4.0	2.10.3
NIST SP 800-53	AC-16
DISA STIG	V-16786
OWASP Top Ten 2021	A05

7. Missing X-Frame-Options Header

LOW | 1

Invicti Enterprise 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

7.1. https://sfs.turkiyeshell.com/(%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)%3f(%23wr%3d%23context%5b%23parameters.obj%5b0%5d%5d.getWriter(),%23rs%3d@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec(%23parameters.command[0]).getInputStream()),%23wr.println(%23rs),%23wr.flush(),%23wr.close()):xx.toString.json?&obj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=expr%20268409241%20-%2099328

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

Certainty

Request | Response

Request

```
GET
/(%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)%3f(%23wr%3d%23context%5b%23parameters.
obj%5b0%5d%5d.getWriter(),%23rs%3d@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRunt
ime().exec(%23parameters.command[0]).getInputStream()),%23wr.println(%23rs),%23wr.flush(),%23wr.clos
e()):xx.toString.json?
&obj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=expr%20268409241%20-%2099328
HTTP/1.1
Host: sfs.turkiyeshell.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: .AspNetCore.Antiforgery.IOH2qP4C9lk=CfDJ8I4hPoQOtxJNkFdlxKdQaaj61YWL07fDpF-ClCDhm_pPgj-
67UZX3w2uryZeXKR60HZMGynGssWi2luhrYfHAfcWHsRTa05TQKE8z2Idgvlgxkc9jNi6X22oqjJCv68RzFXOJ2p3NAe3AlBLw06
LPIE;
.AspNetCore.Session=CfDJ8I4hPoQOtxJNkFdlxKdQaahdraxoML2YikJMr5CtJegWDjJBB4cc7DLrVuZbE1SQ47e%2Bp2rv3A
6QidMg6Qpd4ExEJ2QwFKjm8Lus2I%2Ft3WUvje5SqvKtsGb5dMAIoAtHXJsYsqgSX5V2XPdaNKDY9ghWS6payV%2BcBIOSr2dOFV
qP
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 1113.9101
Total Bytes Received : 179
Body Length : 0
Is Compressed : No

```
HTTP/1.1 400 Bad Request
Server: Microsoft-HTTPAPI/2.0
Connection: close
Content-Length: 324
Content-Type: text/html; charset=us-ascii
Date: Fri, 30 Jun 2023 22:38:18 GMT

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

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
    - `X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.

    - `X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.
    - `X-Frame-Options: ALLOW-FROM` *`URL`* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

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

Remedy References

- Clickjacking Defense Cheat Sheet

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ISO27001	ISO 27001-A.14.2.5
ASVS 4.0	14.4.7
NIST SP 800-53	CM-6
DISA STIG	V-16786
OWASP API Top Ten 2019	API7
OWASP Top Ten 2021	A05

8. [Possible] Phishing by Navigating Browser Tabs

LOW | 1

Invicti Enterprise 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

8.1. https://sfs.turkiyeshell.com/

External Links

- https://www.shell.com.tr/kurumsal-musteriler/filo-cozumleri/istasyon-bulucu.html
- https://www.shell.com.tr/suruculer/shell-yakitlari/akaryakit-pompa-satis-fiyatlari.html
- https://www.shell.com.tr/kurumsal-musteriler/filo-cozumleri.html

Certainty

Request | Response

Request

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

Response

Response Time (ms) : 1007.3124
Total Bytes Received : 874
Body Length : 0
Is Compressed : No

```
…
a href="/bakiye-sorgula" target="_blank" class="login-link-box text-center font-weight-bolder"
id="kt_login_balanceInquiry"><span>Bakiye</span><br /><span>Sorgula</span></a>
<a href="https://www.shell.com.tr/kurumsal-musteriler/filo-cozumleri/istasyon-bulucu.html"
target="_blank" class="login-link-box text-center font-weight-bolder"><span>İstasyon</span><br />
<span>Bulucu</span></a>
<a href="https://www.shell.com.tr/suruculer/shell-yakitlari/akaryakit-pompa-satis-fiyatlari.html"
target="_blank" class="login-link-box text-center font-weight-bolder"><span>Pompa</span><br />
<span>Fiyatları</span></a>
</div>


</div>
<form class="form" id="kt_lo
…
="login-footer">
<div class="text-dark-50 font-size-lg font-weight-bolder text-center">
<span class="mr-1">2023©</span>
<a href="https://www.shell.com.tr/kurumsal-musteriler/filo-cozumleri.html" target="_blank"
style="font-family: Arial,Roboto,Helvetica,sans-serif" class="text-dark-75 text-hover-primary">Shell
Filo Çözümleri</a>
</div>
</div>


…
```

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
ISO27001	ISO 27001-A.14.1.2
ASVS 4.0	14.1.3
NIST SP 800-53	CM-6
DISA STIG	V-16786
OWASP Top Ten 2021	A05

9. Version Disclosure (Jquery)

LOW | 1

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

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

Impact

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

Vulnerabilities

9.1. https://sfs.turkiyeshell.com/

Identified Version

- 3.6.0

Certainty

Request | Response

Request

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

Response

Response Time (ms) : 1007.3124
Total Bytes Received : 874
Body Length : 0
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: .AspNetCore.Antiforgery.IOH2qP4C9lk=CfDJ8I4hPoQOtxJNkFdlxKdQaaj61YWL07fDpF-ClCDhm_pPgj-67UZX3w2uryZeXKR60HZMGynGssWi2luhrYfHAfcWHsRTa05TQKE8z2Idgvlgxkc9jNi6X22oqjJCv68RzFXOJ2p3NAe3AlBLw06LPIE; path=/; secure; samesite=strict; httponly
Set-Cookie: .AspNetCore.Session=CfDJ8I4hPoQOtxJNkFdlxKdQaahdraxoML2YikJMr5CtJegWDjJBB4cc7DLrVuZbE1SQ47e%2Bp2rv3A6QidMg6Qpd4ExEJ2QwFKjm8Lus2I%2Ft3WUvje5SqvKtsGb5dMAIoAtHXJsYsqgSX5V2XPdaNKDY9ghWS6payV%2BcBIOSr2dOFVqP; path=/; secure; samesite=lax; httponly
Referrer-Policy: no-referrer
X-Content-Type-Options: nosniff
Expires: -1
Pragma: no-cache
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=2592000
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Date: Fri, 30 Jun 2023 22:37:53 GMT
Cache-Control: no-store, no-cache

<!DOCTYPE html>
<html lang="en">
<head>
<base href="">
<meta charset="utf-8" />
<title>Giri&#x15F; | SFS Portal&#x131;</title>
<meta name="description" content="Shell Filo &#xC7;&#xF6;z&#xFC;mleri SFS Portal&#x131;" />
<meta property="og:title" content="Shell Filo Çözümleri Portalı" />
<meta name="description" content="Filo yönetiminde ihtiyaç duyduğunuz Shell TTS, Partner Card, Kurumsal HGS ve Pratik Kart ürünlerine buradan ulaşabilir, filonuzu ofisinizden çıkmadan tek merkezden kolayca yönetebilirsiniz.">
<meta property="og:description" content="Filo yönetiminde ihtiyaç duyduğunuz Shell TTS, Partner Card, Kurumsal HGS ve Pratik Kart ürünlerine buradan ulaşabilir, filonuzu ofisinizden çıkmadan tek merkezden kolayca yönetebilirsiniz." />
<meta property="og:site_name" content="Shell Filo Çözümleri Portalı">
<meta name="viewport" content="width=device-width, initial-scale=1.0, shrink-to-fit=no" />

<meta property="og:image" content="~/assets/shell-ographimg.png">
<meta property="og:type" content="website" />
<script>
var tim
…
```

Remedy

Configure your web server to prevent information leakage.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	13
HIPAA	164.306(a) , 164.308(a)
ISO27001	ISO 27001-A.18.1.3
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Top Ten 2021	A05

10. Version Disclosure (Momentjs)

LOW | 1

Invicti Enterprise identified a version disclosure (Momentjs) 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 Momentjs.

Impact

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

Vulnerabilities

10.1. https://sfs.turkiyeshell.com/

Identified Version

- 2.29.1

Certainty

Request | Response

Request

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

Response

Response Time (ms) : 1007.3124
Total Bytes Received : 874
Body Length : 0
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: .AspNetCore.Antiforgery.IOH2qP4C9lk=CfDJ8I4hPoQOtxJNkFdlxKdQaaj61YWL07fDpF-ClCDhm_pPgj-
67UZX3w2uryZeXKR60HZMGynGssWi2luhrYfHAfcWHsRTa05TQKE8z2Idgvlgxkc9jNi6X22oqjJCv68RzFXOJ2p3NAe3AlBLw06
LPIE; path=/; secure; samesite=strict; httponly
Set-Cookie:
.AspNetCore.Session=CfDJ8I4hPoQOtxJNkFdlxKdQaahdraxoML2YikJMr5CtJegWDjJBB4cc7DLrVuZbE1SQ47e%2Bp2rv3A
6QidMg6Qpd4ExEJ2QwFKjm8Lus2I%2Ft3WUvje5SqvKtsGb5dMAIoAtHXJsYsqgSX5V2XPdaNKDY9ghWS6payV%2BcBIOSr2dOFV
qP; path=/; secure; samesite=lax; httponly
Referrer-Policy: no-referrer
X-Content-Type-Options: nosniff
Expires: -1
Pragma: no-cache
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=2592000
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Date: Fri, 30 Jun 2023 22:37:53 GMT
Cache-Control: no-store, no-cache

<!DOCTYPE html>
<html lang="en">
<head>
<base href="">
<meta charset="utf-8" />
<title>Giri&#x15F; | SFS Portal&#x131;</title>
<meta name="description" content="Shell Filo &#xC7;&#xF6;z&#xFC;mleri SFS Portal&#x131;" />
<meta property="og:title" content="Shell Filo Çözümleri Portalı" />
<meta name="description" content="Filo yönetiminde ihtiyaç duyduğunuz Shell TTS, Partner Card,
Kurumsal HGS ve Pratik Kart ürünlerine buradan ulaşabilir, filonuzu ofisinizden çıkmadan tek
merkezden kolayca yönetebilirsiniz.">
<meta property="og:description" content="Filo yönetiminde ihtiyaç duyduğunuz Shell TTS, Partner
Card, Kurumsal HGS ve Pratik Kart ürünlerine buradan ulaşabilir, filonuzu ofisinizden çıkmadan tek
merkezden kolayca yönetebilirsiniz." />
<meta property="og:site_name" content="Shell Filo Çözümleri Portalı">
<meta name="viewport" content="width=device-width, initial-scale=1.0, shrink-to-fit=no" />

<meta property="og:image" content="~/assets/shell-ographimg.png">
<meta property="og:type" content="website" />
<script>
var tim
…
```

Remedy

Configure your web server to prevent information leakage.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	13
HIPAA	164.306(a) , 164.308(a)
ISO27001	ISO 27001-A.18.1.3
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Top Ten 2021	A05

11. Version Disclosure (JqueryValidation)

LOW | 1

Invicti Enterprise identified a version disclosure (JqueryValidation) 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 JqueryValidation.

Impact

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

Vulnerabilities

11.1. https://sfs.turkiyeshell.com/lib/jquery-validation/dist/jquery.validate.js

Identified Version

- 1.19.3

Certainty

Request | Response

Request

```
GET /lib/jquery-validation/dist/jquery.validate.js HTTP/1.1
Host: sfs.turkiyeshell.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: .AspNetCore.Antiforgery.IOH2qP4C9lk=CfDJ8I4hPoQOtxJNkFdlxKdQaaj61YWL07fDpF-ClCDhm_pPgj-
67UZX3w2uryZeXKR60HZMGynGssWi2luhrYfHAfcWHsRTa05TQKE8z2Idgvlgxkc9jNi6X22oqjJCv68RzFXOJ2p3NAe3AlBLw06
LPIE;
.AspNetCore.Session=CfDJ8I4hPoQOtxJNkFdlxKdQaahdraxoML2YikJMr5CtJegWDjJBB4cc7DLrVuZbE1SQ47e%2Bp2rv3A
6QidMg6Qpd4ExEJ2QwFKjm8Lus2I%2Ft3WUvje5SqvKtsGb5dMAIoAtHXJsYsqgSX5V2XPdaNKDY9ghWS6payV%2BcBIOSr2dOFV
qP
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.71 Safari/537.36
```

Response

Response Time (ms) : 2698.1322
Total Bytes Received : 275
Body Length : 0
Is Compressed : No

```
…
GMT
Accept-Ranges: bytes
Strict-Transport-Security: max-age=2592000
Content-Type: text/javascript
Transfer-Encoding: chunked
Date: Fri, 30 Jun 2023 22:39:36 GMT
ETag: "1d858b11d3643f7"

/*!
* jQuery Validation Plugin v1.19.3
*
* https://jqueryvalidation.org/
*
* Copyright (c) 2021 Jörn Zaefferer
* Released under the MIT license
*/
(function( factory ) {
if ( typeof define === "function" && define.amd ) {

…
```

Remedy

Configure your web server to prevent information leakage.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	13
HIPAA	164.306(a), 164.308(a)
ISO27001	ISO 27001-A.18.1.3
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Top Ten 2021	A05

Show Scan Detail

Enabled Security Checks	:	Apache Struts S2-045 RCE, Apache Struts S2-046 RCE, Arbitrary Files (IAST), Backup Files, 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),
Drupal Remote Code Execution,
Expression Language Injection,
File Upload,
GraphQL Library Detection,
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,
LDAP Injection (IAST),
Local File Inclusion,
Local File Inclusion (IAST),
Log4j Code Evaluation (Out of Band),
Login Page Identifier,
Mail Header Injection (IAST),
Malware Analyzer,
Mixed Content,
MongoDB Injection (Blind),
MongoDB Injection (Boolean),
MongoDB Injection (Error Based),
MongoDB Injection (IAST),
MongoDB Injection (Operator),
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,
Security Assertion Markup Language (SAML),
Sensitive Data,
Server-Side Request Forgery (DNS),
Server-Side Request Forgery (Pattern Based),
Server-Side Template Injection,
Server-Side Template Injection (IAST),
Signatures,
Software Composition Analysis (SCA),

		Spring4Shell Remote Code Execution, SQL Injection (Blind), SQL Injection (Boolean), SQL Injection (Error Based), SQL Injection (IAST), SQL Injection (Out of Band), SSL, Static Resources (All Paths), Static Resources (Only Root Path), Unicode Transformation (Best-Fit Mapping), WAF Identifier, Web App Fingerprint, Web Cache Deception, WebDAV, Windows Short Filename, Wordpress Plugin Detection, Wordpress Theme Detection, XML External Entity, XML External Entity (Out of Band), XML External Entity Injection (IAST), XPath Injection (IAST)
URL Rewrite Mode	:	Heuristic
Detected URL Rewrite Rule(s)	:	None
Excluded URL Patterns	:	gtm\.js WebResource\.axd ScriptResource\.axd
Authentication	:	None
Authentication Profile	:	
Scheduled	:	Yes
Additional Website(s)	:	None
Scan Profile	:	Default
Scan Policy	:	Default Security Checks
Report Policy	:	Default Report Policy
Scope	:	Entered Path and Below

Scan Type	:	**Full**
Max Scan Duration	:	**48 hour(s)**

This report created with 1.0.0.0
https://www.netsparker.com