

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Scan Detail

Target	pdf.ssbmultiservices.com
Scan Type	Full Scan
Start Time	Feb 7, 2024, 8:48:21 PM GMT+8
Scan Duration	2 minutes
Requests	11727
Average Response Time	33ms
Maximum Response Time	3443ms
Application Build	v23.7.230728157



High



Medium



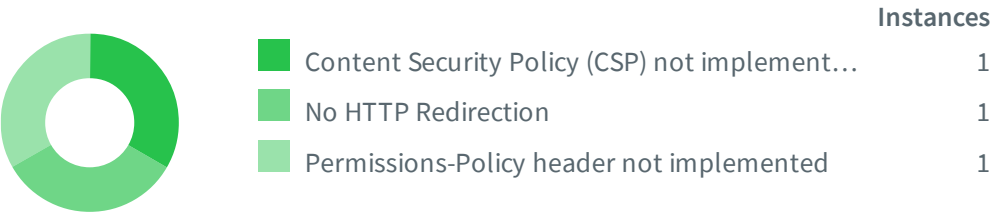
Low



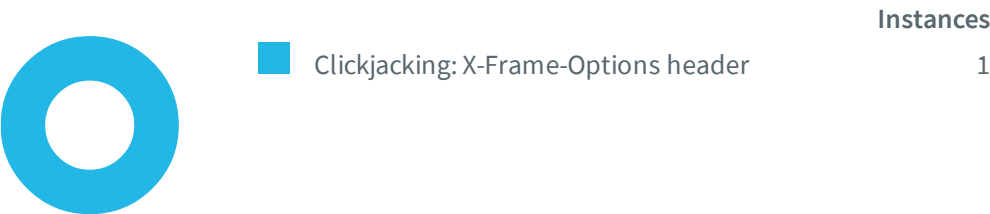
Informational

Severity	Vulnerabilities	Instances
High	0	0
Medium	3	3
Low	1	1
Informational	3	3
Total	7	7

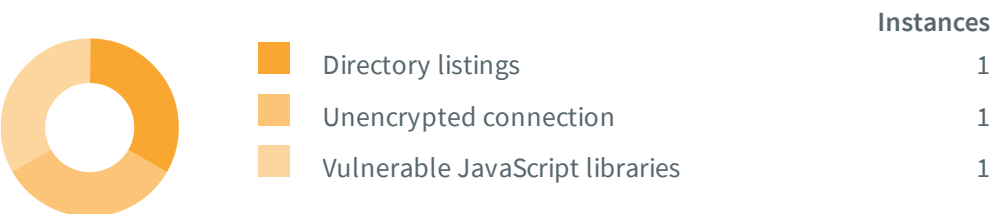
Informational










Low Severity



Medium Severity



Impacts

SEVERITY	IMPACT	
 Medium	1	Directory listings
 Medium	1	Unencrypted connection
 Medium	1	Vulnerable JavaScript libraries
 Low	1	Clickjacking: X-Frame-Options header
 Informational	1	Content Security Policy (CSP) not implemented
 Informational	1	No HTTP Redirection
 Informational	1	Permissions-Policy header not implemented

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

<http://pdf.ssbmultiservices.com/>

Verified

Folders with directory listing enabled:

- <http://pdf.ssbmultiservices.com/dflip/>
- <http://pdf.ssbmultiservices.com/dflip/js/>
- <http://pdf.ssbmultiservices.com/dflip/js/libs/>
- <http://pdf.ssbmultiservices.com/dflip/css/>
- <http://pdf.ssbmultiservices.com/dflip/images/>
- <http://pdf.ssbmultiservices.com/dflip/images/pdfjs/>
- <http://pdf.ssbmultiservices.com/dflip/fonts/>
- <http://pdf.ssbmultiservices.com/dflip/sound/>
- <http://pdf.ssbmultiservices.com/dflip/images/textures/>

Request

```
GET /dflip/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: pdf.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

References

[CWE-548: Exposure of Information Through Directory Listing](https://cwe.mitre.org/data/definitions/548.html)

<https://cwe.mitre.org/data/definitions/548.html>

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

Impact

Possible information disclosure.

<http://pdf.ssbmultiservices.com/>

Verified

Request

```
GET / HTTP/1.1
Referer: http://pdf.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: pdf.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Vulnerable JavaScript libraries

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult References for more information.

- **jQuery 1.11.0**

- URL: <http://pdf.ssbmultiservices.com/>
- Detection method: The library's name and version were determined based on its dynamic behavior.
- CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
- Description: Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- References:
 - <https://github.com/jquery/jquery/issues/2432>
 - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>
 - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
 - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
 - <https://jquery.com/upgrade-guide/3.5/>
 - <https://api.jquery.com/jquery.htmlPrefilter/>
 - <https://www.cvedetails.com/cve/CVE-2020-11022/>
 - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
 - <https://www.cvedetails.com/cve/CVE-2020-11023/>
 - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>

Request

GET / HTTP/1.1

Referer: <http://pdf.ssbmultiservices.com/>

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36

Host: pdf.ssbmultiservices.com

Connection: Keep-alive

Recommendation

Upgrade to the latest version.

Clickjacking: X-Frame-Options header

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

Impact

The impact depends on the affected web application.

<http://pdf.ssbmultiservices.com/>

Paths without secure XFO header:

- <http://pdf.ssbmultiservices.com/>
- <http://pdf.ssbmultiservices.com/index.html>
- <http://pdf.ssbmultiservices.com/dflip/images/>
- <http://pdf.ssbmultiservices.com/dflip/>
- <http://pdf.ssbmultiservices.com/dflip/images/pdfjs/>
- <http://pdf.ssbmultiservices.com/dflip/fonts/>
- <http://pdf.ssbmultiservices.com/dflip/sound/>
- <http://pdf.ssbmultiservices.com/dflip/images/textures/>
- <http://pdf.ssbmultiservices.com/dflip/css/>
- <http://pdf.ssbmultiservices.com/dflip/js/>
- <http://pdf.ssbmultiservices.com/dflip/js/libs/>
- <http://pdf.ssbmultiservices.com/mailman/archives/>

Request

```
GET / HTTP/1.1
Referer: http://pdf.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: pdf.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

[The X-Frame-Options response header](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

[Clickjacking](https://en.wikipedia.org/wiki/Clickjacking)

<https://en.wikipedia.org/wiki/Clickjacking>

[OWASP Clickjacking](https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)

https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

[Frame Buster Buster](https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

<https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed>

Content Security Policy (CSP) not implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

<http://pdf.ssbmultiservices.com/>

Paths without CSP header:

- <http://pdf.ssbmultiservices.com/>
- <http://pdf.ssbmultiservices.com/index.html>
- <http://pdf.ssbmultiservices.com/dflip/images/>
- <http://pdf.ssbmultiservices.com/dflip/>
- <http://pdf.ssbmultiservices.com/dflip/images/pdfjs/>
- <http://pdf.ssbmultiservices.com/dflip/fonts/>
- <http://pdf.ssbmultiservices.com/dflip/sound/>
- <http://pdf.ssbmultiservices.com/dflip/images/textures/>
- <http://pdf.ssbmultiservices.com/dflip/css/>
- <http://pdf.ssbmultiservices.com/dflip/js/>
- <http://pdf.ssbmultiservices.com/dflip/js/libs/>
- <http://pdf.ssbmultiservices.com/mailman/archives/>

Request

GET / HTTP/1.1

Referer: <http://pdf.ssbmultiservices.com/>

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: pdf.ssbmultiservices.com
Connection: Keep-alive

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

[Implementing Content Security Policy](#)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

No HTTP Redirection

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

<http://pdf.ssbmultiservices.com/>

Request

GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: pdf.ssbmultiservices.com
Connection: Keep-alive

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

[HTTP Redirections](https://infosec.mozilla.org/guidelines/web_security#http-redirections)

https://infosec.mozilla.org/guidelines/web_security#http-redirections

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

<http://pdf.ssbmultiservices.com/>

Locations without Permissions-Policy header:

- <http://pdf.ssbmultiservices.com/>
- <http://pdf.ssbmultiservices.com/index.html>
- <http://pdf.ssbmultiservices.com/dflip/images/>
- <http://pdf.ssbmultiservices.com/dflip/>
- <http://pdf.ssbmultiservices.com/dflip/images/pdfjs/>
- <http://pdf.ssbmultiservices.com/dflip/fonts/>
- <http://pdf.ssbmultiservices.com/dflip/sound/>
- <http://pdf.ssbmultiservices.com/dflip/images/textures/>
- <http://pdf.ssbmultiservices.com/dflip/css/>
- <http://pdf.ssbmultiservices.com/dflip/js/>
- <http://pdf.ssbmultiservices.com/dflip/js/libs/>
- <http://pdf.ssbmultiservices.com/mailman/>
- <http://pdf.ssbmultiservices.com/mailman/archives/>

Request

GET / HTTP/1.1

Referer: <http://pdf.ssbmultiservices.com/>

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/114.0.0.0 Safari/537.36

Host: pdf.ssbmultiservices.com

References

[Permissions-Policy / Feature-Policy \(MDN\)](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

[Permissions Policy \(W3C\)](https://www.w3.org/TR/permissions-policy-1/)

<https://www.w3.org/TR/permissions-policy-1/>

Coverage

 http://pdf.ssbmultiservices.com

 cgi-sys

 dflip

 css

 dflip.min.css

 themify-icons.min.css

 fonts

 images

 pdfjs

 textures

 js

 libs

 jquery.min.js

 mockup.min.js

 pdf.min.js

 pdf.worker.min.js

 three.min.js

 dflip.min.js

 sound

 mailman

 archives

 index.html