



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	quizapp.ssbmultiservices.com
Scan Type	Full Scan
Start Time	Jan 14, 2024, 9:59:40 PM GMT+8
Scan Duration	8 minutes
Requests	33535
Average Response Time	33ms
Maximum Response Time	1237ms
Application Build	v23.7.230728157



High







Medium



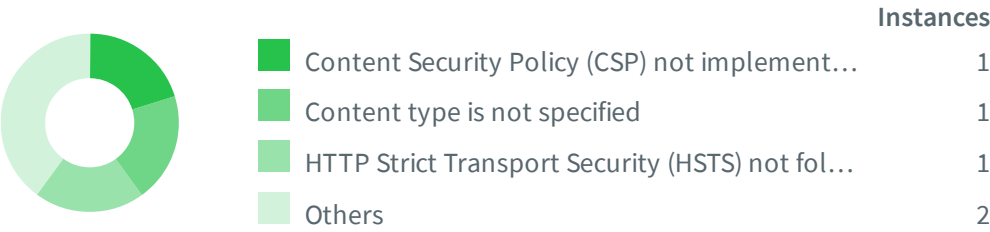
Low



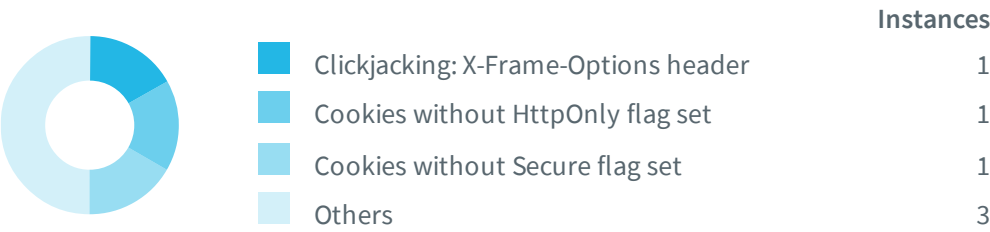
Informational

Severity	Vulnerabilities	Instances
 High	0	0
 Medium	1	1
 Low	6	6
 Informational	5	5
Total	12	12

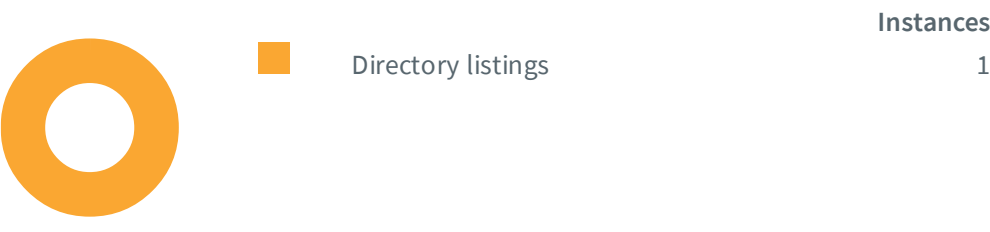
Informational















Low Severity



Medium Severity



Impacts

SEVERITY	IMPACT	
 Medium	1	Directory listings
 Low	1	Clickjacking: X-Frame-Options header
 Low	1	Cookies without HttpOnly flag set
 Low	1	Cookies without Secure flag set
 Low	1	HTTP Strict Transport Security (HSTS) not implemented
 Low	1	Possible sensitive directories
 Low	1	Possible sensitive files
 Informational	1	Content Security Policy (CSP) not implemented
 Informational	1	Content type is not specified
 Informational	1	HTTP Strict Transport Security (HSTS) not following best practices
 Informational	1	Permissions-Policy header not implemented
 Informational	1	Reverse proxy detected

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.

<https://quizapp.ssbmultiservices.com/>

Verified

Folders with directory listing enabled:

- <https://quizapp.ssbmultiservices.com/assets/>
- <https://quizapp.ssbmultiservices.com/assets/default/>
- <https://quizapp.ssbmultiservices.com/assets/default/css/>
- <https://quizapp.ssbmultiservices.com/assets/default/js/>
- <https://quizapp.ssbmultiservices.com/assets/front/>
- <https://quizapp.ssbmultiservices.com/assets/default/select2/>
- <https://quizapp.ssbmultiservices.com/assets/default/toastr/>
- <https://quizapp.ssbmultiservices.com/upload/>
- <https://quizapp.ssbmultiservices.com/upload/admin-image/>
- <https://quizapp.ssbmultiservices.com/upload/batch-image/>
- <https://quizapp.ssbmultiservices.com/upload/class-image/>
- <https://quizapp.ssbmultiservices.com/upload/question-image/>
- <https://quizapp.ssbmultiservices.com/upload/student-image/>
- <https://quizapp.ssbmultiservices.com/upload/subject-image/>
- <https://quizapp.ssbmultiservices.com/upload/teacher-image/>
- <https://quizapp.ssbmultiservices.com/upload/tropic-image/>

Request

```
GET /assets/ HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdiI6IlBZSXU4VTI3dmxYNHB3T2NMSVQ1YkE9PSIsInZhbnVlIjoiwVVVZNUQ1MlhtQUJqQ3hSem5uWmdmam5qSmd4L0
F4bllpa2hHYzR0bWFLYXhlNU0xT1dFdGNMblp0NVoxMjhqSGt5NnBDb2Qxb1VsZ2Ztd0IwRGNLYXRKZnA2SjhjMnAwVXJhYXA2Tz
l1tL2Y2MmIvVvd4dStQcGsyM0VJNkZ1SEYiLCJtYWMiOiIwY2U3M2I3ZTU0NDU4Y2M4Yjc3MTRhZTgyMzBkYmRjMjM1ZTY0NjUxNz
liZTY0YzE0Nzk2ZWRLNW3NGIzNzVLIiwidGFuIjoIIn0%3D;
mangrove_school_quiz_session=HbiKblGoLDuhHyK03wT9eUtmGfnw0I0dZt6Nn3Hg
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
```

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>

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.

<https://quizapp.ssbmultiservices.com/>

Paths without secure XFO header:

- <https://quizapp.ssbmultiservices.com/assets/default/js/app.js>
- <https://quizapp.ssbmultiservices.com/assets/default/css/>
- <https://quizapp.ssbmultiservices.com/assets/>
- <https://quizapp.ssbmultiservices.com/assets/default/js/>

- <https://quizapp.ssbmultiservices.com/assets/default/>
- <https://quizapp.ssbmultiservices.com/password>
- <https://quizapp.ssbmultiservices.com/assets/front/>
- <https://quizapp.ssbmultiservices.com/assets/default/select2/>
- <https://quizapp.ssbmultiservices.com/assets/default/toastr/>
- <https://quizapp.ssbmultiservices.com/cgi-sys/>
- <https://quizapp.ssbmultiservices.com/upload/>
- <https://quizapp.ssbmultiservices.com/mailman/>
- <https://quizapp.ssbmultiservices.com/upload/admin-image/>
- <https://quizapp.ssbmultiservices.com/upload/batch-image/>
- <https://quizapp.ssbmultiservices.com/upload/class-image/>
- <https://quizapp.ssbmultiservices.com/upload/question-image/>
- <https://quizapp.ssbmultiservices.com/upload/student-image/>
- <https://quizapp.ssbmultiservices.com/upload/subject-image/>
- <https://quizapp.ssbmultiservices.com/upload/teacher-image/>
- <https://quizapp.ssbmultiservices.com/upload/tropic-image/>
- <https://quizapp.ssbmultiservices.com/mailman/archives/>

Request

```
GET /assets/default/js/app.js HTTP/1.1
Referer: https://quizapp.ssbmultiservices.com/login
Cookie: XSRF-
TOKEN=eyJpdiI6IlBZSXU4VTI3dmxYNHB3T2NMSVQ1YkE9PSIsInZhbnHVlIjoiWVVZNUQ1MlhtQUJqQ3hSem5uWmdmam5qSmd4L0
F4bl1pa2hHYzR0bWFLYXhlNU0xT1dFdGNMblp0NVoxMjhqSGt5NnBDb2QxbVVsZ2Ztd0IwRGNLXVRKZnA2SjhjMnAwVXJhYXA2Tz
ltL2Y2MmIvVvd4dStQcGsyM0VJNkZ1SEYiLCJtYWMiOiIwY2U3M2I3ZTU0NDU4Y2M4Yjc3MTRhZTgyMzBkYmRjMjM1ZTY0NjUxNz
liZTY0YzE0Nzk2ZWRLNWw3NGIzNzVLIiwidGFuIjoiIn0%3D;
mangrove_school_quiz_session=HbiKblGoLDuhHyK03wT9eUtmGfnw0I0dZt6Nn3Hg
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)
```

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>

Cookies without HttpOnly flag set

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

Cookies can be accessed by client-side scripts.

<https://quizapp.ssbmultiservices.com/>

Verified

Cookies without HttpOnly flag set:

- <https://quizapp.ssbmultiservices.com/>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6Ild6TitEazBlSVVIRnJ2ZURMdUpIVkE9PSIsInZhbnVlIjoiriRlhnUXd0K2Z00FZHtHg2S043cmg4SjZmRzBU0TBQcG90R3FHQkNLR2VWeUt2SmhVN0FiT3NPQnpDVULNUkVycjJowWprSkpCZW5I

VnFCVXNIQjNaRHRVOXNXTUk0YWtIZFLLVEtKK1dlaHJVVDZKanpm0UZNeTRqRUdzNzd2bWUiLCJtYWMiO
iJj0GQ0Y2NjMTAzMWE5MjJkNjRmMTFi0WUxNTQzNGFmMDdkYjRmODY0NmQ0OWViZmVhNWl2YWViNWVhYj
EwYTExIiwidGFuIjoieIn0%3D; expires=Sun, 14-Jan-2024 15:59:42 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/login>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IlpTQWtwb3NoSXV5SVg4NnlzZWpTNlE9PSIsInZhbHVlIjoiektBUUQ5STNlSGFFNlVY0hCcGxhUGFGTmJzRVlqZ2x4U1lHS1MrZmlmN3RKMUJxeXkyYkN2Z2tYVXlRcjM5QUxkbW1K0UE2MldpNHQ1UkpMMmdmaEpU0ThRK2FMNE56cEF0VklxMmJxe1ZEB3RKUVJVdkU2NVB6ZmZrb1RzVGIlLCJtYWMiOiJiMGRhNjU0ZTkzMWQ0OTQ1YTkyYzg1ZGY4M2Q5MTQzMGI2ZGM3NGYyNDZmNWRiMzAwMzY0ZDY2NWY4MGZzZTE3IiwidGFuIjoieIn0%3D; expires=Sun, 14-Jan-2024 16:00:40 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/login>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IlNDVDFKR3dsa3FXR2ExL3d0WE5UR3c9PSIsInZhbHVlIjoieicjUaWltSFdiVjE4SzR4ZitKcnJXMEtnZVhTR2pxeTZrU3VXTXU5ajdVMWtkcGdlK3RFY1lXbWh1SEJ0TldRRHRzNmtUN1lGZHFiczdKejZt0VRXYW9SUjdGNjUxNlVJbVEvV2UwVS9CcjhLbytiSmllL3RXZlNteXFwVmF3YU4iLCJtYWMiOiJhN2IyZDFiMDE0YTY3NzVkMzVlOTc5NWNiMdBhZjZjNWU1ZmU1OGYzY2I3MzczNjJhYTM5MDUxOGJhMjlkZDBhIiwidGFuIjoieIn0%3D; expires=Sun, 14-Jan-2024 16:00:44 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/password/reset>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IitGRzdU0EtoamTEK2NYNUZsV3BBN2c9PSIsInZhbHVlIjoieidllHwXlPZFprR2dUM1NMZzI2N3Rmc09uUjIzZnJvV25Sak5zZkdMWERwb052MG9hUFFTNjJs0EVhOFhjaE1vNlhnWmZRTzVlUTBBRW5Ibk5odWV0dFdBd3luV2ZicnhnaUZ2Q1VsCHNLa29CMmVlV2VDRtUXeWVneHNmYmxPUC8iLCJtYWMiOiIwY2VlYWE2MzM2NzBkNGFmZGQ1MzE5YjQ2Yzc5NDNlYjZhZTA5ZTVjOGRmNjA3MTY5MzdkNGEyMDY0YWZzMTYyIiwidGFuIjoieIn0%3D; expires=Sun, 14-Jan-2024 16:01:27 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/login>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IkJjdzYrV0FXSTNvWi9xWmVrVlhnN3c9PSIsInZhbHVlIjoieil3MydnUxMUppY0g3YzY4NFU5aEVPd25SekV2Vx3cEV1Zi9oS2xLdktseWxrUkQ0YlY2ZEFGU2VmRZclZNd1FMakZ4Nl1XYlhj

TzVnS3lKcE1Ram16UitSL3ZXZHRzbTRG0XNaZjFmZDJYQ3FlNkEzL3prTTBwnFiWllQckUiLCJtYWMiO
iIwNjgwMTUwZWVjYzMwNDAzODk5ZDQxMDM3NDEwOWM3NGFjYjE4NjhkZTBmZjliYmQ4N2NhODllYTU2N2
FiZGYzIiwidGFnIjoiIn0%3D; expires=Sun, 14-Jan-2024 16:01:28 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/password/email>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IjVDMVdSS0UyRG04U294TmJuYXFjSEI9PSIsInZhbnHVLIjoicEdIVS9wMDY1UE55Y3F
KcDFUeitDUlpGWUUhURHk1L083TWJwams5c2ZXEg5dS9ySWJ3SGJFM2JhTG80TVVyK2l4T3YzdktwK0RZ
YlpEQ1RUZ0g4NTdVVFNRVWJIM2NhSkVFRE50bTVtQytjS0tIb090WHYxcDMydWtwQ28zcXYiLCJtYWMiO
iI1MDY4ZWE4ZTJiNTQxMjZhNzk1YjkwMzZDhkJjViYWE5ZjY3ZTg4OTlmYWU1MTI1MmE2MDJkMzU0YT
k4YzcyIiwidGFnIjoiIn0%3D; expires=Sun, 14-Jan-2024 16:01:31 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IlMrBFJlbnklxUVNXNXJBcGpNcnZtZlE9PSIsInZhbnHVLIjoibENPY2xZVGpKVlllMUD
KeC9iUnNwY0J2ZUVMM1NwQlpcXjQYVBFQjFSQVpxbVZBZjZTQVZFZFd3MURIEGZXbDZTlRTOXplejAr
L2tB0VNyb2RyMDY3Yk9IMTFxOTdXeEzLdEhHQ2gydlFkS2kwdWlvQ3RybUdaSmUrMzYyYjU1LCJtYWMiO
iJhMjIwODhkMjkzODc4YzdkNTY0YTI4MGMwZGY0ZjY3NDY5ODhmMjA1MzYzYjI2MmZkMzc3YTU0ZDc4Yz
cyODMxIiwidGFnIjoiIn0%3D; expires=Sun, 14-Jan-2024 16:04:14 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/login>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6InMvN2E5WTc1YThJbHdnUjVUV05YRnc9PSIsInZhbnHVLIjoicQUhnY3hGUUVxb1BITnN
tVklrNDQ3MjIjBR0JNzZXZem02NlhuN1BTbHRxbU1QKzAzVDAwUlFWcmZqdnoyUm94OHJ4cklkaVhTMXJu
UXcvdWpUVHps5NnNtMVpsUlV6T0l3TElUazh6ZGl1RkZwVWl6ejhiUHJiL05JdmZZUHUvdmYiLCJtYWMiO
iJj0GI3MGUwOWVlZGExMTFiMmYxNTY3ODM5MDY0MmRl0ThjNGE0MDE2YjUzNDU1OTUzZmFjYjk2YTRmMG
U4YTIxIiwidGFnIjoiIn0%3D; expires=Sun, 14-Jan-2024 16:04:15 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/password/reset>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6Il03V3I4VnFkL1JoT1l0MWRKSzhlV2c9PSIsInZhbnHVLIjoic0Gd1Zy81WHdKZjcyVkd
wTGIRbWtMNm9CQm10NVg3MUtsblJlY0UvTnBMWDNGUEJzblhSc0w4TVp5NmRJSdI1QjA3RFdEMDRrSDRm

cWdpMml6bFhW0St0QjByN2hLcUd6ZzA4MmFaTjRJeVo0WTNJ0FEyY0NKcmx0QkttUVhJd1IiLCJtYWMiOiI5YTg3YjU1ZTg0ODc1NzQ4NzVmMjhlMWJhMzQ5MWIxOTlhM2ZjODI1YzE1YzQ4ZGJkNjc3YzM0NDkyOWY2NWM1IiwidGFuIjoiaW0%3D; expires=Sun, 14-Jan-2024 16:05:21 GMT; Max-Age=7200; path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/login>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImxtdGZaNDNDNDQ4OVRoOHpqSEFtZWc9PSIsInZhbnVlIjoicVhkt05iQ1ZiVHhkQnZaZEwrd2MzY2JXc1RUSWtiVTc3KzRRbjBjdEJ3SDFKNUZOR3lBOW1KUld0RngwUTBjWkxISHYrMmZJVmhsR1NHeThub1l3MUYrY05FbDU0azBEaLRML1RxYWV4ejYzQVpHemNjODBVN3A4UXMzajl0RVgiLCJtYWMiOiIjZTMzN2M3NDNhNGJjYjI5NzZiN2RlYzRjYjM0ZGJmNDM2Y2FmM2Q3NmY1MzNhYjhlNjhhOWRjMWJlZDUyNGRjIiwidGFuIjoiaW0%3D; expires=Sun, 14-Jan-2024 16:05:11 GMT; Max-Age=7200; path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/password/email>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImpLM2J4ZTRpVXlwNTNkbVdXMTc3QUE9PSIsInZhbnVlIjoiaUFreVNQRkZJSk40ZUc0c2k1ZWhrNklpeXZSZ3U2MWwraWNxZVpMw9yUWdFY2FnN01tTm1CK2pUblJJZd3BybVoyRk50UXlpN1ZQcE1NMmpZQ0hV52VGWlhBNTlQ0EpVbTBMNnhpdHpERFkvenRycDE4UW15dGdVekR3NUw4b2YiLCJtYWMiOiIyODVmNmZhNWJmYTNlYjdiMjc4YWRmZGU1NGRhNzNmNmM1ZjA0ZmE3MjFiOGMyYWQyNTViODNmZTEwOWNkODVhIiwidGFuIjoiaW0%3D; expires=Sun, 14-Jan-2024 16:05:29 GMT; Max-Age=7200; path=/; samesite=lax

Request

GET / HTTP/1.1
Referer: <https://quizapp.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: quizapp.ssbmultiservices.com
Connection: Keep-alive

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Cookies without Secure flag set

One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

Impact

Cookies could be sent over unencrypted channels.

<https://quizapp.ssbmultiservices.com/>

Verified

Cookies without Secure flag set:

- <https://quizapp.ssbmultiservices.com/>

Set-Cookie: XSRF-

```
TOKEN=eyJpdiI6Ild6TitEazBlSVVIRnJ2ZURMdUpIVkE9PSIsInZhbnVlIjoiriRlhnUXd0K2Z00FZHTHg2S043cmg4SjZmRzBU0TBQcG90R3FHQkNLR2VWeUt2SmhVN0FiT3NPQnpDVULNUkVycjJWwprSkpCZW5IVnFCVXNIQjNaRHRV0XNXTUk0YWtIZFllVEtKK1dlaHJVVDZKanpm0UZNeTRqRUdzNzd2bWUiLCJtYWMiOiJjOGQ0Y2NjMTAzMWE5MjJkNjRmMTFiOWUxNTQzNGFmMDdkYjRmODY0NmQ0OWViZmVhNWl2YWViNWVhYyEwYTEuExIiwidGFuIjoiriIn0%3D; expires=Sun, 14-Jan-2024 15:59:42 GMT; Max-Age=7200; path=/; samesite=lax
```

- <https://quizapp.ssbmultiservices.com/>

Set-Cookie:

```
mangrove_school_quiz_session=2ARv9KYHjc5feQAGmxiFekqIZypZfCAgnIbYlaGu; expires=Sun, 14-Jan-2024 15:59:42 GMT; Max-Age=7200; path=/; httponly; samesite=lax
```

- <https://quizapp.ssbmultiservices.com/login>

Set-Cookie: XSRF-

```
TOKEN=eyJpdiI6IilpTQWtwb3NoSXV5SVg4NnIzZWpTNlE9PSIsInZhbnVlIjoiektBUUQ5STNlSGFFNlVY0hCcGxhUGFGTmJzRVlqZ2x4U1lHSlMrZmNmN3RKMUJxeXkyYkN2Z2tYVXlRcjM5QUxkbW1KOUe2MldpNHQ1UkpMMmdmaEpU0ThRK2FMNE56cEF0VklxMmJxe1ZEb3RKUVJVdkU2NVB6ZmZRb1RzVGIiLCJtYWMiOiJiMGRhNjU0ZTkzMWQ0OTQ1YTtk3Yzg1ZGY4M2Q5MTQzMGI2ZGM3NGYyNDZmNWRiMzAwMzY0ZDY2NWY4MG
```

IzZTE3IiwidGFnIjoiIn0%3D; expires=Sun, 14-Jan-2024 16:00:40 GMT; Max-Age=7200; path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/login>

Set-Cookie:

mangrove_school_quiz_session=2ARv9KYHjc5feQAGmxiFekqIZypZfCAgnIbYlaGu;
expires=Sun, 14-Jan-2024 16:00:40 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://quizapp.ssbmultiservices.com/login>

Set-Cookie:

mangrove_school_quiz_session=2ARv9KYHjc5feQAGmxiFekqIZypZfCAgnIbYlaGu;
expires=Sun, 14-Jan-2024 16:00:50 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://quizapp.ssbmultiservices.com/login>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IlNDVDFKR3dsa3FXR2ExL3d0WE5UR3c9PSIsInZhbnVlIjoicjUaWltSFdiVjE4SzR4ZitKcnJXMEtnZVhTR2pxeTZrU3VXTXU5ajdVMWtkcGdlK3RFY1lXbWh1SEJ0TldRRHRzNmtUN1lGZHFIczdKejZtOVRXYW9SUjdGNjUxNlVJbVEvV2UwVS9CcjhLbytiSmllL3RXZ1NteXFwVmF3YU4iLCJtYWMiOiJhN2IyZDFiMDE0YTY3NzVkMzVlOTc5NWNiMDBhZjdjNWU1ZmU1OGYzY2I3MzczNjJhYTMyMDUxOGJhMjlkZDBhIiwidGFnIjoiIn0%3D; expires=Sun, 14-Jan-2024 16:00:44 GMT; Max-Age=7200; path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/login>

Set-Cookie:

mangrove_school_quiz_session=2ARv9KYHjc5feQAGmxiFekqIZypZfCAgnIbYlaGu;
expires=Sun, 14-Jan-2024 16:00:44 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://quizapp.ssbmultiservices.com/assets/default/js/app.js>

Set-Cookie:

mangrove_school_quiz_session=HbiKblGoLDuhHyK03wT9eUtmGfnw0I0dZt6Nn3Hg;

expires=Sun, 14-Jan-2024 16:01:17 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://quizapp.ssbmultiservices.com/password/reset>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IitGRzdU0EtoamtEK2NYNUZsV3BBN2c9PSIsInZhbnHVLIjoidllHwXlPZFprR2dUM1N
MZzI2N3Rmc09uUjIzZnJvV25Sak5zZkdMWERwb052MG9hUFFTNjJsOEVhOFhjaE1vNlhnWmZRTzVlUTBB
RW5Ibk5odWV0dFdBd3luV2ZicnhnaUZ2Q1VscHNLa29CMmVIV2VDRTUxeWVneHNmYmxPUC8iLCJtYWMiO
iIwY2VlYWE2MzM2NzBkNGFmZGQ1MzE5YjQ2Yzc5NDNlYjZhZTA5ZTVjOGRmNjA3MTY5MzdkNGEyMDY0YW
IzMTYyIiwidGFuIjoiIn0%3D; expires=Sun, 14-Jan-2024 16:01:27 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/password/reset>

Set-Cookie:

mangrove_school_quiz_session=HbiKblGoLDuhHyK03wT9eUtmGfnw0I0dZt6Nn3Hg;
expires=Sun, 14-Jan-2024 16:01:27 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://quizapp.ssbmultiservices.com/login>

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IkJjdzYrV0FXSTNvWi9xWmVrVlhnN3c9PSIsInZhbnHVLIjoiL3MydnUxMUUpqY0g3YzY
4NFU5aEVPd25SekV2Vmx3cEV1Zi9oS2xLdktseWxrUkQ0YlY2ZEFGUIGI2VmRZclZNd1FMakZ4NllyYlhj
TzVnS3lKcE1Ram16UitSL3ZXZHRzbTRG0XNaZjFmZDJYQ3FlNkEzL3prTTBwnFiWllQckUiLCJtYWMiO
iIwNjgwMTUwZWVjYzMwNDAzODk5ZDQxMDM3NDEwOWM3NGFjYjE4NjhkZTBmZjliYmQ4N2NhODllyTU2N2
FiZGYyIiwidGFuIjoiIn0%3D; expires=Sun, 14-Jan-2024 16:01:28 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/login>

Set-Cookie:

mangrove_school_quiz_session=HbiKblGoLDuhHyK03wT9eUtmGfnw0I0dZt6Nn3Hg;
expires=Sun, 14-Jan-2024 16:01:28 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://quizapp.ssbmultiservices.com/password>

Set-Cookie:

mangrove_school_quiz_session=cstvJK2RSy95QZe60qAHiRFzxGt7qbdC0XjZndLn;
expires=Sun, 14-Jan-2024 16:01:37 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://quizapp.ssbmultiservices.com/password/email>

Set-Cookie:

mangrove_school_quiz_session=cstvJK2RSy95QZe60qAHiRFzxGt7qbdC0XjZndLn;
expires=Sun, 14-Jan-2024 16:01:37 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://quizapp.ssbmultiservices.com/password/email>

Set-Cookie:

mangrove_school_quiz_session=cstvJK2RSy95QZe60qAHiRFzxGt7qbdC0XjZndLn;
expires=Sun, 14-Jan-2024 16:01:38 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://quizapp.ssbmultiservices.com/password/email>

Set-Cookie: XSRF-

TOKEN=eyJpdjI6IjVDMVdSS0UyRG04U294TmJuYXFjSEE9PSIsInZhbnHVlIjoicEdIVS9wMDY1UE55Y3F
KcDFUeitDUlpGWUhURHk1L083TWJwams5c2ZXeEg5dS9ySWJ3SGJFM2JhTG80TVVyK2l4T3YzdktwK0RZ
YlpEQ1RUZ0g4NTdVVFNRVWJIM2NhSkVFRE50bTVtQytjS0tIb090WHYxcDMydWtwQ28zcXYiLCJtYWMiO
iI1MDY4ZWE4ZTJiNTQxMjZhNzk1YjkwMzMLZDhkNjViYWE5Zjk3ZTg4OTlmYWU1MTI1MmE2MDJkMzU0YT
k4YzcyIiwidGFuIjoiaW0%3D; expires=Sun, 14-Jan-2024 16:01:31 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/password/email>

Set-Cookie:

mangrove_school_quiz_session=HbiKblGoLDuhHyK03wT9eUtmGfnw0I0dZt6Nn3Hg;
expires=Sun, 14-Jan-2024 16:01:31 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://quizapp.ssbmultiservices.com/cgi-sys/>

Set-Cookie:

mangrove_school_quiz_session=qTwXzmdnJfARWkiS00RzYAPQj7csetK987xBV49;
expires=Sun, 14-Jan-2024 16:02:38 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://quizapp.ssbmultiservices.com/mailman/>

Set-Cookie:

mangrove_school_quiz_session=qTwXzmdnJfARWkiS00RzYAPQj7csetK987xBV49;
expires=Sun, 14-Jan-2024 16:02:39 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

- <https://quizapp.ssbmultiservices.com/>

Set-Cookie: XSRF-

TOKEN=eyJpdii6IlMrbFJlbklxUVNXNXJBcGpNcnZtZ1E9PSIsInZhbnVlIjoibENPY2xZVGpKVlllMud
KeC9iUnNwY0J2ZUVMM1NwQlpkcXJQYVBFQjFSQVpxbVZBZjZTQVZFZFd3MURIEGZXbDZTlRTOXplejAr
L2tBOVNyb2RyMDY3Yk9IMTFxOTdXeEZLdEhHQ2gydlFkS2kwdWlvQ3RybUdaSmUrMzkvYjUiLCJtYWMiO
iJhMjIwODhkMjkzODc4YzdkNTY0YTI4MGMwZGY0Zjk5NDY5ODhmMjA1MzYzYjI2MmZkMzc3YTVMODc4Yz
cyODMxIiwidGFniIjoibENPY2xZVGpKVlllMud; expires=Sun, 14-Jan-2024 16:04:14 GMT; Max-Age=7200;
path=/; samesite=lax

- <https://quizapp.ssbmultiservices.com/>

Set-Cookie:

mangrove_school_quiz_session=qTwXzmdnJfARWkiS00RzYAPQj7csetK987xBV49;
expires=Sun, 14-Jan-2024 16:04:14 GMT; Max-Age=7200; path=/; httponly;
samesite=lax

Request

GET / HTTP/1.1

Referer: <https://quizapp.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: quizapp.ssbmultiservices.com

Connection: Keep-alive

Recommendation

If possible, you should set the Secure flag for these cookies.

HTTP Strict Transport Security (HSTS) not implemented

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessible using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

<https://quizapp.ssbmultiservices.com/>

URLs where HSTS is not enabled:

- <https://quizapp.ssbmultiservices.com/assets/default/js/app.js>
- <https://quizapp.ssbmultiservices.com/assets/default/css/>
- <https://quizapp.ssbmultiservices.com/assets/>
- <https://quizapp.ssbmultiservices.com/assets/default/js/>
- <https://quizapp.ssbmultiservices.com/assets/default/>
- <https://quizapp.ssbmultiservices.com/password>
- <https://quizapp.ssbmultiservices.com/assets/front/>
- <https://quizapp.ssbmultiservices.com/assets/default/select2/>
- <https://quizapp.ssbmultiservices.com/assets/default/toastr/>
- <https://quizapp.ssbmultiservices.com/cgi-sys/>
- <https://quizapp.ssbmultiservices.com/mailman/>
- <https://quizapp.ssbmultiservices.com/upload/>
- <https://quizapp.ssbmultiservices.com/upload/admin-image/>
- <https://quizapp.ssbmultiservices.com/upload/batch-image/>
- <https://quizapp.ssbmultiservices.com/upload/class-image/>
- <https://quizapp.ssbmultiservices.com/upload/question-image/>
- <https://quizapp.ssbmultiservices.com/upload/student-image/>
- <https://quizapp.ssbmultiservices.com/upload/subject-image/>
- <https://quizapp.ssbmultiservices.com/upload/teacher-image/>
- <https://quizapp.ssbmultiservices.com/upload/tropic-image/>
- <https://quizapp.ssbmultiservices.com/mailman/archives/>

Request

GET /assets/default/js/app.js HTTP/1.1
Referer: https://quizapp.ssbmultiservices.com/login
Cookie: XSRF-
TOKEN=eyJpdiI6IlBZSXU4VTI3dmxYNHB3T2NMSVQ1YkE9PSIsInZhbnVlIjoiwVWZNUQ1MlhtQUJqQ3hSem5uWmdmam5qSmd4L0F4bl1pa2hHYzR0bWFLYXhlNU0xT1dFdGNMblp0NVoxMjhqSGt5NnBDb2Qxb1VsZ2Ztd0IwRGNLYXRKZnA2SjhjMnAwVXJhYXA2TzltL2Y2MmIvVd4dStQcGsyM0VJNkZ1SEYiLCJtYWMiOiIwY2U3M2I3ZTU0NDU4Y2M4Yjc3MTRhZTgyMzBkYmRjMjM1ZTY0NjUxNzliZTY0YzE0Nzk2ZWRLNW3NGIzNzVLIiwidGFuIjoiIn0%3D;
mangrove_school_quiz_session=HbiKblGoLDuhHyK03wT9eUtmGfnw0I0dZt6Nn3Hg
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: quizapp.ssbmultiservices.com
Connection: Keep-alive

Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

References

hstspreload.org

<https://hstspreload.org/>

[Strict-Transport-Security](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<https://quizapp.ssbmultiservices.com/>

Possible sensitive directories:

- <https://quizapp.ssbmultiservices.com/upload>

Request

```
GET /upload/ HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdjI6IiBZSXU4VTI3dmxYNHB3T2NMSVQ1YkE9PSIsInZhbHVlIjoiwVVZNUQ1MlhtQUJqQ3hSem5uWmdmam5qSmd4L0F4bllpa2hHYzR0bWFLYXhlNU0xT1dFdGNMblpONVoxMjhqSGt5NnBDb2QxbLVsZ2Ztd0IwRGNLXSRKZnA2SjhjMnAwVXJhYXA2TzltL2Y2MmIvVWd4dStQcGsyM0VJNkZ1SEYiLCJtYWMiOiIwY2U3M2I3ZTU0NDU4Y2M4Yjc3MTRhZTgyMzBkYmRjMjM1ZTY0NjUxNzliZTY0YzE0Nzk2ZWRLNWM3NGIzNzVlIiwidGFuIjoiiIn0%3D;
mangrove_school_quiz_session=HbiKblGoLDuhHyK03wT9eUtmGfnw0I0dZt6Nn3Hg
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: quizapp.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Restrict access to these directories or remove them from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitesecurity/webserver-security/>

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

<https://quizapp.ssbmultiservices.com/>

Possible sensitive files:

- <https://quizapp.ssbmultiservices.com/web.config>

Request

```
GET /web.config HTTP/1.1
Accept: musqjowo/xkyx
Cookie: XSRF-
TOKEN=eyJpdiI6IlBZSXU4VTI3dmxYNHB3T2NMSVQ1YkE9PSIsInZhbnVlIjoiwVZNUQ1MlhtQUJqQ3hSem5uWdmam5qSmd4L0
F4bl1pa2hHYzR0bWFLYXhlNU0xTldFdGNMblp0NVoxMjhqSGt5NnBDb2QxbVVsZ2Ztd0IwRGNLYXRKZnA2SjhjMnAwVXJhYXA2Tz
ltL2Y2MmIvVvd4dStQcGsyM0VJNkZ1SEYiLCJtYWMiOiIwY2U3M2I3ZTU0NDU4Y2M4Yjc3MTRhZTgyMzBkYmRjMjM1ZTY0NjUxNz
liZTY0YzE0Nzk2ZWRLNWM3NGIzNzVlIiwidGFuIjoiaW0%3D;
mangrove_school_quiz_session=HbiKblGoLDuhHyK03wT9eUtmGfnw0I0dZt6Nn3Hg
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: quizapp.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Restrict access to this file or remove it from the website.

References

[Web Server Security and Database Server Security](#)

<https://www.acunetix.com/websitesecurity/webserver-security/>

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.

<https://quizapp.ssbmultiservices.com/>

Paths without CSP header:

- <https://quizapp.ssbmultiservices.com/login>
- <https://quizapp.ssbmultiservices.com/assets/default/js/app.js>
- <https://quizapp.ssbmultiservices.com/password/reset>
- <https://quizapp.ssbmultiservices.com/assets/default/css/>
- <https://quizapp.ssbmultiservices.com/assets/>
- <https://quizapp.ssbmultiservices.com/assets/default/js/>
- <https://quizapp.ssbmultiservices.com/assets/default/>
- <https://quizapp.ssbmultiservices.com/password>
- <https://quizapp.ssbmultiservices.com/assets/front/>
- <https://quizapp.ssbmultiservices.com/assets/default/select2/>
- <https://quizapp.ssbmultiservices.com/assets/default/toastr/>
- <https://quizapp.ssbmultiservices.com/cgi-sys/>
- <https://quizapp.ssbmultiservices.com/mailman/>
- <https://quizapp.ssbmultiservices.com/upload/>

- <https://quizapp.ssbmultiservices.com/upload/admin-image/>
- <https://quizapp.ssbmultiservices.com/upload/batch-image/>
- <https://quizapp.ssbmultiservices.com/upload/class-image/>
- <https://quizapp.ssbmultiservices.com/upload/question-image/>
- <https://quizapp.ssbmultiservices.com/upload/student-image/>
- <https://quizapp.ssbmultiservices.com/upload/subject-image/>
- <https://quizapp.ssbmultiservices.com/upload/teacher-image/>

Request

```
GET /login HTTP/1.1
Referer: https://quizapp.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdii6Ild6TitEazBlSVVIRnJ2ZURMdUpIVkE9PSIsInZhbnVlIjoiRlhUd0K2Z0FZHThg2S043cmg4SjZmRzBUOTBQcG90R3FHQkNLR2VWeUt2SmhVN0FiT3NPQnpDVULNUkVycjJoWwprSkpCZW5IVnFCVXNIQjNaRHRVOXNXtUK0YWtIZFlLVEtKK1dlaHJVVDZKanpmOUZNeTRqRUdzNzd2bWUiLCJtYWMiOiJjOGQ0Y2NmMTAzMWE5MjJkNjRmMTFiOWUxNTQzNGFmMDdkYjRmODY0NmQ0OWViZmVhNWII2YWViNWVhYjEwYTExIiwidGFni0iIn0%3D;
mangrove_school_quiz_session=2ARv9KYHjc5feQAGmxIFekqIZypZfCAgnIbYLaGu
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: quizapp.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/>

Content type is not specified

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

Impact

None

<https://quizapp.ssbmultiservices.com/>

Verified

Pages where the content-type header is not specified:

- <https://quizapp.ssbmultiservices.com/web.config>

Request

```
GET /web.config HTTP/1.1
Referer: https://quizapp.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdiI6IkhUeFFRSTNCV2ZwcU0xUU1kOVZlaEE9PSIsInZhbHVlIjojWS9iQVRVTnJyQVF2dDR1YlhqSTdPL1k2WVFrT2
F4WndtVnBXU0hsbmNuWUU0VTBoL1JYLF1cWFERU9P0FBtQ1ZjaWJrekhDS1hjYkxacFl2Q0xuYXkrSUVESetZRjRiYkxIWW1IVT
A1azNiTjllLemxHUFVXTkxPNmh3Mnc4enYiLCJtYWMiOiI2YTdmNzlkOTlkNWRhM2U0N2Q30TRmZTI20TUyYjRmNWl5NzA5MzdiY2
Zm0GRhOTllNDlm0DNmMDc5ZDcxYWY5IiwidGFnIjojIn0%3D;
mangrove_school_quiz_session=qTwXzmdnJfARWkiS00RzYAPQj7csetK987xBV49
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: quizapp.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Set a Content-Type header value for these page(s).

HTTP Strict Transport Security (HSTS) not following best practices

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict Transport Security (HSTS) implementation is not as strict as is typically advisable.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

<https://quizapp.ssbmultiservices.com/>

URLs where HSTS configuration is not according to best practices:

- <https://quizapp.ssbmultiservices.com/login> - max-age is less than 1 year (31536000);
- <https://quizapp.ssbmultiservices.com/password/reset> - max-age is less than 1 year (31536000);

Request

```
GET /login HTTP/1.1
Referer: https://quizapp.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdiI6Ild6TitEazBLSVVIRnJ2ZURMdUpIVkE9PSIsInZhbnVlIjoiriRlhnUXd0K2Z0FZHTHg2S043cmg4SjZmRzBUOT
BQcG90R3FHQkNLR2VWeUt2SmhVN0FiT3NPQnpDVULNUkVycjJOWWprSkpCZW5IVnFCVXNIQjNaRHRV0XNXTUk0YWtIZFllVEtKK1
dlaHJVVDZKanpmOUZNeTRqRUdzNzd2bWUiLCJtYWMiOiJjOGQ0Y2NjMTAzMWE5MjJkNjRmMTFiOWUxNTQzNGFmMDdkYjRmODY0Nm
Q00WViZmVhNWII2YWViNWVhYjEwYTEwIiwidGFuIjoiiIn0%3D;
mangrove_school_quiz_session=2ARv9KYHjc5feQAGmxiFekqIZypZfCAgnIbYlaGu
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: quizapp.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

It is recommended to implement best practices of HTTP Strict Transport Security (HSTS) in your web application. Consult web references for more information.

References

hstspreload.org

<https://hstspreload.org/>

[MDN: Strict-Transport-Security](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>

Permissions-Policy header not implemented

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

Impact

<https://quizapp.ssbmultiservices.com/>

Locations without Permissions-Policy header:

- <https://quizapp.ssbmultiservices.com/login>
- <https://quizapp.ssbmultiservices.com/assets/default/js/app.js>
- <https://quizapp.ssbmultiservices.com/password/reset>
- <https://quizapp.ssbmultiservices.com/assets/default/css/>
- <https://quizapp.ssbmultiservices.com/assets/>
- <https://quizapp.ssbmultiservices.com/assets/default/js/>
- <https://quizapp.ssbmultiservices.com/assets/default/>
- <https://quizapp.ssbmultiservices.com/password>
- <https://quizapp.ssbmultiservices.com/password/email>
- <https://quizapp.ssbmultiservices.com/assets/front/>
- <https://quizapp.ssbmultiservices.com/assets/default/select2/>
- <https://quizapp.ssbmultiservices.com/assets/default/toastr/>
- <https://quizapp.ssbmultiservices.com/cgi-sys/>
- <https://quizapp.ssbmultiservices.com/mailman/>
- <https://quizapp.ssbmultiservices.com/upload/>
- <https://quizapp.ssbmultiservices.com/upload/admin-image/>
- <https://quizapp.ssbmultiservices.com/upload/batch-image/>
- <https://quizapp.ssbmultiservices.com/upload/class-image/>
- <https://quizapp.ssbmultiservices.com/upload/question-image/>
- <https://quizapp.ssbmultiservices.com/upload/student-image/>
- <https://quizapp.ssbmultiservices.com/upload/subject-image/>

Request

```
GET /login HTTP/1.1
Referer: https://quizapp.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdii6Ild6TitEazBlSVVIRnJ2ZURMdUpIVkE9PSIsInZhbHVlIjoiRlhnUXd0K2Z0FZHThg2S043cmg4SjZmRzBUOTBQcG90R3FHQkNLR2VWeUt2SmhVN0FiT3NPQnpDVULNUkVycjJ0WwprSkpCZW5lVnFCVXNIQjNaRHRV0XNXtUk0YWtIZFllVEtKK1dlaHJVVDZKanpmOUZNeTRqRUdzNzd2bWUiLCJtYWMiOiJjOGQ0Y2NmTAzMWE5MjJkNjRmMTFiOWUxNTQzNGFmMDdkYjRmODY0NmQ0OWViZmVhNWII2YWViNWVhYjEwYXNlIiwiaWF0IjoiIn0%3D;
mangrove_school_quiz_session=2ARv9KYHjc5feQAGmxiFekqIZypZfCAgnIbYlaGu
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: quizapp.ssbmultiservices.com
Connection: Keep-alive

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/>

Reverse proxy detected

This server uses a reverse proxy, a load balancer or a CDN (Content Delivery Network) or it's hosted in a cloud provider. Acunetix detected this by sending various payloads and detecting changes in headers and body.

Impact

No impact is associated with this vulnerability.

<https://quizapp.ssbmultiservices.com/>

Detected reverse proxy: Apache httpd

Request

GET / HTTP/1.1
Max-Forwards: 0
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: quizapp.ssbmultiservices.com
Connection: Keep-alive

Recommendation

None

Coverage

https://quizapp.ssbmultiservices.com

Inputs

GET iv, value, mac, tag

assets

Inputs

GET iv, value, mac, tag

default

Inputs

GET iv, value, mac, tag

css

app.css

custom.css

js

app.js

select2

select2.min.css

toastr

Inputs

GET iv, value, mac, tag

front

Inputs

GET iv, value, mac, tag

cgi-sys

Inputs

GET iv, value, mac, tag

mailman

Inputs

GET iv, value, mac, tag

archives

Inputs

GET iv, value, mac, tag

password

Inputs

GET iv, value, mac, tag

email

Inputs

GET iv, value, mac, tag

POST iv, value, mac, tag

POST _token, email

POST _token, email

reset

Inputs

GET iv, value, mac, tag

upload

Inputs

GET iv, value, mac, tag

admin-image

Inputs

GET iv, value, mac, tag

batch-image

Inputs

GET iv, value, mac, tag

class-image

Inputs

GET iv, value, mac, tag

question-image

Inputs

GET iv, value, mac, tag

student-image

Inputs

GET iv, value, mac, tag

subject-image

Inputs

GET iv, value, mac, tag

 teacher-image

 Inputs

GET iv, value, mac, tag

 tropic-image

 Inputs

GET iv, value, mac, tag

 login


 Inputs

POST iv, value, mac, tag

POST _token, email, password

POST _token, email, password, remember

GET iv, value, mac, tag

 password

 Inputs

GET iv, value, mac, tag

 web.config

 Inputs

GET iv, value, mac, tag