Acunetix by Invicti

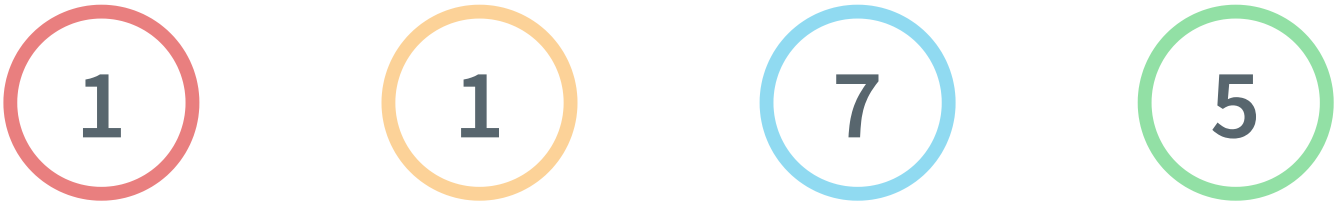
Comprehensive Report

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Scan Detail

Target	https://quizapp.ssbmultiservices.com/
Scan Type	Full Scan
Start Time	Feb 28, 2024, 9:10:28 PM GMT+8
Scan Duration	6 minutes
Requests	33555
Average Response Time	33ms
Maximum Response Time	9222ms
Application Build	v23.7.230728157



Severity	Vulnerabilities	Instances
High	1	1
Medium	1	1
Low	7	7
Informational	5	5
Total	14	14

Informational

	Instances
Content Security Policy (CSP) not implement…	1
Content type is not specified	1
HTTP Strict Transport Security (HSTS) not fol…	1
Others	2

Low Severity

	Instances
Clickjacking: X-Frame-Options header	1
Cookies without HttpOnly flag set	1
Cookies without Secure flag set	1
Others	4

Medium Severity

	Instances
Directory listings	1

High Severity

	Instances
Possible database backup	1

Impacts

SEVERITY	IMPACT	
High	1	Possible database backup
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
Low	1	TLS/SSL certificate about to expire
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

Possible database backup

Manual confirmation is required for this alert.

One or more possible database backups were identified. A database backup contains a record of the table structure and/or the data from a database and is usually in the form of a list of SQL statements. A database backup is most often used for backing up a database so that its contents can be restored in the event of data loss. This information is highly sensitive and should never be found on a production system.

Impact

These file(s) may disclose sensitive information. This information can be used to launch further attacks.

https://quizapp.ssbmultiservices.com/

Pages with possible database backups:

-

Request

```
GET /quizapp.zip HTTP/1.1
Range: bytes=0-99999
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

Sensitive files such as database backups should never be stored in a directory that is accessible to the web server. As a workaround, you could restrict access to these file(s).

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=eyJpdiI6IklCd3lPeFl2VVNqTWZrSGdIZmJLMkE9PSIsInZhbHVlIjoiUzkxbXFmWXIrWlU5b0UwNCt2R3JMMFEzWFdJdU
NXU3RxR1VrdHBFWEdQRGRtcHlCMGt4MHl2enNWTVNnbWdmNW1KRXNmbCtMczJMNnZTTTFTMUNwbUlqS01meHd1dFBTVitBc1J6bk
Y4QnB1emNhMDN5UktvWG9mQ0JDT1hwaTUiLCJtYWMiOiJiYmU5MTgyZTA5NmI0YmE4ZjZhZWRiMmUzNzk1ODBmNmY2ODI0YjdiNj
EyOTc3ZDNlZGE3ZjBlZDE1MDM4YjE1IiwidGFnIjoiIn0%3D;
mangrove_school_quiz_session=EofYUoj8mm2fqmRcISxilC4zgIoH3kVmjrInw0eG
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

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

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/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/question-image/
- https://quizapp.ssbmultiservices.com/upload/class-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=eyJpdiI6ImJIZE1CcXRYb0RtWGY2MXlYQ1lqeUE9PSIsInZhbHVlIjoiZ0psNUMxUmZKa25jZnVZK2FpYnEyVDRuSW43a1
ZWZVJaVzlHSHNZUGhMdjRSK0FkMmM0SzM2Yzl6Q1A2R09zT2dCTjMwSngxSnJFb2JEUlNlbWx0SDBDS1hNNDlWMDkvQzZHemRxR1
ZDd1FBRDQyVUJ5cHFUTGtFQ3Q4L0R5UHciLCJtYWMiOiJkZTBjMzk2YmZkNjA5MjIxNDVmMDYzMTBmM2U2ZDE1ZTY4OTAyMTIwNG
U1MWZjZWVkZTQyNTZhMGQzNTk5ZWE1IiwidGFnIjoiIn0%3D;
mangrove_school_quiz_session=D0TOF8uzq1ehDW5rrHwuUDgA6ERhTzWCczhylwTX
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

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

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

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

Frame Buster Buster
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=eyJpdiI6Im5jVlZnakorL2Z2akd0UTNIR0RXM2c9PSIsInZhbHVlIjoiVTl4bk9XeUdhYXIxenA
vdTFOMUpTd2VGbDgvVUZGaHd5ZGMwZkV1N3lING1RY0YvWE10YmU3NjlxK0Rnd0UrYmYrdnFUQ2k4R2JS
UjE2VVJDVWtoSk4vQytxV0VOREtCcW5VUmRhQkI5bnMyd05DMGJCcDR2SlBjVXFjdzFkeSsiLCJtYWMiO
iI1MGFhODgwZmMzY2Q4OWIwMGEwMjk3YjBlZDY3MTZkMWJiMDQzZDlmMGQ1ZGMwYzc4MGM3MDBiMGI2Mm
VjYjhmIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:10:31 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ilg0bnVUajd1d3VORmhCcDR0Q0M0cnc9PSIsInZhbHVlIjoiYWFNSUQzczBoOWJnYVB
```

```
EYlFtdlMrd0tJV1NjREtBT0N3ZlRST3pIRlllUWQ1cFdBbjhEL3NrbTZmQU1sdUdadStkR3VkTVpoMGRz
QlU5MFhsWjRLM0swcnhBYW01SmFiYXVBa3dnMUMvRDdKdDNzSGdrdGtGamt6MW9ubjFNbGwiLCJtYWMiO
iIzYTZkMTRjMDQ1MDcyZTEzNjczMzAyZjk4NWIwNjY1NzJkNDFhYzM2MTg1NTVlZDFmMjQyMjMxNGU1OG
I4NmI3IiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:19 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik5rQTV3Yi8xS3JCWFpiTGRET3gvT3c9PSIsInZhbHVlIjoiSDU4MmpXRlhoQ3AreHJ
HU0NiMzRIc1NSOFM2bzl5OFJ2TytueEZDajVFNmdQVEkyZXVMUG4vOElxTHZPYWFXRE45NUhNaG9xZTZE
c2NIazVYbDlCRTRYc0R5cEo3NTN1ckx6UmVNSkg3Z1d3VkxnRHMveHljVlU3bVVGazRzUkYiLCJtYWMiO
iI2ODU4MTJmNzk4ZGEzZTc5ZmVlYWEwZjE2ZmZjNWI5MDMyYTE3YjIzYjY3Yzg0ODQzOGZjMWYwOTk4NW
Y3ZTYwIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:26 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IktHUmgySzcvUTNxOHhLRkZCMFNHdUE9PSIsInZhbHVlIjoiZU1tcGVwdjBIM1BSRTk
4cGoyWmlmTFY1K1U0dTdFQnMrOGlnZ2RCajZvUVVLRS8vMHZhRXB1b2U2MHIwSGd3SXdLSmduTkZsNzVv
eUJ6WHhMb0lvUm5XNk1pbjdsNzNNZE0xQndtNnpBSjZOUkY4UDlXL0kwTTRCNjZFODFyc3IiLCJtYWMiO
iI3NjA4NzY0NDNjM2NmM2E2MWQ0ODEyMmU2N2NlZDk2ZjhlZjg2MTFhOGUyM2M5ZTcwZDMwNTA3YmM3MG
QxMjUzIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:23 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImZyL2pkazJObGFVZ2I2TmVaVTh2VlE9PSIsInZhbHVlIjoidDNTYlVOVG9Uc2NESzF
0K05JUkhhYmJYei85ZnJidWhLZFlCclo2Mk9wa20rY3kzS3J5S0w0c2Fac3htU0dlZDVETGR1aFcxdHY5
clp0TXl1eXdaZkNKT0ZPeWo4WVlhWFhuRHVHZFF4bjA0Mk9wTGN6ZEo3TzZMa2FtS0VhRzkiLCJtYWMiO
iIzOTI5Njc2MmQ3NTI0OWNlYjUxMGQ2NDE5MDAzOGQyMDhhYzZlOGRkNjgyYjM1YmFkOTAzYzUxNzQ0Yz
FkMjE4IiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:51 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InBubDRzdmJCQll6ekxXV1hTUjZrTGc9PSIsInZhbHVlIjoib3RrTEdrejlyVit4a1l
```

```
IY20xMFNBV2d6QXdnb0orcWZUMDRZYitrS3ZuU0U3L0hZVkx4dlp2b2c1cjltTnVZQUU1dDFod0UrOWxq
clAyTnNMNnBPcnlRRnE5L2RvYWZxcDJDd295ampQNEVpWll6cEFGQkpBWW5KQjhnbnJUeDQiLCJtYWMiO
iJjZDUzZWRlMzUwMzVmYTYyOGM5ZTU5YzJiOTAzYjNkMTY4OWI3YjdjZWQyZTNmZWFjYWJlMzdjZTY4M2
IxNTY4IiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:52 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkxadExXbFBSZU83ZnYxZmlySVRpb3c9PSIsInZhbHVlIjoiR2VOMjlWWDhCbjNNams
ydE1sZUE0YVhxbGhQMUNyY0xKMkswbmpIMlZOS1YyQW9SeURVOWpUUjBwcm83R2lvdnRpWlNlVUpCeXJi
NTAxTmpHdlQ5VDZYN2d1eWsyZ1JVMXl5SjdjS3g5R2hQNGtPa1RaejdsU0xMcXcwaUk5NWIiLCJtYWMiO
iJiMzkyYjBkMDRhZjY3OGFkN2YxZDU5MDhiYzcyNzgwOGVkNjU4OGQzMDI0YWYwNjFjMDZmNDgwZTk1YW
ZmNmQ2IiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:59 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IitCNlVGYVVObUxsU0tvaXd5NHRjSHc9PSIsInZhbHVlIjoidnE1enJYYjZqYkJ1SU1
vemZDTTZTOFZZMGFlOFpuZml6Z1B1NHlOam9Kcng0V3J1RytPN0pKK0hDb255a1VqRklib252NVRva3lu
MncwM1EvcWdPV0dKUFQzWnM0L1RldE8zMGtQN2NReXRKR1RVemJZbmF3YndKeUFsTGVkVm4iLCJtYWMiO
iJjZTAxMTBhYzE4Njc3MGUxOTIzYjJlNzRmMWZhMzUwNWYzMWI0MWZhZjg3ZjhmNTczMzM3ZTc2YmJjYj
lmMjNjIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:54 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://quizapp.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Iko3dldnSkxBaE5GTW9HQzJndGtrQ1E9PSIsInZhbHVlIjoiVVJYRWthSWRkUDVEL0V
ZRDNEZlBlRW9kakFvckNsOHNJNG5iMUxmVkdMUVFwNTRIdGxJZlBMNFlLbGZvZ3VOT1RDemZIcWlFM2Mw
a2IrNEd1WHByM1Bkd2M0NE5DTjU1MDQvZDFKMEtsaTcrQ0U1NXBhSmhjUVp6YTFvRHdMRzkiLCJtYWMiO
iIzMDBhNDRjYzQwMTM1ZTg2OGE2MTFiYmE4NDhkOWE3ZWUyNjc0OTk5YjAyNzAwMzA3ZmM0NjBlOGQ5OD
dkNTlhIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:13:10 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik9JaGdiMzlCam5zZWRsRWF0cndLMVE9PSIsInZhbHVlIjoiVUs2MUZYbWcxY2g1K0J
```

```
VQTdNd2swQ1FyR0REV0gyWSs2Y2Z4eUduSUlENmp4YWFuampTMlc3L241WWpMUUZqNk8rQ2h6ZWZWYlJq
c25kMStrSDlDTDI2NFRUSmxCOWJJb3NYUHZvaDBFd0h0UnkraU1vQkU4TmNuNkx6ZkdXbTkiLCJtYWMiO
iI0OGUxMjFhNjZjMTljZTY4OWE0ODg2NjA5ZmE2MzY2MzRhM2Y5NTY4YTE5ZmViZTYyZTQ5ZGQ5MmM0NT
NiZDUwIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:13:11 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InlEQ2VscWx0eER0aFE5ZWVUZmRCeGc9PSIsInZhbHVlIjoiNkRQcmNCY2dzMUY3SjU
1S0ZRVmcxak43TnpmdkpFWnEyRWw1bEtlR2dvMmc1S0o2bjZZa0kwL0xTZU1hY2JnZThSOHNsZ3F3Q1Ja
cW44S3V2T2FrM2UvblliaHZOQ0JERGhKWUprMThKbGQ1Mko4T3hSMWhXdWJsNWJrdnIzdWsiLCJtYWMiO
iI5ODI0YmExYjIxODM4MjA1OTM2ZWY0ZWRmYzcyOWEwYmUyOWUyNzAxZTUyYjE4MjI2YjQzYjFmYzlhN2
VlNDcxIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:14:42 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ii9IUi9BU1pXcFAwSEZlamdGQ3dzZWc9PSIsInZhbHVlIjoia2QvR0t5QkVzUkMwb1J
mbE4wRUM1NTVIby8xSVNmbnE3R3h5K01UQU1ZeHlsbUhiTWdpSEs2bkJBbVdBWldsVkU5M1YrWlhYbmhP
WmgvWUF2UVpUa2N2bmo2R2NnN3FPTnl0NWdKdnowc1UrNk5BRzM3T25UQUp5RUNPWTBCRU8iLCJtYWMiO
iI0NWU1OWM3NjdhYWVkZjQ1YWUxYjcwODNhOWFiNTI5OWQ4ZGVjM2JiY2VhZWNkZmZkYTQ0YTZkMDMyNG
UyZWZhIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:14:37 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik9DZmo2aHVkOGltVWFMOVdTN25DU0E9PSIsInZhbHVlIjoiREZmelJPUEg4cDE2YkN
ia0JIVnBST0xoWkdpWkFORDJLaysxZTh3a2lFYXBnU0FQSC9BcnZwQmtveGwwTUhhZUpOdnVhUlpYSGFG
MlZwVmdmSFZ6QUV3a1ZtcUpna09wZzRlbXhMMm1GOHpnL3E0Wmo2VWkyYllrYnlFL0I4RkMiLCJtYWMiO
iIxMDUzZmQ0NjhjMWRmNTQxYTdjMzc5NDVmMGE0NTZjYWFlNzgyNDRhZGRlNTZjMDEzOGMwY2JlOTY0Yj
AyZjRlIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:14:50 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=eyJpdiI6Im5jVlZnakorL2Z2akd0UTNIR0RXM2c9PSIsInZhbHVlIjoiVTl4bk9XeUdhYXIxenA
vdTFOMUpTd2VGbDgvVUZGaHd5ZGMwZkV1N3lING1RY0YvWE10YmU3NjlxK0Rnd0UrYmYrdnFUQ2k4R2JS
UjE2VVJDVWtoSk4vQytxV0VOREtCcW5VUmRhQkI5bnMyd05DMGJCcDR2SlBjVXFjdzFkeSsiLCJtYWMiO
iI1MGFhODgwZmMzY2Q4OWIwMGEwMjk3YjBlZDY3MTZkMWJiMDQzZDlmMGQ1ZGMwYzc4MGM3MDBiMGI2Mm
VjYjhmIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:10:31 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://quizapp.ssbmultiservices.com/

```
Set-Cookie:
mangrove_school_quiz_session=EofYUoj8mm2fqmRcISxilC4zgIoH3kVmjrInw0eG;
expires=Wed, 28-Feb-2024 15:10:31 GMT; Max-Age=7200; path=/; httponly;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ilg0bnVUajd1d3VORmhCcDR0Q0M0cnc9PSIsInZhbHVlIjoiYWFNSUQzczBoOWJnYVB
EYlFtdlMrd0tJV1NjREtBT0N3ZlRST3pIRlllUWQ1cFdBbjhEL3NrbTZmQU1sdUdadStkR3VkTVpoMGRz
QlU5MFhsWjRLM0swcnhBYW01SmFiYXVBa3dnMUMvRDdKdDNzSGdrdGtGamt6MW9ubjFNbGwiLCJtYWMiO
iIzYTZkMTRjMDQ1MDcyZTEzNjczMzAyZjk4NWIwNjY1NzJkNDFhYzM2MTg1NTVlZDFmMjQyMjMxNGU1OG
I4NmI3IiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:19 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
mangrove_school_quiz_session=EofYUoj8mm2fqmRcISxilC4zgIoH3kVmjrInw0eG;
expires=Wed, 28-Feb-2024 15:11:19 GMT; Max-Age=7200; path=/; httponly;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik5rQTV3Yi8xS3JCWFpiTGRET3gvT3c9PSIsInZhbHVlIjoiSDU4MmpXRlhoQ3AreHJ
HU0NiMzRIc1NSOFM2bzl5OFJ2TytueEZDajVFNmdQVEkyZXVMUG4vOElxTHZPYWFXRE45NUhNaG9xZTZE
c2NIazVYbDlCRTRYc0R5cEo3NTN1ckx6UmVNSkg3Z1d3VkxnRHMveHljVlU3bVVGazRzUkYiLCJtYWMiO
iI2ODU4MTJmNzk4ZGEzZTc5ZmVlYWEwZjE2ZmZjNWI5MDMyYTE3YjIzYjY3Yzg0ODQzOGZjMWYwOTk4NW
Y3ZTYwIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:26 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
mangrove_school_quiz_session=EofYUoj8mm2fqmRcISxilC4zgIoH3kVmjrInw0eG;
expires=Wed, 28-Feb-2024 15:11:26 GMT; Max-Age=7200; path=/; httponly;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IktHUmgySzcvUTNxOHhLRkZCMFNHdUE9PSIsInZhbHVlIjoiZU1tcGVwdjBIM1BSRTk
```

```
4cGoyWmlmTFY1K1U0dTdFQnMrOGlnZ2RCajZvUVVLRS8vMHZhRXB1b2U2MHIwSGd3SXdLSmduTkZsNzVv
eUJ6WHhMb0lvUm5XNk1pbjdsNzNNZE0xQndtNnpBSjZOUkY4UDlXL0kwTTRCNjZFODFyc3IiLCJtYWMiO
iI3NjA4NzY0NDNjM2NmM2E2MWQ0ODEyMmU2N2NlZDk2ZjhlZjg2MTFhOGUyM2M5ZTcwZDMwNTA3YmM3MG
QxMjUzIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:23 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
mangrove_school_quiz_session=EofYUoj8mm2fqmRcISxilC4zgIoH3kVmjrInw0eG;
expires=Wed, 28-Feb-2024 15:11:23 GMT; Max-Age=7200; path=/; httponly;
samesite=lax
```

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

```
Set-Cookie:
mangrove_school_quiz_session=D0TOF8uzq1ehDW5rrHwuUDgA6ERhTzWCczhylwTX;
expires=Wed, 28-Feb-2024 15:11:50 GMT; Max-Age=7200; path=/; httponly;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImZyL2pkazJObGFVZ2I2TmVaVTh2VlE9PSIsInZhbHVlIjoidDNTYlVOVG9Uc2NESzF
0K05JUkhhYmJYei85ZnJidWhLZFlCclo2Mk9wa20rY3kzS3J5S0w0c2Fac3htU0dlZDVETGR1aFcxdHY5
clp0TXl1eXdaZkNKT0ZPeWo4WVlhWFhuRHVHZFF4bjA0Mk9wTGN6ZEo3TzZMa2FtS0VhRzkiLCJtYWMiO
iIzOTI5Njc2MmQ3NTI0OWNlYjUxMGQ2NDE5MDAzOGQyMDhhYzZlOGRkNjgyYjM1YmFkOTAzYzUxNzQ0Yz
FkMjE4IiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:51 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
mangrove_school_quiz_session=D0TOF8uzq1ehDW5rrHwuUDgA6ERhTzWCczhylwTX;
expires=Wed, 28-Feb-2024 15:11:51 GMT; Max-Age=7200; path=/; httponly;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InBubDRzdmJCQll6ekxXV1hTUjZrTGc9PSIsInZhbHVlIjoib3RrTEdrejlyVit4a1l
IY20xMFNBV2d6QXdnb0orcWZUMDRZYitrS3ZuU0U3L0hZVkx4dlp2b2c1cjltTnVZQUU1dDFod0UrOWxq
clAyTnNMNnBPcnlRRnE5L2RvYWZxcDJDd295ampQNEVpWll6cEFGQkpBWW5KQjhnbnJUeDQiLCJtYWMiO
iJjZDUzZWRlMzUwMzVmYTYyOGM5ZTU5YzJiOTAzYjNkMTY4OWI3YjdjZWQyZTNmZWFjYWJlMzdjZTY4M2
IxNTY4IiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:52 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
mangrove_school_quiz_session=D0TOF8uzq1ehDW5rrHwuUDgA6ERhTzWCczhylwTX;
expires=Wed, 28-Feb-2024 15:11:52 GMT; Max-Age=7200; path=/; httponly;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkxadExXbFBSZU83ZnYxZmlySVRpb3c9PSIsInZhbHVlIjoiR2VOMjlWWDhCbjNNams
ydE1sZUE0YVhxbGhQMUNyY0xKMkswbmpIMlZOS1YyQW9SeURVOWpUUjBwcm83R2lvdnRpWlNlVUpCeXJi
NTAxTmpHdlQ5VDZYN2d1eWsyZ1JVMXl5SjdjS3g5R2hQNGtPa1RaejdsU0xMcXcwaUk5NWIiLCJtYWMiO
iJiMzkyYjBkMDRhZjY3OGFkN2YxZDU5MDhiYzcyNzgwOGVkNjU4OGQzMDI0YWYwNjFjMDZmNDgwZTk1YW
ZmNmQ2IiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:59 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
mangrove_school_quiz_session=D0TOF8uzq1ehDW5rrHwuUDgA6ERhTzWCczhylwTX;
expires=Wed, 28-Feb-2024 15:11:59 GMT; Max-Age=7200; path=/; httponly;
samesite=lax
```

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

```
Set-Cookie:
mangrove_school_quiz_session=D0TOF8uzq1ehDW5rrHwuUDgA6ERhTzWCczhylwTX;
expires=Wed, 28-Feb-2024 15:11:59 GMT; Max-Age=7200; path=/; httponly;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IitCNlVGYVVObUxsU0tvaXd5NHRjSHc9PSIsInZhbHVlIjoidnE1enJYYjZqYkJ1SU1
vemZDTTZTOFZZMGFlOFpuZml6Z1B1NHlOam9Kcng0V3J1RytPN0pKK0hDb255a1VqRklib252NVRva3lu
MncwM1EvcWdPV0dKUFQzWnM0L1RldE8zMGtQN2NReXRKR1RVemJZbmF3YndKeUFsTGVkVm4iLCJtYWMiO
iJjZTAxMTBhYzE4Njc3MGUxOTIzYjJlNzRmMWZhMzUwNWYzMWI0MWZhZjg3ZjhmNTczMzM3ZTc2YmJjYj
lmMjNjIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:11:54 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
mangrove_school_quiz_session=D0TOF8uzq1ehDW5rrHwuUDgA6ERhTzWCczhylwTX;
expires=Wed, 28-Feb-2024 15:11:54 GMT; Max-Age=7200; path=/; httponly;
samesite=lax
```

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

```
Set-Cookie:
mangrove_school_quiz_session=v9GejO3Gi0aurZz4ytaa8R00A91lx2BogXtAxO6v;
expires=Wed, 28-Feb-2024 15:12:30 GMT; Max-Age=7200; path=/; httponly;
samesite=lax
```

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

```
Set-Cookie:
mangrove_school_quiz_session=v9GejO3Gi0aurZz4ytaa8R00A91lx2BogXtAxO6v;
expires=Wed, 28-Feb-2024 15:12:30 GMT; Max-Age=7200; path=/; httponly;
samesite=lax
```

- https://quizapp.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Iko3dldnSkxBaE5GTW9HQzJndGtrQ1E9PSIsInZhbHVlIjoiVVJYRWthSWRkUDVEL0V
ZRDNEZlBlRW9kakFvckNsOHNJNG5iMUxmVkdMUVFwNTRIdGxJZlBMNFlLbGZvZ3VOT1RDemZIcWlFM2Mw
a2IrNEd1WHByM1Bkd2M0NE5DTjU1MDQvZDFKMEtsaTcrQ0U1NXBhSmhjUVp6YTFvRHdMRzkiLCJtYWMiO
iIzMDBhNDRjYzQwMTM1ZTg2OGE2MTFiYmE4NDhkOWE3ZWUyNjc0OTk5YjAyNzAwMzA3ZmM0NjBlOGQ5OD
```

```
dkNTlhIiwidGFnIjoiIn0%3D; expires=Wed, 28-Feb-2024 15:13:10 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 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 accessable 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/question-image/
- https://quizapp.ssbmultiservices.com/upload/class-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=eyJpdiI6ImJIZE1CcXRYb0RtWGY2MXlYQ1lqeUE9PSIsInZhbHVlIjoiZ0psNUMxUmZKa25jZnVZK2FpYnEyVDRuSW43a1
ZWZVJaVzlHSHNZUGhMdjRSK0FkMmM0SzM2Yzl6Q1A2R09zT2dCTjMwSngxSnJFb2JEUlNlbWx0SDBDS1hNNDlWMDkvQzZHemRxR1
ZDd1FBRDQyVUJ5cHFUTGtFQ3Q4L0R5UHciLCJtYWMiOiJkZTBjMzk2YmZkNjA5MjIxNDVmMDYzMTBmM2U2ZDE1ZTY4OTAyMTIwNG
U1MWZjZWVkZTQyNTZhMGQzNTk5ZWE1IiwidGFnIjoiIn0%3D;
mangrove_school_quiz_session=D0TOF8uzq1ehDW5rrHwuUDgA6ERhTzWCczhylwTX
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

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=eyJpdiI6ImJIZE1CcXRYb0RtWGY2MXlYQ1lqeUE9PSIsInZhbHVlIjoiZ0psNUMxUmZKa25jZnVZK2FpYnEyVDRuSW43a1
ZWZVJaVzlHSHNZUGhMdjRSK0FkMmM0SzM2Yzl6Q1A2R09zT2dCTjMwSngxSnJFb2JEUlNlbWx0SDBDS1hNNDlWMDkvQzZHemRxR1
ZDd1FBRDQyVUJ5cHFUTGtFQ3Q4L0R5UHciLCJtYWMiOiJkZTBjMzk2YmZkNjA5MjIxNDVmMDYzMTBmM2U2ZDE1ZTY4OTAyMTIwNG
U1MWZjZWVkZTQyNTZhMGQzNTk5ZWE1IiwidGFnIjoiIn0%3D;
mangrove_school_quiz_session=D0TOF8uzq1ehDW5rrHwuUDgA6ERhTzWCczhylwTX
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: xhsaxrpe/wcbj
Cookie: XSRF-
TOKEN=eyJpdiI6ImJIZE1CcXRYb0RtWGY2MXlYQ1lqeUE9PSIsInZhbHVlIjoiZ0psNUMxUmZKa25jZnVZK2FpYnEyVDRuSW43a1
ZWZVJaVzlHSHNZUGhMdjRSK0FkMmM0SzM2Yzl6Q1A2R09zT2dCTjMwSngxSnJFb2JEUlNlbWx0SDBDS1hNNDlWMDkvQzZHemRxR1
ZDd1FBRDQyVUJ5cHFUTGtFQ3Q4L0R5UHciLCJtYWMiOiJkZTBjMzk2YmZkNjA5MjIxNDVmMDYzMTBmM2U2ZDE1ZTY4OTAyMTIwNG
U1MWZjZWVkZTQyNTZhMGQzNTk5ZWE1IiwidGFnIjoiIn0%3D;
mangrove_school_quiz_session=D0TOF8uzq1ehDW5rrHwuUDgA6ERhTzWCczhylwTX
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/

TLS/SSL certificate about to expire

One of the TLS/SSL certificates used by your server is about to expire.

Once the certificate has expired, most web browsers will present end-users with a security warning, asking them to manually confirm the authenticity of your certificate chain. Software or automated systems may silently refuse to connect to the server.

This alert is not necessarily caused by the server (leaf) certificate, but may have been triggered by an intermediate certificate. Please refer to the certificate serial number in the alert details to identify the affected certificate.

Impact

If an application server detects an expired certificate with a system it is communicating with, the application server may continue processing data as if nothing happened, or the connection may be abruptly terminated.

https://quizapp.ssbmultiservices.com/ Confidence: 100%

The TLS/SSL certificate (serial: 00d9775e5b85f74c10ca509ad025f1ed8f) will expire in less than **60** days. The certificate validity period is from **Sun Jan 14 2024 08:00:00 GMT+0800 (CST)** to **Sun Apr 14 2024 07:59:59 GMT+0800 (CST)** (45 days left)

Recommendation

Contact your Certificate Authority to renew the SSL certificate.

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/question-image/
- https://quizapp.ssbmultiservices.com/upload/class-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=eyJpdiI6Im5jVlZnakorL2Z2akd0UTNIR0RXM2c9PSIsInZhbHVlIjoiVTl4bk9XeUdhYXIxenAvdTFOMUpTd2VGbDgvVU
ZGaHd5ZGMwZkV1N3lING1RY0YvWE10YmU3NjlxK0Rnd0UrYmYrdnFUQ2k4R2JSUjE2VVJDVWtoSk4vQytxV0VOREtCcW5VUmRhQk
I5bnMyd05DMGJCcDR2SlBjVXFjdzFkeSsiLCJtYWMiOiI1MGFhODgwZmMzY2Q4OWIwMGEwMjk3YjBlZDY3MTZkMWJiMDQzZDlmMG
Q1ZGMwYzc4MGM3MDBiMGI2MmVjYjhmIiwidGFnIjoiIn0%3D;
mangrove_school_quiz_session=EofYUoj8mm2fqmRcISxilC4zgIoH3kVmjrInw0eG
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=eyJpdiI6IlRCTmRybkVaTW85di81TkxGbVNIMFE9PSIsInZhbHVlIjoiUE11R3U3SEszZ1FhbXVtN1Ixb0t0Nm9UY1U3Sj
Z4SjlVV2V3aS9vTnZIeEF3RHFQTlFLU1RJeUZPbUxLellSVEdBREJCWUEyZFRkekRLbXIyTCtod1NBT05rRWZOc01ENy9CYkhGU1
FyYXduVmErZEh6YmthLysyOWdhZlMvZzYiLCJtYWMiOiI4OGZiOGM5NmU1N2JiMTdhYWIzYmZlNTBjMTQ0NTY1YTNiZDM5M2MyMm
Q5MzdiZjk1MjY3ZWJkM2RmMzVkOTYxIiwidGFnIjoiIn0%3D;
mangrove_school_quiz_session=v9GejO3Gi0aurZz4ytaa8R00A91lx2BogXtAxO6v
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 that 1 year (31536000);
- https://quizapp.ssbmultiservices.com/password/reset - max-age is less that 1 year (31536000);

Request

```
GET /login HTTP/1.1
Referer: https://quizapp.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdiI6Im5jVlZnakorL2Z2akd0UTNIR0RXM2c9PSIsInZhbHVlIjoiVTl4bk9XeUdhYXIxenAvdTFOMUpTd2VGbDgvVU
ZGaHd5ZGMwZkV1N3lING1RY0YvWE10YmU3NjlxK0Rnd0UrYmYrdnFUQ2k4R2JSUjE2VVJDVWtoSk4vQytxV0VOREtCcW5VUmRhQk
I5bnMyd05DMGJCcDR2SlBjVXFjdzFkeSsiLCJtYWMiOiI1MGFhODgwZmMzY2Q4OWIwMGEwMjk3YjBlZDY3MTZkMWJiMDQzZDlmMG
Q1ZGMwYzc4MGM3MDBiMGI2MmVjYjhmIiwidGFnIjoiIn0%3D;
mangrove_school_quiz_session=EofYUoj8mm2fqmRcISxilC4zgIoH3kVmjrInw0eG
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

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/question-image/
- https://quizapp.ssbmultiservices.com/upload/class-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=eyJpdiI6Im5jVlZnakorL2Z2akd0UTNIR0RXM2c9PSIsInZhbHVlIjoiVTl4bk9XeUdhYXIxenAvdTFOMUpTd2VGbDgvVU
ZGaHd5ZGMwZkV1N3lING1RY0YvWE10YmU3NjlxK0Rnd0UrYmYrdnFUQ2k4R2JSUjE2VVJDVWtoSk4vQytxV0VOREtCcW5VUmRhQk
I5bnMyd05DMGJCcDR2SlBjVXFjdzFkeSsiLCJtYWMiOiI1MGFhODgwZmMzY2Q4OWIwMGEwMjk3YjBlZDY3MTZkMWJiMDQzZDlmMG
Q1ZGMwYzc4MGM3MDBiMGI2MmVjYjhmIiwidGFnIjoiIn0%3D;
mangrove_school_quiz_session=EofYUoj8mm2fqmRcISxilC4zgIoH3kVmjrInw0eG
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

Permissions Policy (W3C)
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