دائـــــرة الـصـــحـــة
DEPARTMENT OF HEALTH

Security Assessment Report –

247tech.net

Security Audit

Threat level

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.

Alerts distribution

Total alerts found	5
Critical	0
High	1
Medium	0
Low	4

Alerts details

Weak Secret is Used to Sign JWT

Severity	**High**
Reported by module	/httpdata/JWT_JSON_Response_Audit.js

Description

JSON Web Token (JWT) can be digitally signed for protection against data tampering. For this purpose the web application uses the HMAC algorithm with a secret key. It's very important that an attacker doesn't know the value of this secret key. Your application is using a weak/known secret key and Acunetix managed to guess this key.

Impact

An attacker can tamper data in the JWT token. The impact varies depending on how the token is used.

Recommendation

Change the value of secret to a long random string

References

JSON Web Token

Affected items

/api/login
Verified vulnerability
Details
JWT: 'eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjUsImVtYWlsIjoiYWRtaW5AMjR4N3RlbGVoLmNvbSIsInJvbGUiOiJhZG1pbiIsImlhdCI6MTc2NzMyOTE4MiwiZXhwIjoxNzY3NDE1NTgyfQ.QJ3nDPCH6RwoFBnC9ekVQAgT0-LQcZUvogSAIQ6Z53w' HMAC algorithm: 'HS256' Secret: your-secret-key
Request headers
POST /api/login HTTP/1.1 Host: 247tech.net Content-Length: 53 Pragma: no-cache Cache-Control: no-cache accept: */* accept-language: en-US content-type: application/json cookie: GAESA=Cp4BMDAwN2UyNmQ2ODY1YjQ0YmIyOWRhMDFiZmVlY2QzYTU5ZDk4YzUxOWJhOTQ1MjAyYWQ2ODRhZmU2YWMyOGViYjQyYjgzYTQwMzRmOGE4YjM3NDRkZDcyM2JmYzViZmNhNGM1OTIwMzhmN2NiMDA0NWFlZWIxNjhhMzg4MjM1ZmE0ODk3NGQwOTJlYTg0MjMwYWRmN2IwMjZkMTc0MDUQtJyc6Lcz origin: https://247tech.net sec-ch-ua: "Chromium";v="135", "Not-A.Brand";v="8" sec-ch-ua-mobile: ?0 sec-ch-ua-platform: "Windows" Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://247tech.net/ Connection: keep-alive Accept-Encoding: gzip,deflate,br User-Agent: Mozilla/5.0 (Windows

```
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/135.0.0.0 Safari/537.36
{"email":"admin@24x7teleh.com","password":"admin123"}
```

Cookies Not Marked as HttpOnly

Severity	**Low**
Reported by module	/RPA/Cookie_Without_HttpOnly.js

Description

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.

Recommendation

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

References

Cookie Not Marked as HttpOnly | Invicti

Affected items

Web Server
Verified vulnerability
Details
Cookies without HttpOnly flag set:

- https://247tech.net/

```
Set-Cookie:
GAESA=Cp4BMDAwN2UyNmQ2ODY1YjQ0YmIyOWRhMDFiZmVlY2QzYTU
5ZDk4YzUxOWJhOTQ1MjAyYWQ2ODRhZmU2YWMyOGViYjQyYjgzYTQw
MzRmOGE4YjM3NDRkZDcyM2JmYzViZmNhNGM1OTIwMzhmN2NiMDA0N
WFlZWIxNjhhMzg4MjM1ZmE0ODk3NGQwOTJlYTg0MjMwYWRmN2IwMj
ZkMTc0MDUQtJyc6Lcz; expires=Sun, 01-Feb-2026 04:46:13
GMT; path=/
```

Request headers

```
GET / HTTP/1.1 Host: 247tech.net Pragma: no-cache Cache-
Control: no-cache accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7 accept-language: en-US upgrade-
insecure-requests: 1 sec-ch-ua: "Chromium";v="135", "Not-
A.Brand";v="8" sec-ch-ua-mobile: ?0 sec-ch-ua-platform:
"Windows" Sec-Fetch-Site: none Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Connection:
keep-alive Accept-Encoding: gzip,deflate,br User-Agent:
Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0
Safari/537.36
```

Cookies Not Marked as Secure

Severity	**Low**
Reported by module	/RPA/Cookie_Without_Secure.js

Description

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.

Recommendation

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

References

SameSite None Cookie Not Marked as Secure - Invicti

Affected items

Web Server
Verified vulnerability
Details
Cookies without Secure flag set: • https://247tech.net/ Set-Cookie: GAESA=Cp4BMDAwN2UyNmQ2ODY1YjQ0YmIyOWRhMDFiZmVlY2QzYTU5ZDk4YzUxOWJhOTQ1MjAyYWQ2ODRhZmU2YWMyOGViYjQyYjgzYTQwMzRmOGE4YjM3NDRkZDcyM2JmYzViZmNhNGM1OTIwMzhmN2NiMDA0NWFlZWIxNjhhMzg4MjM1ZmE0ODk3NGQwOTJlYTg0MjMwYWRmN2IwMjZkMTc0MDUQtJyc6Lcz; expires=Sun, 01-Feb-2026 04:46:13 GMT; path=/
Request headers
GET / HTTP/1.1 Host: 247tech.net Pragma: no-cache Cache-Control: no-cache accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 accept-language: en-US upgrade-insecure-requests: 1 sec-ch-ua: "Chromium";v="135", "Not-A.Brand";v="8" sec-ch-ua-mobile: ?0 sec-ch-ua-platform: "Windows" Sec-Fetch-Site: none Sec-Fetch-Mode: navigate

```
Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Connection:
keep-alive Accept-Encoding: gzip,deflate,br User-Agent:
Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0
Safari/537.36
```

Cookies with missing, inconsistent or contradictory properties

Severity	**Low**
Reported by module	/RPA/Cookie_Validator.js

Description

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie
Securing cookies with cookie prefixes
Cookies: HTTP State Management Mechanism
SameSite Updates - The Chromium Projects
draft-west-first-party-cookies-07: Same-site Cookies

Affected items

Web Server

Verified vulnerability

Details

List of cookies with missing, inconsistent or contradictory properties:

- https://247tech.net/

  Cookie was set with:

```
Set-Cookie:
GAESA=Cp4BMDAwN2UyNmQ2ODY1YjQ0YmIyOWRhMDFiZmVlY2QzYTU
5ZDk4YzUxOWJhOTQ1MjAyYWQ2ODRhZmU2YWMyOGViYjQyYjgzYTQw
MzRmOGE4YjM3NDRkZDcyM2JmYzViZmNhNGM1OTIwMzhmN2NiMDA0N
WFlZWIxNjhhMzg4MjM1ZmE0ODk3NGQwOTJlYTg0MjMwYWRmN2IwMj
ZkMTc0MDUQtJyc6Lcz; expires=Sun, 01-Feb-2026 04:46:13
GMT; path=/
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web
browsers may apply different and sometimes unexpected
defaults. It is therefore recommended to add a
SameSite attribute with an appropriate value of
either "Strict", "Lax", or "None".
```

Request headers

```
GET / HTTP/1.1 Host: 247tech.net Pragma: no-cache Cache-
Control: no-cache accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7 accept-language: en-US upgrade-
insecure-requests: 1 sec-ch-ua: "Chromium";v="135", "Not-
A.Brand";v="8" sec-ch-ua-mobile: ?0 sec-ch-ua-platform:
"Windows" Sec-Fetch-Site: none Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Connection:
keep-alive Accept-Encoding: gzip,deflate,br User-Agent:
Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0
Safari/537.36
```

Sensitive pages could be cached

Severity	**Low**
Reported by module	/RPA/Cacheable_Sensitive_Page.js

Description

One or more pages contain possible sensitive information (e.g. a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the HTTP response header.

References

OWASP - Caching of Sensitive Information
MDN Web Docs - Cache-Control
CWE-524: Use of Cache Containing Sensitive Information

Affected items

Web Server
Details
List of pages that could be cached: • https://247tech.net/?email=testing@example.com&password=u]H[ww6KrA9F.x-F • https://247tech.net/api/login?email=testing@example.com&password=u]H[ww6KrA9F.x-F

Request headers

GET /?email=testing%40example.com&password=u%5DH%5Bww6KrA9F.x-F HTTP/1.1 Referer: https://247tech.net/ Cookie: GAESA=Cp4BMDAwN2UyNmQ2ODY1YjQ0YmIyOWRhMDFiZmVlY2QzYTU5ZDk4YzUxOWJhOTQ1MjAyYWQ2ODRhZmU2YWMyOGViYjQyYjgzYTQwMzRmOGE4YjM3NDRkZDcyM2JmYzViZmNhNGM1OTIwMzhmN2NiMDA0NWFlZWIxNjhhMzg4MjM1ZmE0ODk3NGQwOTJlYTg0MjMwYWRmN2IwMjZkMTc0MDUQtJyc6Lcz 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/135.0.0.0 Safari/537.36 Host: 247tech.net Connection: Keep-alive