netsparker®

web application security scanner

NETSPARKER SCAN REPORT SUMMARY

TARGET URL	https://fire-watch-kohl.vercel.app/
SCAN DATE	3/26/2025 5:46:19 PM (UTC+05:30)
REPORT DATE	3/26/2025 5:52:01 PM (UTC+05:30)
SCAN DURATION	00:02:42
NETSPARKER VERSION	5.3.0.23162-master-9c20172

Total Requests
2482

Average Speed
15.3 req/sec
req/sec.

4
Identified

4
Confirmed

0
Critical

0
High

SCAN SETTINGS

ENABLED ENGINES	SQL Injection, SQL Injection (Boolean), SQL Injection (Blind), Cross-site Scripting, Command Injection, Command Injection (Blind), Local File Inclusion, Remote File Inclusion, Code Evaluation, Server-Side Template Injection, HTTP Header Injection, Open Redirection, Expression Language Injection, Web App Fingerprint, RoR Code Execution, WebDAV, Reflected File Download, Insecure Reflected Content, XML External Entity, File Upload, Windows Short Filename, Cross-Origin Resource Sharing (CORS), HTTP Methods, Unicode Transformation (Best-Fit Mapping), Server-Side Request Forgery (Pattern Based), Server-Side Request Forgery (DNS), SQL Injection (Out of Band), XML External Entity (Out of Band), Cross-site Scripting (Blind), Remote File Inclusion (Out of Band), Code Evaluation (Out of Band)
URL REWRITE MODE	Heuristic
DETECTED URL REWRITE RULES	None
EXCLUDED URL PATTERNS	(log|sign)\-?(out|off) exit endsession

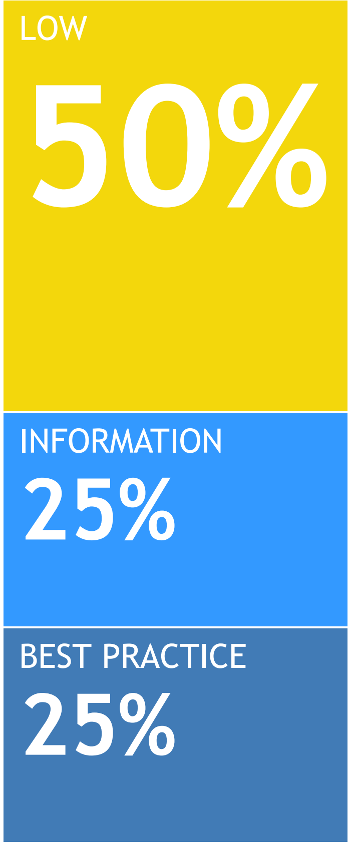
Authentication

Scheduled

```
                gtm\.js
                WebResource\.axd
                ScriptResource\.axd
```

VULNERABILITIES

	ISSUES	INSTANCES	CONFIRMED
CRITICAL	0	0	0
HIGH	0	0	0
MEDIUM	0	0	0
LOW	2	2	2
INFORMATION	1	1	1
BEST PRACTICE	1	1	1
TOTAL	4	4	4



VULNERABILITY SUMMARY

URL	Parameter	Method	Vulnerability	Confirmed
https://fire-watch-kohl.vercel.app/		POST	Forbidden Resource	Yes
https://fire-watch-kohl.vercel.app/.svn/all-wcprops		GET	Cookie Not Marked as HttpOnly	Yes
		GET	Cookie Not Marked as Secure	Yes
		GET	SameSite Cookie Not Implemented	Yes

1. Cookie Not Marked as HttpOnly

3 TOTAL

LOW

CONFIRMED

1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnel to bypass HTTPOnly protection.

External References

- Netsparker - Security Cookies - HTTPOnly Flag
- OWASP HTTPOnly Cookies
- MSDN - ASP.NET HTTPOnly Cookies

Classification

OWASP 2013-A5 OWASP 2017-A6 CWE-16 CAPEC-107 WASC-15

1.1. https://fire-watch-kohl.vercel.app/.svn/all-wcprops

Confirmed

https://fire-watch-kohl.vercel.app/.svn/all-wcprops

Identified Cookie(s)

__clerk_redirection_loop

Cookie Source

CustomField_CookieSourceHeader

Request

```
GET /.svn/all-wcprops HTTP/1.1
Host: fire-watch-kohl.vercel.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://fire-watch-kohl.vercel.app/.svn/all-wcprops
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 401 Unauthorized
Set-Cookie: __clerk_redirection_loop=1; Path=/; Expires=Wed, 26 Mar 2025 12:16:27 GMT; Max-Age=3

Server: Vercel
X-Clerk-Auth-Reason: uat-missing
X-Clerk-Auth-Status: interstitial
X-Vercel-Id: bom1::kwqht-1742991384656-f0b6fad76529
Strict-Transport-Security: max-age=63072000; includeSubDomain
…
```

2. Cookie Not Marked as Secure

3 TOTAL

LOW

CONFIRMED

1

Netsparker identified a cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

Impact

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (*such as a session cookie*), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

Actions to Take

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

Remedy

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to be understand layer 2, have physical access to systems either as waypoints for the traffic, or have locally gained access to to a system between the victim and the web server.

External References

- Netsparker - Security Cookies - Secure Flag
- .NET Cookie.Secure Property
- How to Create Totally Secure Cookies

Classification

OWASP 2013-A6 OWASP 2017-A3 PCI V3.2-6.5.10 CWE-614 CAPEC-102 WASC-15

CVSS 3.0

CVSS Vector String: CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Base: 2.0 (Low)
Temporal: 2.0 (Low)
Environmental: 2.0 (Low)

2.1. https://fire-watch-kohl.vercel.app/.svn/all-wcprops

Confirmed

https://fire-watch-kohl.vercel.app/.svn/all-wcprops

Identified Cookie(s)

`__clerk_redirection_loop`

Cookie Source

`CustomField_CookieSourceHeader`

Request

```
GET /.svn/all-wcprops HTTP/1.1
Host: fire-watch-kohl.vercel.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://fire-watch-kohl.vercel.app/.svn/all-wcprops
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 401 Unauthorized
Set-Cookie: __clerk_redirection_loop=1; Path=/; Expires=Wed, 26 Mar 2025 12:16:27 GMT; Max-Age=3

Server: Vercel
X-Clerk-Auth-Reason: uat-missing
X-Clerk-Auth-Status: interstitial
X-Vercel-Id: bom1::kwqht-1742991384656-f0b6fad76529
Strict-Transport-Security: max-age=63072000; includeSubDomain
…
```

3. Forbidden Resource

11 TOTAL

INFORMATION

CONFIRMED

1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Classification

OWASP-PC-C8

3.1. https://fire-watch-kohl.vercel.app/ Confirmed

https://fire-watch-kohl.vercel.app/

Request

```
POST / HTTP/1.1
Host: fire-watch-kohl.vercel.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

Response

```
HTTP/1.1 403 Forbidden

X-Vercel-Challenge-Token:
2.1742991389.60.NzYzOWM5YWI1NDIyN2NhMDJjZTMxZDYwOWMxMjBkZTE7OGQ3M2EyYjg7YmQ4MjhkZDZiNWY0NzU4MTNkOWFlODNiMmU4ZDcyZmQzZWQxZTg4NzszO7cF8qTTgjBMz0Eoqf
Ka67SrouVkPpgFq9c35eEaL7V8O
…
```

4. SameSite Cookie Not Implemented

3 TOTAL

BEST PRACTICE

CONFIRMED

1

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite* was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

Remedy

The server can set a same-site cookie by adding the SameSite=... attribute to the Set-Cookie header:

```
Set-Cookie: key=value; SameSite=strict
```

There are two possible values for the same-site attribute:

- Lax
- Strict

In the strict mode, the cookie is not sent with any cross-site usage even if the user follows a link to another website. Lax cookies are only sent with a top-level get request.

External References

- Netsparker - Security Cookies - SameSite Attribute
- Using the Same-Site Cookies Attribute to Prevent CSRF Attacks
- Same-site Cookies
- Preventing CSRF with the same-site cookie attribute

Classification

4.1. https://fire-watch-kohl.vercel.app/.svn/all-wcprops

Confirmed

https://fire-watch-kohl.vercel.app/.svn/all-wcprops

Identified Cookie(s)

__clerk_redirection_loop

Cookie Source

CustomField_CookieSourceHeader

Request

```
GET /.svn/all-wcprops HTTP/1.1
Host: fire-watch-kohl.vercel.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://fire-watch-kohl.vercel.app/.svn/all-wcprops
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
X-Scanner: Netsparker
```

Response

```
HTTP/1.1 401 Unauthorized
Set-Cookie: __clerk_redirection_loop=1; Path=/; Expires=Wed, 26 Mar 2025 12:16:27 GMT; Max-Age=3

Server: Vercel
X-Clerk-Auth-Reason: uat-missing
X-Clerk-Auth-Status: interstitial
X-Vercel-Id: bom1::kwqht-1742991384656-f0b6fad76529
Strict-Transport-Security: max-age=63072000; includeSubDomain
…
```