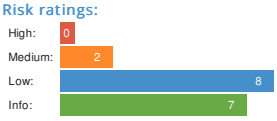
Website Vulnerability Scanner Report (Light)

✔ https://oilprice.com

Summary

Overall risk level:
Medium

Risk ratings:



Scan information:

Start time:	2021-03-19 10:25:15 UTC+02
Finish time:	2021-03-19 10:26:07 UTC+02
Scan duration:	52 sec
Tests performed:	17/17
Scan status:	Finished

Findings

Insecure cookie setting: domain too loose

Cookie Name	URL	Evidence
oilprice_ci	https://oilprice.com	Set-Cookie: .oilprice.com
productionop_csrf_cookie	https://oilprice.com	Set-Cookie: .oilprice.com

Details

Risk description:
A cookie may be used in multiple subdomains belonging to the same domain. For instance, a cookie set for example.com, may be sent along with the requests sent to dev.example.com, calendar.example.com, hostedsite.example.com. Potentially risky websites under your main domain may access those cookies and use the victim session on the main site.

Recommendation:
The Domain attribute should be set to the origin host to limit the scope to that particular server. For example if the application resides on server app.mysite.com, then it should be set to Domain=app.mysite.com

Insecure cookie setting: missing HttpOnly flag

Cookie Name	URL	Evidence
AWSALB	https://oilprice.com/robots.txt	Set-Cookie: AWSALB=E6MehFHBIBLGfauY8ETPW4kRxAsNDJzNWeDhsfWgJxFgm0cLTiU1o5VqcWhYABRengLjDZzq0GypEGOznj5hzkLOcfZ9YAyPz8WivUcs9tyt15KqORNAOpYZLzXA; Expires=Fri, 26 Mar 2021 08:25:49 GMT; Path=/, AWSALBCORS=E6MehFHBIBLGfauY8ETPW4kRxAsNDJzNWeDhsfWgJxFgm0cLTiU1o5VqcWhYABRengLjDZzq0GypEGOznj5hzkLOcfZ9YAyPz8WivUcs9tyt15KqORNAOpYZLzXA; Expires=Fri, 26 Mar 2021 08:25:49 GMT; Path=/; SameSite=None; Secure

Details

Risk description:
A cookie has been set without the HttpOnly flag, which means that it can be accessed by the JavaScript code running inside the web page. If an attacker manages to inject malicious JavaScript code on the page (e.g. by using an XSS attack) then the cookie will be accessible and it can be transmitted to another site. In case of a session cookie, this could lead to session hijacking.

Recommendation:
Ensure that the HttpOnly flag is set for all cookies.
https://owasp.org/www-community/HttpOnly

Missing security header: Strict-Transport-Security

URL	Evidence

https://oilprice.com	Response headers do not include the HTTP Strict-Transport-Security header

Details

Risk description:
The HTTP Strict-Transport-Security header instructs the browser to initiate only secure (HTTPS) connections to the web server and deny any unencrypted HTTP connection attempts. Lack of this header permits an attacker to force a victim user to initiate a clear-text HTTP connection to the server, thus opening the possibility to eavesdrop on the network traffic and extract sensitive information (e.g. session cookies).

Recommendation:
The Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

```
Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]
```

The parameter `max-age` gives the time frame for requirement of HTTPS in seconds and should be chosen quite high, e.g. several months. A value below 7776000 is considered as too low by this scanner check. The flag `includeSubDomains` defines that the policy applies also for sub domains of the sender of the response.

Missing security header: Content-Security-Policy

URL	Evidence
https://oilprice.com	Response headers do not include the HTTP Content-Security-Policy security header

Details

Risk description:
The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site Scripting vulnerabilities (XSS). If the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

Read more about CSP:
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Missing security header: X-Frame-Options

URL	Evidence
https://oilprice.com	Response headers do not include the HTTP X-Frame-Options security header

Details

Risk description:
Because the `X-Frame-Options` header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:
https://owasp.org/www-community/attacks/Clickjacking

Recommendation:
We recommend you to add the `X-Frame-Options` HTTP header with the values `DENY` or `SAMEORIGIN` to every page that you want to be protected against Clickjacking attacks.

More information about this issue:
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Missing security header: X-XSS-Protection

URL	Evidence
https://oilprice.com	Response headers do not include the HTTP X-XSS-Protection security header

Details

Risk description:
The `X-XSS-Protection` HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

Recommendation:
We recommend setting the X-XSS-Protection header to `X-XSS-Protection: 1; mode=block` .

More information about this issue:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

Missing security header: X-Content-Type-Options

URL	Evidence
https://oilprice.com	Response headers do not include the X-Content-Type-Options HTTP security header

Details

Risk description:
The HTTP header `X-Content-Type-Options` is addressed to the Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

More information about this issue:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options.

Missing security header: Referrer-Policy

URL	Evidence
https://oilprice.com	Response headers do not include the Referrer-Policy HTTP security header

Details

Risk description:
The Referrer-Policy HTTP header controls how much referrer information the browser will send with each request originated from the current web application.
For instance, if a user visits the web page "http://example.com/pricing/" and it clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

Read more:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Server software and technology found

Software / Version	Category
Amazon EC2	Web Servers
Apache 2.4.46	Web Servers
Google PageSpeed 1.13.35.2	Cache Tools, Web Server Extensions
PHP 7.2.34	Programming Languages
Prebid	Advertising Networks
DoubleClick for Publishers (DFP)	Advertising Networks
Google Font API	Font Scripts
Google Tag Manager	Tag Managers
jQuery 3.4.1	JavaScript Frameworks

Details

Risk description:
An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

More information about this issue:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html.

Screenshot:

Robots.txt file found

https://oilprice.com/robots.txt

Details

Risk description:
There is no particular security risk in having a robots.txt file. However, this file is often misused by website administrators to try to hide some web pages from the users. This should not be considered a security measure because these URLs can be easily read directly from the robots.txt file.

Recommendation:

We recommend you to manually review the entries from robots.txt and remove the ones which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

More information about this issue:
https://www.theregister.co.uk/2015/05/19/robotstxt/

Website is accessible.

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

Nothing was found for use of untrusted certificates.

Nothing was found for Secure flag of cookie.

Nothing was found for directory listing.

Nothing was found for secure communication.

Scan coverage information

List of tests performed (17/17)

- Checking for website accessibility...
- Checking for domain too loose set for cookies...
- Checking for missing HTTP header - Strict-Transport-Security...
- Checking for missing HTTP header - Content Security Policy...
- Checking for missing HTTP header - X-Frame-Options...
- Checking for missing HTTP header - X-XSS-Protection...
- Checking for missing HTTP header - X-Content-Type-Options...
- Checking for missing HTTP header - Referrer...
- Checking for website technologies...
- Checking for vulnerabilities of server-side software...
- Checking for HttpOnly flag of cookie...
- Checking for robots.txt file...
- Checking for client access policies...
- Checking for use of untrusted certificates...
- Checking for Secure flag of cookie...
- Checking for directory listing...
- Checking for secure communication...

Scan parameters

Website URL:	https://oilprice.com
Scan type:	Light
Authentication:	False