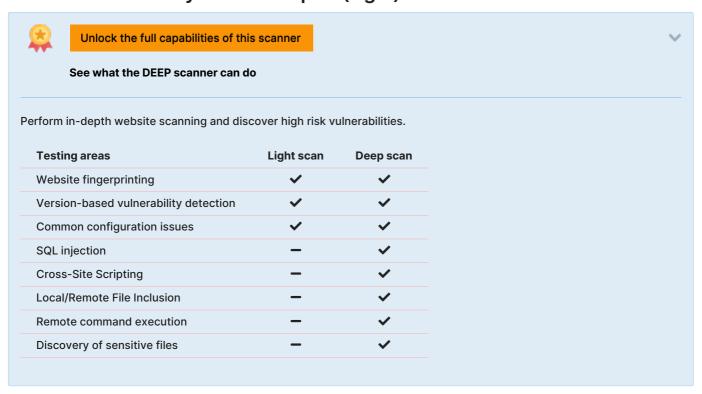


# Website Vulnerability Scanner Report (Light)



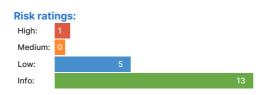
## ✓ https://digiglass.com/

Target added due to a redirect from https://digiglass.com

The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.

## **Summary**





## **Scan information:**

Start time: Oct 29, 2024 / 11:43:27 UTC+02
Finish time: Oct 29, 2024 / 11:44:20 UTC+02

Scan duration: 53 sec
Tests performed: 19/19
Scan status: Finished

## **Findings**

# Vulnerabilities found for server-side software



Risk Level	cvss	CVE	Summary	Affected software
•	9.8	CVE-2022-37454	The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge function interface.	php 7.3.33

•	9.8	CVE-2024-4577	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.	php 7.3.33
•	7.5	CVE-2017-8923	The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.	php 7.3.33
•	6.5	CVE-2022-31629	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a `_Host-` or `_Secure-` cookie by PHP applications.	php 7.3.33
•	6.1	CVE-2022-31160	jQuery UI is a curated set of user interface interactions, effects, widgets, and themes built on top of jQuery. Versions prior to 1.13.2 are potentially vulnerable to cross-site scripting. Initializing a checkboxradio widget on an input enclosed within a label makes that parent label contents considered as the input label. Calling `.checkboxradio( "refresh" )` on such a widget and the initial HTML contained encoded HTML entities will make them erroneously get decoded. This can lead to potentially executing JavaScript code. The bug has been patched in jQuery UI 1.13.2. To remediate the issue, someone who can change the initial HTML can wrap all the non-input contents of the `label` in a `span`.	jquery_ui 1.11.4
•	5.5	CVE-2022-31628	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop.	php 7.3.33
•	4.3	CVE-2016-7103	Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.	jquery_ui 1.11.4
•	4.3	CVE-2021-41182	jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.	jquery_ui 1.11.4
•	4.3	CVE-2021-41183	jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `*Text` options from untrusted sources.	jquery_ui 1.11.4
•	4.3	CVE-2021-41184	jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.	jquery_ui 1.11.4

#### ✓ Details

## Risk description:

The risk is that an attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

#### **Recommendation:**

In order to eliminate the risk of these vulnerabilities, we recommend you check the installed software version and upgrade to the latest version.

## Classification:

OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities OWASP Top 10 - 2021 : A6 - Vulnerable and Outdated Components

# Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
https://digiglass.com/	Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response

#### Risk description:

The risk is that 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.

#### References:

https://cheatsheetseries.owasp.org/cheatsheets/Content\_Security\_Policy\_Cheat\_Sheet.html https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

#### Classification:

**CWE: CWE-693** 

OWASP Top 10 - 2017: A6 - Security Misconfiguration OWASP Top 10 - 2021: A5 - Security Misconfiguration

## Missing security header: Strict-Transport-Security

CONFIRMED

URL	Evidence
https://digiglass.com/	Response headers do not include the HTTP Strict-Transport-Security header Request / Response

#### ▼ Details

#### **Risk description:**

The risk is that 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.

#### Classification:

CWE: CWE-693

OWASP Top 10 - 2017 : A6 - Security Misconfiguration OWASP Top 10 - 2021 : A5 - Security Misconfiguration

## Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
https://digiglass.com/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta/> tag with name 'referrer' is not present in the response.  Request / Response

#### ✓ Details

### Risk description:

The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and 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 Referer-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.

#### References:

https://developer.mozilla.org/en-US/docs/Web/Security/Referer\_header:\_privacy\_and\_security\_concerns

#### Classification:

CWE: CWE-693

OWASP Top 10 - 2017 : A6 - Security Misconfiguration OWASP Top 10 - 2021 : A5 - Security Misconfiguration

## Missing security header: X-Content-Type-Options



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

#### ▼ Details

#### **Risk description:**

The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

#### **Recommendation:**

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

#### References:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

#### Classification:

**CWE: CWE-693** 

OWASP Top 10 - 2017 : A6 - Security Misconfiguration OWASP Top 10 - 2021 : A5 - Security Misconfiguration

## Server software and technology found



Software / Version	Category
Google Font API	Font scripts
iQuery UI 1.11.4	JavaScript libraries
php PHP 7.3.33	Programming languages
<u></u> Cloudflare	CDN
Animate.css	UI frameworks
<> cdnjs	CDN
B Bootstrap	UI frameworks
Tiny Slider	JavaScript libraries
	Web servers
Isotope	JavaScript libraries
© jQuery 3.6.0	JavaScript libraries
₩ OWL Carousel	JavaScript libraries
Swiper	JavaScript libraries
PMA PWA	Miscellaneous

## ▼ Details

### Risk description:

The risk is that 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.

#### References

 $https://owasp.org/www-project-web-security-testing-guide/stable/4-Web\_Application\_Security\_Testing/01-Information\_Gathering/02-Fingerprint\_Web\_Server.html$ 

#### Classification:

OWASP Top 10 - 2017: A6 - Security Misconfiguration

Website is accessible. Nothing was found for client access policies. Nothing was found for robots.txt file. Nothing was found for absence of the security.txt file. Nothing was found for use of untrusted certificates. Nothing was found for enabled HTTP debug methods. Nothing was found for enabled HTTP OPTIONS method. Nothing was found for secure communication. Nothing was found for directory listing. Nothing was found for domain too loose set for cookies. Nothing was found for HttpOnly flag of cookie. Nothing was found for Secure flag of cookie.

## Scan coverage information

### List of tests performed (19/19)

- Starting the scan...
- ✓ Checking for missing HTTP header Content Security Policy...

Nothing was found for unsafe HTTP header Content Security Policy.

- ✓ Checking for missing HTTP header Strict-Transport-Security...
- ✓ Checking for missing HTTP header Referrer...
- Checking for missing HTTP header X-Content-Type-Options...
- Checking for website technologies...
- Checking for vulnerabilities of server-side software...
- Checking for client access policies...
- Checking for robots.txt file...
- Checking for absence of the security.txt file...
- Checking for use of untrusted certificates...
- Checking for enabled HTTP debug methods...
- ✓ Checking for enabled HTTP OPTIONS method...
- Checking for secure communication...
- Checking for directory listing...

- Checking for domain too loose set for cookies...
- Checking for HttpOnly flag of cookie...
- Checking for Secure flag of cookie...
- ✓ Checking for unsafe HTTP header Content Security Policy...

## **Scan parameters**

Target: https://digiglass.com/

Scan type: Light Authentication: False

## Scan stats

Unique Injection Points Detected: 103 URLs spidered: 6 Total number of HTTP requests: 16

Average time until a response was 253ms

received:

Total number of HTTP request errors: