Website Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

See what the DEEP scanner can do

Perform in-depth website scanning and discover high risk vulnerabilities.

Testing areas	Light scan	Deep scan
Website fingerprinting	✔	✔
Version-based vulnerability detection	✔	✔
Common configuration issues	✔	✔
SQL injection	–	✔
Cross-Site Scripting	–	✔
Local/Remote File Inclusion	–	✔
Remote command execution	–	✔
Discovery of sensitive files	–	✔

✔ **https://esluzby.bratislava.sk/**

Target added due to a redirect from https://esluzby.bratislava.sk

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

Overall risk level:

Medium

Risk ratings:

High:	0
Medium:	1
Low:	5
Info:	13

Scan information:

Start time:	Jan 11, 2025 / 13:47:03 UTC+02
Finish time:	Jan 11, 2025 / 13:47:45 UTC+02
Scan duration:	42 sec
Tests performed:	19/19
Scan status:	Finished

Findings

Vulnerabilities found for server-side software

UNCONFIRMED

Risk Level	CVSS	CVE	Summary	Affected software

	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 1.11.2
	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 1.11.2
	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 1.11.2
	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 1.11.2
	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 1.11.2
	4.3	CVE-2015-9251	jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.	jquery 1.11.2
	4.3	CVE-2019-11358	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.	jquery 1.11.2
	4.3	CVE-2020-11023	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	jquery 1.11.2
	4.3	CVE-2020-11022	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	jquery 1.11.2

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:
CWE : CWE-1026
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2021 : A6 - Vulnerable and Outdated Components

Missing security header: X-Content-Type-Options

CONFIRMED

URL	Evidence
https://esluzby.bratislava.sk/	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

Missing security header: Content-Security-Policy

CONFIRMED

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

Details

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: Referrer-Policy

CONFIRMED

URL	Evidence
https://esluzby.bratislava.sk/	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 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.

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

Robots.txt file found

CONFIRMED

URL
https://esluzby.bratislava.sk/robots.txt

Details

Risk description:
There is no particular security risk in having a robots.txt file. However, it's important to note that adding endpoints in it should not be considered a security measure, as this file can be directly accessed and read by anyone.

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).

References:
https://www.theregister.co.uk/2015/05/19/robotstxt/

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

Server software and technology found

UNCONFIRMED

Software / Version	Category
Babel	Miscellaneous
Google Hosted Libraries	CDN
Fourthwall \1	Ecommerce
Choices	JavaScript libraries
core-js 2.6.10	JavaScript libraries
Google Font API	Font scripts
Java	Programming languages
jQuery 1.11.2	JavaScript libraries
jQuery UI 1.11.2	JavaScript libraries
MariaDB	Databases
Modernizr 2.8.3	JavaScript libraries
Open Graph	Miscellaneous
parcel	Miscellaneous
SWC	Miscellaneous
Apache Tomcat	Web servers
PWA	Miscellaneous
Cloudflare	CDN
HSTS	Security
Skolengo \1	CMS, LMS

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
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Security.txt file is missing

CONFIRMED

URL
Missing: https://esluzby.bratislava.sk/.well-known/security.txt

Details

Risk description:
There is no particular risk in not having a security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

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

Website is accessible.

Nothing was found for client access policies.

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 missing HTTP header - Strict-Transport-Security.

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.

Nothing was found for unsafe HTTP header Content Security Policy.

Scan coverage information

List of tests performed (19/19)

- Starting the scan...
- Checking for missing HTTP header - X-Content-Type-Options...
- Checking for missing HTTP header - Content Security Policy...
- Checking for missing HTTP header - Referrer...
- 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 missing HTTP header - Strict-Transport-Security...
- 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://esluzby.bratislava.sk/
scan_type:	Light
authentication:	False

Scan stats

Unique Injection Points Detected:	118
URLs spidered:	10
Total number of HTTP requests:	20
Average time until a response was received:	127ms