Website Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

See what the FULL scanner can do

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

Testing areas	Light scan	Full 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://tigertek.org.uk**

Summary

Overall risk level:

Medium

Risk ratings:

High:	0
Medium:	3
Low:	5
Info:	11

Scan information:

Start time:	2022-07-03 10:48:00 UTC+03
Finish time:	2022-07-03 10:48:15 UTC+03
Scan duration:	15 sec
Tests performed:	19/19
Scan status:	Finished

Findings

Insecure cookie setting: missing Secure flag CONFIRMED

URL	Cookie Name	Evidence
https://tigertek.org.uk	PHPSESSID	Set-Cookie: PHPSESSID=5f62a73462c149b11b851; path=/

Details

Risk description:

Since the `Secure` flag is not set on the cookie, the browser will send it over an unencrypted channel (plain HTTP) if such a request is made. Thus, the risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Recommendation:

Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

References:

https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Classification:

CWE : CWE-614
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Insecure cookie setting: missing HttpOnly flag CONFIRMED

URL	Cookie Name	Evidence
https://tigertek.org.uk	PHPSESSID	Set-Cookie: PHPSESSID=5f62a73462c149b11b851; path=/

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.

References:

https://owasp.org/www-community/HttpOnly

Classification:

CWE : CWE-1004
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Vulnerabilities found for server-side software UNCONFIRMED

Risk Level	CVSS	CVE	Summary	Exploit	Affected software
	4.3	CVE-2014-5191	Cross-site scripting (XSS) vulnerability in the Preview plugin before 4.4.3 in CKEditor allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	N/A	CKEditor 4.3.1
	4.3	CVE-2018-17960	CKEditor 4.x before 4.11.0 allows user-assisted XSS involving a source-mode paste.	N/A	CKEditor 4.3.1
	4.3	CVE-2020-9281	A cross-site scripting (XSS) vulnerability in the HTML Data Processor for CKEditor 4.0 before 4.14 allows remote attackers to inject arbitrary web script through a crafted "protected" comment (with the cke_protected syntax).	N/A	CKEditor 4.3.1
	4.3	CVE-2021-26271	It was possible to execute a ReDoS-type attack inside CKEditor 4 before 4.16 by persuading a victim to paste crafted text into the Styles input of specific dialogs (in the Advanced Tab for Dialogs plugin).	N/A	CKEditor 4.3.1
	4.3	CVE-2021-26272	It was possible to execute a ReDoS-type attack inside CKEditor 4 before 4.16 by persuading a victim to paste crafted URL-like text into the editor, and then press Enter or Space (in the Autolink plugin).	N/A	CKEditor 4.3.1
	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.	N/A	jQuery 2.2.4
	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.	N/A	jQuery 2.2.4
	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.	N/A	jQuery 2.2.4
	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.	N/A	jQuery 2.2.4

Details

Risk description:
These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. 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:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

Classification:
CWE : CWE-1026
OWASP Top 10 - 2013 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities

Robots.txt file found CONFIRMED

URL
https://tigertek.org.uk/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).

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

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: Content-Security-Policy CONFIRMED

URL	Evidence
https://tigertek.org.uk	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.

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 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: X-XSS-Protection CONFIRMED

URL	Evidence
https://tigertek.org.uk	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` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: Referrer-Policy CONFIRMED

URL	Evidence
https://tigertek.org.uk	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.

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.

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

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Server software and technology found UNCONFIRMED

Software / Version	Category
Apache	Web servers
PHP 7.4.30	Programming languages
jQuery-pjax	Mobile frameworks
CKEditor 4.3.1	Rich text editors
animate.css	UI frameworks
Bootstrap 3.3.0	UI frameworks
Font Awesome	Font scripts
Select2	JavaScript libraries
Moment.js 2.10.2	JavaScript libraries
jQuery UI 1.12.0	JavaScript libraries
jQuery Migrate 1.4.1	JavaScript libraries
jQuery 2.2.4	JavaScript libraries

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.

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 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Security.txt file is missing CONFIRMED

URL
Missing: https://tigertek.org.uk/.well-known/security.txt

Details

Risk description:
We have detected that the server is missing the security.txt file. There is no particular risk in not creating a valid 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 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Nothing was found for directory listing.

Nothing was found for missing HTTP header - X-Content-Type-Options.

Nothing was found for missing HTTP header - X-Frame-Options.

Nothing was found for missing HTTP header - Strict-Transport-Security.

Website is accessible.

Nothing was found for secure communication.

Nothing was found for enabled HTTP debug methods.

Nothing was found for use of untrusted certificates.

Nothing was found for client access policies.

Nothing was found for domain too loose set for cookies.

Scan coverage information

List of tests performed (19/19)

- Checking for website accessibility...
- Checking for HttpOnly flag of cookie...
- Checking for Secure flag of cookie...
- Checking for missing HTTP header - Content Security Policy...
- Checking for missing HTTP header - X-XSS-Protection...
- 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 secure communication...
- Checking for directory listing...
- Checking for missing HTTP header - Strict-Transport-Security...
- Checking for missing HTTP header - X-Frame-Options...
- Checking for missing HTTP header - X-Content-Type-Options...
- Checking for domain too loose set for cookies...

Scan parameters

Website URL:	https://tigertek.org.uk
Scan type:	Light
Authentication:	False

Scan stats

Unique Injection Points Detected:	3
URLs spidered:	68
Total number of HTTP requests:	78