

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	✗	✓

✓ <http://www.fpk.ac.ma>

Summary

Overall risk level:

High

Risk ratings:

High:	1
Medium:	1
Low:	5
Info:	12

Scan information:

Start time:	2022-06-11 01:36:20 UTC+03
Finish time:	2022-06-11 01:36:40 UTC+03
Scan duration:	20 sec
Tests performed:	19/19
Scan status:	Finished

Findings



Vulnerabilities found for server-side software

UNCONFIRMED ⓘ

Risk Level	CVSS	CVE	Summary	Exploit	Affected software
●	9.3	CVE-2020-13664	Arbitrary PHP code execution vulnerability in Drupal Core under certain circumstances. An attacker could trick an administrator into visiting a malicious site that could result in creating a carefully named directory on the file system. With this directory in place, an attacker could attempt to brute force a remote code execution vulnerability. Windows servers are most likely to be affected. This issue affects: Drupal Drupal Core 8.8.x versions prior to 8.8.8; 8.9.x versions prior to 8.9.1; 9.0.1 versions prior to 9.0.1.	N/A	Drupal 8
●	7.5	CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.	N/A	http_server 2.4.18
●	7.5	CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.	N/A	http_server 2.4.18
●	7.5	CVE-2017-7668	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.	N/A	http_server 2.4.18
●	7.5	CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.	N/A	http_server 2.4.18
●	7.5	CVE-2021-26691	In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow	N/A	http_server 2.4.18
●	7.5	CVE-2017-6920	Drupal core 8 before versions 8.3.4 allows remote attackers to execute arbitrary code due to the PECL YAML parser not handling PHP objects safely during certain operations.	N/A	Drupal 8
●	7.5	CVE-2017-6925	In versions of Drupal 8 core prior to 8.3.7; There is a vulnerability in the entity access system that could allow unwanted access to view, create, update, or delete entities. This only affects entities that do not use or do not have UUIDs, and entities that have different access restrictions on different revisions of the same entity.	N/A	Drupal 8
●	7.5	CVE-2018-7600	Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1 allows remote attackers to execute arbitrary code because of an issue affecting multiple subsystems with default or common module configurations.	EDB-ID:44448 EDB-ID:44449 EDB-ID:44482	Drupal 8
●	7.5	CVE-2018-7602	A remote code execution vulnerability exists within multiple subsystems of Drupal 7.x and 8.x. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being compromised. This vulnerability is related to Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-002. Both SA-CORE-2018-002 and this vulnerability are being exploited in the wild.	EDB-ID:44542 EDB-ID:44557	Drupal 8
●	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 3.2.1
●	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 3.2.1
●	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 3.2.1

▼ 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](#)

Communication is not secure CONFIRMED

URL	Evidence
http://www.fpk.ac.ma	Communication is made over unsecure, unencrypted HTTP.

▼ Details

Risk description:

The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:

We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

Classification:

CWE : [CWE-311](#)

OWASP Top 10 - 2013 : [A6 - Sensitive Data Exposure](#)

OWASP Top 10 - 2017 : [A3 - Sensitive Data Exposure](#)

Missing security header: Content-Security-Policy CONFIRMED

URL	Evidence
http://www.fpk.ac.ma	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
http://www.fpk.ac.ma	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
http://www.fpk.ac.ma	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](#)

🚩 Robots.txt file found CONFIRMED

URL
http://www.fpk.ac.ma/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](#)

Server software and technology found UNCONFIRMED ⓘ

Software / Version	Category
 Ubuntu	Operating systems
 Apache 2.4.18	Web servers
 PHP	Programming languages
 Drupal 8	CMS
 YouTube	Video players
 Bootstrap 3.3.7	UI frameworks
 Font Awesome	Font scripts
 jQuery 3.2.1	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: <http://www.fpk.ac.ma/.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:

Classification:

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

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

🚩 Nothing was found for HttpOnly flag of cookie.

🚩 Nothing was found for domain too loose set for cookies.

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

🚩 Website is accessible.

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

🚩 Nothing was found for directory listing.

🚩 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 Secure flag of cookie.

Scan coverage information

List of tests performed (19/19)

- ✓ Checking for website accessibility...
- ✓ Checking for secure communication...
- ✓ 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 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...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for Secure flag of cookie...

Scan parameters

Website URL: http://www.fpk.ac.ma
Scan type: Light
Authentication: False

Scan stats

Unique Injection Points Detected: 117
URLs spidered: 16
Total number of HTTP requests: 26
