Drupal Vulnerability Scanner Report

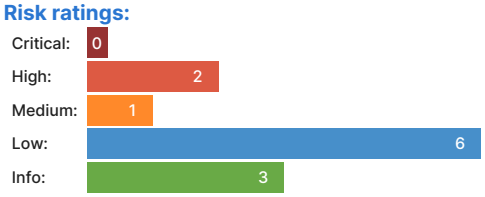
✔ http://testing1.pentest-tools.com:9001/

Summary

Overall risk level:

High

Risk ratings:



Scan information:

Start time:	Feb 12, 2025 / 08:06:59 UTC+02
Finish time:	Feb 12, 2025 / 08:07:03 UTC+02
Scan duration:	4 sec
Tests performed:	12/12
Scan status:	Finished

Findings

Vulnerabilities found for Drupal version 7.73

Risk level	CVSS	CVE	Summary	Exploit	Affected Software
	7.5	CVE-2022-25275	In some situations, the Image module does not correctly check access to image files not stored in the standard public files directory when generating derivative images using the image styles system. Access to a non-public file is checked only if it is stored in the "private" file system. However, some contributed modules provide additional file systems, or schemes, which may lead to this vulnerability. This vulnerability is mitigated by the fact that it only applies when the site sets (Drupal 9) $config['image.settings']['allow_insecure_derivatives'] or (Drupal 7) $conf['image_allow_insecure_derivatives'] to TRUE. The recommended and default setting is FALSE, and Drupal core does not provide a way to change that in the admin UI. Some sites may require configuration changes following this security release. Review the release notes for your Drupal version if you have issues accessing files or image styles after updating.	N/A	drupal 7.73
	6.8	CVE-2020-28948	Archive_Tar through 1.4.10 allows an unserialization attack because phar: is blocked but PHAR: is not blocked.	N/A	drupal 7.73
	6.8	CVE-2020-28949	Archive_Tar through 1.4.10 has :// filename sanitization only to address phar attacks, and thus any other stream-wrapper attack (such as file:// to overwrite files) can still succeed.	N/A	drupal 7.73
	6.5	CVE-2020-13671	Drupal core does not properly sanitize certain filenames on uploaded files, which can lead to files being interpreted as the incorrect extension and served as the wrong MIME type or executed as PHP for certain hosting configurations. This issue affects: Drupal Drupal Core 9.0 versions prior to 9.0.8, 8.9 versions prior to 8.9.9, 8.8 versions prior to 8.8.11, and 7 versions prior to 7.74.	N/A	drupal 7.73
	6.5	CVE-2023-31250	The file download facility doesn't sufficiently sanitize file paths in certain situations. This may result in users gaining access to private files that they should not have access to. Some sites may require configuration changes following this security release. Review the release notes for your Drupal version if you have issues accessing private files after updating.	N/A	drupal 7.73
	5	CVE-2020-36193	Tar.php in Archive_Tar through 1.4.11 allows write operations with Directory Traversal due to inadequate checking of symbolic links, a related issue to CVE-2020-28948.	N/A	drupal 7.73
	4.3	CVE-2010-5312	Cross-site scripting (XSS) vulnerability in jquery.ui.dialog.js in the Dialog widget in jQuery UI before 1.10.0 allows remote attackers to inject arbitrary web script or HTML via the title option.	N/A	drupal 7.73

🟠	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.	N/A	drupal 7.73
🟠	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.	N/A	drupal 7.73
🟠	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.	N/A	drupal 7.73
🟠	4.3	CVE-2022-25271	Drupal core's form API has a vulnerability where certain contributed or custom modules' forms may be vulnerable to improper input validation. This could allow an attacker to inject disallowed values or overwrite data. Affected forms are uncommon, but in certain cases an attacker could alter critical or sensitive data.	N/A	drupal 7.73
🔵	2.6	CVE-2020-13672	Cross-site Scripting (XSS) vulnerability in Drupal core's sanitization API fails to properly filter cross-site scripting under certain circumstances. This issue affects: Drupal Core 9.1.x versions prior to 9.1.7; 9.0.x versions prior to 9.0.12; 8.9.x versions prior to 8.9.14; 7.x versions prior to 7.80.	N/A	drupal 7.73

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.

Notes:
- The vulnerabilities are identified based on the server's version information
- Only the highest risk 20 vulnerabilities are shown for each port.

Recommendation:
We recommend you to upgrade Drupal to the latest version in order to eliminate the risk of these vulnerabilities.

Communication is not secure

The communication between the browser and web the server is done via HTTP, which is a clear-text protocol. All information is sent unencrypted over the network (including login details).
http://testing1.pentest-tools.com:9001/
Details

Risk description:
An attacker could read the information transmitted between the client and the server, including confidential information such as usernames and passwords.
This attack could be implemented by using a technique called 'man-in-the-middle', which permits the attacker to intercept the network traffic of the victim user.

Recommendation:
We recommend you to reconfigure the web server in order to use HTTPS for communication, which protects the data transmitted via encryption.
Furthermore, you should configure a trusted SSL certificate for the web server.

User discovery is possible (using Forgot Password)

The Forgot Password functionality can be abused to discover if a username is valid or not. This is possible because the application returns an explicit message saying that the entered username is not recognized.
http://testing1.pentest-tools.com:9001/?q=user/password
Details

Risk description:
An attacker could extract a list of existing usernames from Drupal and use them in brute-force attacks in order to guess their passwords and authenticate in the application.

Recommendation:
We recommend you to install a Drupal module such as Username Enumeration Prevention that mitigates this vulnerability.

Server software and technology found

Category	Details
Technology	PHP 7.4.12
Server	Apache 2.4.38
Operating system	unknown

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 may allow an attacker to identify the software platform, technology, server and operating system (ex. HTTP server headers, meta information, etc).

Drupal installation found from fingerprint

Drupal - version(s) 7.73
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 may allow an attacker to identify the software platform, technology, server and operating system (ex. HTTP server headers, meta information, etc).

Drupal modules found

Modules	Evidence
system	http://testing1.pentest-tools.com:9001/modules/system
comment	http://testing1.pentest-tools.com:9001/modules/comment
field	http://testing1.pentest-tools.com:9001/modules/field
node	http://testing1.pentest-tools.com:9001/modules/node
search	http://testing1.pentest-tools.com:9001/modules/search
user	http://testing1.pentest-tools.com:9001/modules/user

Details

Risk description:
An attacker could use this information to mount specific attacks against the modules.

Recommendation:
We recommend you to make sure the Drupal modules are updated to the latest version.

Drupal theme found

Theme name: bartik
Details

Risk description:
An attacker could use this information to mount specific attacks against the theme.

Recommendation:
We recommend you to make sure the Drupal theme is updated to the latest version.

Login page is accessible

http://testing1.pentest-tools.com:9001/?q=user/login
Details

Risk description:
An attacker could try to authenticate in the application if he knows the correct username and password.
Furthermore, if the attacker knows only the username, he could try multiple passwords in order to guess the correct one.

Recommendation:
We recommend you to decide if the login page must be accessible from any IP address from the Internet. If not, we recommend restricting the source IP addresses that can access the login page.

Install files found

The following default Drupal installation files were found:
http://testing1.pentest-tools.com:9001/install.php
http://testing1.pentest-tools.com:9001/CHANGELOG.txt
http://testing1.pentest-tools.com:9001/INSTALL.txt
http://testing1.pentest-tools.com:9001/INSTALL.mysql.txt
http://testing1.pentest-tools.com:9001/INSTALL.pgsql.txt
http://testing1.pentest-tools.com:9001/LICENSE.txt
http://testing1.pentest-tools.com:9001/MAINTAINERS.txt
http://testing1.pentest-tools.com:9001/UPGRADE.txt
Details

Risk description:
An attacker could use these files to fingerprint the Drupal installation and its current version.

Recommendation:
We recommend you to remove these files from the server.
More details on this topic: https://www.drupal.org/upgrade/finished

Directory listing is not enabled

User enumeration did not succeed (using Views module)

User registration is disabled

Scan coverage information

List of tests performed (12/12)

- Fingerprinting the server software and technology...
- Fingerprinting the Drupal installation...
- Searching for vulnerabilities of current Drupal version...
- Searching for Drupal modules...
- Searching for Drupal theme...
- Testing for directory listing...
- Attempting user enumeration using Views module...
- Attempting user discovery using Forgot Password...
- Checking for the presence of login page...
- Checking for secure communication...
- Searching for default install files...
- Checking if user registration is enabled...

Scan parameters

Target:	http://testing1.pentest-tools.com:9001/