Pentest-Tools.com

Drupal Vulnerability Scan Report

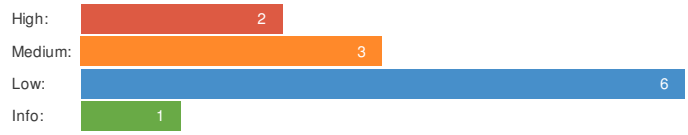
http://www.sample-drupal.com/

Summary

Overall risk level:

High

Risk ratings:



Scan information:

Start time:	2017-01-10 12:39:42
Finish time:	2017-01-10 12:40:29
Scan duration:	47.0 seconds
Tests performed:	12/12
Scan status:	Finished

Findings

User enumeration is possible (using Views module)

Found 8 users:
admin
admin2
alex_202
bdulau
daniel.peer
goya_203
john.snow
kenny.steel

Details

Risk description:
The Views module of Drupal can be abused to extract the list of all users from the platform. This method is particularly useful for finding the Drupal super user account (id 1) and other accounts that might not be exposed anywhere on the public facing site. An attacker could use these usernames to try brute-force authentication attacks in order to gain unauthorized access to those users' accounts.

Recommendation:
We recommend you to update Drupal to a recent version that fixes this vulnerability.
Otherwise, you could install a Drupal module such as Username Enumeration Prevention that mitigates this vulnerability.

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://www.sample-drupal.com/

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.

Drupal vulnerabilities found

Date	Vulnerability	Affected versions	Advisory URL
2016-Nov-16	Multiple vulnerabilities	before 7.52,before 8.2.3,	https://www.drupal.org/SA-CORE-2016-005

2016-Jun-15	Access bypass, Multiple vulnerabilities	before 7.44,before 8.1.3,	https://www.drupal.org/SA-CORE-2016-002
2015-Oct-21	Open Redirect	before 7.41,	https://www.drupal.org/SA-CORE-2015-004

Details

Risk description:
An attacker could exploit these vulnerabilities in order to affect the confidentiality, integrity or availability of the application.
The specific risk can be found in the Drupal Advisory (see the provided URL).

Recommendation:
We recommend you to upgrade Drupal to the latest version.

User enumeration is possible (using Forgot Password)

The Forgot Password functionality can be abused to check 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://www.sample-drupal.com/?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.

User registration is possible

http://www.sample-drupal.com/?q=user/register

Details

Risk description:
An attacker could try to create fake accounts in order to access privileged functionality in the application.

Recommendation:
We recommend you to analyze and decide if users must create their own accounts in Drupal. If not, we recommend disabling this functionality.
In order to remove the register functionality, you need to browse to admin/user/settings (for Drupal 6) or admin/config/people/accounts (for Drupal 7 and 8) and select the the 'Only site administrators can create new user accounts' option.

Server software and technology found

Technology	PHP 5.4.45
Server	Apache 2.4.23
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) 7.38

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

Found 12 modules

colorbox	http://www.sample-drupal.com/sites/all/modules/contrib/colorbox/README.txt

google_analytics	http://www.sample-drupal.com/sites/all/modules/contrib/google_analytics/README.txt
shadi_profile	http://www.sample-drupal.com/sites/all/modules/custom/shadi_profile
views_slideshow	http://www.sample-drupal.com/sites/all/modules/contrib/views_slideshow/README.txt
user_relationships	http://www.sample-drupal.com/sites/all/modules/contrib/user_relationships/LICENSE.txt
jquery_update	http://www.sample-drupal.com/sites/all/modules/contrib/jquery_update/README.txt
system	http://www.sample-drupal.com/modules/system
date	http://www.sample-drupal.com/sites/all/modules/contrib/date/CHANGELOG.txt
views	http://www.sample-drupal.com/sites/all/modules/contrib/views/README.txt
invite	http://www.sample-drupal.com/sites/all/modules/contrib/invite/README.txt
ctools	http://www.sample-drupal.com/sites/all/modules/contrib/ctools/CHANGELOG.txt
field	http://www.sample-drupal.com/modules/field

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: druptheme2

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://www.sample-drupal.com/?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://www.sample-drupal.com/install.php
http://www.sample-drupal.com/CHANGELOG.txt
http://www.sample-drupal.com/INSTALL.txt
http://www.sample-drupal.com/INSTALL.mysql.txt
http://www.sample-drupal.com/INSTALL.pgsql.txt
http://www.sample-drupal.com/LICENSE.txt
http://www.sample-drupal.com/MAINTAINERS.txt
http://www.sample-drupal.com/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

Scan coverage information

List of tests performed (12/12)

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

Scan parameters

- Target: http://www.sample-drupal.com/