Scan Report

Started scanning network 192.168.111.132/32 at June 17, 2022 14:39:13.618528.

Network scan completed at 14:39:13.618528

Found 1 active IPs:

Active IP: 192.168.111.132

Starting full port scan on ip 192.168.111.132 at June 17, 2022 14:39:23.700577

Port 22 was found with details:

name: ssh
state: open

Port 80 was found with details:

name: http
state: open

Port 5000 was found with details:

name: upnp
state: open

Port 8081 was found with details:

name: blackice-icecap
state: open

Port 9001 was found with details:

name: tor-orport
state: open

Port 9001 of IP 192.168.111.132 was updated with details:

name: http
state: open
product: nginx
version: 1.14.0
extrainfo: Ubuntu

Vulnerabilities and Exploits search started on port 9001 of IP 192.168.111.132 at

June 17, 2022 14:41:36.340194

Id: DRUPAL-SA-CORE-2019-008
Type: drupal
Title: drupal
Score: 6.8
Description: In Drupal 8.7.4, when the experimental Workspaces module is enabled, an access bypass condition is created. This can be mitigated by disabling the Workspaces module. It does not affect any release other than Drupal 8.7.4. Drupal 8.7.3 and earlier, Drupal 8.6.x and earlier, and Drupal 7.x are not affected.

Id: EDB-ID:50841

Title: Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XSS)
Type: exploitdb
Score: 0.0
Description:
Id: 1337DAY-ID-37549
Title: Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting Vulnerability
Type: zdt
Score: 0.0
Description:
Id: PACKETSTORM:166409
Title: Drupal Avatar Upload 7.x-1.0-beta8 Cross Site Scripting
Type: packetstorm
Score: 0.0
Description:
Id: B41082A1-4177-53E2-A74C-8ABA13AA3E86
Title: Exploit for Injection in Apache Solr
Type: githubexploit
Score: 10.0
Description: # Notice
～～终究还是觉得每个漏洞每个单独的脚本很不方便，故将所有的poc和exp脚本整在一起，可以一键扫描＋漏洞利用，...
Id: 2C119FFA-ECE0-5E14-A4A4-354A2C38071A
Title: Exploit for Vulnerability in Oracle Fusion Middleware
Type: githubexploit
Score: 10.0
Description: # TOP
TOP All bugbounty pentesting CVE-2022- POC Exp Things
...
Id: MSF:AUXILIARY/GATHER/DRUPAL_OPENID_XXE/
Title: Drupal OpenID External Entity Injection
Type: metasploit
Score: 0.0
Description: This module abuses an XML External Entity Injection vulnerability on the OpenID module from Drupal. The vulnerability exists in the parsing of a malformed XRDS file coming from a malicious OpenID endpoint. This module has been tested successfully on Drupal 7.15 and 7.2 with the OpenID module enabled.

Id: EC76E06B-65FA-5E72-A707-6B2F18F549F2
Title: Exploit for Deserialization of Untrusted Data in Drupal
Type: githubexploit
Score: 6.8
Description: # CVE-2019-6340 Drupal8's REST RCE, SA-CORE-2019-003

0x01 d...
Id: PACKETSTORM:164354
Title: Drupal MiniorangeSAML 8.x-2.22 Privilege Escalation
Type: packetstorm
Score: 0.0
Description:
Id: EDB-ID:50361
Title: Drupal Module MiniorangeSAML 8.x-2.22 - Privilege escalation
Type: exploitdb
Score: 0.0

Description:
Id: 1337DAY-ID-36836
Title: MiniOrange SAML Drupal Module 8.x-2.22 Privilege escalation via XML Signature Wrapping Vulnerability
Type: zdt
Score: 0.0
Description:
Id: D9F421A6-5B20-56B3-AA86-5C0A2116D651
Title: Exploit for Deserialization of Untrusted Data in Drupal
Type: githubexploit
Score: 6.8
Description: # Drupal Drupal 8.6.x RCE Exploit

exploit CV...
Id: 09E34186-172A-5F90-8972-04A10AA785BA
Title: Exploit for Deserialization of Untrusted Data in Drupal
Type: githubexploit
Score: 6.8
Description: # CVE-2019-6340

This is part of Cved: *a tool to ...
Id: MSF:EXPLOIT/UNIX/WEBAPP/DRUPAL_DRUPALGEDDON2/
Title: Drupal Drupalgeddon 2 Forms API Property Injection
Type: metasploit
Score: 0.0
Description: This module exploits a Drupal property injection in the Forms API. Drupal 6.x, < 7.58, 8.2.x, < 8.3.9, < 8.4.6, and < 8.5.1 are vulnerable.

Id: MSF:EXPLOIT/UNIX/WEBAPP/DRUPAL_RESTWS_UNSERIALIZE/
Title: Drupal RESTful Web Services unserialize() RCE
Type: metasploit
Score: 0.0
Description: This module exploits a PHP unserialize() vulnerability in Drupal RESTful Web Services by sending a crafted request to the /node REST endpoint. As per SA-CORE-2019-003, the initial remediation was to disable POST, PATCH, and PUT, but Ambionics discovered that GET was also vulnerable (albeit cached). Cached nodes can be exploited only once. Drupal updated SA-CORE-2019-003 with PSA-2019-02-22 to notify users of this alternate vector. Drupal < 8.5.11 and < 8.6.10 are vulnerable.

Id: 0B0F940B-BBCE-52B1-8A3F-6FF63D7BDA4E
Title: Exploit for Improper Input Validation in Drupal
Type: githubexploit
Score: 7.5
Description: # drupal8-REST-RCE
CVE-2019-6340 drupal8-REST-RCE (/node/1) , CV...
Id: MSF:AUXILIARY/SCANNER/HTTP/DRUPAL_VIEWS_USER_ENUM/
Title: Drupal Views Module Users Enumeration
Type: metasploit
Score: 0.0
Description: This module exploits an information disclosure vulnerability in the 'Views' module of Drupal, brute-forcing the first 10 usernames from 'a' to 'z'. Drupal 6 with 'Views' module <= 6.x-2.11 are vulnerable. Drupal does not

consider disclosure of usernames as a weakness.

Id: MSF:EXPLOIT/UNIX/WEBAPP/DRUPAL_CODER_EXEC/
Title: Drupal CODER Module Remote Command Execution
Type: metasploit
Score: 0.0
Description: This module exploits a Remote Command Execution vulnerability in the Drupal CODER Module. Unauthenticated users can execute arbitrary commands under the context of the web server user. The CODER module doesn't sufficiently validate user inputs in a script file that has the PHP extension. A malicious unauthenticated user can make requests directly to this file to execute arbitrary commands. The module does not need to be enabled for this to be exploited. This module was tested against CODER 2.5 with Drupal 7.5 installed on Ubuntu Server.

Id: MSF:EXPLOIT/UNIX/WEBAPP/DRUPAL_CODER_EXEC
Title: Drupal CODER Module Remote Command Execution
Type: metasploit
Score: 0.0
Description: This module exploits a Remote Command Execution vulnerability in the Drupal CODER Module. Unauthenticated users can execute arbitrary commands under the context of the web server user. The CODER module doesn't sufficiently validate user inputs in a script file that has the PHP extension. A malicious unauthenticated user can make requests directly to this file to execute arbitrary commands. The module does not need to be enabled for this to be exploited. This module was tested against CODER 2.5 with Drupal 7.5 installed on Ubuntu Server.

Id: MSF:EXPLOIT/UNIX/WEBAPP/DRUPAL_RESTWS_EXEC
Title: Drupal RESTWS Module Remote PHP Code Execution
Type: metasploit
Score: 0.0
Description: This module exploits a Remote PHP Code Execution vulnerability in the Drupal RESTWS Module. Unauthenticated users can execute arbitrary code under the context of the web server user. RESTWS alters the default page callbacks for entities to provide additional functionality. A vulnerability in this approach allows an unauthenticated attacker to send specially crafted requests resulting in arbitrary PHP execution. RESTWS 2.x prior to 2.6 and 1.x prior to 1.7 are affected by this issue. This module was tested against RESTWS 2.5 with Drupal 7.5 installed on Ubuntu Server.

Id: MSF:EXPLOIT/UNIX/WEBAPP/DRUPAL_RESTWS_EXEC/
Title: Drupal RESTWS Module Remote PHP Code Execution
Type: metasploit
Score: 0.0
Description: This module exploits a Remote PHP Code Execution vulnerability in the Drupal RESTWS Module. Unauthenticated users can execute arbitrary code under the context of the web server user. RESTWS alters the default page callbacks for entities to provide additional functionality. A vulnerability in this approach allows an unauthenticated attacker to send specially crafted requests resulting in arbitrary PHP execution. RESTWS 2.x prior to 2.6 and 1.x prior to 1.7 are affected by this issue. This module was tested against RESTWS 2.5 with Drupal 7.5 installed on Ubuntu Server.

Exploit executed at June 17, 2022 14:41:41.160269

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

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-nVkKyhlVulEcBDY4RmCCu7xtGOTjwiBRLw711V6ddGQ
[*] Triggering exploit to execute: ls
CHANGELOG.txt
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
README.txt
UPGRADE.txt
authorize.php
cron.php
includes
index.php
install.php
misc
modules
profiles
scripts
sites
themes
update.php
web.config
xmlrpc.php
```