CSC Workshop presentation

Access to Our Workshop

- Nullcon Wifi pass:
  - NullconG0@
- Discord server for yours questions:
  - https://discord.gg/GTSm5dfD
- Software requirements:
  - Python3 with requests library
  - Netcat
  - Web Browser
  - Vmware for local copy of workshop

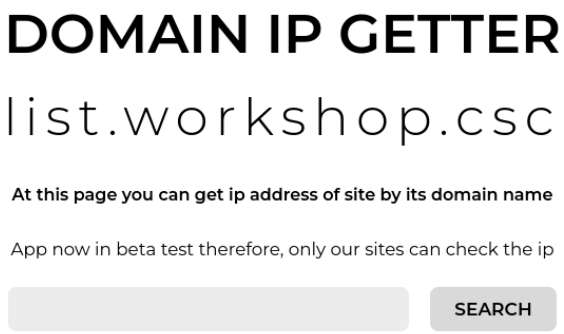
One ip, many apps

- We only have one ip address
- First step — nmap scanning with command
  - sudo nmap -sS -sV <ip addr>
- Result: open ssh, http and mysql ports

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
3306/tcp open  mysql   MySQL 5.5.5-10.7.4-MariaDB-1:10.7.4+maria~focal
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

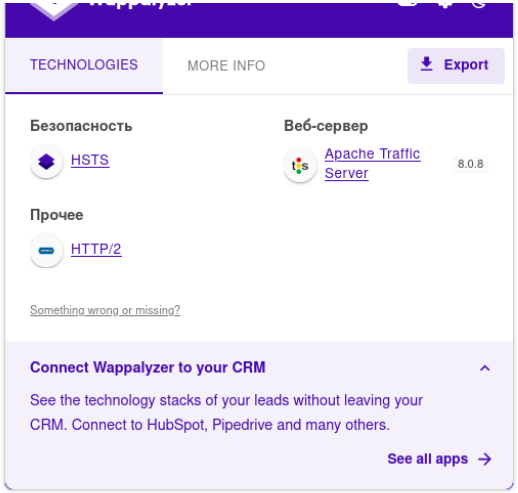
Checking http

- Nginx server is running at port 80
- Going through the browser to this port, we found a web application
- In the search form we've found an SQL injection and with help of a payload string **` or 1=1 #** we received a complete list of web-resources and add it to **/etc/hosts**



Determine the version of the web application

- To determine the version of the web application, we use the Wappalyzer browser extension.
- This plugin shows a list of web technologies, their versions and even versions of some protection tools.
-



Invulnerable WordPress and leaky Drupal

- WordPress has been updated to the latest version and has no vulnerabilities.
- Drupal version is 8. If we check this version at **exploit-db.com,** we can see that this version of Drupal is vulnerable to the Drupalgeddon 2.

Show 15 Search: drupal 8

Date	D	A	V	Title	Type	Platform	Author
2022-03-30			✗	Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XSS)	WebApps	PHP	Milad karimi
2021-10-01			✗	Drupal Module MiniorangeSAML 8.x-2.22 - Privilege escalation	WebApps	PHP	Cristian \'void\' Giustini
2019-03-07			✓	Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit)	Remote	PHP	Metasploit
2019-02-25			✗	Drupal < 8.6.9 - REST Module Remote Code Execution	WebApps	PHP	leonjza
2019-02-23			✗	Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution	WebApps	PHP	Charles Fol
2018-04-30			✓	Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)	WebApps	PHP	SixP4ck3r
2018-04-25			✓	Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)	WebApps	PHP	Blaklis
2018-04-23			✗	Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure	WebApps	PHP	Larry W. Cashdollar
2018-04-17			✓	Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)	Remote	PHP	José Ignacio Rojo
2018-04-13			✓	Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution	WebApps	PHP	Hans Topo & g0tmi1k
2018-04-13			✓	Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)	WebApps	PHP	Vitalii Rudnykh
2014-11-03			✗	Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)	WebApps	PHP	Stefan Horst
2017-03-09			✓	Drupal 7.x Module Services - Remote Code Execution	WebApps	PHP	Charles Fol

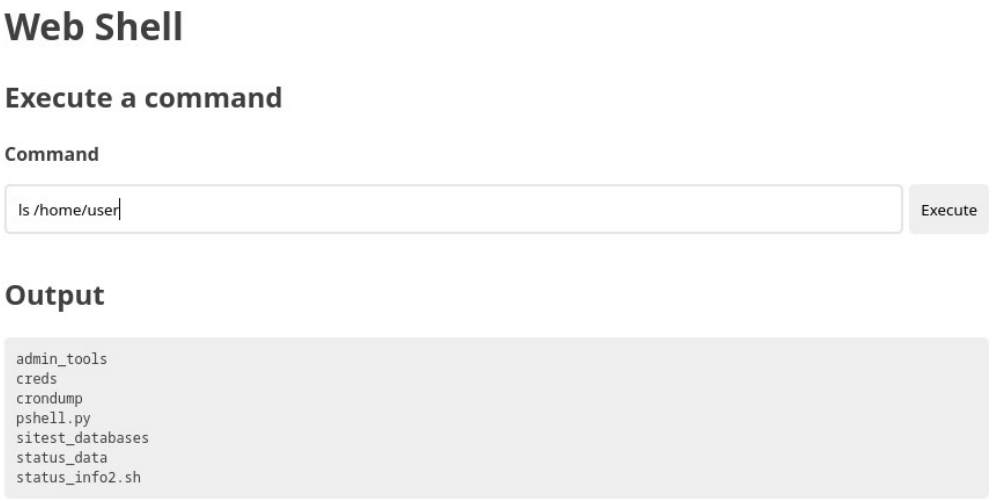
Drupalgeddon 2

- We’ve had an exploit for this vulnerability, so we’ve tried it immediately. We were able to launch reverse-shell on this site, so we were able to gain access to command prompt shell.
- In our example, we will use an exploit that creates a web shell

```
(venv) [vsevolodk@vk-ntb Workshop]$ python3 drupalgeddon2.py -t http://news.workshop.csc
Drupal Installation detected on the given target.

Look's like the target is running Drupal version: 8

Checking if the target is vulnerable...


Initial Vuln check on the target success. Target is vulnerable to mail.
Moving on with uploading the actual web shell...


Web Shell Payload uploaded successfully to http://news.workshop.csc/pwrJTcka.php
```

whoami

- We are user with restricted rights.
- But we can read files of a regular user



Privilege escalation through scripts

- In regular user home directory we found crondump file.
- This file contains record:
  - * * * * * /home/user/status_info2.sh
- Thus, a regular user runs a status_info2.sh script every minute.
- Let's look at this script

Privilege promotion through scripts

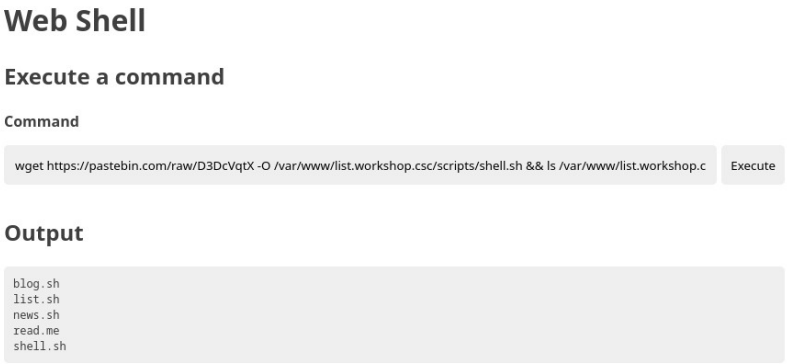
This script runs another scripts from **/var/www/list.workshop.csc/scripts**

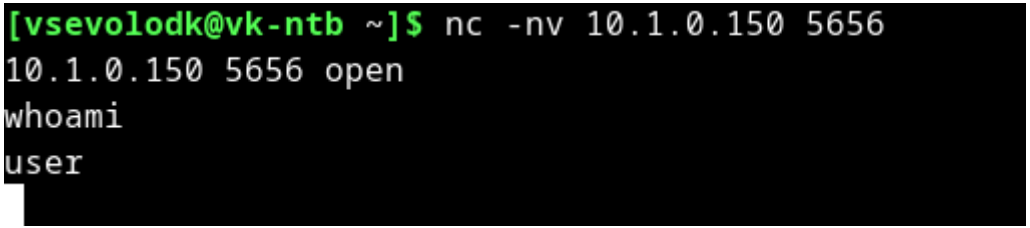
- And we can write scripts in this directory
- Congratulatuions! We can promote rights with bind or reverse shell in script.

Privilege escalation through scripts

Steps:

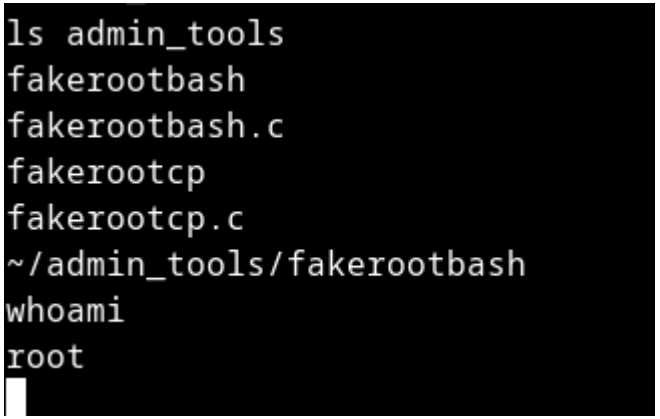
- Write server part of shell in any script in **/var/www/list.workshop.csc/** scripts
- Add rights to read script for all users
- Wait for one minute
- Run client





Road to root

- We are almost at the goal, it remains to elevate the rights to the administrator
- In user’s home directory we’ve found admin_tools folder.
- This folder contains some root executable files with suid flag
- Coool! Just run fakerootbash and…. We have root rights!



Practice

- Now try to gain root rights by yourself!
- Service IP: 5.252.22.41
- Files for practice: http://5.252.22.41/files
- Credentials:
  - Login: workshopmember
  - Pass: nullc0nworkshopuser