





Sharename	Type	Comment
-----	----	-----
print\$	Disk	Printer Drivers
helios	Disk	Helios personal share
anonymous	Disk	
IPC\$	IPC	IPC Service (Samba 4.5.16-Debian)

Reconnecting with SMB1 for workgroup listing.

Server	Comment
-----	-----
Workgroup	Master
-----	-----
WORKGROUP	SYMFONOS

Found SMB shares and a possible username named "Helios"

```
(root@CyberCreedPC)-[/home/sohamt/Downloads]
# smbclient //192.168.122.11/anonymous/
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D            0   Sat Jun 29 06:44:49 2019
..               D            0   Sat Jun 29 06:42:15 2019
attention.txt    N          154  Sat Jun 29 06:44:49 2019

19994224 blocks of size 1024. 17305072 blocks available
smb: \> get attention.txt
getting file \attention.txt of size 154 as attention.txt (50.1 KiloBytes/sec) (average 50.1 KiloBytes/sec)
smb: \> exit
```

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.

```
(root@CyberCreedPC)-[/home/sohamt/Downloads]  
# smbclient //192.168.122.11/helios/ -U Helios  
Password for [WORKGROUP\Helios]:  
Try "help" to get a list of possible commands.  
smb: \> ls  


|              |   |     |                          |
|--------------|---|-----|--------------------------|
| .            | D | 0   | Sat Jun 29 06:02:05 2019 |
| ..           | D | 0   | Sat Jun 29 06:07:04 2019 |
| research.txt | A | 432 | Sat Jun 29 06:02:05 2019 |
| todo.txt     | A | 52  | Sat Jun 29 06:02:05 2019 |

  
19994224 blocks of size 1024. 17305072 blocks available  
smb: \> get research.txt  
getting file \research.txt of size 432 as research.txt (84.4 KiloBytes/sec) (average 84.4 KiloBytes/sec)  
smb: \> get todo.txt  
getting file \todo.txt of size 52 as todo.txt (16.9 KiloBytes/sec) (average 59.1 KiloBytes/sec)  
smb: \> exit
```

got two more possible files and pass was "qwerty"

```
(sohamt@CyberCreedPC)-[~/Downloads]
```

```
$ cat research.txt
```

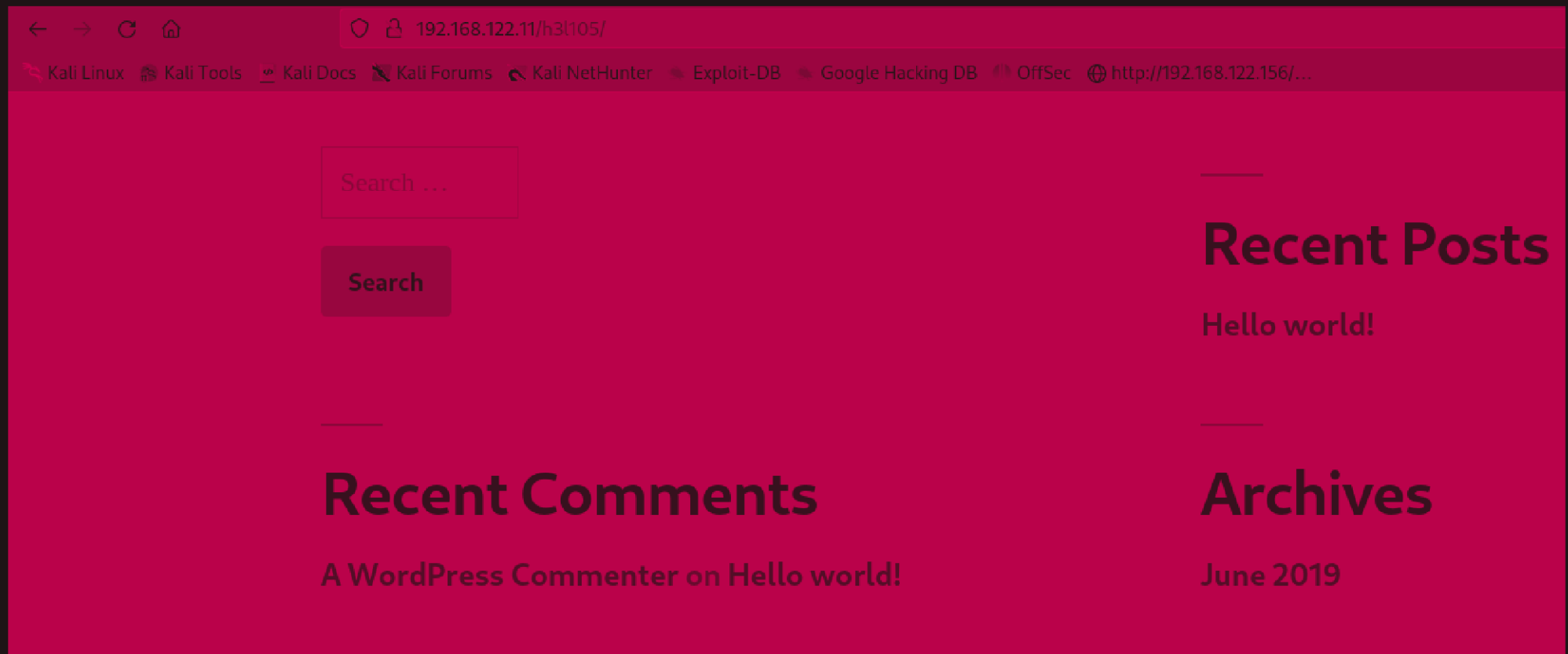
Helios (also Heliuss) was the god of the Sun in Greek mythology. He was thought to ride a golden chariot which brought the Sun across the skies each day from the east (Ethiopia) to the west (Hesperides) while at night he did the return journey in leisurely fashion lounging in a golden cup. The god was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

```
(sohamt@CyberCreedPC)-[~/Downloads]
```

```
$ cat todo.txt
```

1. Binge watch Dexter
2. Dance
3. Work on /h3l105

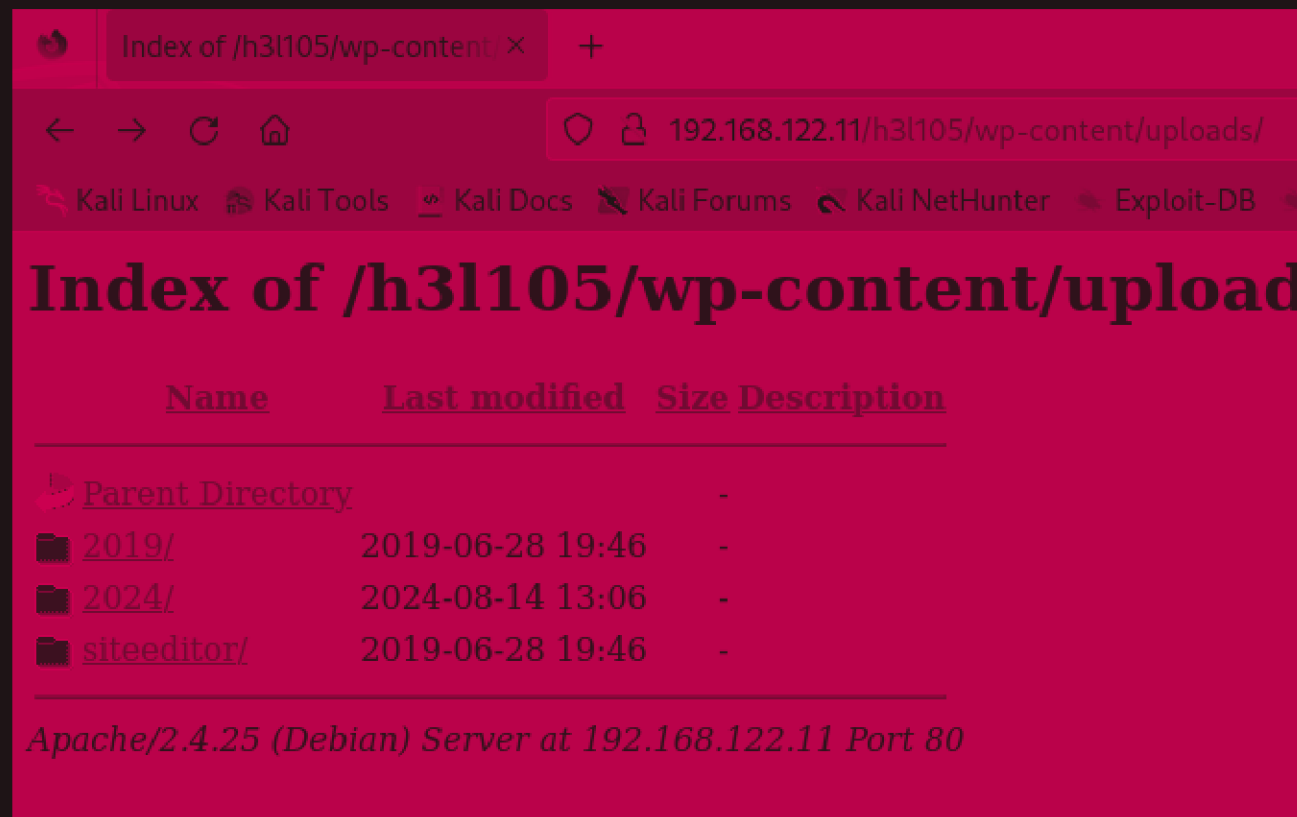
let's see /h3li05



got wordpress let's run wpscan.

```
[+] Upload directory has listing enabled: http://192.168.122.11/h3l105/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
```

found an uploads directory for local file inclusion.



The screenshot shows a web browser window with the address bar displaying `192.168.122.11/h3l105/wp-content/uploads/`. The page title is "Index of /h3l105/wp-content/upload". Below the title is a table with the following columns: Name, Last modified, Size, and Description. The table lists the following items:

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">2019/</a>	2019-06-28 19:46	-	
<a href="#">2024/</a>	2024-08-14 13:06	-	
<a href="#">siteeditor/</a>	2019-06-28 19:46	-	

At the bottom of the page, it says "Apache/2.4.25 (Debian) Server at 192.168.122.11 Port 80".

found this in uploads directory.....

EXPLOIT  
DATABASE

WordPress Plugin Site Editor 1.1.1 - Local File Inclusion

EDB-ID:

44340

CVE:

2018-7422

Author:

NICOLAS BUZY-DEBAT

Type:

WEBAPPS

Platform:

PHP

Date:

2018-03-23

EDB Verified: ✓

Exploit: [↓](#) / [{}  
View raw](#)

Vulnerable App: [📄  
View raw](#)

←

will be using this exploit.....









# WordPress Plugin Mail Masta 1.0 - Local File Inclusion

**EDB-ID:**

40290

**CVE:**

N/A

**Author:**

GUILLERMO GARCIA  
MARCOS

**Type:**

WEBAPPS

**EDB Verified:** ✓

**Exploit:** ⬇️ / {}

**Platform:**

PHP

**Date:**

2016-08-23

**Vulnerable App:** 📄











