

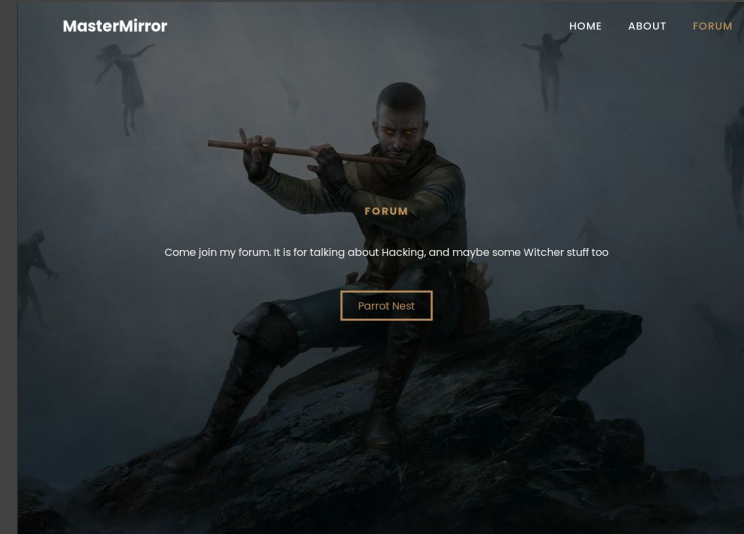
# >FORUM CTF

---

Challenge by Womenz Team for Originally for CyberSCI

## > whoami

- Emma
- Computer Science Student at Carleton U
- Past President and Current Technical Advisor of Carleton Cyber Security Club
- Created this challenge with the goal of doing something different
  - wanted to make something challenging but fun to explore





```
> cat scenario.txt
```

The admin of the forum Parrot's Nest, a forum for cybersecurity, and CD Projekt Red game enthusiasts is in way over his head.

Several of the users on the forum have pwned his server, and are discussing how they did it.

Figure out what has happened, and use this information to progress.

> cat background.txt



- **6 FLAGS:**

- Total of 110 points
- Flag format is:  
`TRYHARDER{md5sum}`
- Pay attention, they are hidden in plain sight.



```
> cat parts.txt
```

```
Flag 0 - Warm Up/Intro Flag - 10 points
```

```
Flag 1 - 10 points
```

```
Flag 2 - 10 points
```

```
Flag 3 - 10 points
```

```
Flag 4 - user flag - 20 points
```

```
Flag 5 - root flag - 30 points
```



```
> nmap -PS forum.ctf
```

```
Starting Nmap 7.80 ( https://nmap.org ) at home
```

```
PORT STATE SERVICE
```

```
22/tcp open  ssh
```

```
80/tcp open  http
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

```
> Port Scanning or Web Enumeration won't get you  
anywhere, the box is set up so everything you need  
is available.
```



```
> cat additional_info.txt
```

- This is an almost entirely “tool less” CTF
- There is only a few very basic tools that you need
  - strings, stego, other basic commands
- It is really easy to get side tracked



```
> cat bonus_hint.txt
```

- Information found earlier will be important later.
- All flags that you may find that are not in the format TRYHARDER{md5sum} are not part of this CTF
  - There are only a couple in initial static site



> Part 1: Finding Flag 1

---



```
> cat flag1/hint_1.txt
```

- There are only 3 threads that contain important information
  - What are they?
  - One is obvious, the other 2 are not.
- What is the username of the admin?
- Most of the posts were taken from r/Hacking
- Try to create a timeline of events that occurred (ie.start at the oldest thread)



```
> cat flag1/hint_2.txt
```

```
- QUACK QUACK QUACK
```



```
> cat flag1/hint_3.txt
```

- Text is embedded (and encrypted) in the images in a particular thread, not files
  - What tool does this??
    - Stegosuite

> Part 2: Finding Flag 2

---



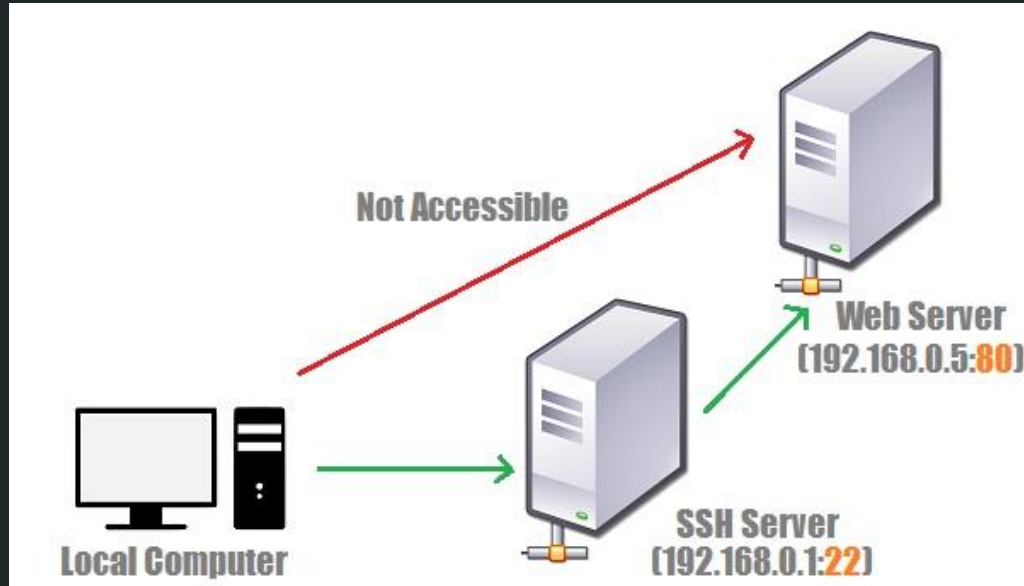
```
> cat flag2/hint_1.txt
```

- Thread with Last Post on 07-14-2020, 6:01 pm

# Flag 2: Hint 2:

(Just an example not the actual scenario)

ssh port forwarding: (try a normal ssh connection first)



# Proxying and Tunneling

## What is pivoting?

- Using a foothold to be able to move from place to place (host to host) within a compromised network

## What is port forwarding or tunneling?

- a technique that is used to allow external devices access to computers services on private networks
- does this by mapping an external port to an internal IP address and port



## Example of port forwarding:

How do you connect to a service running locally on a lab server, but that is blocked by a firewall?

- ie. httpd - port 80
- wget http://university.lab.remote - does not work
- You could run:

```
ssh shark@university.lab.remote  
//Once logged in:  
wget http://localhost
```

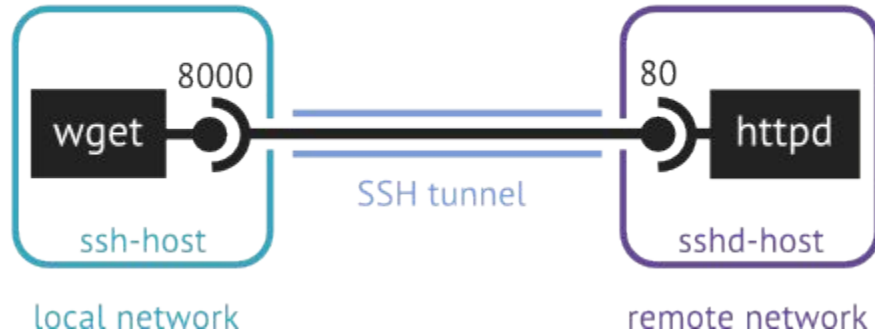
## Example of port forwarding:

How do you connect to a service running locally on a lab server, but that is blocked by a firewall?

Or to connect directly:

```
ssh -L 8888:localhost:80 shark@university.lab.remote  
//In a different window  
wget http://localhost:8888
```

```
ssh -L 8000:localhost:80 sshd-host
```



> Part 3: Finding Flag 3

---



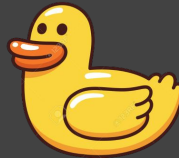
```
> cat flag3/hint_1.txt
```

Did you read the admin's Resume/Blog?

- What can this new information be used for that was mentioned earlier?

> cat flag3/hint\_2.txt

- Don't try and brute force the `admin` login for the BC Banking Tool, the password is not on any wordlist
- Look back to the time of the Rubber Ducks and recall the previous hint



A terminal window with a dark gray background and a light gray border. In the top right corner, there are three colored circles: yellow, green, and red. The terminal shows a command prompt and a command.

```
> cat flag3/hint_3.txt
```

- Check each BC Banking page carefully

## > Part 4: User Flag

---



```
> cat flag4/hint_1.txt
```

- See the about page (and replace RCE with cmd injection)





```
> cat flag4/hint_2.txt
```

On the vulnerable page:

- What tools might return the response shown?
  - Ie. cat, stat, head, tail, ...
- Try multiple files at a time
- How does the response change?
  - What might this suggest?



```
> cat flag4/hint_3.txt
```

- A captured packet is shown in the README, the "." are new lines
- What does the server do with it?
  - There is a line of code that parses it
- What is in the comments directly above that line?

## Extra:

- 40 Bonus Points to anyone who can exploit this in a different way than the way it is intended
- Extra Bonus Hints:
  - Backend: nodejs
  - All responses besides the my keys one are static
  - Uses exec with a 300 ms timeout, ie. If the command called takes longer than 300 ms to return it kills the process, and returns an error
  - If uses regex for input sanitization
  - The command must return a success status code in order for its output to be returned
  - There is a set list of allowed files that must be included in the request, but it only checks that at least one of them is in the request
  - The command executed by exec is: `stat [FILENAME]; cat [FILENAME];`

## > Part 5: Root Flag

---



```
> cat flag5/hint_1.txt
```

- The user is practicing for his oscp, what did he leave by accident?
- NOTE: \*\*Please don't touch the version in var\*\*

A terminal window with a dark gray background and a light gray border. In the top right corner, there are three colored circles: yellow, green, and red. The text is displayed in a monospaced font. The prompt character is green, while the command and list items are white.

> cat flag5/hint\_2.txt

- Search tar priv esc
- What are wildcards?
  - Can file names be used as parameters?



```
> cat flag5/hint_3.txt
```

- If you followed the white rabbit, then the answer you seek does not appear in the result of strings
- Try analysing the code with ghidra, or objdump

## Bonus:

Where did I mess up when doing this? There is one (I am aware of) huge mistake I made when I set this up.



> Solutions

---

> Forum CTF: Finding Flag 0

---

# WELCOME TO THE GAUNTER O'DIMM FANSITE

"ALL WHO HAVE LEARNED MY TRUE NAME ARE NOW EITHER DEAD OR HAVE MET AN EVEN WORSE FATE." - GAUNTER O'DIMM

Gaunter O'Dimm is a character from the Witcher 3.

[Learn More](#)

# Scroll to the bottom:

## Some great videos:

- [Witcher 3 - The Secret of Gaunter O'Dimm](#)
- [Who is Gaunter O'Dimm Really?](#)
- [Witcher 3 - Gaunter O'Dimm Strikes Again](#)

WITCHER 3

HEARTS OF STONE

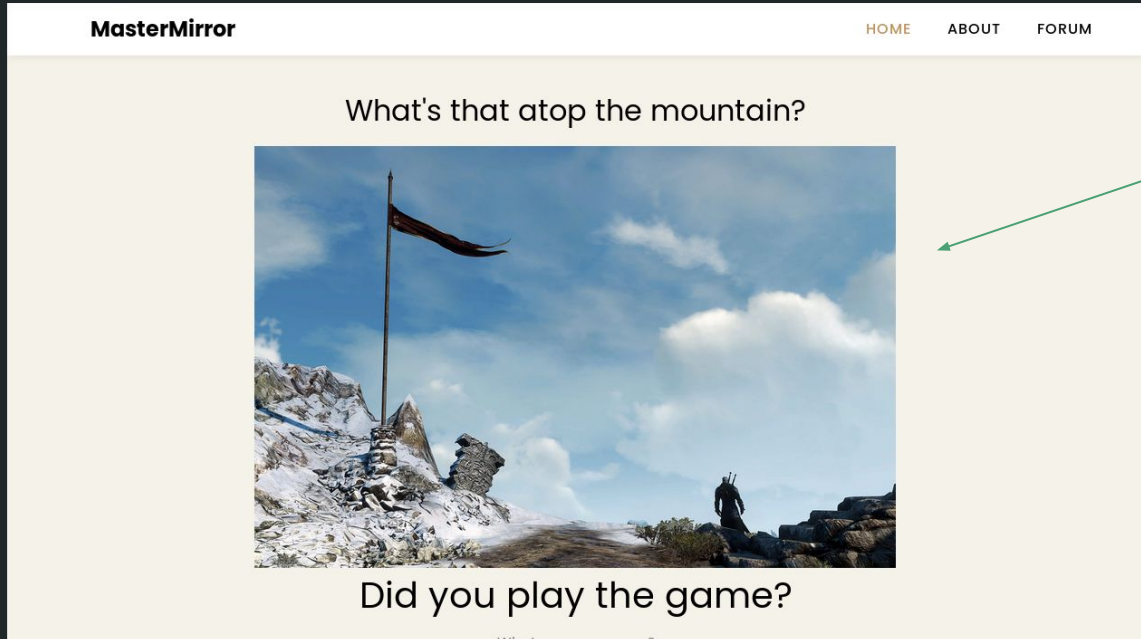
FLAG 0



## George Washington

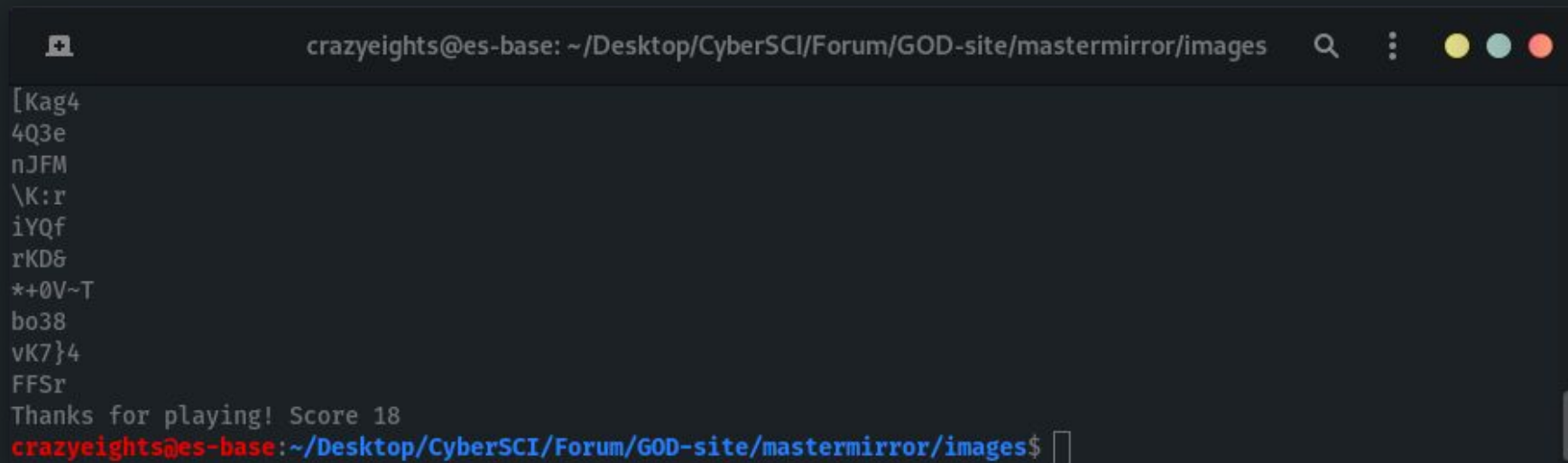
Lorem ipsum dolor sit amet, consectetur adipisicing elit. Ducimus itaque, autem necessitatibus voluptate quod mollitia delectus aut, sunt placeat nam vero culpa sapiente consectetur similique, inventore eos fugit cupiditate numquam!

# Download this image:



# Run strings on the image:

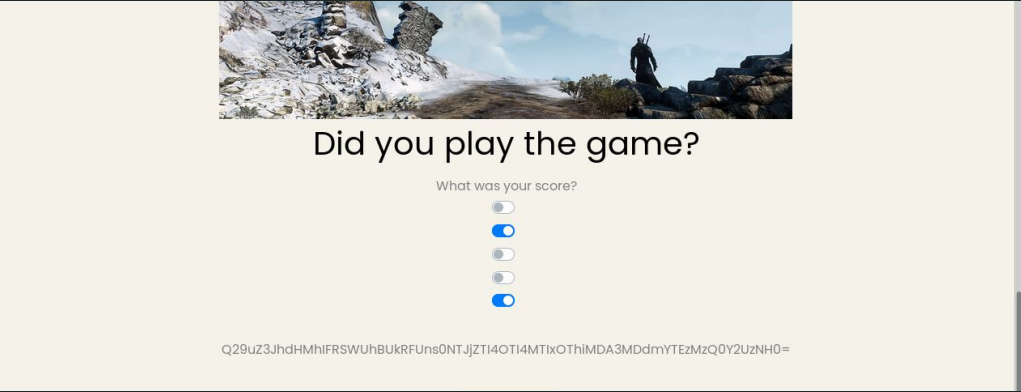
```
strings geralt_flag.jpg
```



```
crazyeights@es-base: ~/Desktop/CyberSCI/Forum/GOD-site/mastermirror/images
[Kag4
4Q3e
nJFM
\K:r
iYQf
rKD&
*+0V~T
bo38
vK7}4
FFSr
Thanks for playing! Score 18
crazyeights@es-base:~/Desktop/CyberSCI/Forum/GOD-site/mastermirror/images$
```

Go back to the page and answer the question "What was the score?":

- Score 18 - appears in the image source
- A switch: On - 1 , Off - 0
- A sequence of switches: binary
- 18 in binary = 00010010 or OFF ON OFF OFF ON (Least Significant Bit to Most Significant Bit)



The screenshot shows a web form with a light beige background. At the top, there is a rectangular image of a person in a dark, rocky landscape. Below the image, the text "Did you play the game?" is centered. Underneath this, the text "What was your score?" is centered. Below the text, there are five toggle switches arranged vertically. The second and fifth switches from the top are turned on (blue), while the first, third, and fourth are turned off (grey). At the bottom of the form, there is a long, alphanumeric string of text.

Did you play the game?

What was your score?

☐ ☒ ☐ ☐ ☒

Q29uz3JhdHMhIFRSWUhbUKRFUns0NTJjZTI4OTI4MTIxOTIhMDA3MDdmYTEzMzQ0Y2UzNH0=

# Decoding the Response:

Q29uZ3JhdHMhIFRSWUhBUkRFUns0NTJjZTI4OTI4MTIxOThiMDA3MDdmYTEzMzQ0Y2UzNH0=

Decode from Base64:

Congrats! TRYHARDER{452ce2892812198b00707fa13344ce34}

The screenshot shows the CyberChef web application interface. On the left is a sidebar with 'Operations' and 'Favourites' sections. The 'Favourites' section is expanded, showing a list of operations including 'To Base64', 'From Base64', 'To Hex', 'From Hex', 'To Hexdump', 'From Hexdump', 'URL Decode', 'Regular expression', 'Entropy', 'Fork', 'Magic', 'Data format', 'Encryption / Encoding', and 'Public Key'. The 'From Base64' operation is selected and highlighted in green. The 'Recipe' panel shows the 'From Base64' operation with a dropdown menu set to 'Alphabet A-Za-z0-9+/='. The 'Remove non-alphabet chars' checkbox is checked. The 'Input' panel shows the Base64 string 'Q29uZ3JhdHMhIFRSWUhBUkRFUns0NTJjZTI4OTI4MTIxOThiMDA3MDdmYTEzMzQ0Y2UzNH0=' with metadata: start: 70, end: 71, length: 1, lines: 1. The 'Output' panel shows the decoded result 'Congrats! TRYHARDER{452ce2892812198b00707fa13344ce34}' with metadata: start: 53, end: 53, length: 53, lines: 1, time: 7ms. At the bottom, there is a 'BAKE!' button and an 'Auto Bake' checkbox.



## Alternatively:

- You could decode the JS source
- It is in JSF\*CK
- There are sites that will do it for you



FIN.

---