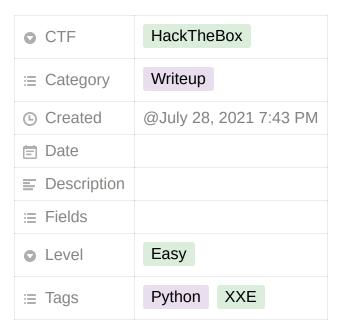


# **BountyHunter**



# Info

#### Credential

<u>Aa</u> User	<b>■</b> Password	=	Service	=	Note
<u>development</u>	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)

BountyHunter 1

```
<br/>
<br/>
<br/>
<br/>
<title>aa</title>
<br/>
<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)

BountyHunter 2