


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.

 **bumblebee.zip**  
83 KB

Download Files

Name	Date modified	Type	Size
access.log	26/04/2023 3:07	Text Document	193 KB
phpbb.sqlite3	26/04/2023 3:13	SQLITE3 File	1,020 KB

What was the username of the external contractor?

apoo1e	\$2y\$10\$Zdv/...	1682423286	apoo1e@contractor.net	312440918521
apoo1e1	\$2y\$10\$X6g4kRz1GjLcQh0t8t26f.qpatOQ...	1682424941	apoo1e1@contractor.net	365438717222

Task 1

What was the username of the external contractor?

apoo1e1

✓

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

50	0	2		0	10.255.254.2	1681827495	rsavage001	rsavage001
51	0	2		0	10.10.0.78	1682420899	apoo1e	apoo1e
52	0	2	000000000000v81mc...	0	10.10.0.78	1682424941	apoo1e1	apoo1e1

Task 2

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

10.10.0.78

✓

What is the post\_id of the malicious post that the contractor made?

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	po
1	1	1	2	2	0 10.255.254.2	1681296980	0	1	1	1	1	
2	2	1	2	50	0 10.255.254.2	1681832510	0	1	1	1	1	
3	9	2	2	52	0 10.10.0.78	1682425042	0	1	1	1	1	

**What is the post\_id of the malicious post that the contractor made?**

2

Copy the full post:

The screenshot shows the 'Data' menu in Microsoft Excel. The menu items are as follows:

- Use as Exact Filter
- Use in Filter Expression
- Edit Conditional Formats...
- Set to NULL (Alt+Del)
- Cut (Ctrl+X)
- Copy (Ctrl+C)
- Copy with Headers (Ctrl+Shift+C)
- Copy as SQL (Ctrl+Alt+C)
- Paste (Ctrl+V)
- Print... (Ctrl+P)

Task 4

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

`http://10.10.0.78/update.php` ✓

**What is the full URI that the credential stealer sends its data to?**



Bumblebee Page 2

```
C:\Users\Avior\Desktop\bumblebee
λ cat access.log | grep admin
10.255.254.2 - - [25/Apr/2023:12:46:08 +0100] "GET /adm/style/admin.css?assets_version=4 HTTP/1.1" 200 10308 "http://10.10.0.27/adm/index.php?i=acp_extensions&sid=041ca559047513b2267dfc066187582&mode=main&action=enable&ext_name=roxx%2Fdborldap&hash=f8bbcf4e" "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"
10.255.254.2 - - [25/Apr/2023:12:46:10 +0100] "GET /adm/style/admin.js?assets_version=4 HTTP/1.1" 200 2568 "http://10.10.0.27/adm/index.php?i=acp_extensions&sid=041ca559047513b2267dfc066187582&mode=main&action=list" "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"
10.10.0.78 - - [26/Apr/2023:11:53:12 +0100] "GET /adm/style/admin.css?assets_version=4 HTTP/1.1" 200 10308 "http://10.10.0.27/adm/index.php?i=acp_help_phpbb&mode=help_phpbb&sid=eca30c1b75dc3eed1720423aa1ff9577" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:12 +0100] "GET /adm/style/admin.js?assets_version=4 HTTP/1.1" 200 2568 "http://10.10.0.27/adm/index.php?i=acp_help_phpbb&mode=help_phpbb&sid=eca30c1b75dc3eed1720423aa1ff9577" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:13 +0100] "GET /adm/images/phpbb_logo.png HTTP/1.1" 200 6948 "http://10.10.0.27/adm/style/admin.css?assets_version=4" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:13 +0100] "GET /adm/images/innerbox_bg.gif HTTP/1.1" 200 2265 "http://10.10.0.27/adm/style/admin.css?assets_version=4" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:13 +0100] "GET /adm/images/arrow_right.gif HTTP/1.1" 200 331 "http://10.10.0.27/adm/style/admin.css?assets_version=4" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
```

26/Apr/2023:11:53:12 convert to UTC

Task 5
Hint

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

26/04/2023 10:53:12
☒

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

Table: phpbb_config			
Filter	config_name	config_value	is_dynamic
178	ldap_email		0
179	ldap_password	Passw0rd1	0
180	ldap_port		0
181	ldap_server	10.10.0.11	0
182	ldap_uid	sAMAccountName	0
183	ldap_user	CN=phpbb-...	0

Task 6

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

Passw0rd1
☒

What is the user agent of the Administrator user?

Table: phpbb_users									
Filter	user_id	user_type	group_id	user_permissions	user_perm_from	user_ip	user_regdate	username	username
1	2	1	0000000000g13yd...	0	1681296980	Anonymous	anonymous		
2	3	5		0	10.255.254.2	1681296980	admin	admin	

```
C:\Users\Avior\Desktop\bumblebee
λ cat access.log | grep admin
10.255.254.2 - - [25/Apr/2023:12:46:08 +0100] "GET /adm/style/admin.css?assets_version=4 HTTP/1.1" 200 10308 "http://10.10.0.27/adm/index.php?i=acp_extensions&sid=041ca559047513b2267dfc066187582&mode=main&action=enable&ext_name=roxx%2Fdborldap&hash=f8bbcf4e" "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"
10.255.254.2 - - [25/Apr/2023:12:46:10 +0100] "GET /adm/style/admin.js?assets_version=4 HTTP/1.1" 200 2568 "http://10.10.0.27/adm/index.php?i=acp_extensions&sid=041ca559047513b2267dfc066187582&mode=main&action=list" "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"
10.10.0.78 - - [26/Apr/2023:11:53:12 +0100] "GET /adm/style/admin.css?assets_version=4 HTTP/1.1" 200 10308 "http://10.10.0.27/adm/index.php?i=acp_help_phpbb&mode=help_phpbb&sid=eca30c1b75dc3eed1720423aa1ff9577" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:12 +0100] "GET /adm/style/admin.js?assets_version=4 HTTP/1.1" 200 2568 "http://10.10.0.27/adm/index.php?i=acp_help_phpbb&mode=help_phpbb&sid=eca30c1b75dc3eed1720423aa1ff9577" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:13 +0100] "GET /adm/images/phpbb_logo.png HTTP/1.1" 200 6948 "http://10.10.0.27/adm/style/admin.css?assets_version=4" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:13 +0100] "GET /adm/images/innerbox_bg.gif HTTP/1.1" 200 2265 "http://10.10.0.27/adm/style/admin.css?assets_version=4" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:13 +0100] "GET /adm/images/arrow_right.gif HTTP/1.1" 200 331 "http://10.10.0.27/adm/style/admin.css?assets_version=4" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
```



### What is the user agent of the Administrator user?

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



What time did the contractor add themselves to the Administrator group? (UTC)

```
C:\Users\Avior\Desktop\bumblebee
C:\at access.log | grep group
10.10.0.78 - - [26/Apr/2023:11:53:34 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff957781-acp_groups&icat=12&mode=manage HTTP/1.1" 200 3418 "http://10.10.0.27/adm/index.php?i=acp_users&sid=eca30c1b75dc3eed1720423aa1ff957781cat=12&mode=overview" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:37 +0100] "GET /adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff957781cat=12&mode=manage&action=list&g=5 HTTP/1.1" 200 3941 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff957781-acp_groups&icat=12&mode=manage" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:51 +0100] "POST /adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff957781cat=12&mode=manage&g=5 HTTP/1.1" 200 2623 "http://10.10.0.27/adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff957781cat=12&mode=manage&action=list&g=5" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:54 +0100] "GET /adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff957781cat=12&mode=manage&action=list&g=5 HTTP/1.1" 200 3966 "http://10.10.0.27/adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff957781cat=12&mode=manage&g=5" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:54:02 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff957781-25 HTTP/1.1" 200 3683 "http://10.10.0.27/adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff957781cat=12&mode=manage&g=5" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
```

26/Apr/2023:11:53:51 +0100 -> 26/04/2023 10:53:51 UTC

**What time did the contractor add themselves to the Administrator group? (UTC)**

26/04/2023 10:53:51



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

```
C:\Users\Avior\Desktop\bumblebee
C:\cat access.log | grep backup
10.10.0.78 - [26/Apr/2023:11:54:17 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95778i=acp_database&mode=backup HTTP/1.1" 200 3768 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95778i=25" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - [26/Apr/2023:11:54:22 +0100] "POST /adm/index.php?i=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95778i=mode=backup&action=download HTTP/1.1" 200 2463 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95778i=acp_database&mode=backup" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - [26/Apr/2023:11:54:24 +0100] "GET /adm/index.php?i=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95778i=mode=backup HTTP/1.1" 200 3771 "http://10.10.0.27/adm/index.php?i=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95778i=mode=backup&action=download" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - [26/Apr/2023:11:54:30 +0100] "POST /adm/index.php?i=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95778i=mode=backup&action=download HTTP/1.1" 200 2474 "http://10.10.0.27/adm/index.php?i=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95778i=mode=backup" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - [26/Apr/2023:11:56:28 +0100] "GET /adm/index.php?i=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95778i=mode=backup HTTP/1.1" 200 3770 "http://10.10.0.27/adm/index.php?i=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95778i=mode=backup&action=download" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - [26/Apr/2023:11:56:32 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95778i=acp_database&mode=restore HTTP/1.1" 200 3100 "http://10.10.0.27/adm/index.php?i=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95778i=mode=backup" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - [26/Apr/2023:11:57:07 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95778i=acp_database&mode=backup HTTP/1.1" 200 3770 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95778i=acp_logs&mode=admin" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - [26/Apr/2023:11:57:36 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95778i=21 HTTP/1.1" 200 3431 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95778i=acp_database&mode=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=eca30c1b75dc3eed1720423aa1ff95778i=acp_database&mode=backup HTTP/1.1" 200 3770 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95778i=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_dcsr7ip7fyijoyg8.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 /cup.php?mode=logout&sid=eca30c1b75dc3eed1720423aa1ff95778i=acp_database&mode=backup HTTP/1.1" 302 949 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95778i=acp_database&mode=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=be3cc6e2de08bafa4044f552813ec2be HTTP/1.1" 200 3796 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95778i=acp_database&mode=backup" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
```

[26/Apr/2023:12:01:38 +0100] -> 26/04/2023 11:01:38 UTC

**What time did the contractor download the database backup? (UTC)**

26/04/2023 11:01:38




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

```
php?id=eca30c1b75dc3eed1720423aa1ff9577&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_dcsr7lp7fyijoyq8.sql.gz HTTP/1.1" 200 [4707] "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) G
ecko/20100101 Firefox/112.0"
10.10.0.78 - [26/Apr/2023:12:01:52 +0100] "GET /ucp.php?mode=logout&id=eca30c1b75dc3eed1720423aa1ff9577 HTTP/1.1" 302 949 "http://10.10.27/adm/index.php?id=eca30c1b75dc3e
eed1720423aa1ff9577&i=acp_database&mode=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?id=be3cc6e2de08baf4a44f552813e2cbe HTTP/1.1" 200 3796 "http://10.10.27/adm/index.php?id=eca30c1b75dc3eed1720423
aa1ff9577&i=acp_database&mode=backup" Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
```

Task 10

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

34707



## Bumblebee has been Solved!

Congratulations  **4vior**, best of luck in capturing flags ahead!

<b>#2571</b>	<b>24 Jan 2025</b>	<b>RETIRED</b>
SHERLOCK RANK	SOLVE DATE	SHERLOCK STATE