Report on Broken Access Control: Insecure Direct Object Reference (IDOR)

Anuja Panchariya

Report on Broken Access Control: Insecure Direct Object Reference (IDOR)

Introduction

Broken Access Control is a critical security vulnerability that occurs when an application fails to enforce proper restrictions on authenticated users, allowing them to access data or perform actions beyond their authorized permissions. Insecure Direct Object References (IDOR) is a subset of this vulnerability where an application directly references an object, such as a file or database entry, without adequate access controls.

Details of the Vulnerability

During the assessment, an IDOR vulnerability was identified on the bWAPP application. This issue enables unauthorized modification of sensitive data or performance of actions through predictable or insecure object references. The findings are outlined below:

Steps Demonstrated

1. Selecting a Vulnerable Feature:
   The `Insecure DOR (Order Tickets)` functionality was chosen for testing.

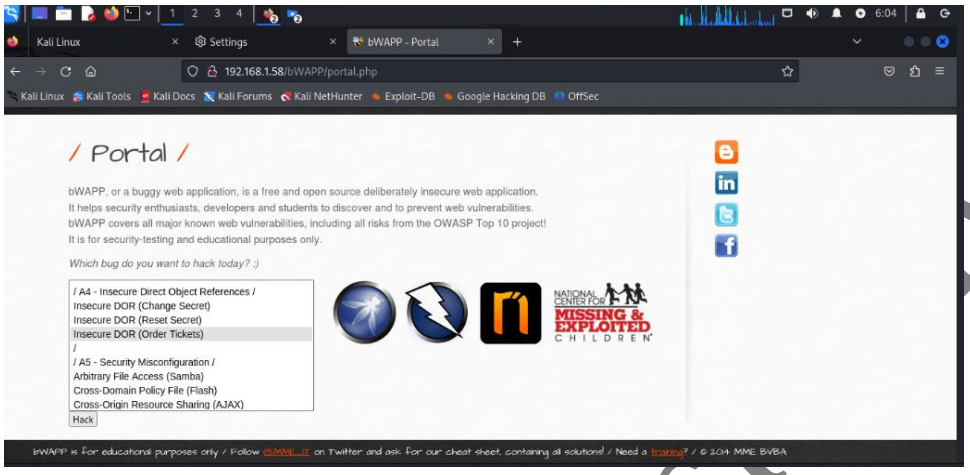
2. Performing the Exploit:
   a. Initially, 1 ticket was ordered through the application interface, resulting in a charge of 15 EUR.
   b. Using a web application testing tool, the HTTP request for the ticket purchase was intercepted and modified. The parameter responsible for the ticket quantity was altered to a higher value (e.g., 10).

3. Observing the Results: The application processed the request without validating user permissions or ensuring the integrity of the parameters. Consequently, 10 tickets were successfully ordered, bypassing the intended checks.

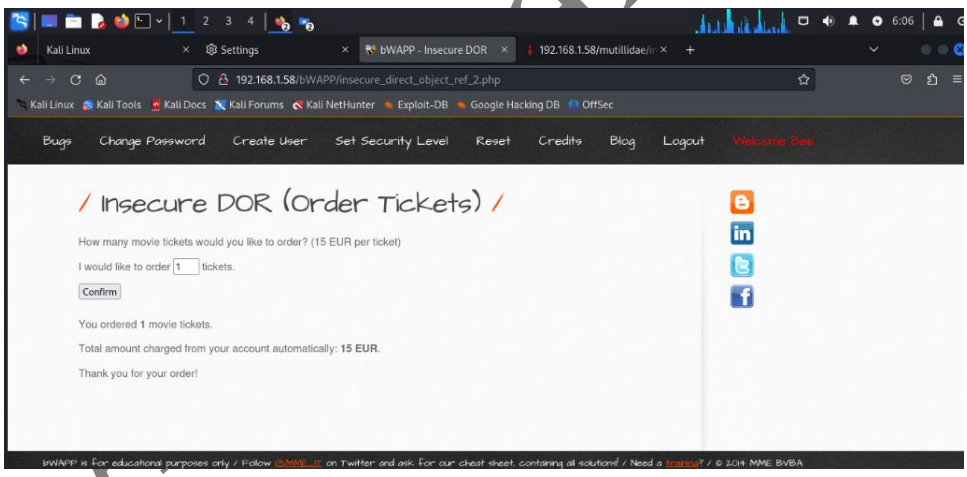
Evidence

Screenshots demonstrating the exploitation process are attached below.

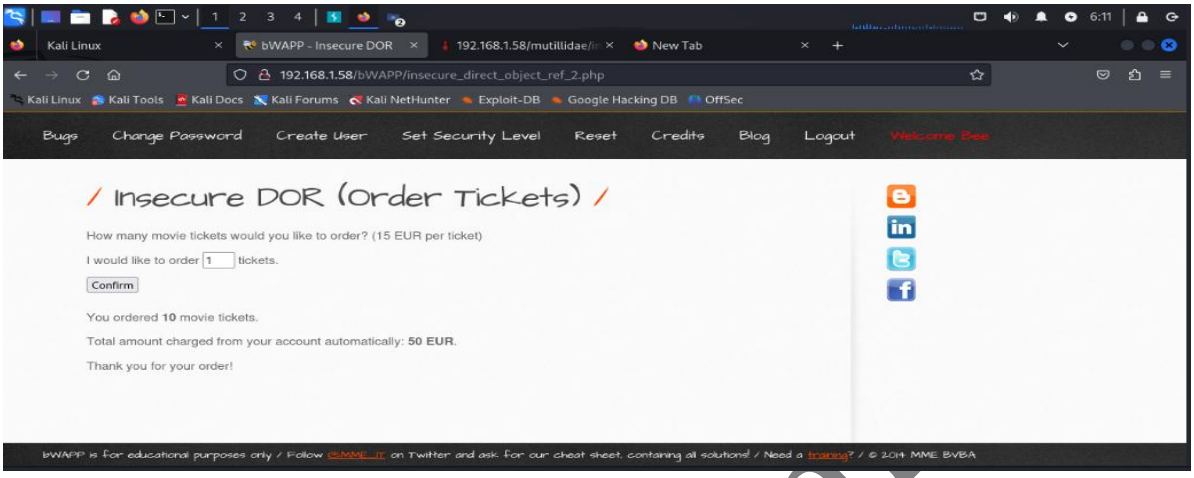
- GO TO bWAPP and select IDOR (Order Tickets)



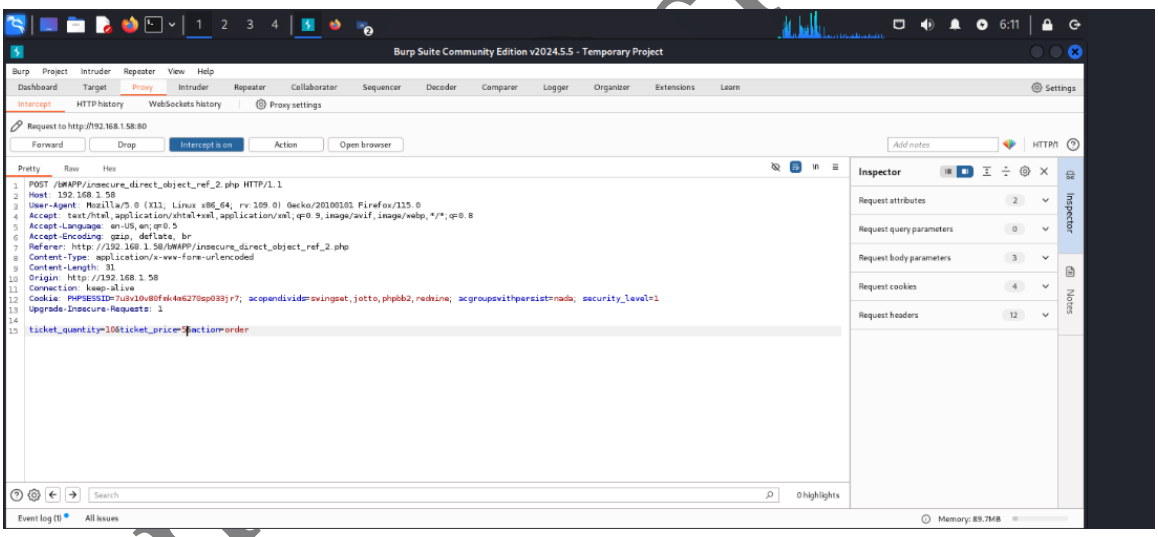
- Check the Tickets



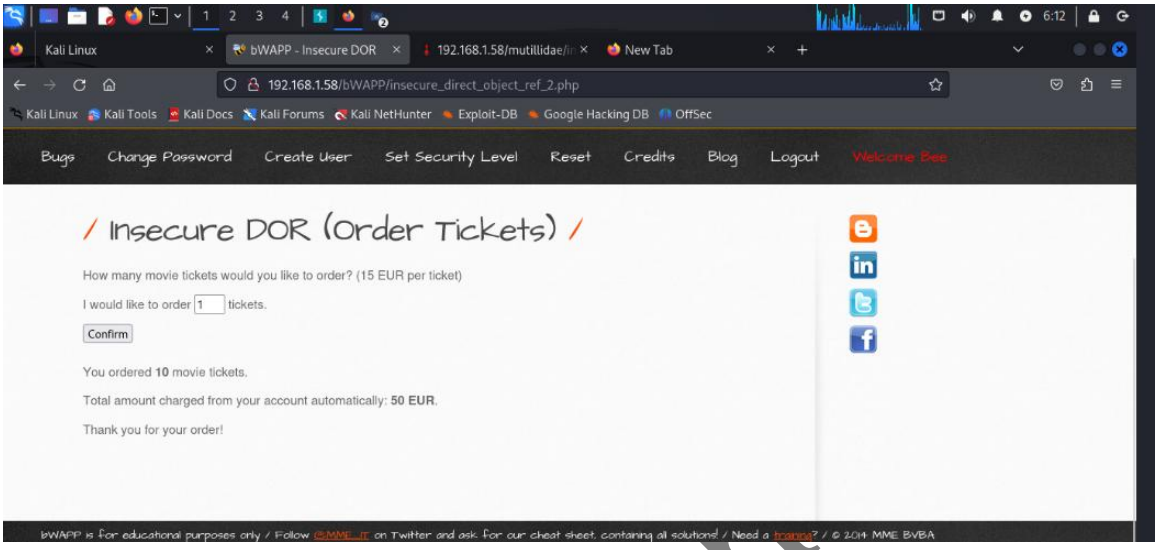
- It will reflect on the web page and10 tickets =50 EUR



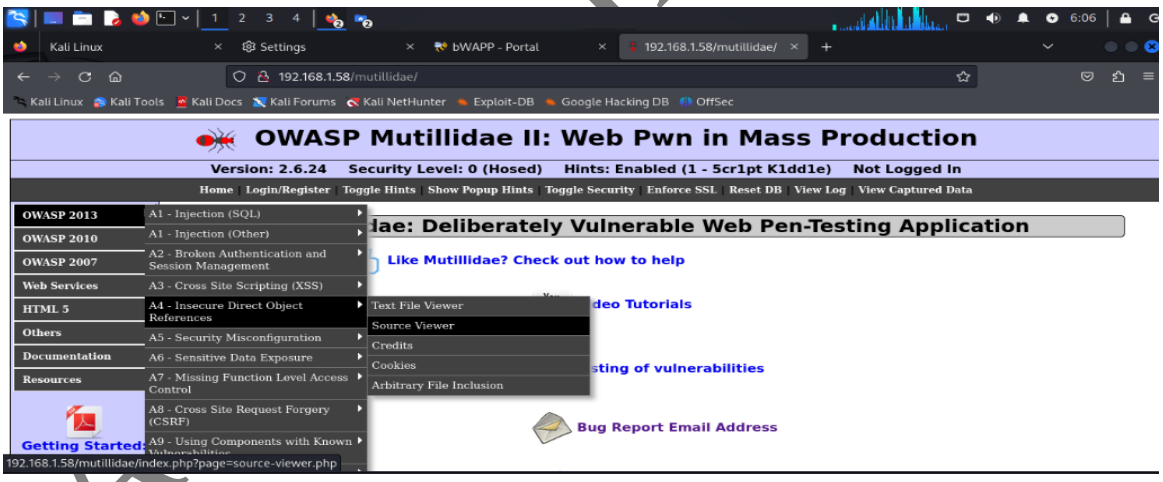
- Intercept the request and change the price tag



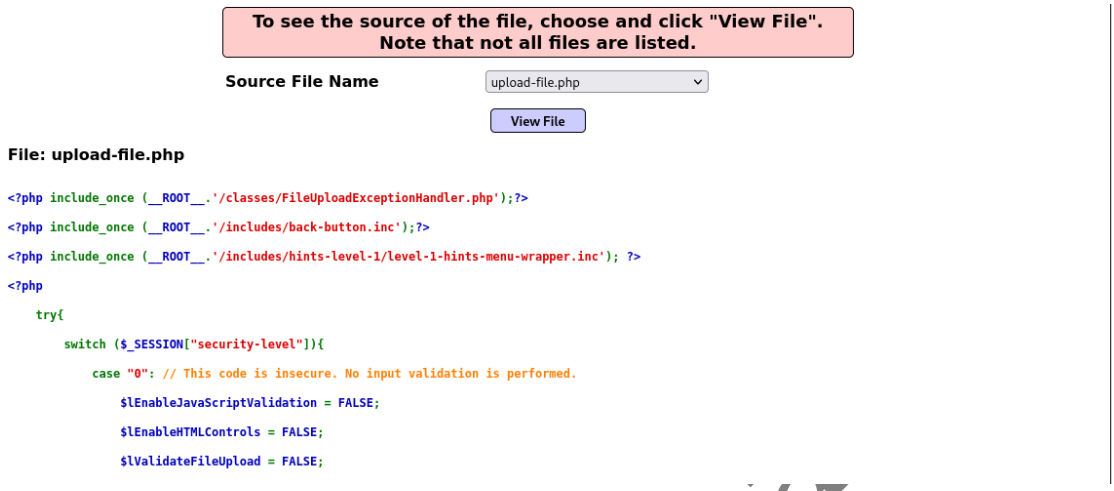
- It may reflect on webpage



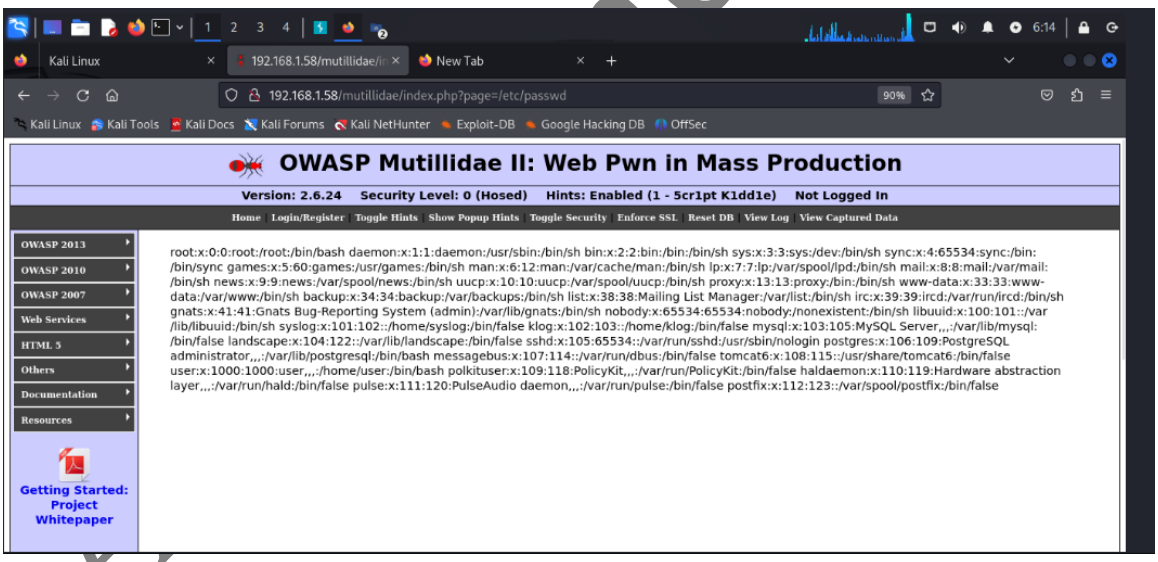
- Go to source viewer



- Open a file



- For viewing password , add /etc/passwd to URL



Conclusion

The presence of IDOR in the bWAPP application highlights the need for strict access control mechanisms. It is crucial to ensure proper validation of user permissions and parameter integrity to prevent unauthorized access or manipulation of data. This vulnerability can be mitigated by security practice.