

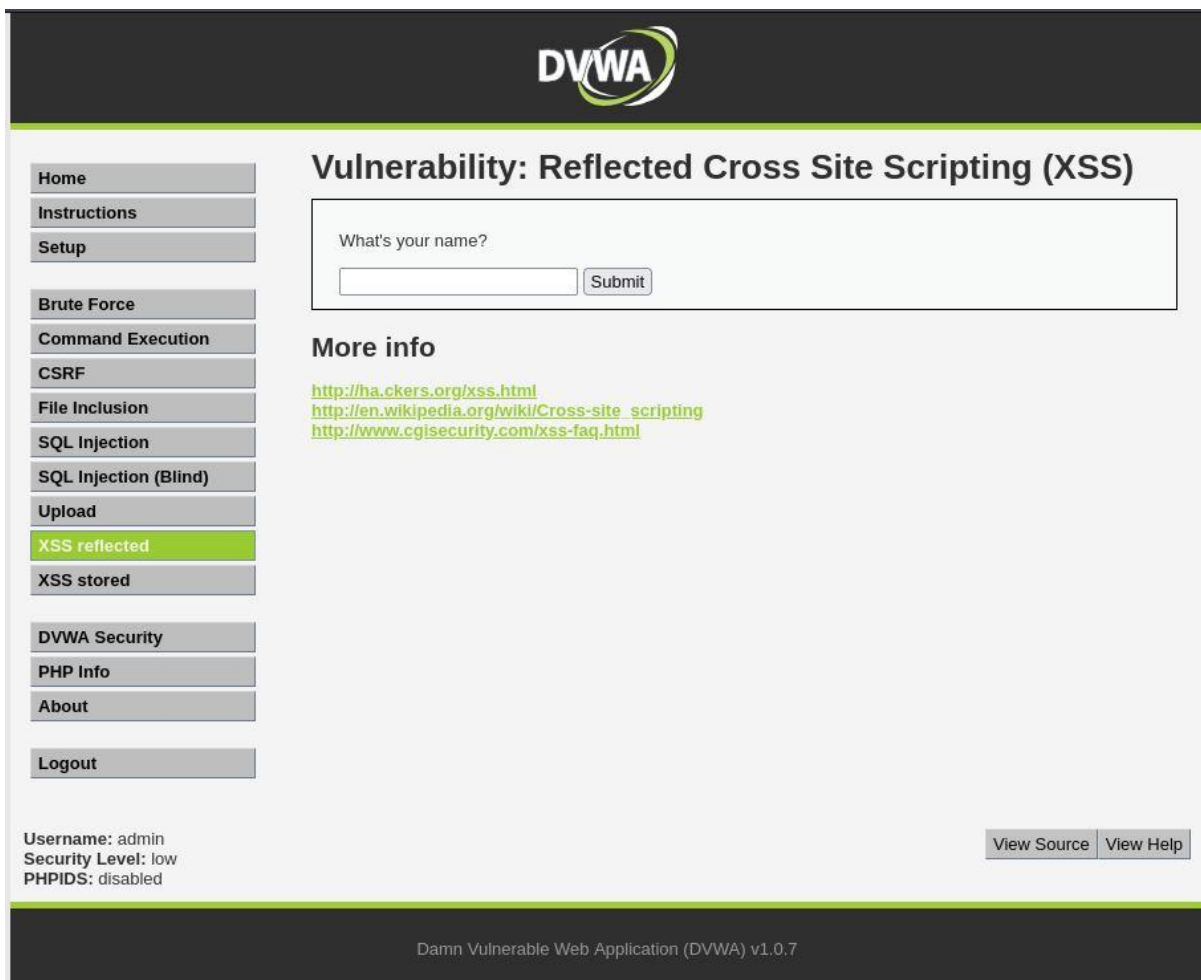
ESERCIZIO DI OGGI SPIEGAZIONE

1. Impostazione della DVWA:

Prima di tutto entro in dvwa con curl (IP meta), imposto la security su low e poi posso iniziare a sfruttare le vulnerabilità di XSS e SQL;

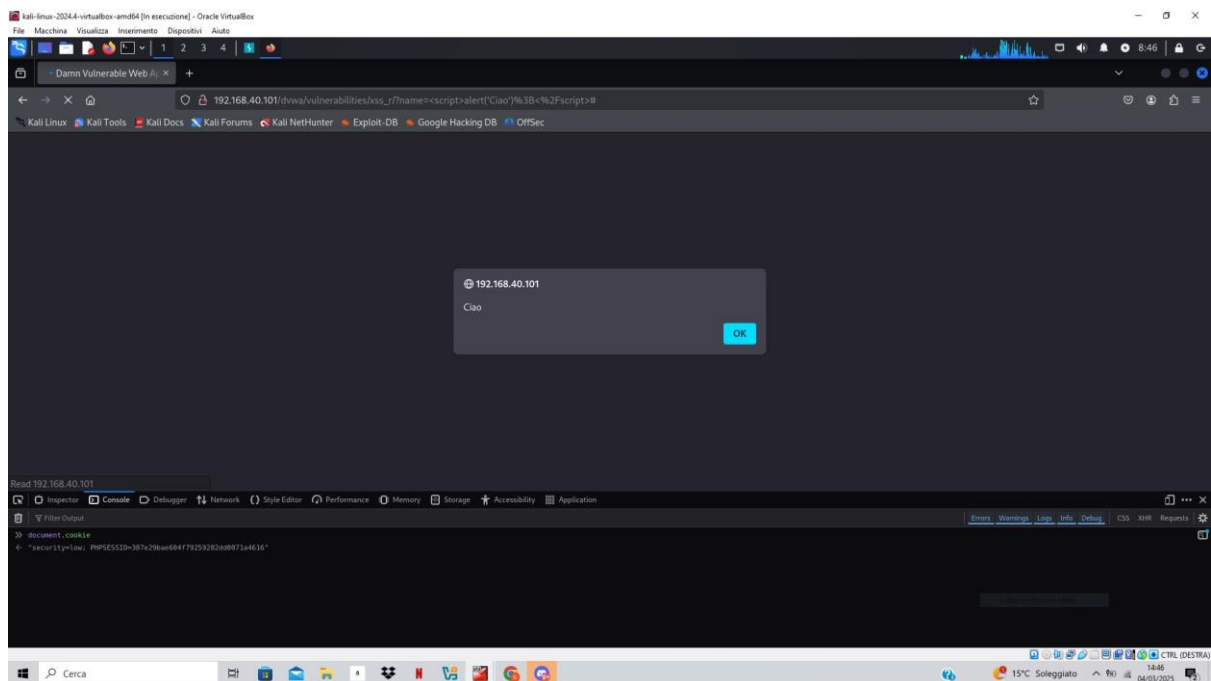
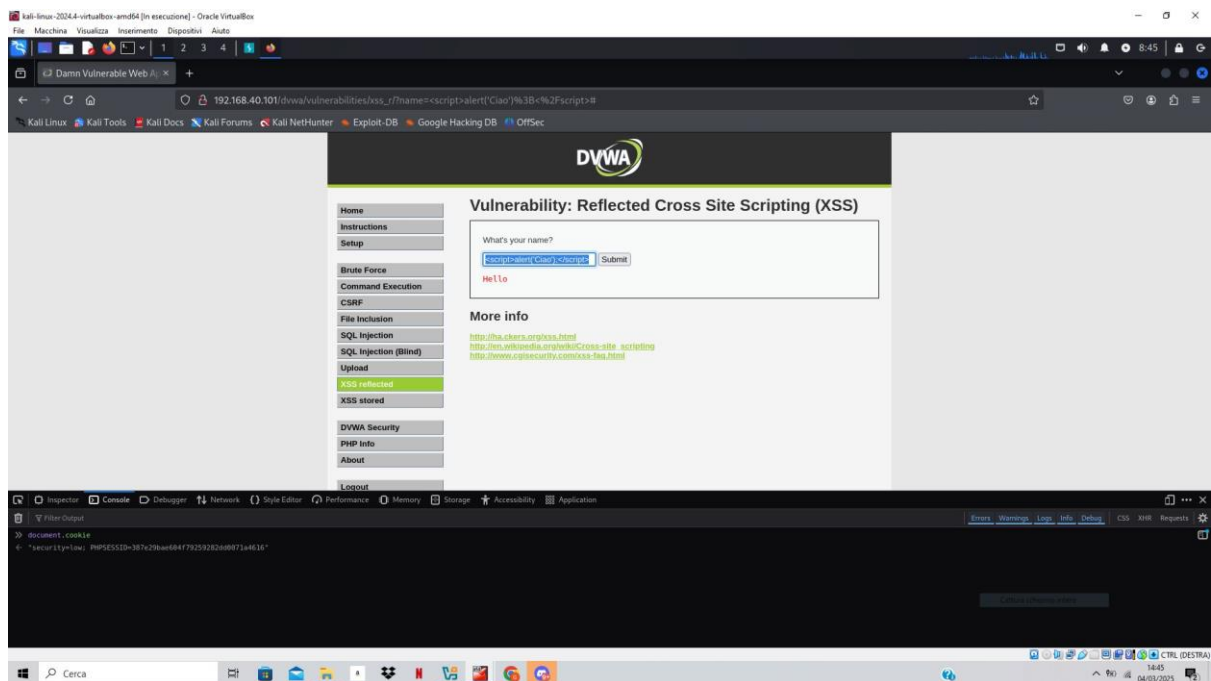
2. Sfruttamento delle Vulnerabilità

-XSS Reflected:



The screenshot displays the DVWA web application interface. At the top, the DVWA logo is visible. On the left side, there is a navigation menu with buttons for Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected (highlighted in green), XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled 'Vulnerability: Reflected Cross Site Scripting (XSS)'. It contains a form with the text 'What's your name?' and a 'Submit' button. Below the form, there is a 'More info' section with three links: <http://ha.ckers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>. At the bottom left, the status information shows 'Username: admin', 'Security Level: low', and 'PHPIDS: disabled'. At the bottom right, there are buttons for 'View Source' and 'View Help'. The footer at the very bottom reads 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

Qui posso preparare un link malevolo da inserire nel campo di input un payload XSS (<script>alert('Ciao');</script>) che poi le vittime potrebbero cliccare attivando il vettore di attacco;



-SQL Injection (Non Blind):



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection**
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

Vulnerability: SQL Injection

User ID:

Submit

More info

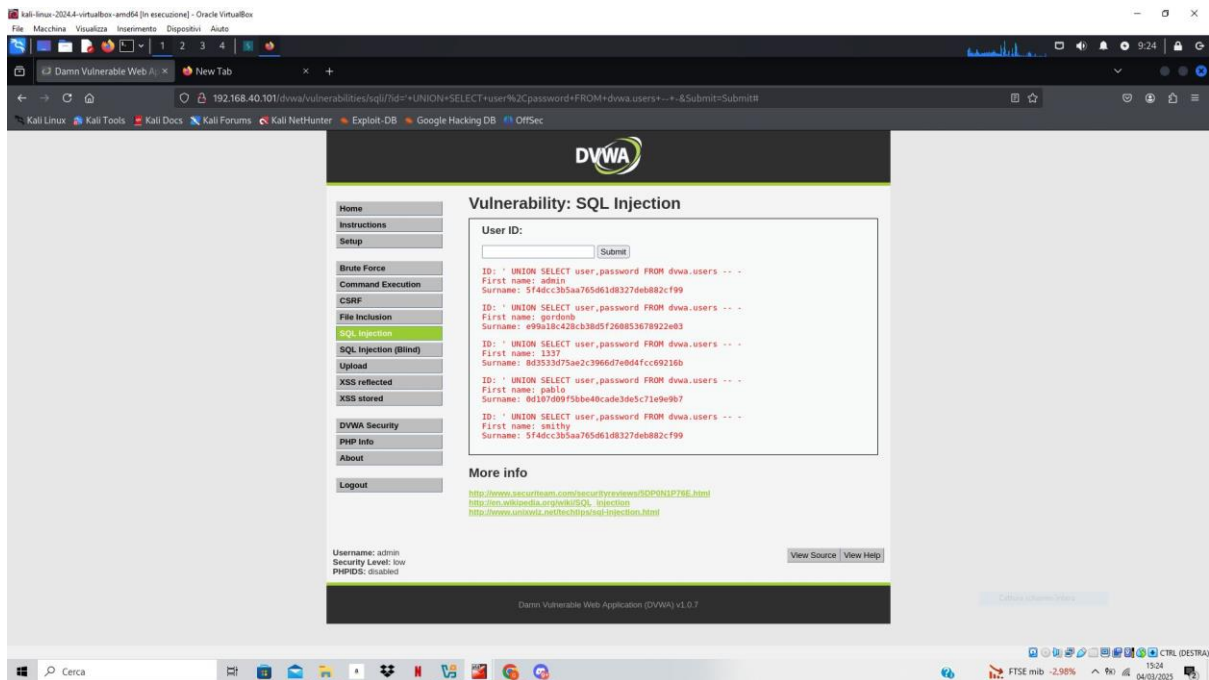
<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View Help](#)

Per sfruttare una SQL injection di questo tipo bisogna sapere quanti campi vengono selezionati dalla query vulnerabili. Possiamo dedurlo procedendo per tentativi: ' UNION SELECT null ... ' UNION SELECT null, null ... ' UNION SELECT null, null, null ... ;

[illegible]



Considerazioni su XSS Reflected

Si verifica quando un'applicazione web include dati non sanitizzati provenienti dall'input dell'utente nelle risposte HTTP. L'attaccante può iniettare script maligni che vengono eseguiti nel browser della vittima.

Se sfruttata con successo, un attaccante può rubare cookie, eseguire azioni a nome dell'utente. Il rischio aumenta quando la vulnerabilità si verifica in applicazioni web in cui gli utenti sono autenticati.

Considerazioni su SQL Injection (non blind)

La SQL Injection consente a un attaccante di manipolare le query SQL attraverso input mal formati. In modalità "non blind", l'applicazione restituisce direttamente i risultati della query, facilitando l'estrazione di informazioni sensibili. Con questa vulnerabilità, l'attaccante può ottenere accesso non autorizzato ai dati del database, eseguire comandi arbitrari o addirittura compromettere l'intera infrastruttura. È una delle vulnerabilità più critiche in quanto può portare a furto di dati, alterazioni o cancellazioni.