

SQL INJECTION BLIND E XSS STORED

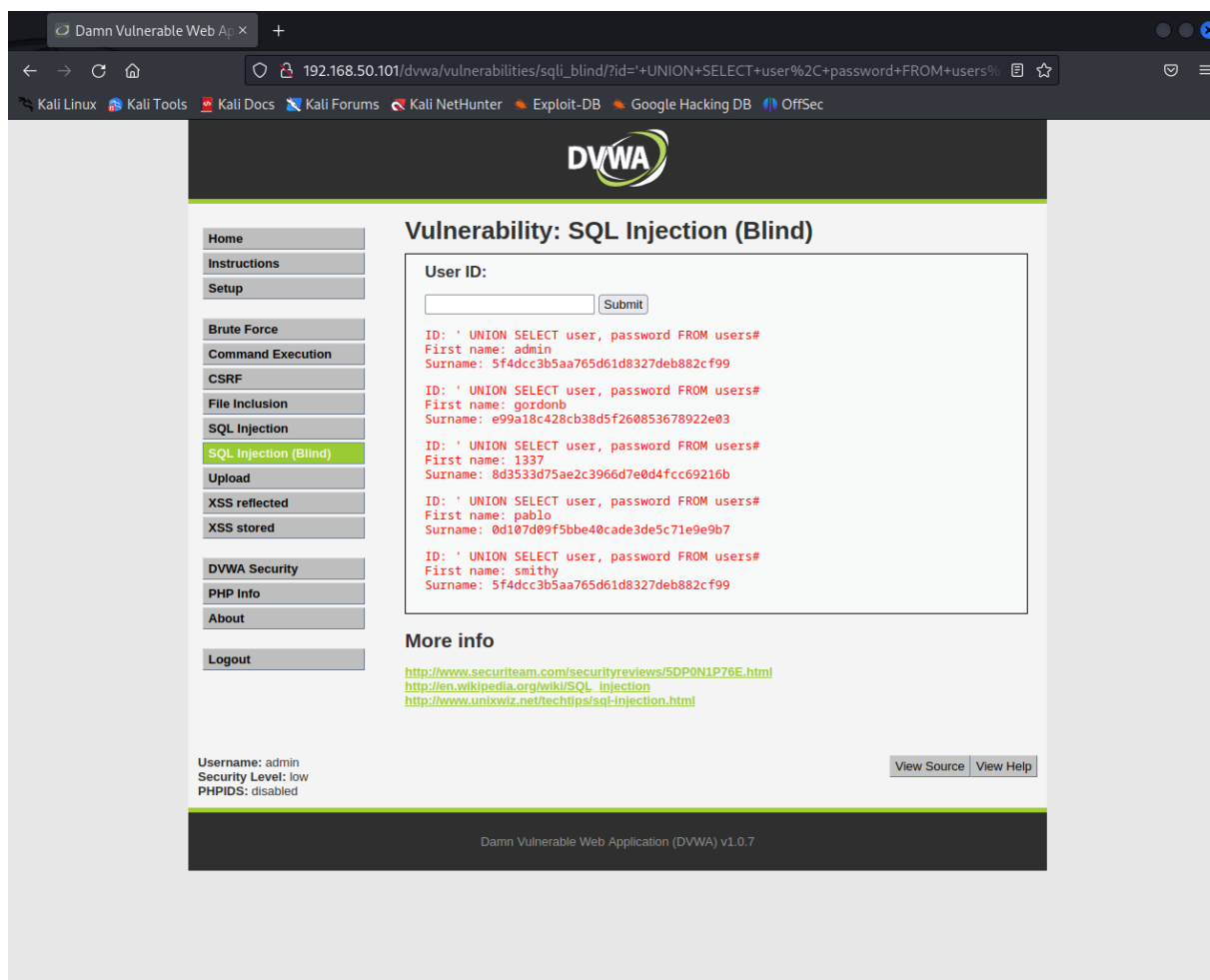
Con il report di oggi andremo a visualizzare come recuperare le password di un database attraverso l'exploitation di una SQL Injection Blind e come inviare i cookie di sessione delle vittime ad un web server dell'attaccante attraverso l'exploitation della XSS Stored su DVWA.

SQL INJECTION BLIND

La prima cosa che ho fatto è recarmi sulla DVWA di Metasploitable e selezionato come da traccia il livello LOW.

Dopodichè mi sono recato nella schermata relativa alla SQLi Blind ed ho applicato nel campo infetto la stringa in linguaggio SQL `` UNION SELECT user, password FROM users #` che mi è servita per unificare e contraddistinguere quindi gli user con le relative password come risposta dal server.

Possiamo notare la response nell'immagine sotto.

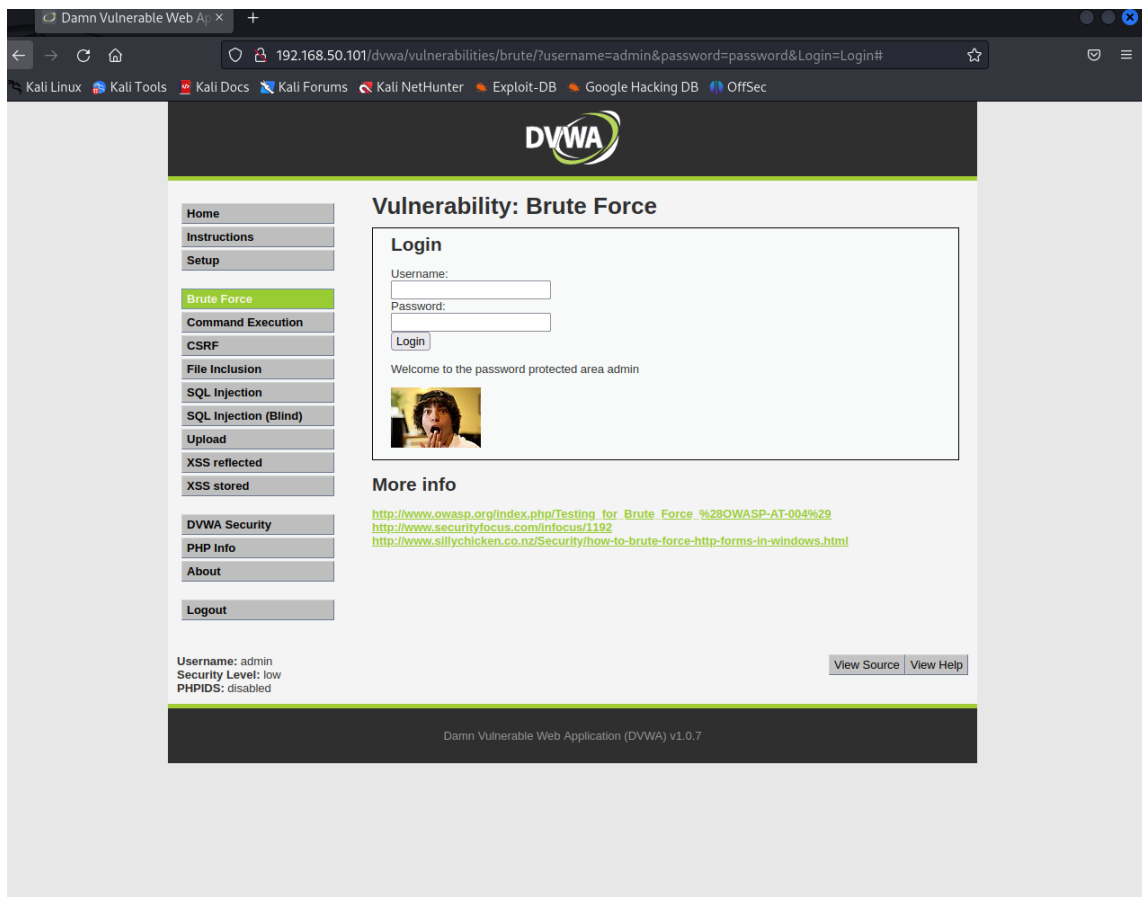


Subito dopo ho conservato tutte le password hashate in un unico file che chiamerò password ed attraverso l'utilizzo dello strumento **John The Ripper** ho richiesto con il comando `john -show -format=Raw-MD5 passwords.txt` che mi ha restituito come risultato la schermata seguente e quindi tutte le password richieste messe in ordine.

SQL INJECTION BLIND E XSS STORED



Per rendere l'evidenza della buona riuscita allego le varie log in con i vari users qui di seguito.



SQL INJECTION BLIND E XSS STORED

Damn Vulnerable Web A x +

192.168.50.101/dvwa/vulnerabilities/brute/?username=pablo&password=letmein&Login=Login#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

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


Username: admin
Security Level: low
PHPIDS: disabled

Vulnerability: Brute Force

Login

Username:
Password:

Welcome to the password protected area pablo



More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
<http://www.securityfocus.com/infocus/1192>
<http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

Damn Vulnerable Web Application (DVWA) v1.0.7

Damn Vulnerable Web A x +

192.168.50.101/dvwa/vulnerabilities/brute/?username=1337&password=charley&Login=Login#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

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


Username: admin
Security Level: low
PHPIDS: disabled

Vulnerability: Brute Force

Login

Username:
Password:

Welcome to the password protected area 1337



More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
<http://www.securityfocus.com/infocus/1192>
<http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

Damn Vulnerable Web Application (DVWA) v1.0.7

SQL INJECTION BLIND E XSS STORED

Damn Vulnerable Web A x +

192.168.50.101/dvwa/vulnerabilities/brute/?username=gordonb&password=abc123&Login=Login#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

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


Username: admin
Security Level: low
PHPIDS: disabled

Vulnerability: Brute Force

Login

Username:
Password:
Login

Welcome to the password protected area gordonb



More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
<http://www.securityfocus.com/infocus/1192>
<http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

Damn Vulnerable Web A x +

192.168.50.101/dvwa/vulnerabilities/brute/?username=smithy&password=password&Login=Login#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

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


Username: admin
Security Level: low
PHPIDS: disabled

Vulnerability: Brute Force

Login

Username:
Password:
Login

Welcome to the password protected area smithy



More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
<http://www.securityfocus.com/infocus/1192>
<http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

SQL INJECTION BLIND E XSS STORED

Per quanto riguarda la **XSS Stored** sono riuscito con uno script molto semplice a far venire fuori il pop up “STORED” ed a renderlo fisso con qualsiasi browser si collegasse allo stesso URL da un solo client, mentre non sono riuscito ad inviare come richiesto da traccia ad un webserver il cookie di sessione prelevandolo dall’exploit.

Lo script inserito è il seguente `<script>alert ("Stored")</script>`

Qui di seguito la dimostrazione, nella prima foto operavo con Firefox nella seconda con Chromium sempre dallo stesso client che in questo caso era Kali.

