

## Report Cracking Password

Per crackare delle password cryptate possiamo andare a utilizzare vari tool già preimpostati su kali, oggi abbiamo utilizzato Jack the Ripper per decryptare le password trovate nel database del dvwa di metasploitable. Le password erano cryptate in HASH e quello che abbiamo fatto è:

```
(root@kali)-[~]
# john --format=raw-MD5 /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8
x3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 12 candidates buffered for the current salt, minimum 24 needed
for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (admin)
password      (smithy)
abc123 come,  (gordonb)
letmein       (pablo)
Proceeding with incremental:ASCII
charley       (1337)
5g 0:00:00:00 DONE 3/3 (2024-02-28 08:58) 13.51g/s 492610p/s 492610c/s 539097
C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passw
ords reliably
```

Creare prima di tutto un file "hash.txt" con all'interno tutte le password in formato hash con il corrispondente nome utente, (user:password).

Successivamente andiamo a utilizzare un comando che ci consente di decryptarle per averle in chiaro, il comando è **john --format=raw-MD5** dove MD5 è il formato di decryptazione che utilizziamo.

Come possiamo vedere tutte e 5 le password sono state trovate e adesso proviamo ad accedere al DVWA di metasploitable usando un altro account con la password che abbiamo appena trovato, e come vediamo:



Username

Password

Login

192.168.49.102/dvwa/index.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Damn Vulnerable Web...

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

## Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

### WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

### Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

### General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

E siamo dentro!