

S6 L3

Svolgimento Esercizio

Giulia Salani

Consegna

Traccia: password cracking

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate ieri.

Nella lezione pratica di ieri, abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB come visto ieri, e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro. Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica.

John the Ripper: definizione

John the Ripper è un popolare software open-source utilizzato per testare la sicurezza delle password in sistemi Unix e simili.

Fornisce strumenti per craccare password con vari metodi, come l'attacco a dizionario e la forza bruta. È altamente configurabile e può gestire una vasta gamma di algoritmi di hash. Può eseguire attacchi a dizionario, tentando combinazioni di parole e stringhe comuni per trovare corrispondenze con password hash.

Nello specifico, per l'esercizio di oggi, John the Ripper è un valido strumento per craccare password MD5 perché è progettato per eseguire attacchi sofisticati contro vari tipi di hash, inclusi gli hash MD5; può testare rapidamente una vasta gamma di possibili combinazioni di password, confrontandole con gli hash MD5 forniti.

John the Ripper: esecuzione

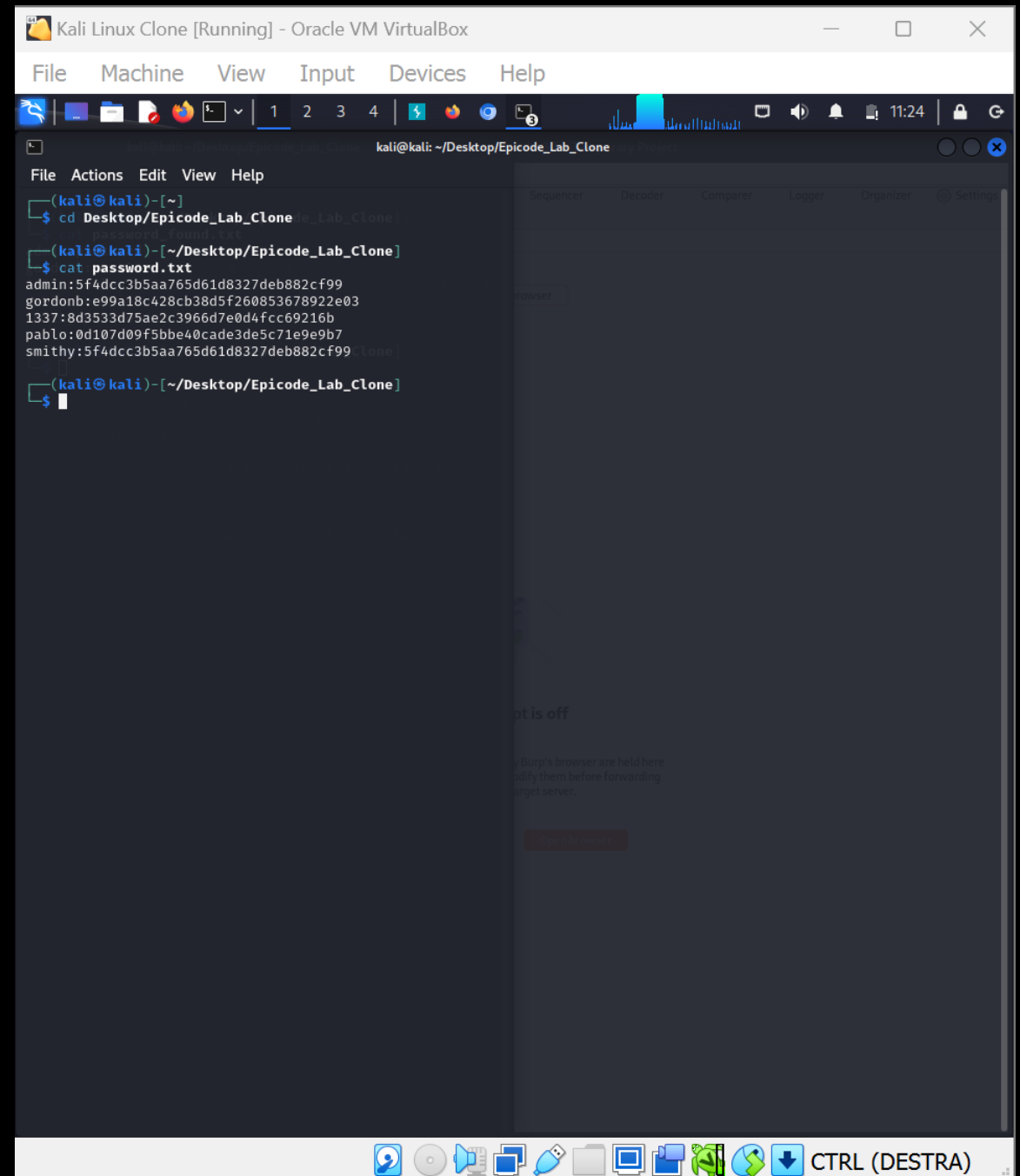
Durante l'esercizio di ieri abbiamo già recuperato 5 password hash con relativo nome utente (in realtà, a ben guardare gli hash, ci sono due utenti che hanno la stessa password).

Creeremo dunque due file che daremo in pasto a John the Ripper: il file con le password hash recuperate tramite SQL injection e una wordlist con cui John the Ripper possa confrontarle.

Recuperate le password «in chiaro», tenteremo il login alla pagina DVWA per verificarne la correttezza.

Spostiamoci nella Directory in cui vogliamo lavorare e creiamo un semplice file di testo dove incollare le password hash trovati ieri.

Le password saranno precedute dallo user e i due punti, senza spazi.



The screenshot shows a Kali Linux virtual machine running in Oracle VM VirtualBox. The window title is "Kali Linux Clone [Running] - Oracle VM VirtualBox". The menu bar includes File, Machine, View, Input, Devices, and Help. The top toolbar shows various icons for file operations and system status, with a system clock displaying 11:24. The main area is a terminal window titled "kali@kali: ~/Desktop/Epicode_Lab_Clone". The terminal shows the following commands and output:

```
(kali@kali)-[~]  
$ cd Desktop/Epicode_Lab_Clone  
$ cat password.txt  
admin:5f4dcc3b5aa765d61d8327deb882cf99  
gordonb:e99a18c428cb38d5f260853678922e03  
1337:8d3533d75ae2c3966d7e0d4fcc69216b  
pablo:0d107d09f5bbe40cade3de5c71e9e9b7  
smithy:5f4dcc3b5aa765d61d8327deb882cf99  
(kali@kali)-[~/Desktop/Epicode_Lab_Clone]  
$
```

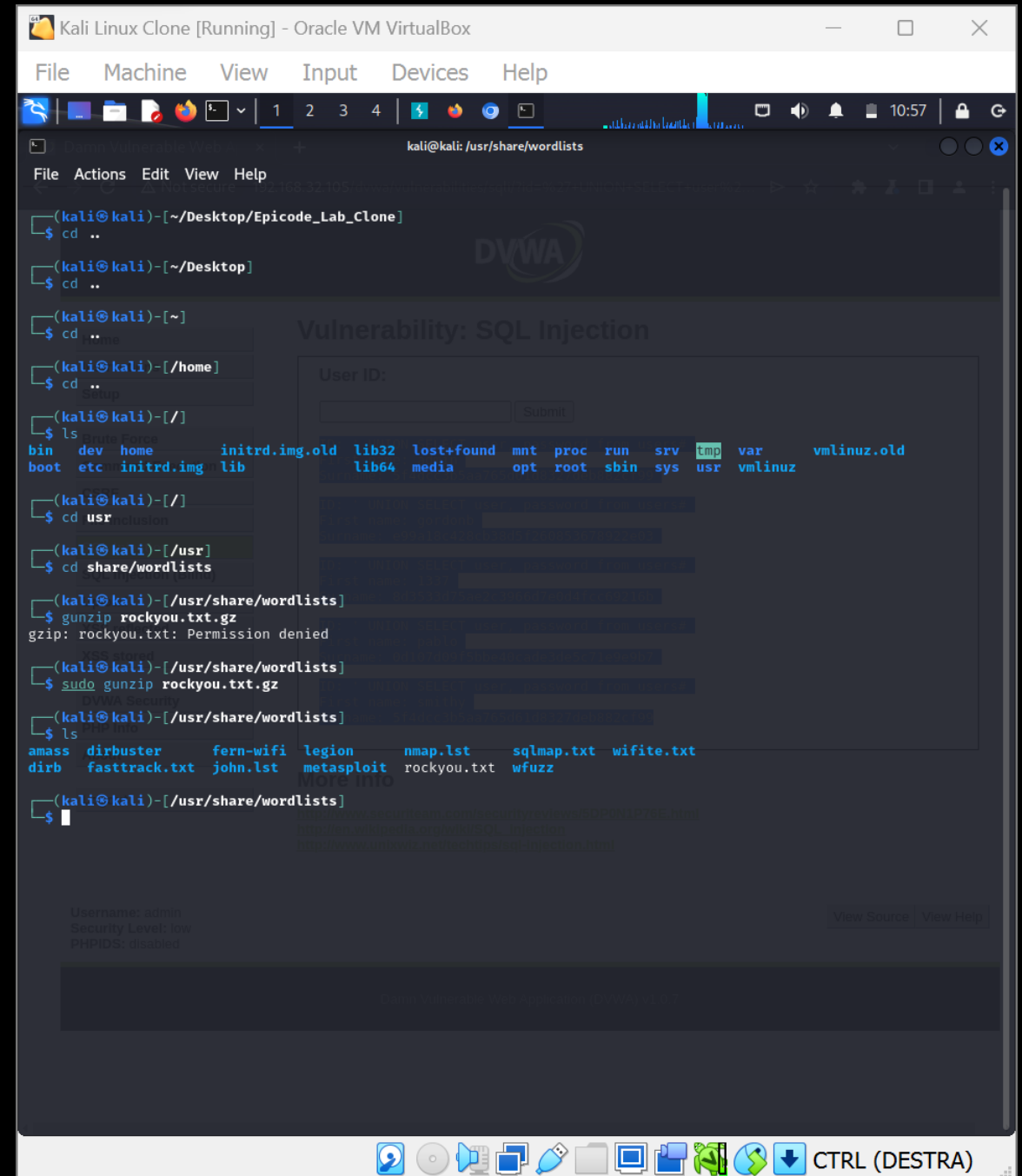
To the right of the terminal, a portion of the Burp Suite application is visible, showing tabs for Sequencer, Decoder, Comparer, Logger, Organizer, and Settings. The main workspace of Burp Suite is currently empty.

Il secondo file da dare in pasto a John the Ripper è già presente in Kali, al percorso `/usr/share/wordlists`.

`rockyou.txt` è una delle liste di parole o "wordlist" più popolari utilizzate per testare la sicurezza delle password. Deriva da un database di breach chiamato RockYou, che è stato compromesso nel 2009. La lista contiene milioni di password, rendendola utile per attacchi di forza bruta e altre analisi di sicurezza.

Dall'estensione deduciamo che il file è stato compresso con gzip, quindi lo estraiamo grazie al comando **`gunzip rockyou.txt.gz`**.

A questo punto possiamo lavorare con John the Ripper.

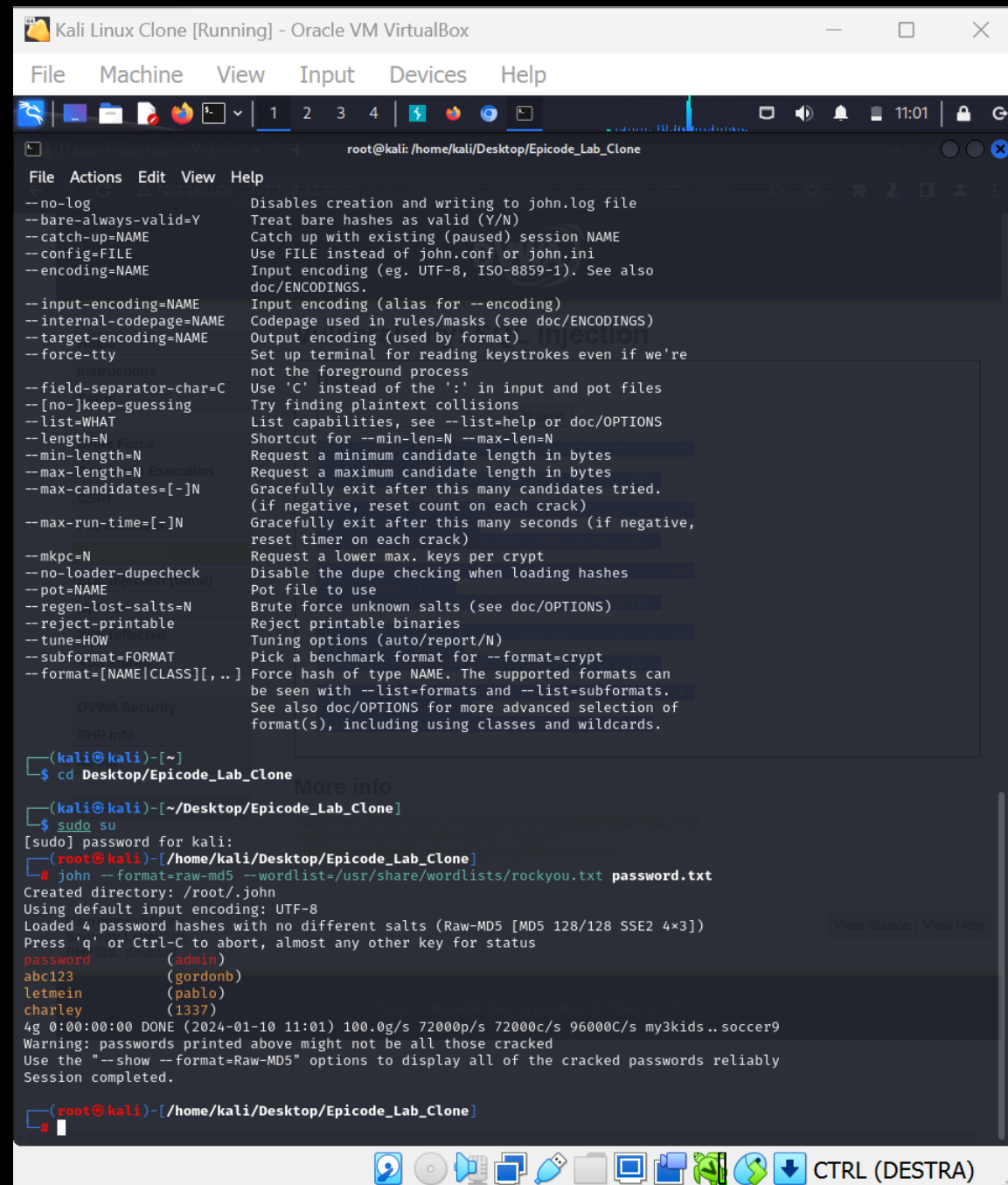


Eseguiamo il comando: **john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt password.txt**

Tale comando specifica il formato dell'hash come "raw-md5", dopodiché utilizza la wordlist rockyou.txt situata nel percorso specificato per tentare di craccare le password contenute nel file password.txt.

Nello specifico, John the Ripper cercherà corrispondenze fra gli hash MD5 delle password nel file password.txt e quelli presenti nella wordlist rockyou.txt, fornendo così le password in chiaro trovate.

Recuperate le pwd, proviamo a fare il login su DVWA con ciascuna coppia user/pwd trovata.



```
Kali Linux Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Desktop/Epicode_Lab_Clone
File Actions Edit View Help
--no-log Disables creation and writing to john.log file
--bare-always-valid=Y Treat bare hashes as valid (Y/N)
--catch-up=NAME Catch up with existing (paused) session NAME
--config=FILE Use FILE instead of john.conf or john.ini
--encoding=NAME Input encoding (eg. UTF-8, ISO-8859-1). See also doc/ENCODINGS.
--input-encoding=NAME Input encoding (alias for --encoding)
--internal-codepage=NAME Codepage used in rules/masks (see doc/ENCODINGS)
--target-encoding=NAME Output encoding (used by format)
--force-tty Set up terminal for reading keystrokes even if we're not the foreground process
--field-separator-char=C Use 'C' instead of the ':' in input and pot files
--[no-]keep-guessing Try finding plaintext collisions
--list=WHAT List capabilities, see --list=help or doc/OPTIONS
--length=N Shortcut for --min-len=N --max-len=N
--min-length=N Request a minimum candidate length in bytes
--max-length=N Request a maximum candidate length in bytes
--max-candidates=[-]N Gracefully exit after this many candidates tried. (if negative, reset count on each crack)
--max-run-time=[-]N Gracefully exit after this many seconds (if negative, reset timer on each crack)
--mkpc=N Request a lower max. keys per crypt
--no-loader-dupecheck Disable the dupe checking when loading hashes
--pot=NAME Pot file to use
--regen-lost-salts=N Brute force unknown salts (see doc/OPTIONS)
--reject-printable Reject printable binaries
--tune=HOW Tuning options (auto/report/N)
--subformat=FORMAT Pick a benchmark format for --format=crypt
--format=[NAME|CLASS][, ..] Force hash of type NAME. The supported formats can be seen with --list=formats and --list-subformats. See also doc/OPTIONS for more advanced selection of format(s), including using classes and wildcards.
DVWA Security
PHP Info
(kali@kali)-[~]
$ cd Desktop/Epicode_Lab_Clone
(kali@kali)-[~/Desktop/Epicode_Lab_Clone]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali/Desktop/Epicode_Lab_Clone]
# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt password.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
password (admin)
abc123 (gordonb)
letmein (pablo)
charley (1337)
4g 0:00:00:00 DONE (2024-01-10 11:01) 100.0g/s 72000p/s 72000c/s 96000C/s my3kids..soccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
(kali@kali)-[/home/kali/Desktop/Epicode_Lab_Clone]
#
```

TENTATIVO DI LOGIN UTENTE ADMIN

Kali Linux Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~/Desktop/Epicode_Lab_Clone

File Actions Edit View Help

(kali@kali) - [~/Desktop/Epicode_Lab_Clone] settings

\$ cat password_found.txt

admin:password

gordonb:abc123

1337:charley

pablo:letmein

smithy:password

(kali@kali) - [~/Desktop/Epicode_Lab_Clone]

\$

Damn Vulnerable Web Ap x +

← → ↻ ⚠ Not secure 192.168.32.105/dvwa/login.php



Username

admin

Password

Login

You have logged out

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

CTRL (DESTRA)

kali@kali: ~/Desktop/Epicode_Lab_Clone

File Actions Edit View Help

```
(kali@kali)~[~/Desktop/Epicode_Lab_Clone] settings
$ cat password_found.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password
```

```
(kali@kali)~[~/Desktop/Epicode_Lab_Clone]
$
```

Damn Vulnerable Web App x +

← → ↻ ⚠ Not secure 192.168.32.105/dvwa/index.php 🔑 ▶ ☆ ⚙ 👤 □



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.

You have logged in as 'admin'

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

TENTATIVO DI LOGIN UTENTE GORDONB

Kali Linux Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~/Desktop/Epicode_Lab_Clone

File Actions Edit View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions

(kali@kali) - [~/Desktop/Epicode_Lab_Clone] settings

\$ cat password_found.txt

admin:password

gordonb:abc123

1337:charley

pablo:letmein

smithy:password

(kali@kali) - [~/Desktop/Epicode_Lab_Clone]

\$

Damn Vulnerable Web App x +

← → ↻ ⚠ Not secure 192.168.32.105/dvwa/login.php 🔑 ▶ ☆ ⚙ 👤 □



Username

gordonb

Password

Login

You have logged out

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

CTRL (DESTRA)

```
(kali@kali)~[~/Desktop/Epicode_Lab_Clone] settings
```

```
$ cat password_found.txt
```

```
admin:password
```

```
gordonb:abc123
```

```
1337:charley
```

```
pablo:letmein
```

```
smithy:password
```

```
(kali@kali)~[~/Desktop/Epicode_Lab_Clone]
```

```
$
```



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.

You have logged in as 'gordonb'

Username: gordonb
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

TENTATIVO DI LOGIN UTENTE 1337

Kali Linux Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~/Desktop/Epicode_Lab_Clone

File Actions Edit View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions

(kali@kali)~[~/Desktop/Epicode_Lab_Clone] settings

\$ cat password_found.txt

admin:password

gordonb:abc123

1337:charley

pablo:letmein

smithy:password

(kali@kali)~[~/Desktop/Epicode_Lab_Clone]

\$

Damn Vulnerable Web App x +

← → ↻ ⚠ Not secure 192.168.32.105/dvwa/login.php 🔑 ▶ ☆ ⚙ 👤 □



Username

1337

Password

Login

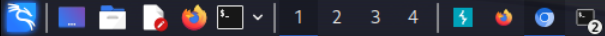
You have logged out

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

CTRL (DESTRA)

File Machine View Input Devices Help



kali@kali: ~/Desktop/Epicode_Lab_Clone

File Actions Edit View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions

(kali@kali) - [~/Desktop/Epicode_Lab_Clone] settings

\$ cat password_found.txt

admin:password

gordonb:abc123

1337:charley

pablo:letmein

smithy:password

(kali@kali) - [~/Desktop/Epicode_Lab_Clone]

\$

Damn Vulnerable Web App x +

← → ↺ Not secure 192.168.32.105/dvwa/index.php

🔑 ▶ ☆ ⚙️ 👤 🗑️



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.

You have logged in as '1337'

Username: 1337
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

TENTATIVO DI LOGIN UTENTE PABLO

Kali Linux Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~/Desktop/Epicode_Lab_Clone

File Actions Edit View Help

```
(kali@kali)~[~/Desktop/Epicode_Lab_Clone] settings
$ cat password_found.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password
```

```
(kali@kali)~[~/Desktop/Epicode_Lab_Clone]
$
```

Damn Vulnerable Web App x +

← → ↻ ⚠ Not secure 192.168.32.105/dvwa/login.php 🔑 ▶ ☆ ⚙ 👤 □ ⋮



Username

Password

Login

You have logged out

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

🔄 📀 🔊 🖨 🗑 📁 📄 📧 🌐 ⬇️ CTRL (DESTRA)


File Actions Edit View Help

```

kali@kali:~/Desktop/Epicode_Lab_Clone$ cat password_found.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

kali@kali:~/Desktop/Epicode_Lab_Clone$
kali@kali:~/Desktop/Epicode_Lab_Clone$ --help or doc/OPTIONS
--min-length=N Request a minimum candidate length in bytes
--max-length=N Request a maximum candidate length in bytes
--max-candidates=N Gracefully exit after this many candidates tried,
                    (if negative, reset count on each crash)
--max-run-times=N Gracefully exit after this many seconds (if negative
                  reset timer on each crash)
--mkpesh Request a lower max. keys per crypt
--no-loader-dupcheck Disable the dup check when loading hashes
--pot-NAME Pot file to use
--regen-lost-salts=N Brute force unknown salts (see doc/OPTIONS)
--strict-plaintext Select printable binaries
--tune-show Tuning options (auto/report/N)
--subformat=FORMAT Pick a benchmark format for --format-crypt
--format=[NAME|CLASS][[:...]] Force hash of type NAME. The supported formats can
be seen with --list-formats and --list-subformats.
See also doc/OPTIONS for more advanced selection of
formats(), including many names and wildcards.

```



← → ↻ ⚠ Not secure 192.168.32.105/dvwa/index.php



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.

You have logged in as 'pablo'

```
Username: pablo
Security Level: low
PHPIDS: disabled
```

TENTATIVO DI LOGIN UTENTE SMITHY

Kali Linux Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~/Desktop/Epicode_Lab_Clone

File Actions Edit View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions

(kali@kali) - [~/Desktop/Epicode_Lab_Clone] settings

\$ cat password_found.txt

admin:password

gordonb:abc123

1337:charley

pablo:letmein

smithy:password

(kali@kali) - [~/Desktop/Epicode_Lab_Clone]

\$

Damn Vulnerable Web A x +

← → ↻ ⚠ Not secure 192.168.32.105/dvwa/login.php 🔑 ▶ ☆ ⚙ 👤 □



Username

smithy

Password

Login

You have logged out

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

CTRL (DESTRA)

LOGIN AVVENUTO CON
SUCCESSO

Kali Linux Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~/Desktop/Epicode_Lab_Clone

File Actions Edit View Help

(kali@kali) - [~/Desktop/Epicode_Lab_Clone] settings

\$ cat password_found.txt

admin:password

gordonb:abc123

1337:charley

pablo:letmein

smithy:password

(kali@kali) - [~/Desktop/Epicode_Lab_Clone]

\$

Damn Vulnerable Web App x

← → ↻ ⚠ Not secure 192.168.32.105/dvwa/index.php



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.

You have logged in as 'smithy'

Username: smithy
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

CTRL (DESTRA)