Diario di lavoro

Luogo	Canobbio
Data	04.10.2019

Lavori svolti

13h15 – 14h00

Ho creato l'articolo relativo alla vulnerabilità di tipo SQL Injection all'interno del sito web.

SQL Injection

di Administrator

Pubblicato il 04.10.2019 alle 13:51

Nella sicurezza informatica SQL injection è una tecnica di code injection, usata per attaccare applicazioni di gestione dati, con la quale vengono inserite delle stringhe di codice SQL malevole all'interno di campi di input in modo che queste ultime vengano poi eseguite. Questa tecnica viene utilizzata per ricavare dati non direttamente visibili o accessibili dalle banche dati all'interno di siti web. Questa falla è molto comune e pericolosa.
Una falla di questo tipo è presente all'interno di HackerLab, più precisamente nella barra di ricerca. Per eseguire un attacco di questo tipo si ha bisogno di una conoscenza di SQL Injection e un po' di fortuna.
All'interno della barra di ricerca è quindi possibile inserire del codice SQL malevolo e farlo eseguire.

Un esempio di semplice query all'interno della barra di ricerca che si può utilizzare è la seguente:

```
test%' OR 1=1; --
```

Questo codice non è malevolo ma dimostra la vulnerabilità, stiamo completando la query utilizzata per eseguire la ricerca che possiamo presumere sia simile a:

```
SELECT * FROM articles WHERE title LIKE $ricerca;
```

E la stiamo trasformando nella seguente query:

```
SELECT * FROM articles WHERE title LIKE '%test%' OR 1=1; --
```

Quindi questa query ritornerà tutti gli articoli presenti nel sito web.
Ci sono moltissime altre possibilità, sta a te scoprirle!

Fonti

Figura 1 Articolo SQL Injection

14h00 – 14h45

15h00 – 16h20

Ho iniziato a creare le guide dettagliate di come eseguire le vulnerabilità, ho iniziato dalla vulnerabilità di tipo Broken Authentication che ho terminato. È disponibile nella cartella documentazione/vulnerabilità.
Ho inoltre completato la guida sulla vulnerabilità File Inclusion o Directory Traversal e mi sono documentato sul formato della cartella .git per la gestione di GitHub.
https://www.siteground.com/tutorials/git/directory-structure/

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate
Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione
Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro
Continuare a documentare le vulnerabilità in un file word.