

Auditoria informatica a Twitter:cuarto incremental



Jorge González

Profesor: Maximiliano Vega

02/ 11 /2017

que es SQLmap

Pruebas de inyecciones SQL

¿Que es SQLmap? Sqlmap es una herramienta desarrollada en el lenguaje python y es muy util para hacer inyeccciones sql automatizados.



Inyección SQL

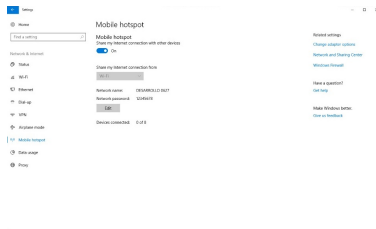
Pruebas de inyecciones SQL



Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

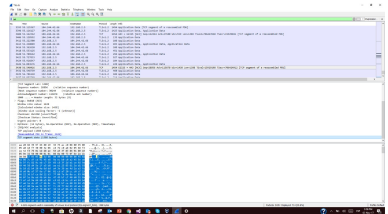
Prueba de Men in the middle

punto de acceso al computador



Prueba de Men in the middle

Prueba
de men in the middle con wireshark



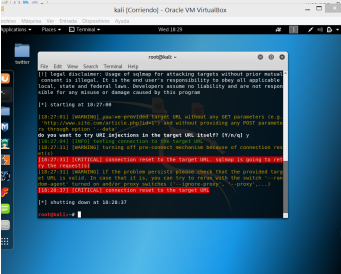
escaneos de las cuentas con SQLmap
la la direccion twitter.com/account



Pruebas con SQLmap

Pruebas de inyecciones SQL

escaneos de las cuentas
con SQLmap con twitter.com/follow



```
kali [Corriendo] - Oracle VM VirtualBox
Applications - Places - Terminal - Files
Wed 18:28

root@kali: ~
[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal law. Downloader assume no liability and are not responsible for any misuse or damage caused by this program

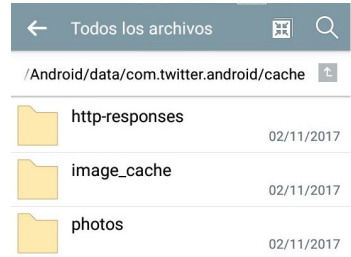
[*] starting at 18:27:00

[18:27:01] [WARNING] you've provided target URL without any GET parameters (e.g. http://www.sik.com/article.php?id=1) and without providing any POST parameters through option '-data'
do you want to try URL injections in the target URL itself? (Y/n/q) y
[18:27:01] [INFO] establishing connection to the target URL
[18:27:01] [WARNING] turning off pre-connect mechanism because of connection reset
[18:27:01] [CRITICAL] connection reset to the target URL... sqlmap is going to try to re-connect
[18:27:01] [WARNING] if the problem persists please check that the provided target URL is valid. In case that is so, you can try to switch the switch '--random-agent' turned on and/or proxy switch ('--proxy-IP', '--proxy-PORT')
[18:27:02] [CRITICAL] connection reset to the target URL
[*] shutting down at 18:28:07

root@kali:~#
```

archivos en el telefono

carpetas internas de twitter



archivos en el telefono

archivos en android de twitter



fin de la presentacion



Gracias por su atención