SQLMAP METODO POST

Para esto usaremos un target muy interesante: http://oagra.unac.edu.pe/record.htm

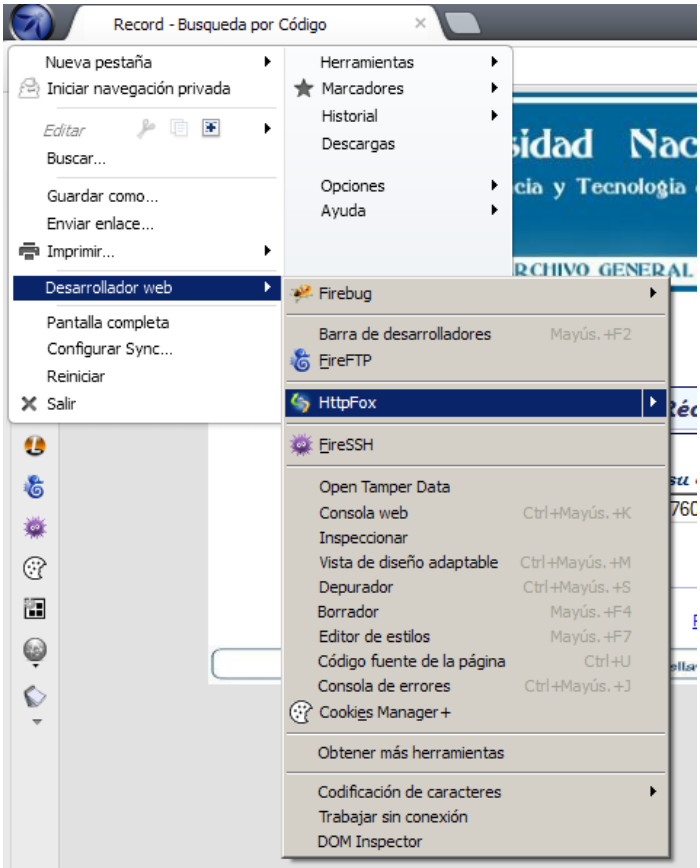
Y Usaremos los datos de esta estudiante XD!

Nombre: ARBIETO-MOLINA-ANTONIA

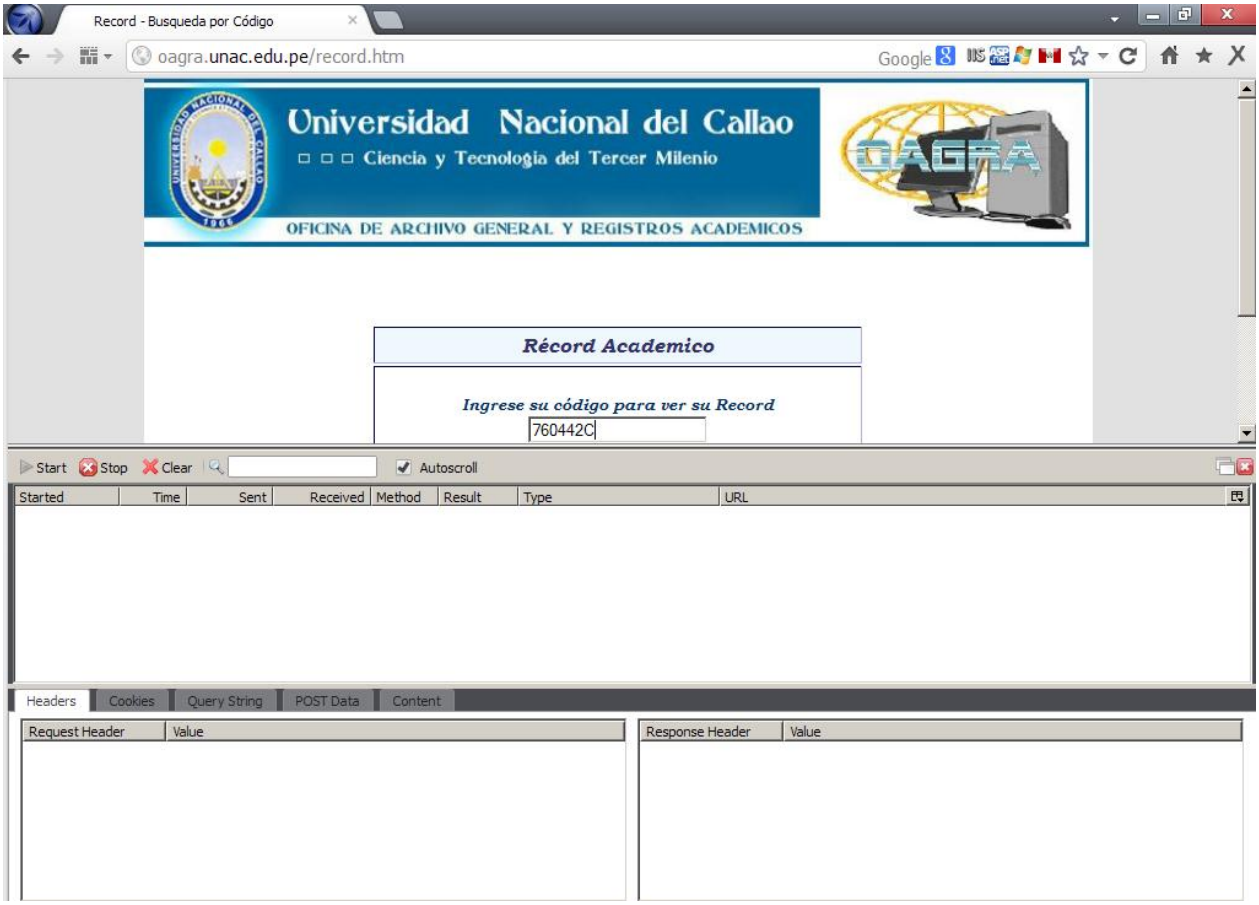
Código: 760442C

Bueno empezaremos con la acción para eso debemos saber cuál es el parámetro del método post que usa para enviar los datos insertados al servidor para eso usaremos una herramienta de nuestro navegador OWASP MANTRA.

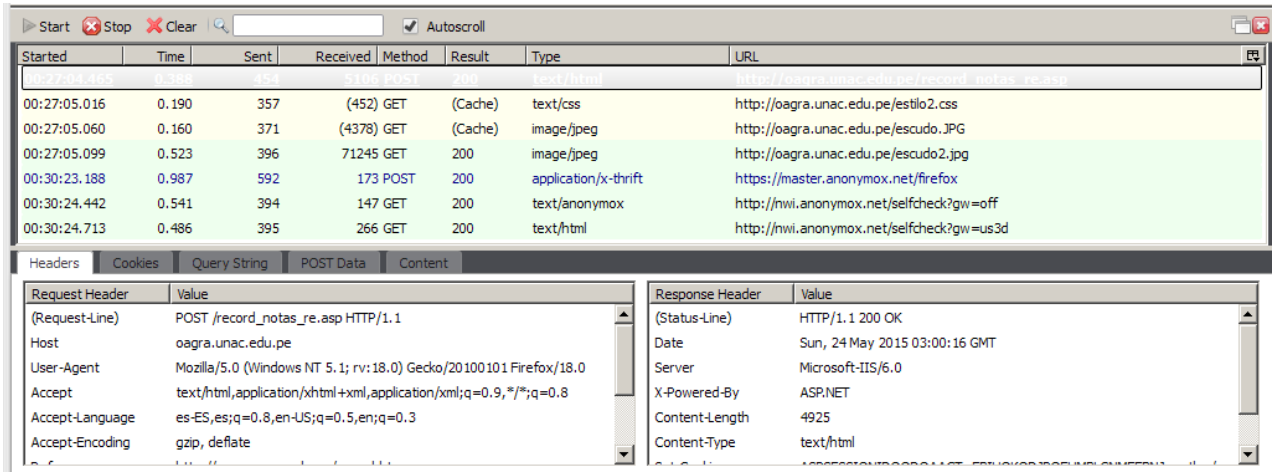
La herramienta se llama HttpFox y la encontramos asi:



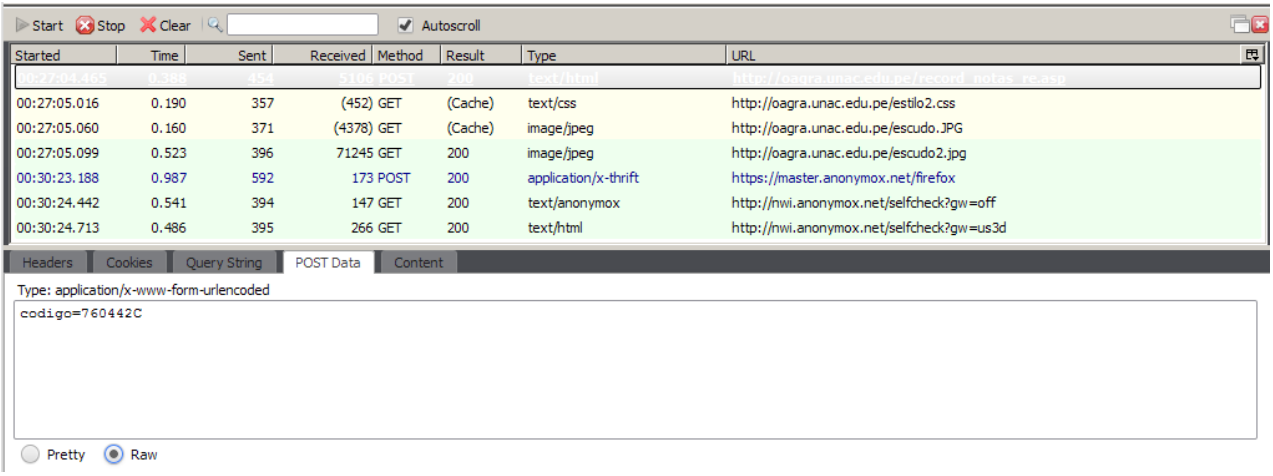
Ya activada la herramienta le damos a Start y empezara a capturar todo el trafico



Luego le damos a mostrar luego de ingresar el código y veremos lo que aparece en La parte de la herramienta hay uno que dice post ese es el que necesitamos.



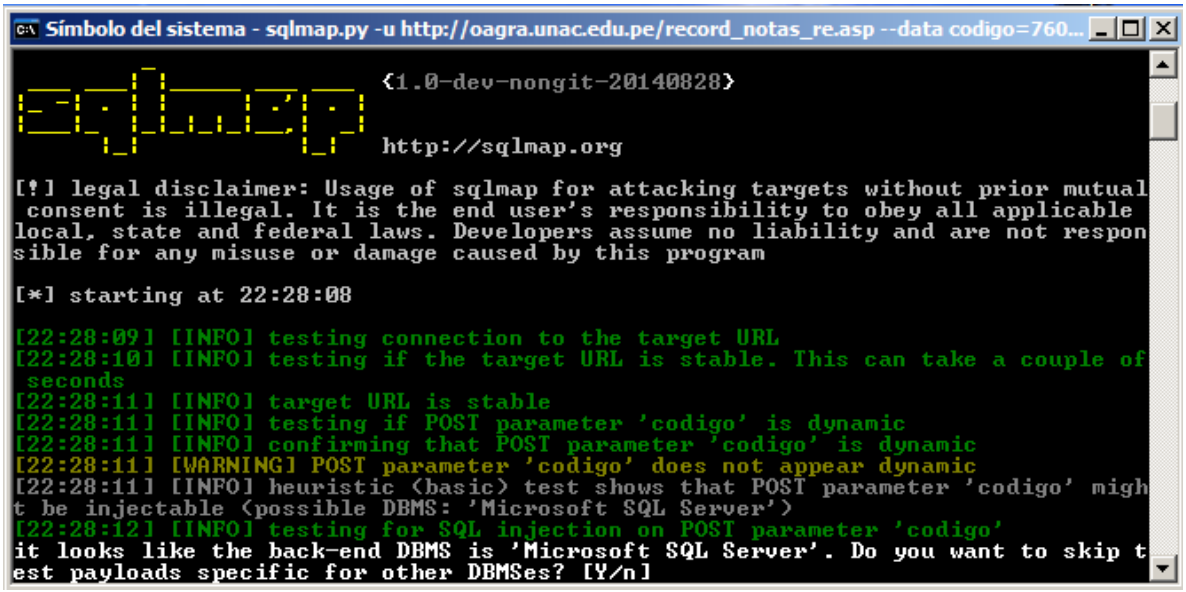
Ahora nos vamos a donde dice PostData y luego hacemos clic en Raw



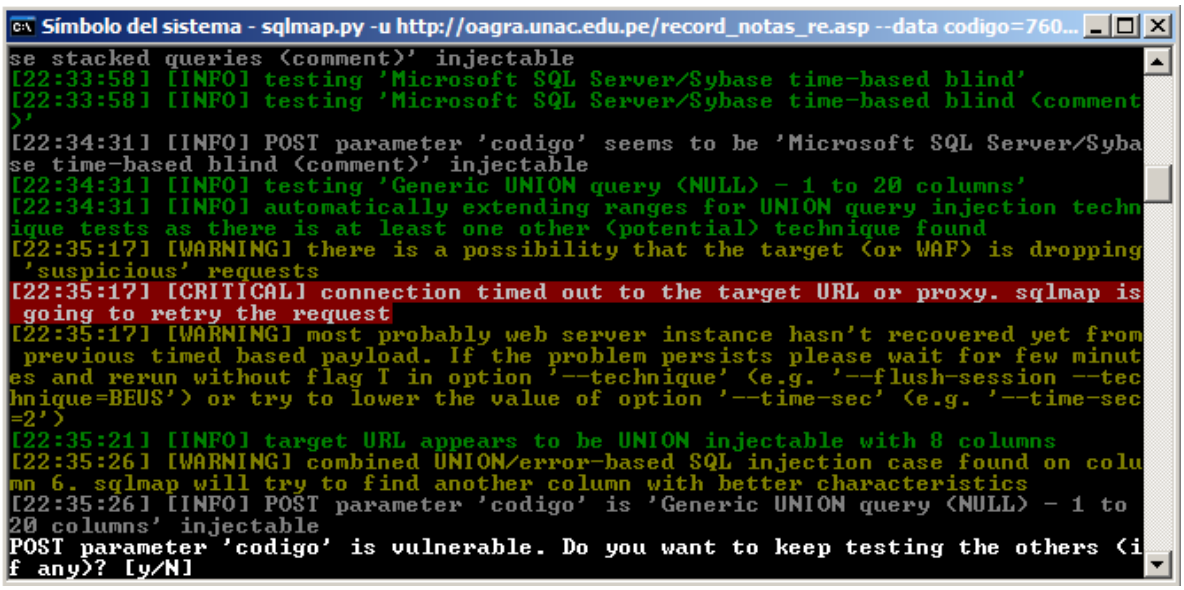
De esto sacamos que la url donde ocurre todo es http://oagra.unac.edu.pe/record_notas_re.asp el parámetro sería ‘ codigo=760442C ‘ ahora abrimos el sqlmap y usamos el siguiente comando

sqlmap.py -u http://oagra.unac.edu.pe/record_notas_re.asp --data codigo=760442C --dbs

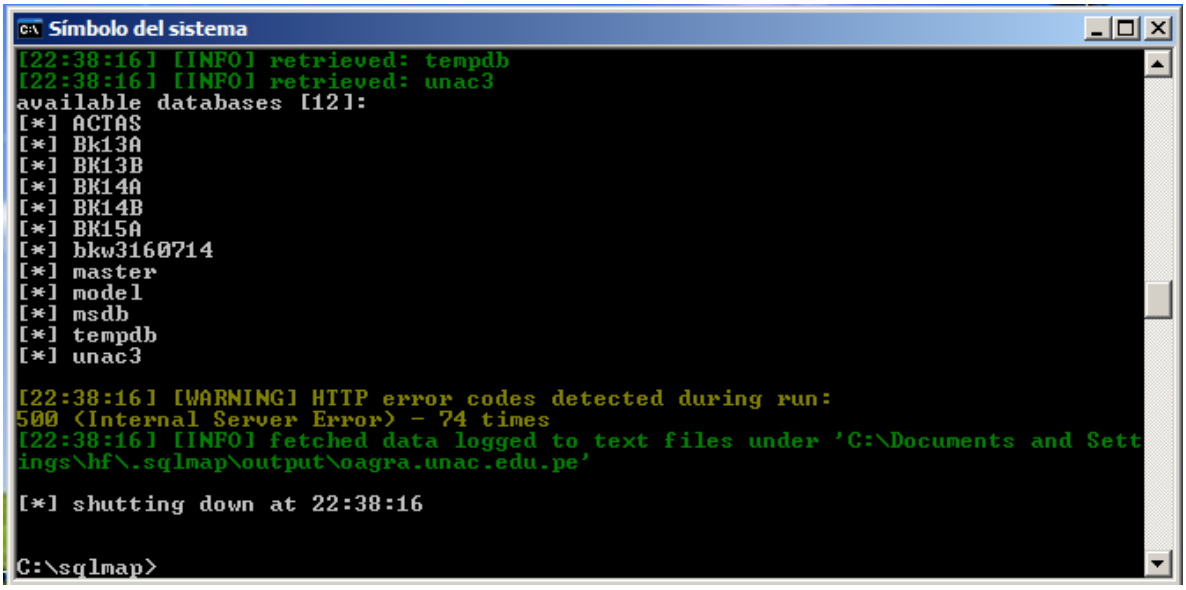
Lo que hay de nuevo es el comando “ --data ” este comando sirve para señalar los parametos post para realizar la inyección SQL



Luego le damos en Y y luego de nuevo Y . Dejamos que cargue todo y nos dira que el parámetro es vulnerable y si queremos analizar otro parámetro le diremos que no. (Los mismos pasas que el antiguo tutorial xD!)



Entonces al Darle que N , esperaremos que bote las Bases de Datos.



Después de esto ya todo lo pueden hacer ustedes usando los mismos comandos usados en el otro tutorial. (Sin Borrar el comando " --data "

Esto es todo por ahora, Se despide Eduardo Desdes ^^!