Hacking Web

- Este curso se hará con los recursos que nos dan en un fichero zip

INJECTIONS

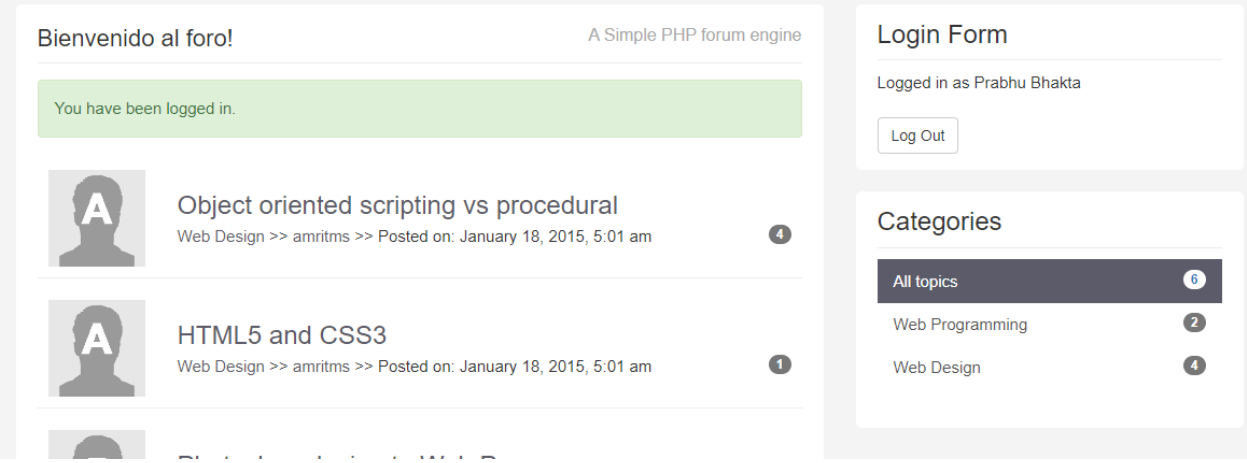
Loggearse sin contraseña (SQL Injection)

Estos son los users

	name	email	avatar	username	password
1	Prabhu Bhakta	dprabin@yahoo.com	dprabin.jpg	dprabin	dprabin
2	Amrit Man	amritms@gmail.com	amritms.jpg	amritms	amritms
3	Ramesh Bhusal	vol222@gmail.com	rkbhushal.jpg	rkbhushal	rkbhushal

Usaremos para el usuario: 999' or '1' = '1' # ya que interpretará esto como una consulta en la que cogerá el primer usuario ya que 1 = 1 siempre

Usando esto en el campo user y cualquier contraseña podremos entrar



Para evitar este tipo de problemas, nuestros formularios deberán filtrar bien las entradas, es decir, que el campo introducido cumpla ciertas condiciones.

Cross Site Scripting (XSS)

En este caso insertaremos código php dentro de un campo:

<script>alert("hola")</script>

Este será ejecutado y saltará:

Volvemos a la misma cuestión, hay que filtrar bien los campos

Robo de sesión

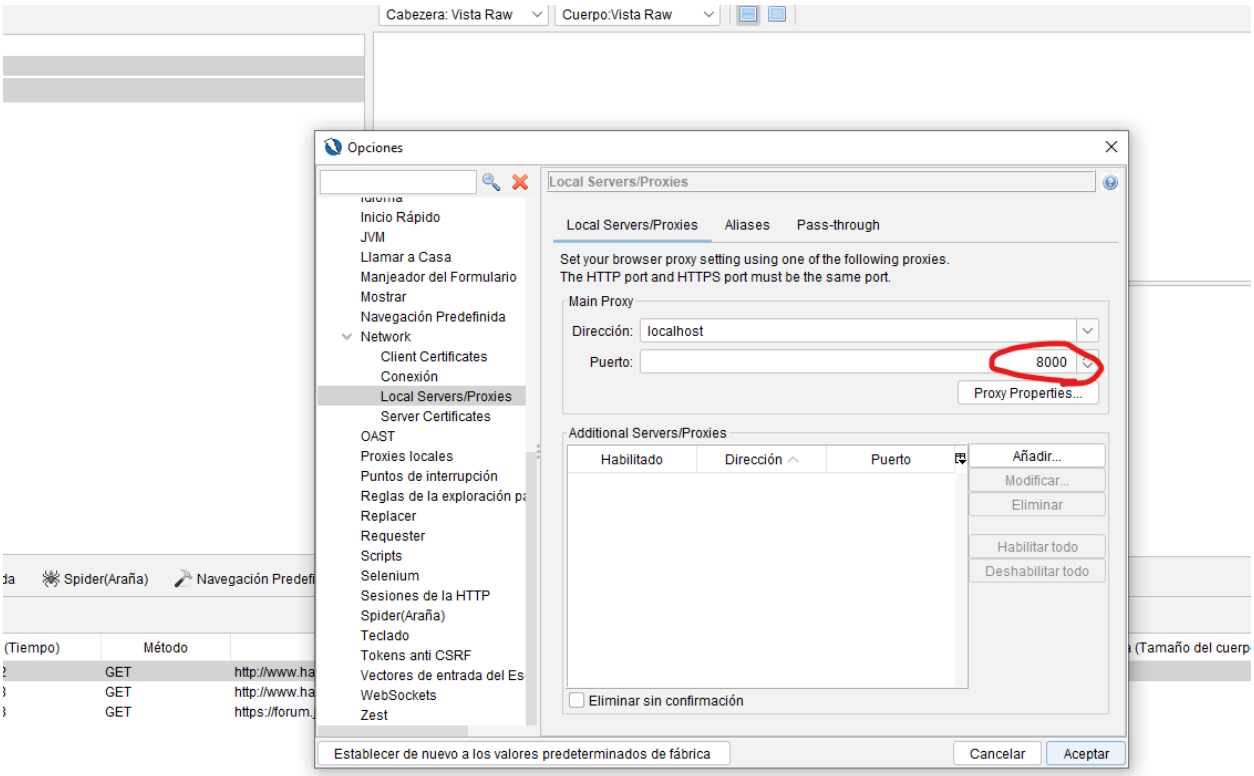
Sesion prediction

Para esto usaremos el OWASP ZAP

https://www.zaproxy.org/download/

La usaremos para recoger que peticiones son enviadas en la web que nos encontremos

Deberemos configurar nuestro programa en opciones para que pase por el puerto que indiquemos



Y nuestro buscador deberemos redireccionar la conexion a ese puerto.

Dependiendo del buscador se hace de una manera u otra

Una vez que hagamos un par de navegaciones se irán registrando en el ZAP

Para hacer un debug por pasos para inyectar el código que queramos deberemos usar el botón

Ahora usaremos el login y se pausará a la espera de que nosostros ejecutemos el código

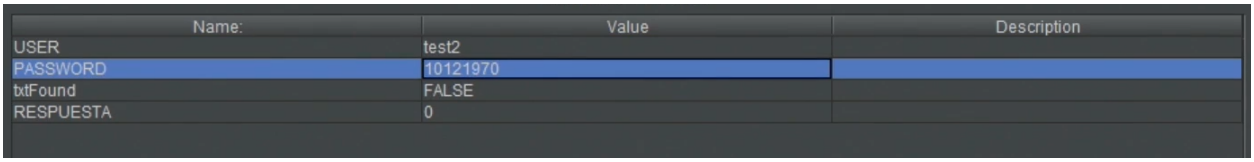
```
GET http://192.168.1.102/demos/demos/sqliDatos.php HTTP/1.1
Host: 192.168.1.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Referer: https://192.168.1.102/demos/demos/sqli.php?user=user1&pass=pass1
Connection: keep-alive
Cookie: PHPSESSID=user2
Upgrade-Insecure-Requests: 1
```

Ahí podremos cambiar el valor de que user somos entonces nos podremos colar en la sesión de otra persona

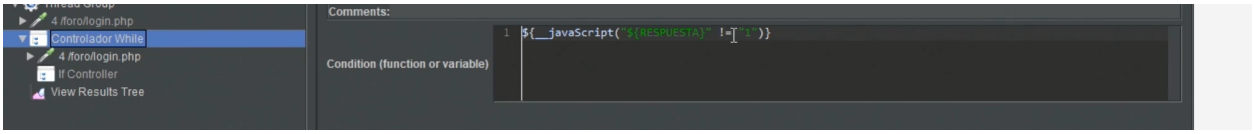
Fuerza Bruta

Para esto descargaremos el Apache JMeter

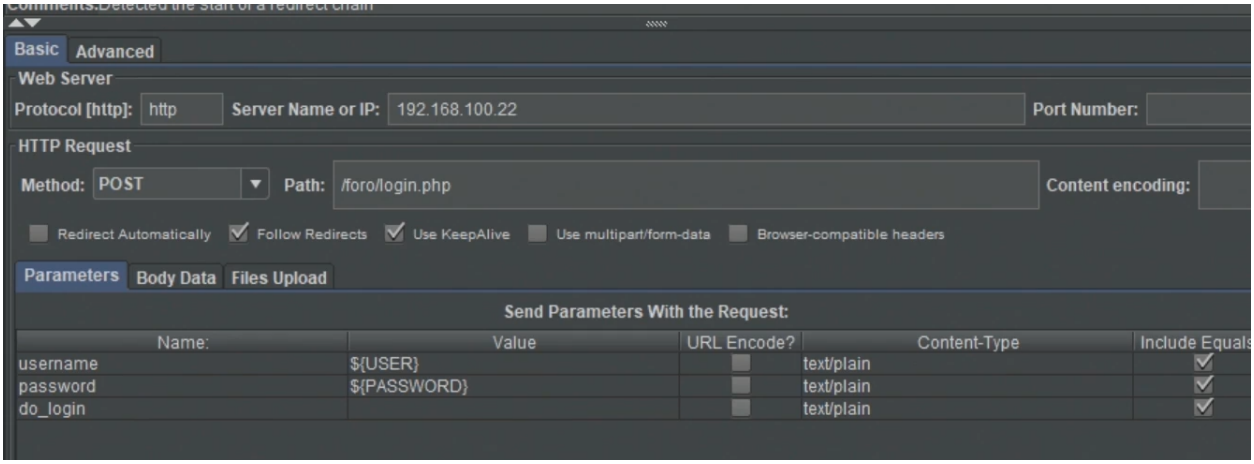
Una vez instalado cargaremos el script que nos vendrá en el repositorio



Aquí pondremos los valores iniciales que queremos usar

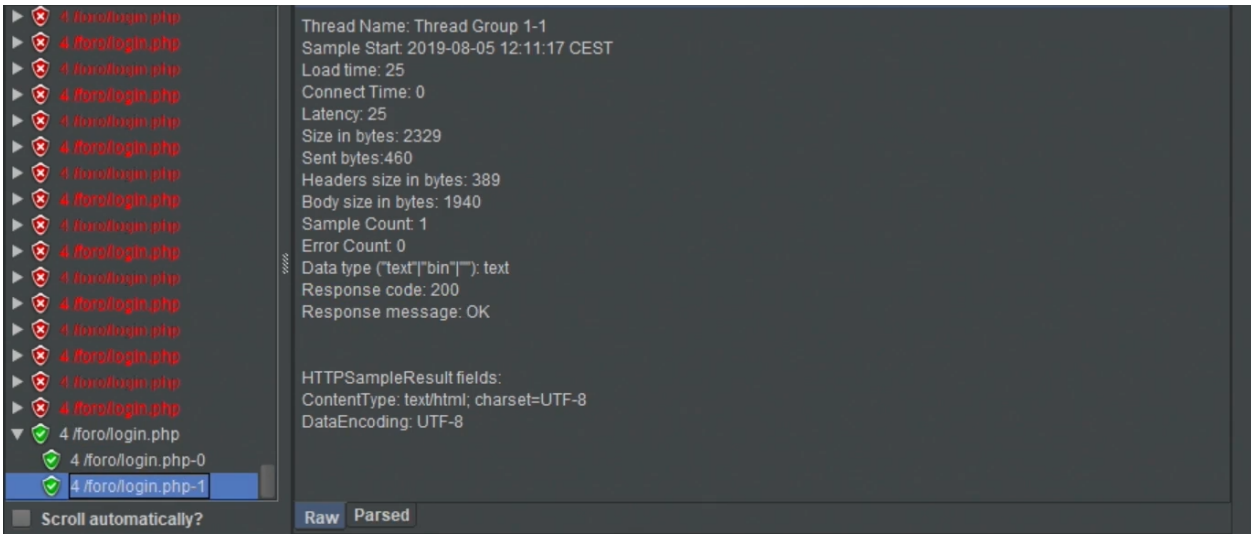


Aquí pondremos que código queremos que devuelva la web



Configuraremos la ip y el puerto y la ruta

Lo ejecutaremos y si la página lo permite hará intentos de login con distintos valores hasta que entre



Accesos ilegales

Este apartado simplemente nos mostrará que si modificamos la url en la que estamos y adivinamos cual es el url del panel de admin, podremos acceder a el.