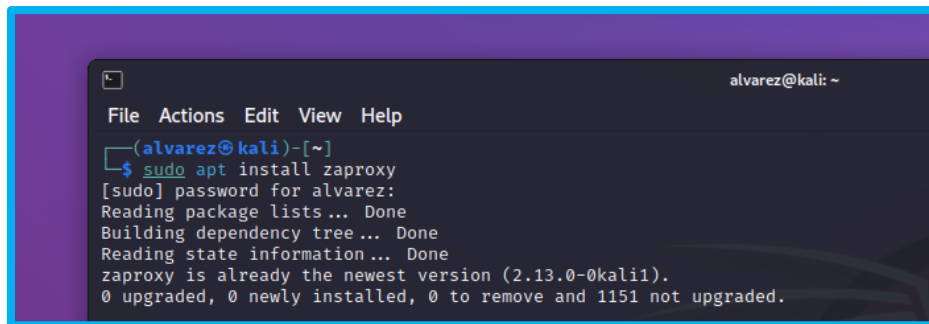


## Act. 3.1 Practica Ataques de inyección SQL usando OWASP Zap Fuzzer

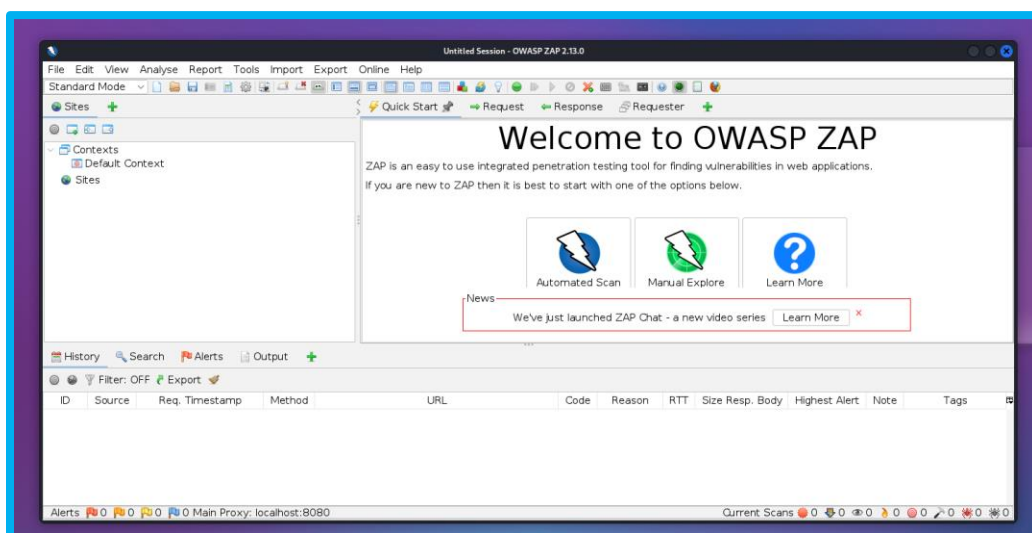
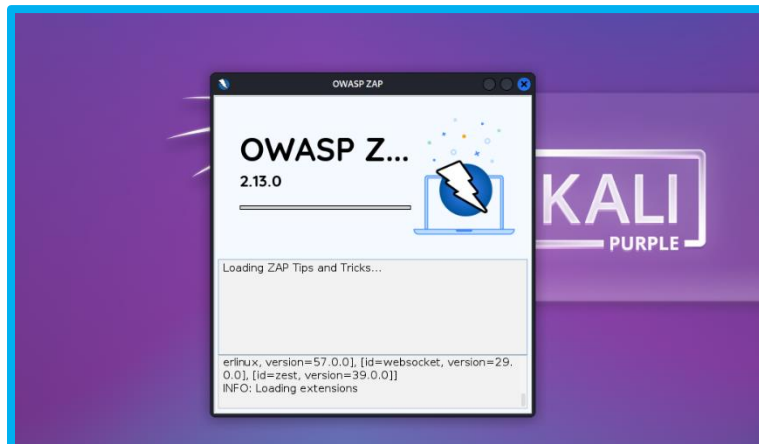
Lo primero que realice es instalar OWASP Zap Fuzzer en Kali Linux

Comando: `sudo apt install zapproxy`

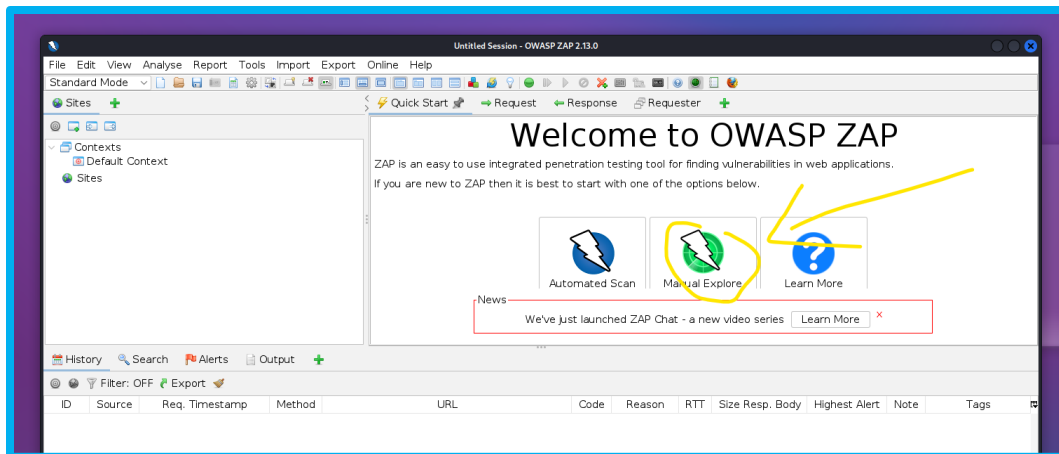


```
alvarez@kali: ~  
File Actions Edit View Help  
alvarez@kali)~  
$ sudo apt install zapproxy  
[sudo] password for alvarez:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
zapproxy is already the newest version (2.13.0-0kali1).  
0 upgraded, 0 newly installed, 0 to remove and 1151 not upgraded.
```

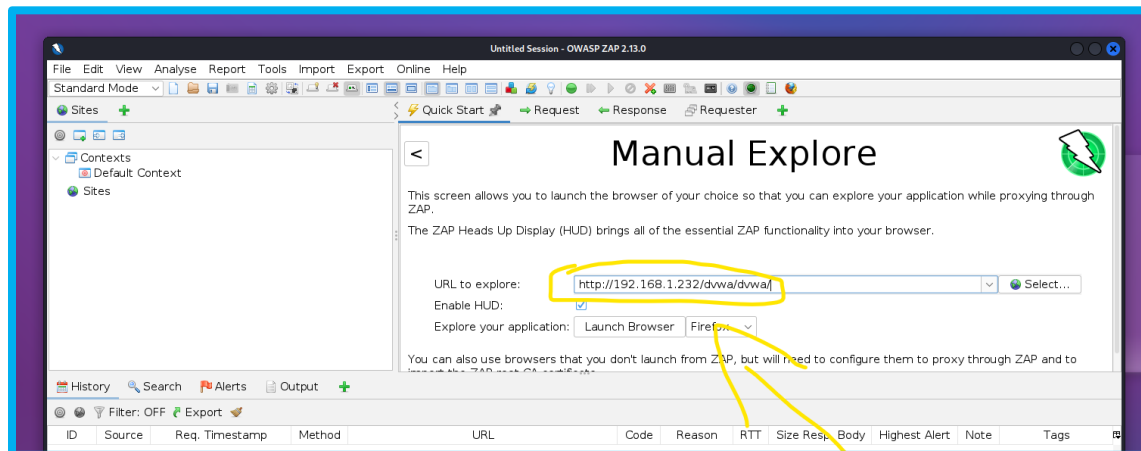
Después de haberlo instalado nos mostrara la siguiente interfaz grafica



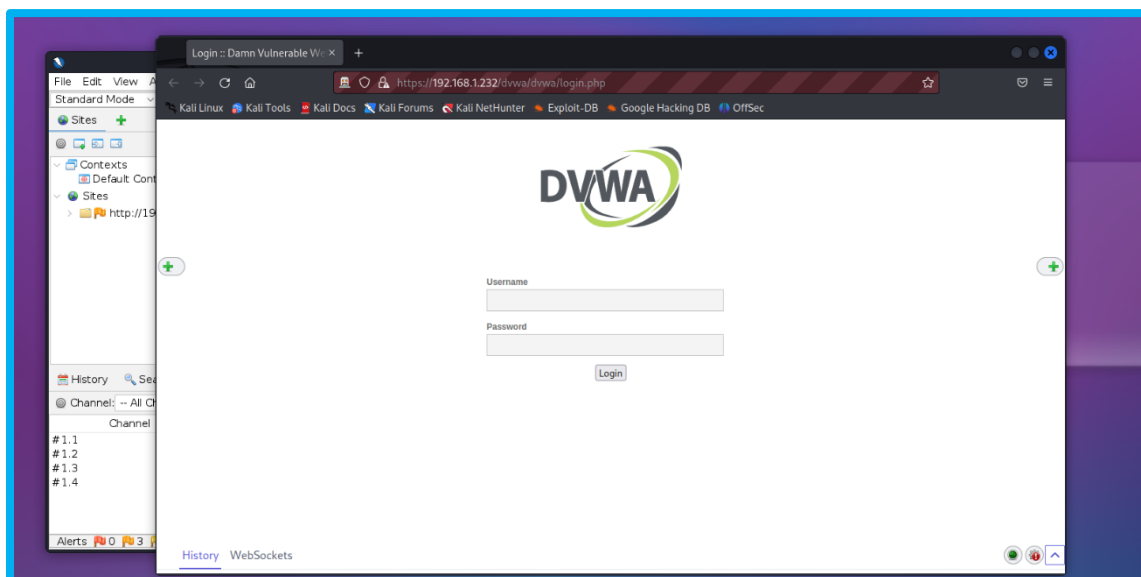
le daremos clic a exploración manual



Y tendremos la siguiente ventana, donde pondríamos la ip donde tenemos nuestro servicio, en este caso yo puse la ip de mi máquina virtual Ubuntu ya que es ahí donde tengo mi servicio DVWA.



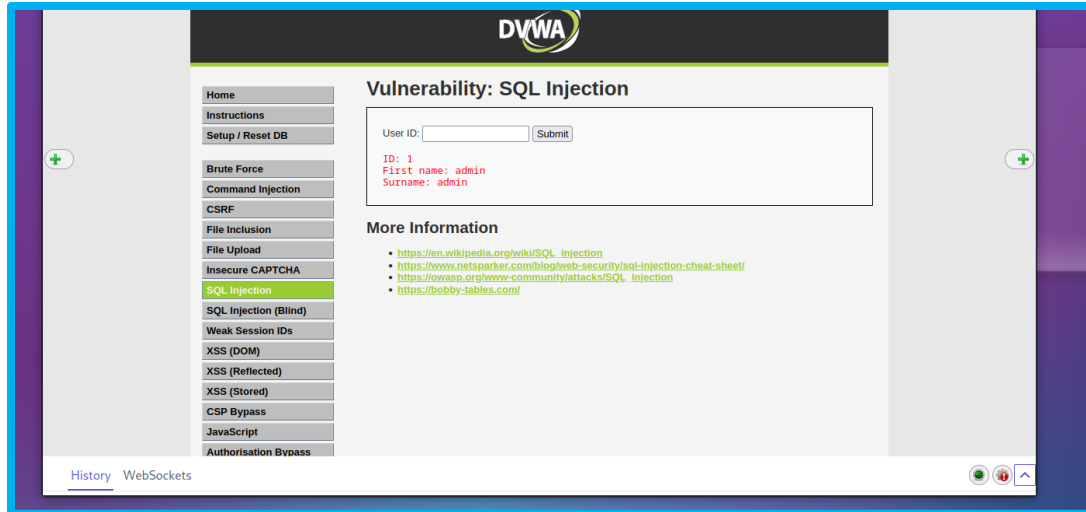
Posteriormente la damos launch Browser, y nos habría el login del DVWA



Después de habernos logueado será importante que cambiemos la seguridad a low para que no tengamos problemas al momento de cambiar el parámetro GET.

Nos ubicamos en la pestaña de sql ijection,

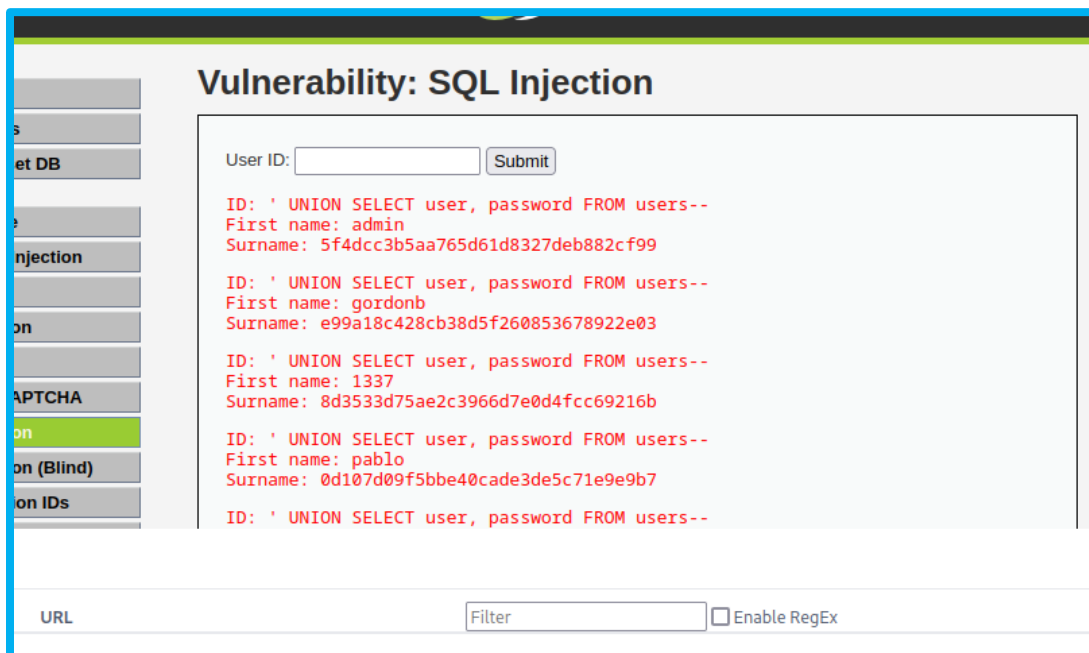
Y nos vamos a la pestaña inferior del lado derecho que dice History



Una vez dado clic a la pestaña History nos vamos a la última opción y cambiamos la el parámetro GET por lo siguiente

GET <https://archive.mozilla.org/pub/system-addons/addons-restricted-domains/addons-restricted-domains-1.0.0-build1/addons-restricted-domains.xpi> HTTP/1.1

posteriormente nos desglosaría los usuarios y sus contraseñas



Como las contraseñas no son del todo clara lo que use fue una pagina que me pudiera descifrar las contraseñas.

La página se llama CrackStation

### Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

5f4dcc3b5aa765d61d8327deb882cf99  
e99a18c428cb38d5f260853678922e03  
8d3533d75ae2c3966d7e0d4fcc69216b  
0d107d09f5bbe40cade3de5c71e9e9b7  
5f4dcc3b5aa765d61d8327deb882cf99

No soy un robot

reCAPTCHA

Privacidad - Condiciones

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f260853678922e03	md5	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

**Color Codes:** Green Exact match, Yellow Partial match, Red Not found.

Como podemos notar nos descifra todas las contraseñas que nosotros agregamos.

LICENCIATURA EN INGENIERIA EN DESARROLLO Y TECNOLOGIAS DE SOFTWARE