# Desarrollo Seguro de Aplicaciones Web con OWASP

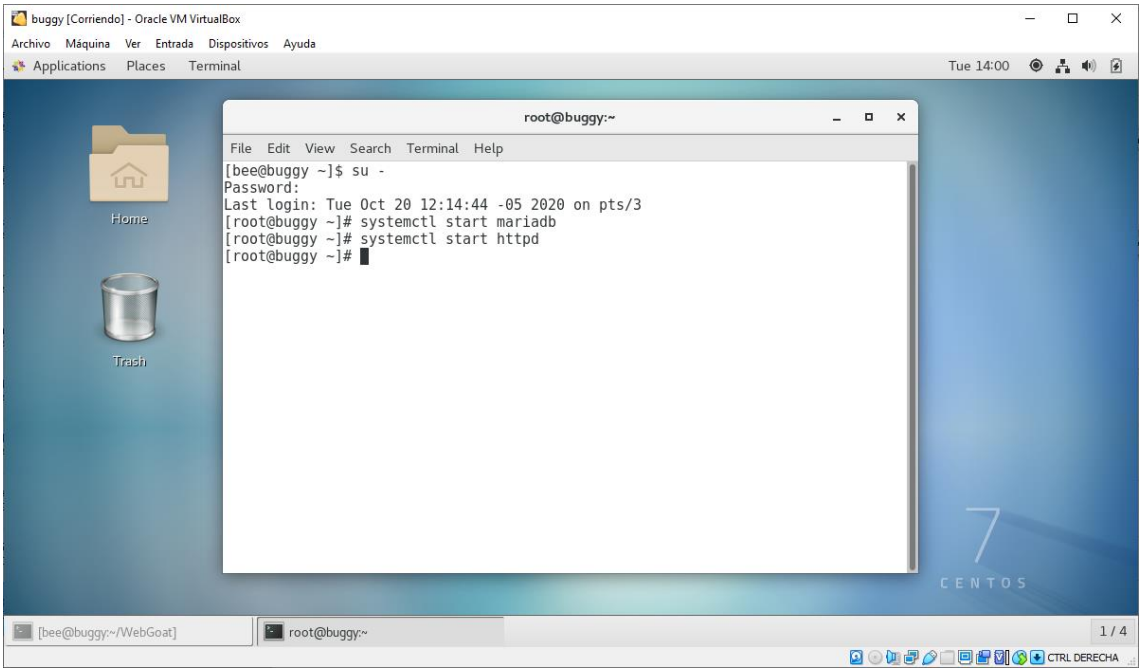
## Lab: Sensitive Data Exposure

### Objetivo

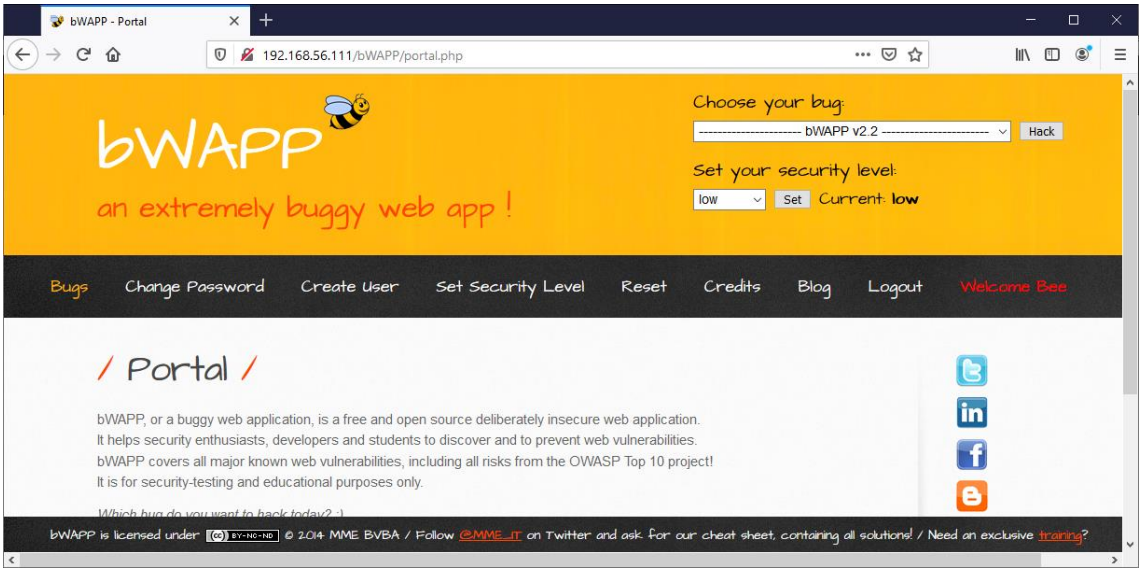
- Revisar el vector de ataque sensitive data intersect

### Procedimiento

1. Inicia los servicios de la aplicación bWAPP

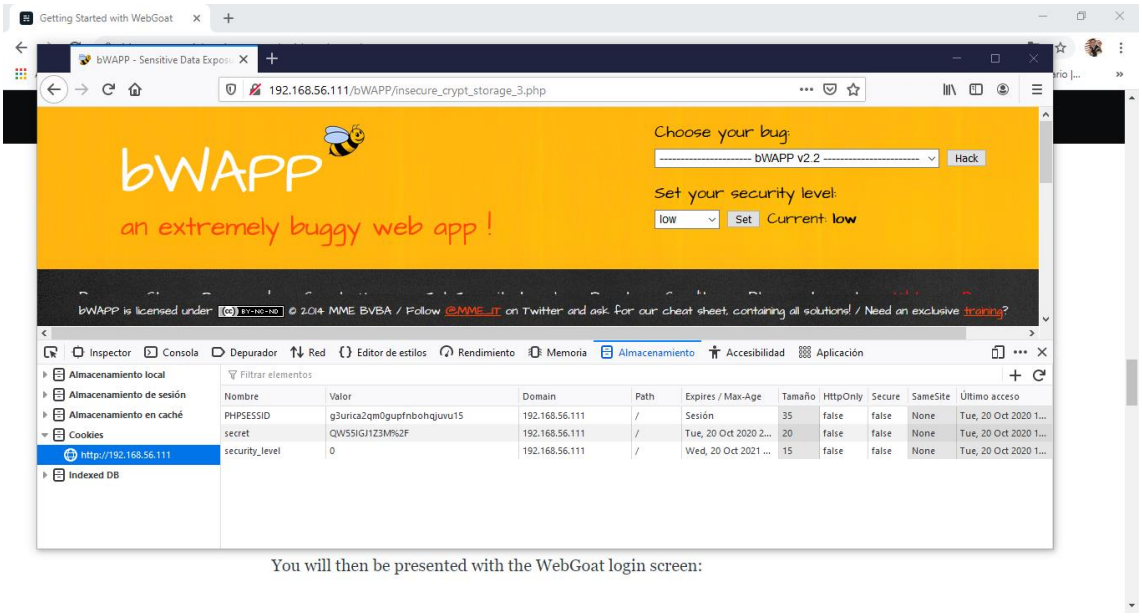



2. Ingresa a la aplicación bWAPP



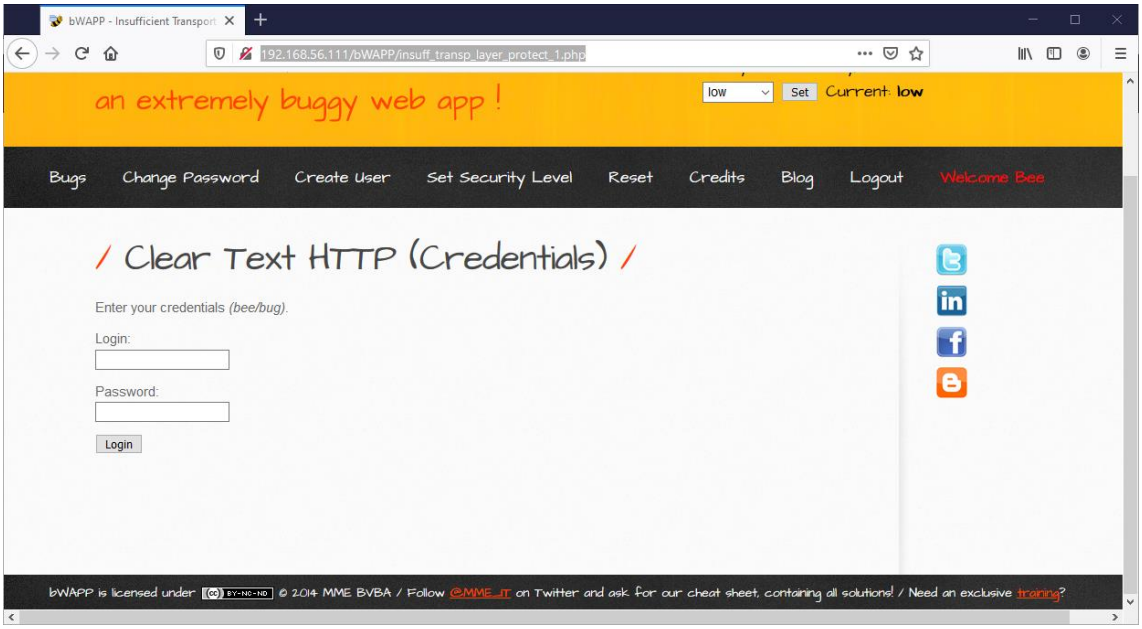
3. Abre la url http://192.168.56.111/bWAPP/insecure_crypt_storage_3.php


4. Obten la cadena encriptada del Cookie.

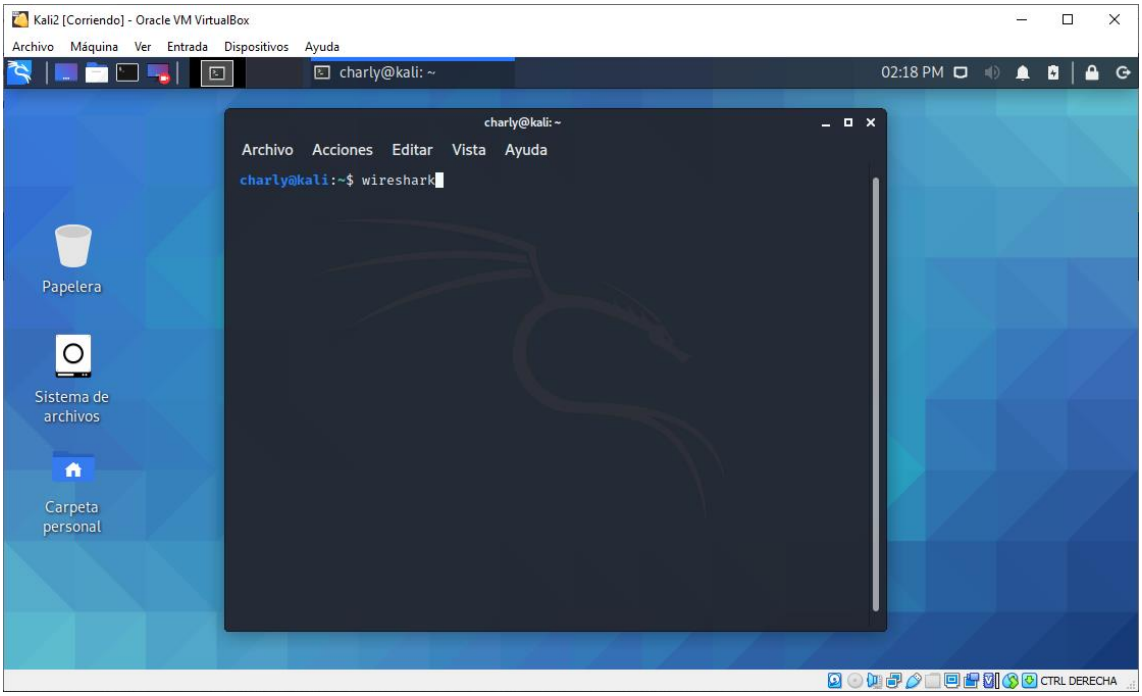


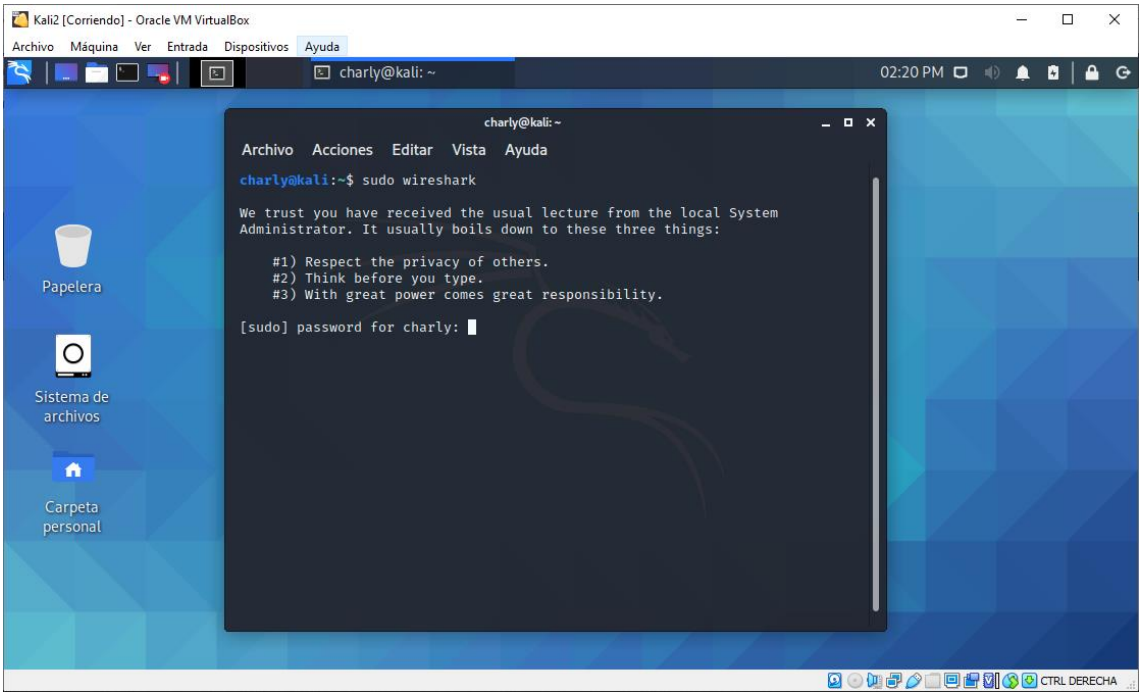

You will then be presented with the WebGoat login screen:

5. Abre el url http://192.168.56.111/bWAPP/insuff_transp_layer_protect_1.php

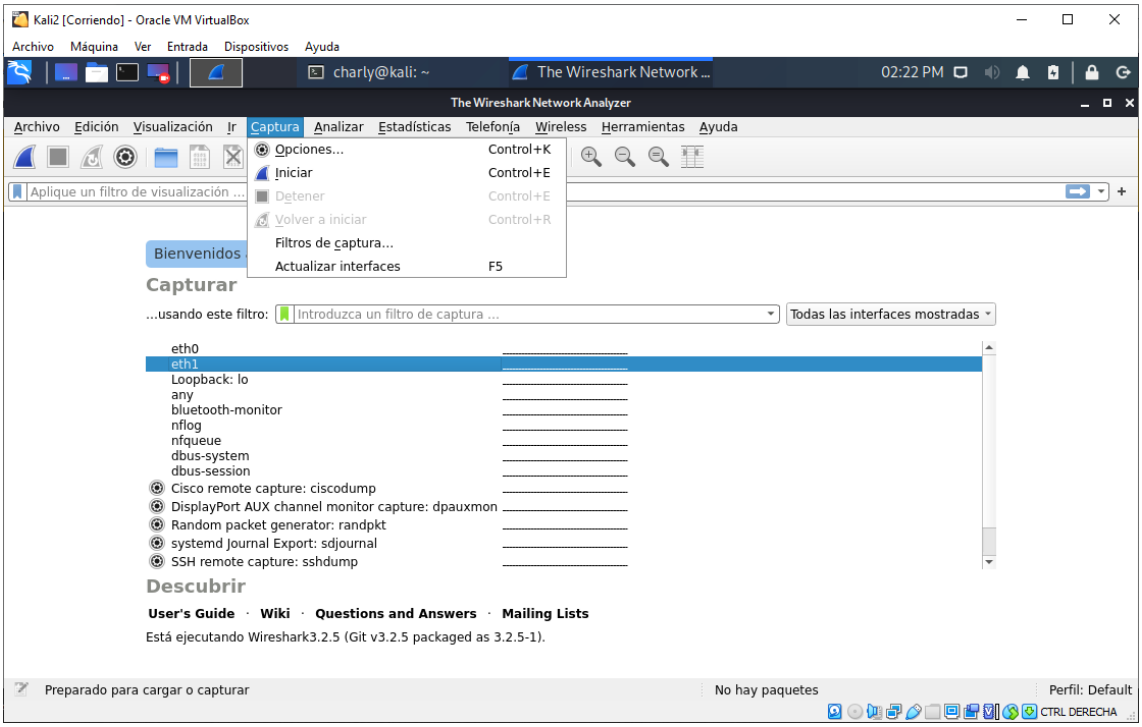


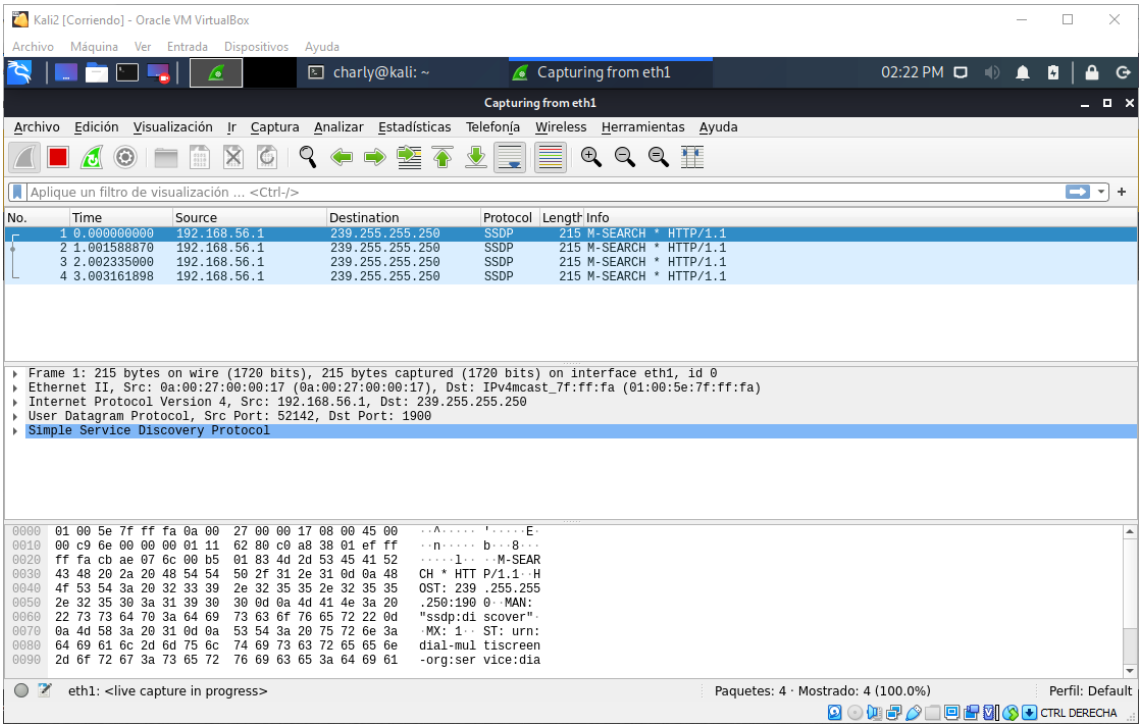

6. Inicia en Kali Linux la herramienta wireshark



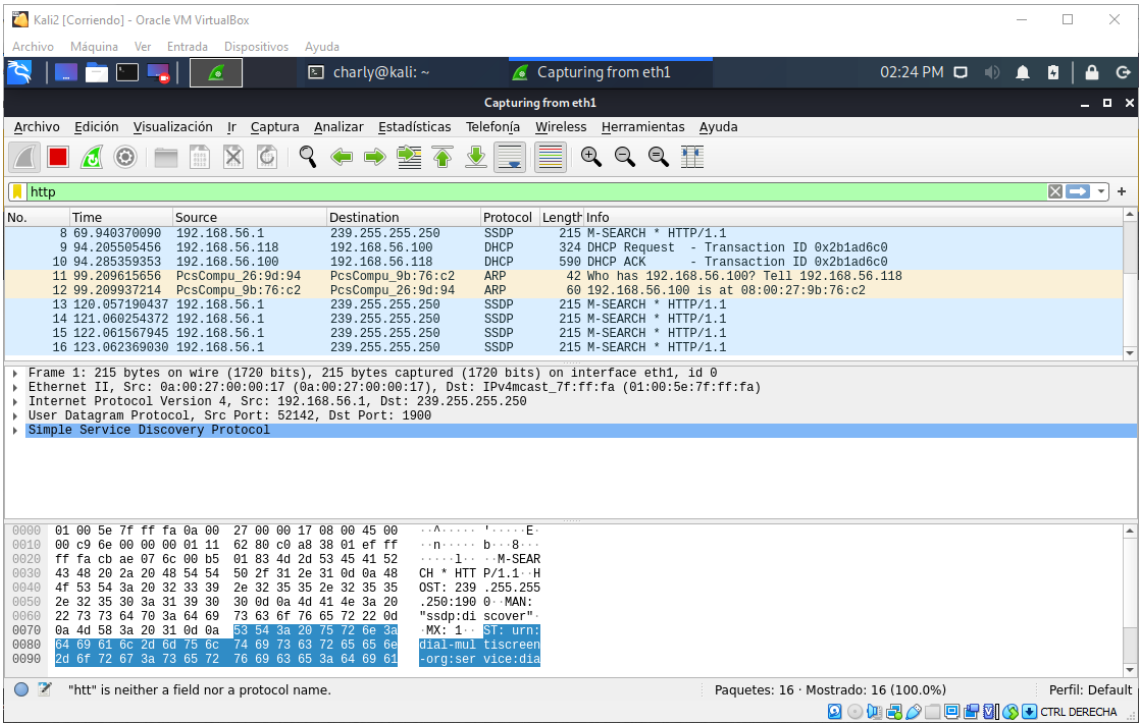



Seleccionamos la interface de la red solo anfitrión.

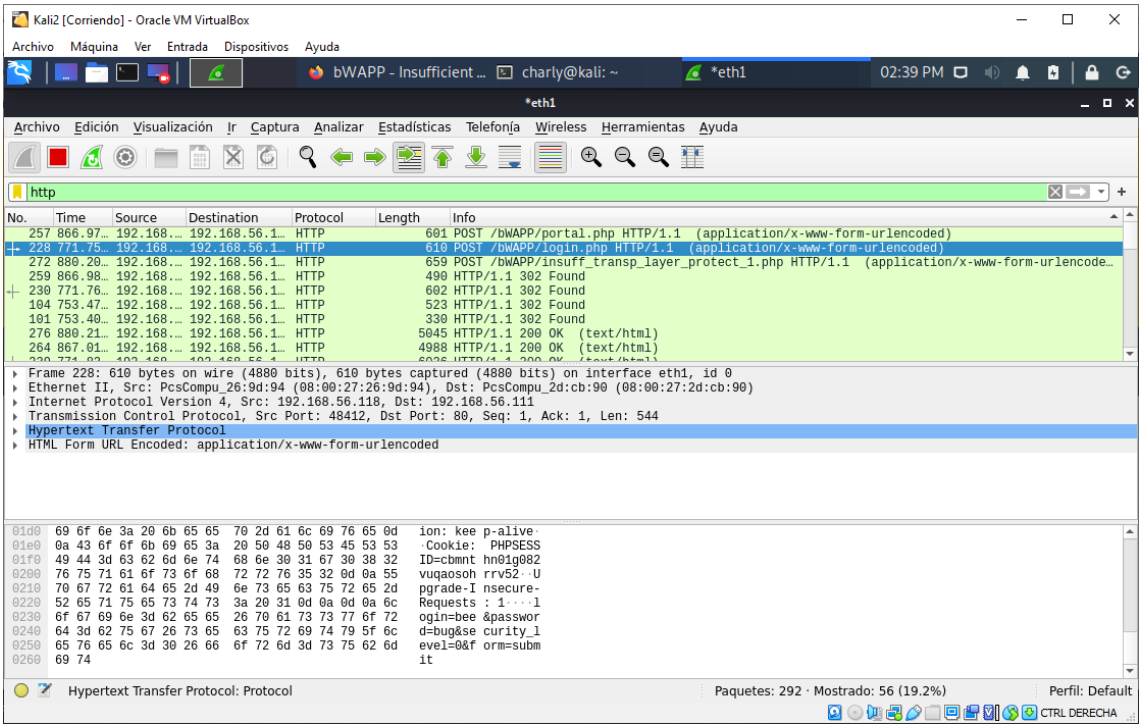





7. Filtra http protocol.




8. Descubre el password del usuario bee


Kali2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
bWAPP - Insufficient ...
charly@kali: ~
*eth1
02:39 PM
*eth1
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
http
No. Time Source Destination Protocol Length Info
257 866.97… 192.168.… 192.168.56.1… HTTP 601 POST /bWAPP/portal.php HTTP/1.1 (application/x-www-form-urlencoded)
228 771.75… 192.168.… 192.168.56.1… HTTP 610 POST /bWAPP/login.php HTTP/1.1 (application/x-www-form-urlencoded)
272 880.20… 192.168.… 192.168.56.1… HTTP 659 POST /bWAPP/insuff_transp_layer_protect_1.php HTTP/1.1 (application/x-www-form-urlencode…
259 866.98… 192.168.… 192.168.56.1… HTTP 490 HTTP/1.1 302 Found
230 771.76… 192.168.… 192.168.56.1… HTTP 602 HTTP/1.1 302 Found
104 753.47… 192.168.… 192.168.56.1… HTTP 523 HTTP/1.1 302 Found
101 753.40… 192.168.… 192.168.56.1… HTTP 330 HTTP/1.1 302 Found
276 880.21… 192.168.… 192.168.56.1… HTTP 5045 HTTP/1.1 200 OK (text/html)
264 867.01… 192.168.… 192.168.56.1… HTTP 4988 HTTP/1.1 200 OK (text/html)
Frame 228: 610 bytes on wire (4880 bits), 610 bytes captured (4880 bits) on interface eth1, id 0
Ethernet II, Src: PcsCompu_26:9d:94 (08:00:27:26:9d:94), Dst: PcsCompu_2d:cb:90 (08:00:27:2d:cb:90)
Internet Protocol Version 4, Src: 192.168.56.118, Dst: 192.168.56.111
Transmission Control Protocol, Src Port: 48412, Dst Port: 80, Seq: 1, Ack: 1, Len: 544
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
01d0 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d ion: kee p-alive·
01e0 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 45 53 53 ·Cookie: PHPSESS
01f0 49 44 3d 63 62 6d 6e 74 68 6e 30 31 67 30 38 32 ID=cbmnt hn01g082
0200 76 75 71 61 6f 73 6f 68 72 72 76 35 32 0d 0a 55 vuqaosoh rrv52··U
0210 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-
0220 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 0d 0a 6c Requests : 1····l
0230 6f 67 69 6e 3d 62 65 65 26 70 61 73 73 77 6f 72 ogin=bee &passwor
0240 64 3d 62 75 67 26 73 65 63 75 72 69 74 79 5f 6c d=bug&se curity_l
0250 65 76 65 6c 3d 30 26 66 6f 72 6d 3d 73 75 62 6d evel=0&f orm=subm
0260 69 74 it
Hypertext Transfer Protocol: Protocol
Paquetes: 292 · Mostrado: 56 (19.2%)
Perfil: Default
CTRL DERECHA