Curso de Hacking Web

En este curso he aprendido como se deben tratar los datos que introducen los usuarios en páginas web, es decir nunca se deben tomar los datos directamente del usuario y realizar consultas con ellos, esto para evitar el uso de sql injection del tipo 999' or '1'='1'--, XSS que consiste en la ejecución de código mediante código del tipo <script> alert(hola) <script> esta consulta es inofensiva a priori pero se puede usar otras como window.location para realizar ataque del tipo phising, robo de sesión o deface redirigiendo al usuario a una página creada por el atacante.

Problemas con los ficheros que pueden ser de dos tipos principalmente,

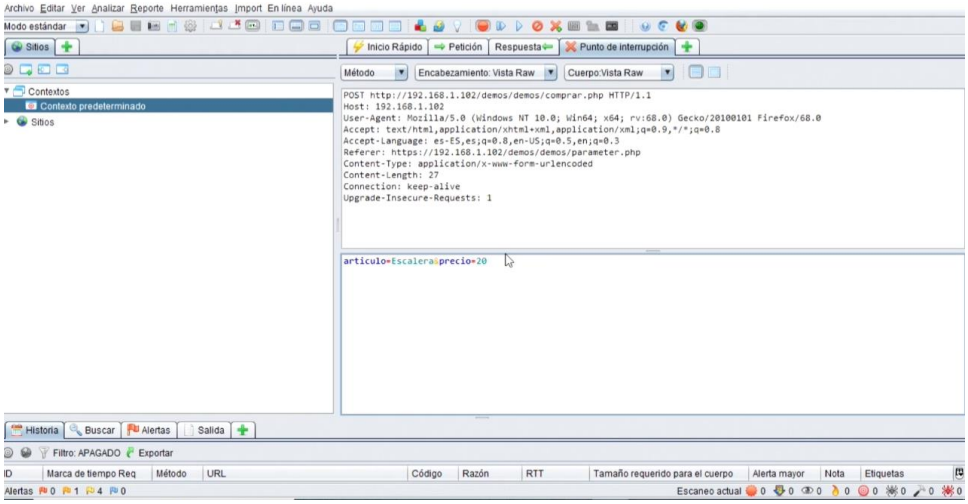
- Unrestricted file upload en los que se suben archivos para que se ejecuten, se pueden subir archivos excesivamente grandes para intentar llenar la memoria del servidor y bloquearlo...
- Local file inclusion que se basa en modificar la ruta a un fichero para acceder a otro de manera fraudulenta

Para combatir estos problemas se deberían poner restricciones como del tipo de archivo, tamaño, sanear el nombre y descargar el fichero subido, no ejecutarlo en el servidor.

Robo de sesiones mediante distintas técnicas como lo pueden ser session prediction que se basa en analizar un patrón en la creación de sesiones para hacerse pasar por otro usuario. Esto puede ser evitado creando las sesiones en el servidor y haciendo que sean únicas y aleatorias, poniendo un tiempo en el cual expira la sesión, encriptar la información sobre las sesiones.

Ataque de fuerza bruta mediante el cual se intenta acceder probando todas las posibles combinaciones mediante sistemas que automatizan este proceso, además esto se puede optimizar ya que por ejemplo el uso de alguna fecha como contraseña es muy utilizado así que se podrían probar todas las fechas de los últimos 100 años puesto que es el intervalo más probable en el que se encuentre dicha fecha. Para evitarlo se puede usar un contador de intentos pasados los cuales no se puede seguir probando, mediante el uso de captcha lo cual suele bloquear a este tipo de sistemas automatizados.

Otros problemas son el parameter tampering por los cuales se modifican los parámetros que se le envían al servidor, ya sean parámetros que se pasan por url o capturando los parámetros mediante aplicaciones como OWASP-ZAP, esto se puede evitar eliminando parámetros no necesarios y realizando las validaciones en el servidor no a nivel usuario.



Uso de zap

Otro problema es el control inseguro de roles por los cuales se ocultan los accesos a ciertas funcionalidades dependiendo del rol, pero si conseguimos conocer la ruta completa dará igual el rol que tengamos ya que podremos acceder, para evitar esto se deben comprobar los permisos de cada usuario y validar todas sus acciones.