Sistemas de Gestión de Seguridad de Sistemas de Información

Ingeniería Informática de Gestión y Sistemas de Información

Sistema Web

Autores:

Xabier Gabiña
Ainhize Martinez
Marcos Martín

13 de diciembre de 2023

Índice general

Introducción

Vulnerabilidades

2.1. Rotura de control de acceso

2.1.1. Acceso mediante URL

2.2. Fallos criptográficos

2.2.1. Sniffing

2.2.2. MITM

2.3. Inyecciones

2.3.1. SQL Injection

La primera vulnerabilidad que vamos a probar es la de SQL Injection con la intencion de obtener información de la base de datos. Para el analisis de esta vulnerabilidad vamos a utilizar la herramienta sqlmap. Esta herramienta nos permite analizar una url y comprobar si es vulnerable a SQL Injection de forma sencilla y automatizada. En caso de querer usarla, se puede instalar con el siguiente comando:

```
sudo apt-get install sqlmap
```

Una vez instalada, hemos ejecutado el siguiente comando para realizar las pruebas:

```
sqlmap -u http://localhost:81/login.php --wizard
```

Este analisis nos ha dado como resultado que la url es vulnerable a 3 tipos de SQL Injection:

- Boolean-based blind SQL injection
- Error-based SQL injection
- Time-based blind SQL injection

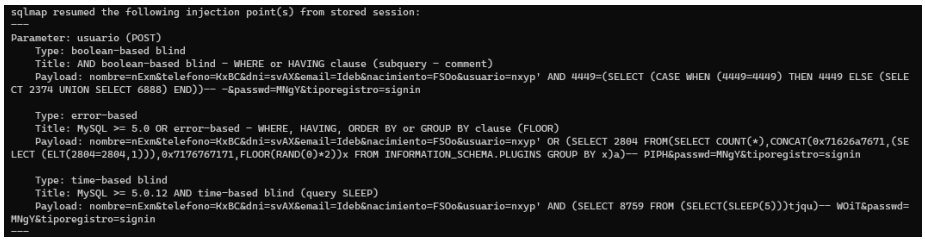

Figura 2.1: Puntos de injección

Y es mediante el uso de estas vulnerabilidades que sqlmap, automaticamente, ha conseguido obtener las dos tablas de la base de datos:

Database: database
Table: usuarios
[1 entry]

dni	email	telef	nombre	passwd	usuario	nacimiento
46368446-D	imanolm.upv@gmail.com	684399392	Imanol Martinez	imanolMM	ImanolMM	2003-08-08

Figura 2.2: Tabla usuarios de la base de datos

Database: database
Table: eventos
[2 entries]

titulo	opcion1	opcion2	usuario	enunciado	resultado1	resultado2
Las aventuras de WIP games	Oro! Tenemos que coger todo lo que podamos! Nos haremos ricos!!	No hacemos nada, podría ser una trampa	Imanol	Era un día soleado cuando nos encontramos una cueva misteriosa, estaba muy oscura y nos dieron ganas de entrar. Poco a poco se hacía la luz dentro de la cueva y de repente vimos una estatua gigante rodeada de oro	Era una trampa, hemos caido en un agujero sin salida...	Nos vamos con las manos vacías pero con una increible historia que contar a nuestros hijos
¡¡Enanos!!	Te intentas liberar y peleas contra ellos	Usas tu linterna para intentar sorprenderles	ImanolMM	Te despiertas de una larga siesta y estas rodeado de enanos, Quita! Son demasiados y te estan intentando agarrar para meterte en una caja! Despues de un tiempo siendo transportado ves que te han llevado a su aldea.	Te dañan pero consigues escapar	Están sorprendidos. Nunca antes habían visto algo así, te toman por su dios y te dan de comer y beber

Figura 2.3: Tabla eventos de la base de datos

2.3.2. Cross Site Scripting

Tal y como hemos visto en la Introducción mediante el uso de ZAP hemos encontrado una vulnerabilidad de tipo XSS. En este caso, vamos a explotarlas de forma manual para ver que podemos hacer con ellas. Para ello accedemos al menu de 'Crear Evento' y en el campo 'Titulo' podemos introducir los siguientes codigos:

1. `<script>alert("XSS")</script>`
    - Este codigo nos muestra un mensaje de alerta con el texto 'XSS'

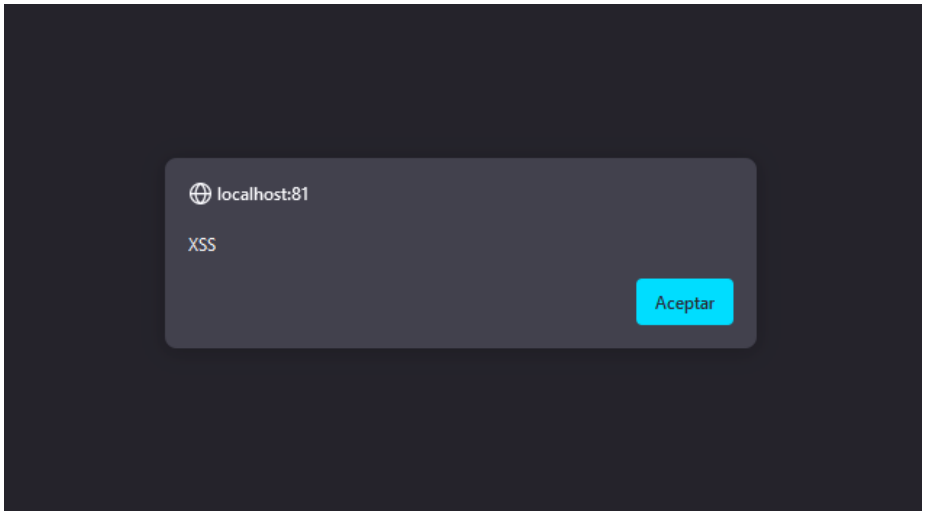

Figura 2.4: Alerta XSS

2. `<script>document.location="https://github.com/Xabierland«/script>`
    - Este codigo nos redirige a mi pagina de Github
3. `<img src="https://shorturl.at/avFJO»`
    - Este codigo nos muestra una imagen con el texto Pwned!

Figura 2.5: Imagen XSS

4. `<script>var paragraph = document.createElement('p');paragraph.textContent = 'Cookie: ' + document.cookie;document.body.appendChild(paragraph);</script>`

    - Este codigo nos muestra el contenido de la cookie de php

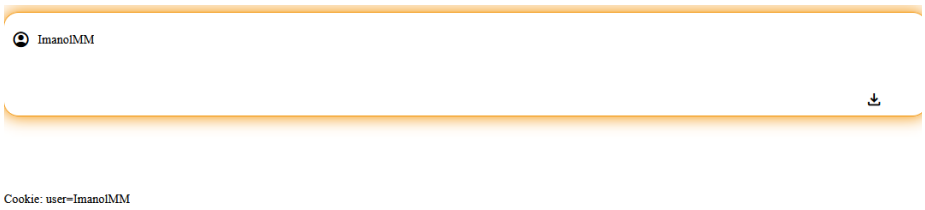

Figura 2.6: Cookie XSS

Este tipo de vulnerabilidad es muy peligrosa ya que permite a un atacante ejecutar codigo en el navegador de la victima y realizar acciones en su nombre.

Tambien hemos visto que podemos redirigir a la victima a una pagina maliciosa, lo que nos permitiria realizar un ataque de tipo Phishing.

Aunque la carga de la imagen no parezca muy peligrosa, esta, en realidad puede darnos informacion como la IP de los usuarios que visitan la pagina ya que para cargar dicha imagen se realiza una peticion al servidor donde esta alojada dejando su IP en el camino.

En este caso, hemos visto que podemos llegar incluso a ver la cookie de la victima, lo que nos permitiria hacer un ataque de tipo Session Hijacking.

2.4. Configuración de seguridad insuficiente

2.4.1. Fuga de información

2.4.2. Enumeración de directorios

2.4.3. Fuerza bruta

2.5. Componentes vulnerables y obsoletos

2.5.1. Vulnerabilidades mediante MF

2.6. Fallos de identificación y autenticación

2.6.1. Invalidación de sesiones

Bibliografia