PRÁCTICA 12

Seguridad en la Web

Grupo 06 – GIW

ÍNDICE

1. [Vulnerabilidades inyección SQL 4](#SQLVulnera)

1.1Vulnerabilidad 1 4

1.2 Vulnerabilidad 2 6

1.3 Vulnerabilidad 3 8

2. [Vulnerabilidades XSS persistente 10](#XSSPersistenteVulnera)

2.1 Vulnerabilidad 1 11

2.2 Vulnerabilidad 2 18

3. [Vulnerabilidades XSS reflejada 22](#XSSReflejadaVulnera)

3.1 Vulnerabilidad 1 23

3.2 Vulnerabilidad 2

1. **Vulnerabilidades inyección SQL**

|  |
| --- |
| **INFORME DE VULNERABILIDAD** |
| **Ruta(s) de la aplicación involucrada(s)** |
| http://localhost:8080/search\_question |
| **Tipo de vulnerabilidad** |
| SQL Injection |
| **Situaciones peligrosas o no deseadas que puede provocar** |
| Exposición de muchísimos datos de la base de datos. Aunque en este caso sean de carácter público, podrían ser privados. |
| **Ejemplo paso a paso de cómo explotar la vulnerabilidad (con capturas de pantalla)** |
| 1. Ir por ejemplo a la web que se muestra a continuación y colocar la siguiente declaración SQL:   C:\hlocal\P12 Seguridad en la Web\Capturas de pantalla\BuscadorSQLinjection.png   1. Una vez que nos introducimos en la dirección web, podemos comprobar cómo nos ha relevado todos los datos de la tabla Questions, debido a que ‘search\_question’ no comprueba los datos que le han llegado. |
| **Medidas para mitigar la vulnerabilidad** |
| COMPLETAR |

1. **Vulnerabilidad 1.1**
2. **Vulnerabilidad 1.2**

|  |
| --- |
| **INFORME DE VULNERABILIDAD** |
| **Ruta(s) de la aplicación involucrada(s)** |
| http://localhost:8080/insert\_question |
| **Tipo de vulnerabilidad** |
| SQL Injection |
| **Situaciones peligrosas o no deseadas que puede provocar** |
| Esta vulnerabilidad puede provocar la inserción de instrucciones SQL, provocando por ejemplo el borrado de tablas de la base de datos. |
| **Ejemplo paso a paso de cómo explotar la vulnerabilidad (con capturas de pantalla)** |
| 1. Colocarse en cualquiera de las rutas siguientes:   http://localhost:8080/show\_all\_questions  http://localhost:8080/search\_question?tag=Editor  http://localhost:8080/show\_question?id=1   1. Colocar la siguiente instrucción SQL a la hora de crear una pregunta:   C:\hlocal\P12 Seguridad en la Web\Capturas de pantalla\BodySQLinjection.png  También puedes introducir la declaración SQL en los campos Autor, Título o Etiquetas:  C:\hlocal\P12 Seguridad en la Web\Capturas de pantalla\AutorSQLinjection.pngC:\hlocal\P12 Seguridad en la Web\Capturas de pantalla\TituloSQLinjection.pngC:\hlocal\P12 Seguridad en la Web\Capturas de pantalla\EtiquetasSQLinjection.png |
| **Medidas para mitigar la vulnerabilidad** |
| COMPLETAR |

1. **Vulnerabilidades XSS persistente**
   1. **- Vulnerabilidad 2.1**

|  |
| --- |
| **INFORME DE VULNERABILIDAD** |
| **Ruta(s) de la aplicación involucrada(s)** |
| http://localhost:8080/insert\_reply |
| **Tipo de vulnerabilidad** |
| XSS persistente |
| **Situaciones peligrosas o no deseadas que puede provocar** |
| Esta vulnerabilidad puede provocar la inserción de instrucciones SQL, provocando por ejemplo el borrado de tablas de la base de datos. |
| **Ejemplo paso a paso de cómo explotar la vulnerabilidad (con capturas de pantalla)** |
| 1. Colocarse en cualquiera de las rutas siguientes:   http://localhost:8080/show\_question?id=1   1. Colocar la siguiente instrucción SQL a la hora de realizar una respuesta:   También puedes introducir la declaración SQL en los campos Autor, Título o Etiquetas: |
| **Medidas para mitigar la vulnerabilidad** |
| COMPLETAR |

1. **Vulnerabilidades XSS reflejada**
2. **Vulnerabilidad 3.1**

|  |
| --- |
| **INFORME DE VULNERABILIDAD** |
| **Ruta(s) de la aplicación involucrada(s)** |
| http://localhost:8080/search\_question |
| **Tipo de vulnerabilidad** |
| XSS reflejada |
| **Situaciones peligrosas o no deseadas que puede provocar** |
| Esta vulnerabilidad permite introducir ¿HTML? ¿JAVASCRIPT? en un buscador, provocando el direccionamiento a webs maliciosas. |
| **Ejemplo paso a paso de cómo explotar la vulnerabilidad (con capturas de pantalla)** |
| 1. Vamos a la ruta involucrada colocando una etiqueta existente como parámetro, como la siguiente:   C:\hlocal\P12 Seguridad en la Web\Capturas de pantalla\EditorTagXSSReflejada.png   1. Introducimos lo siguiente en “Búsqueda por etiqueta:” :   <META HTTP-EQUIV="REFRESH" CONTENT="5;URL=http://www.webmaliciosa.com">   1. La ruta de la aplicación nos redirija a los 5 segundos a la web maliciosa |
| **Medidas para mitigar la vulnerabilidad** |
|  |