Experto Universitario en Ethical Hacking

SQL Injection / XSS

Ejercicio 1 Unidad 4

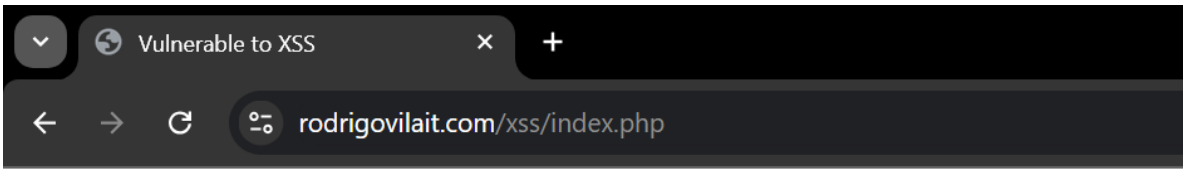
Buscar en Internet, sitios que sean vulnerables a XSS, utilizando únicamente el <script>alert("hola");</script>

La idea es que chequeen y vean que muchos sitios web son vulnerables a este tipo de técnicas, lo cual las medidas de seguridad que deberían aplicarse, no se encuentran aplicadas.

Exponer la captura únicamente, y dar su punto de vista sobre la técnica.

Respuesta:

Para realizar éste ejercicio cree un entorno vulnerable en mi propio laboratorio.



Pagina de búsqueda

Search: Submit

Pagina de práctica para curso de Hacking Ético de UTN.

Codigo fuente de la página:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
```

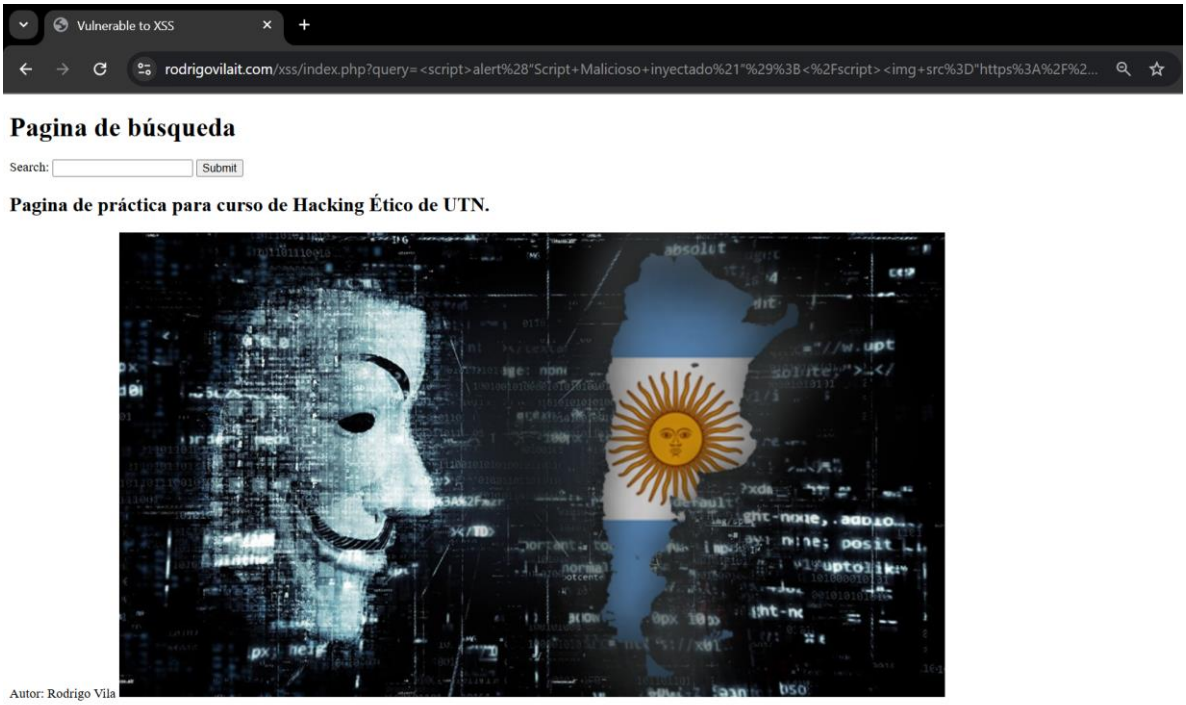
```
    <title>Vulnerable to XSS</title>
</head>
<body>
    <h1>Pagina de búsqueda</h1>
    <form method="GET" action="">
        <label for="query">Search:</label>
        <input type="text" id="query" name="query">
        <button type="submit">Submit</button>
    </form>

    <h2>Pagina de práctica para curso de Hacking Ético de UTN.</h2>
    <p>
        <?php
        if (isset($_GET['query'])) {
            // Inserta directamente sin sanitización
            echo "Autor: Rodrigo Vila " . $_GET['query'];
        }
        ?>
    </p>
</body>
</html>
```

Ingresamos <script>alert("Script Malicioso inyectado!");</script> en el campo de búsqueda:

Ahora procedemos a inyectar código para insertar una imagen en la estructura de la web:

“<script>alert(“Script Malicioso inyectado!”);</script>”



Una vez demostrado procedo a eliminar el sitio por cuestiones de seguridad.

Saludos!!!

Rodrigo Vila.-