



# Cross Site Scripting (XSS)

## From alert to pownage



# OWASP

The Open Web Application Security Project



@dcotelo13



dcotelo@outlook.co  
m



# OWASP

The Open Web Application Security Project

# Que es XSS?

- Típicamente encontrada en aplicaciones web.
- Ocurre cuando una aplicación toma datos ingresados por el usuario y los envía nuevamente al navegador
- El navegador de la víctima renderiza el código HTML y ejecuta el código seleccionado por el atacante típicamente JavaScript
- Esta vulnerabilidad no afecta directamente a la aplicación sino a los usuarios.
- Variantes
  - Reflejado (Indirecto)
  - Almacenado (Directo)
  - Basado en DOM



# OWASP

The Open Web Application Security Project

# XSS Reflejado

- El atacante genera un link que contiene el código malicioso
- Se hace disponible ese link a la víctima (E-mail, redes sociales, etc.)
- La víctima ingresa mediante el link a la aplicación
- La aplicación **Refleja** el código malicioso en el navegador de la víctima donde es renderizado y ejecutado.
- Comúnmente encontrado en
  - Formularios de login
  - Páginas de mensajes

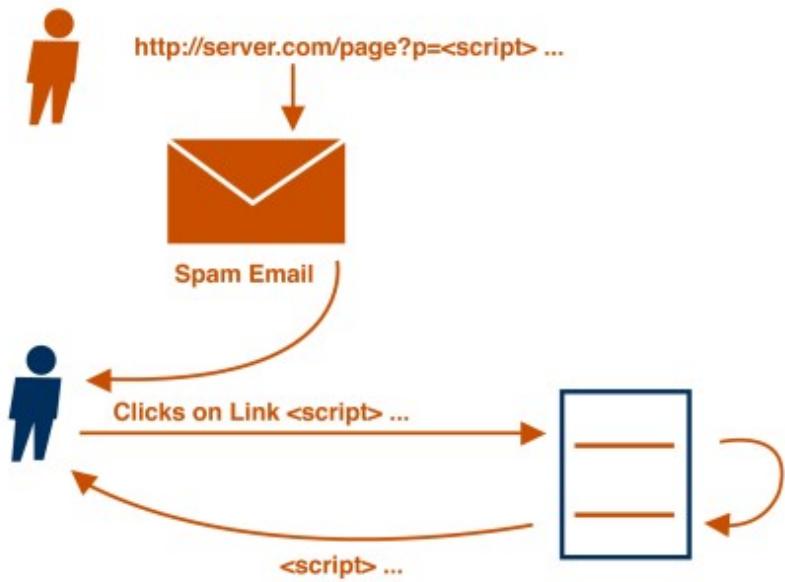


# OWASP

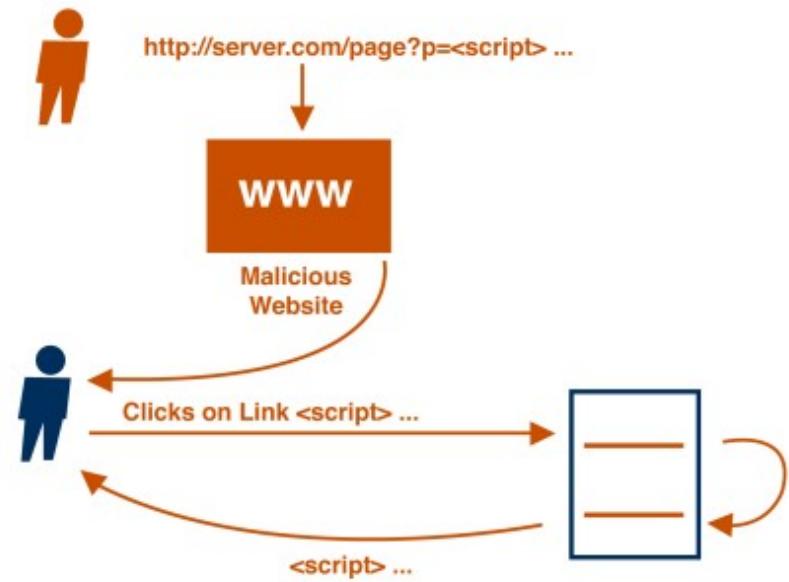
The Open Web Application Security Project

# XSS Reflejado

EX: 1



EX: 2





# OWASP

The Open Web Application Security Project

# Ejemplo XSS Reflejado

A screenshot of a web browser displaying a search results page. The URL bar shows a redacted URL followed by '/nuevo\_buscador.php?buscada=><img src%3Dx onerror%3Dalert("XSS-R' and a search term 'Buscar'. The main content area shows a search form with a placeholder 'Ingrese aquí su búsqueda' and a 'BUSCAR' button. A modal dialog box is open, displaying the text 'XSS-Reflejado' and a 'Aceptar' button. At the bottom of the page, the source code of the reflected payload is visible in the browser's developer tools, specifically the 'Elements' tab:

```
<input id="buscada" type="hidden" value="" name="buscada"></input>
</img>
```

**Díganos Cómo somos**

Vea aquí nuestros **Servicios**



# OWASP

The Open Web Application Security Project

# XSS Almacenado

- El atacante postea código malicioso o payload en el sitio afectado el cual persiste en el almacenamiento de la aplicación (SQL, XML, Etc.)
- La víctima visita el sitio donde se es ejecutado por el navegador del usuario.
- Comúnmente encontrado en
  - CMS
  - Foros
  - Sistemas de comentarios

```
209 public function getDateLastUpdated($format = '%x') {
210
211
212     if ($this->date_last_updated === null || $this->date_l
213         return null;
214     } elseif (!is_int($this->date_last_updated)) {
215         // A non-timestamp value was set externally, so we
216         // assume it's a timestamp and convert it.
217         $ts = strtotime($this->date_last_updated);
218         if ($ts === -1 || !$ts)
219             throw new ProprietaryException(
220                 'The date last updated value is invalid');
221         else
222             $ts = $this->date_last_updated;
223     }
224     if ($format === null) {
225         return $ts;
226     } elseif (strpos($format, '%') !== false) {
227         return strftime($format, $ts);
228     } else {
229         return date($format, $ts);
230     }
231 }
```

You appear to be writing a PHP CMS.  
Would you like me to automatically insert XSS vulnerabilities?

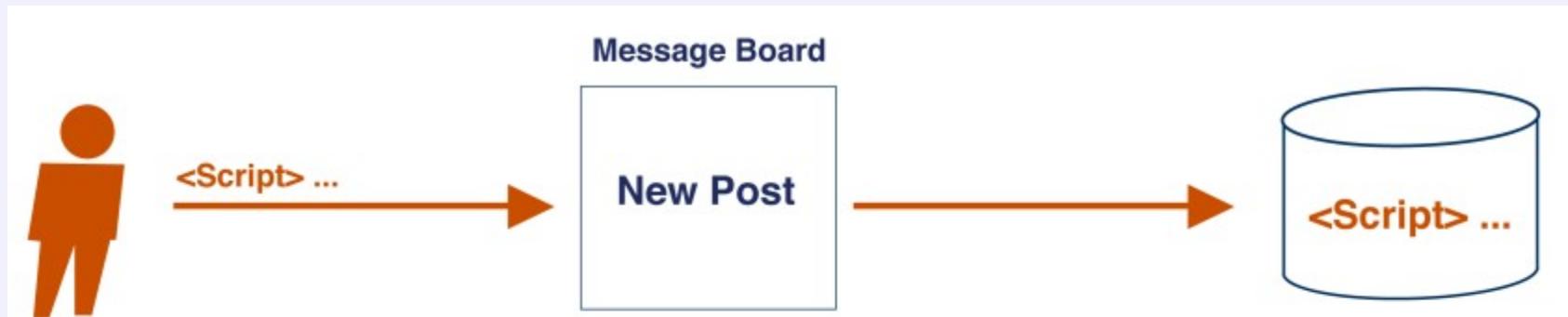
Yes



# OWASP

The Open Web Application Security Project

# XSS Almacenado





# OWASP

The Open Web Application Security Project

# Ejemplo XSS Almacenado

modificar\_domicilio.php?idDomicilio=595899

Chat Online Contacto Ayuda

Modificar Domicilio

Pais: Departamento / Provincia: Localidad / Barrio:

Uruguay \* Treinta y Tres \* Treinta y Tres \*

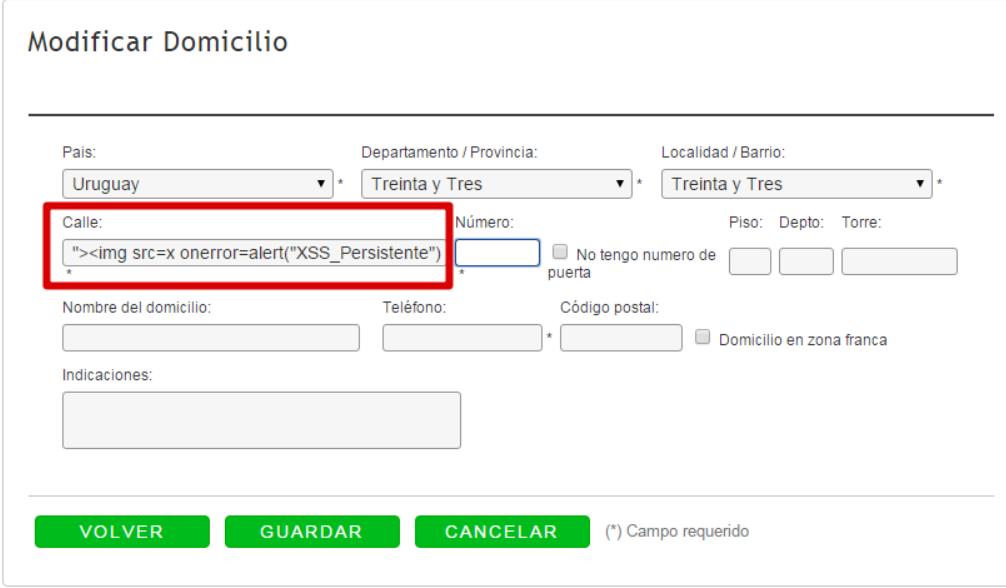
Calle: Número: Piso: Depto: Torre:

"><img src=x onerror=alert("XSS\_Persistente")" \* No tengo numero de puerta

Nombre del domicilio: Teléfono: Código postal: \* Domicilio en zona franca

Indicaciones:

VOLVER GUARDAR CANCELAR (\*) Campo requerido





# OWASP

The Open Web Application Security Project

# Ejemplo XSS Almacenado

A screenshot of a web browser displaying a web page. The URL bar shows a redacted URL ending in 'domicilios.php?r'. The page content includes a form titled 'Seleccione domicilio de entrega' with a 'Dirección' field containing '>'. A modal dialog box is overlaid on the page, titled 'Mensaje de la página https://[redacted]'. The dialog contains the text 'XSS\_Persistente' and a checkbox labeled 'Evita que esta página cree cuadros de diálogo adicionales.' A blue 'Aceptar' button is at the bottom right of the dialog. The bottom left corner of the image shows a portion of the page's source code in a code editor, highlighting a section of JavaScript code:

```
<td class="td_border">
  ">
    <script src="x" onerror="alert("XSS_Persistente");">...</script>
  </td>
</tr>
```



# OWASP

The Open Web Application Security Project

# XSS basado en DOM

- El atacante genera un link que contiene el código malicioso
- Se hace disponible ese link a la víctima (E-mail, redes sociales, etc.)
- La víctima ingresa mediante el link a la aplicación
- Permite controlar el flujo del objeto (toma de decisiones)
- Elementos potencialmente vulnerables.
  - document.URL
  - document.URLUnencoded
  - document.location (y demás propiedades)
  - document.referrer
  - window.location (y demás propiedades)



# OWASP

The Open Web Application Security Project

# Impacto del XSS

- Impacto moderado
- Posibles resultados de un ataque
  - Web defasment
  - Secuestro de navegador
  - Robo de sesión
  - Propagación de malware
- Utilizado para ataques mas elaborados y de mayor impacto





# OWASP

The Open Web Application Security Project

## Algunas consideraciones

- Validación de campos y parámetros ingresados por el usuario
  - Que largo debe tener?
  - Que caracteres son adecuados?
  - Que patrón seria valido?
  - Es un capo requerido?
- Encoding de la salidas.
- Recordar que todas las peticiones HTTP están bajo el control del atacante (Parámetros, POTS, GET, Headers, etc.)

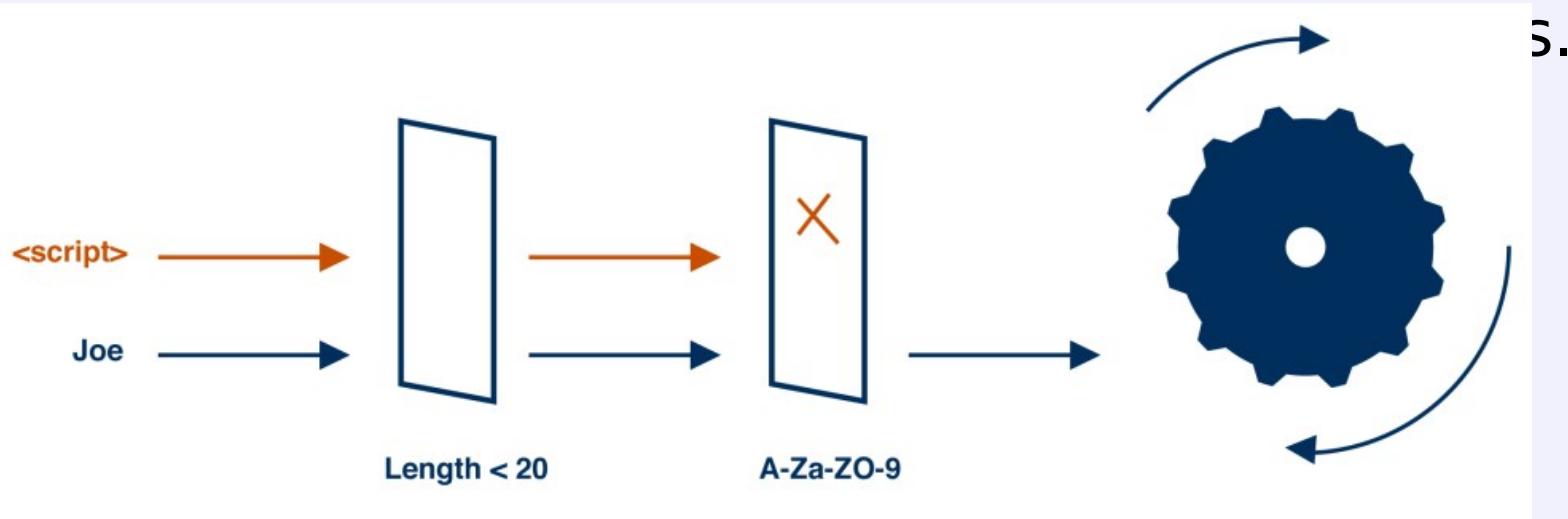


# OWASP

The Open Web Application Security Project

# Validación de lista negra

- Filtrar los males conocidos
- Requiere mantenimiento ya que la lista debe ser actualizada permanentemente con sets caracteres y nuevos patrones





# OWASP

The Open Web Application Security Project



## Validación lista blanca

- Chequear que los datos estén comprendidos entre la lista de valores aceptables.
- Los datos deben ser
  - Fuertemente tipados
  - Chequear y minimizar el largo de los campos.
  - Chequear si es un campo numérico.
  - Se debe corroborar la sintaxis antes de ser usados.



# OWASP

The Open Web Application Security Project

# Medidas preventivas

- Es altamente recomendable utilizar una biblioteca especialmente diseñada para esta tarea
- Algunas bibliotecas:
  - HtmlSanitizer (.NET) - <https://github.com/mganss/HtmlSanitizer>
  - OWASP Java HTML Sanitizer -  
[https://www.owasp.org/index.php/OWASP\\_Java\\_HTML\\_Sanitizer\\_Project](https://www.owasp.org/index.php/OWASP_Java_HTML_Sanitizer_Project)
  - -PHP Html Purifier - <http://htmlpurifier.org/>
  - -JavaScript/Node.JS Bleach - <https://github.com/ecto/bleach>
  - -Python Bleach - <https://pypi.python.org/pypi/bleach>



# OWASP

The Open Web Application Security Project

# ¿Preguntas?





# OWASP

The Open Web Application Security Project



@dcotelo13



dcotelo@outlook.co  
m