

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 victima 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 victima (E-mail, redes sociales, etc.)
- La victima ingresa mediante el link a la aplicación
- La aplicación **Refleja** el código malicioso en el navegador de la victima donde es renderizado y ejecutado.
- Comúnmente encontrado en
 - Formularios de login
 - Paginas de mensajes

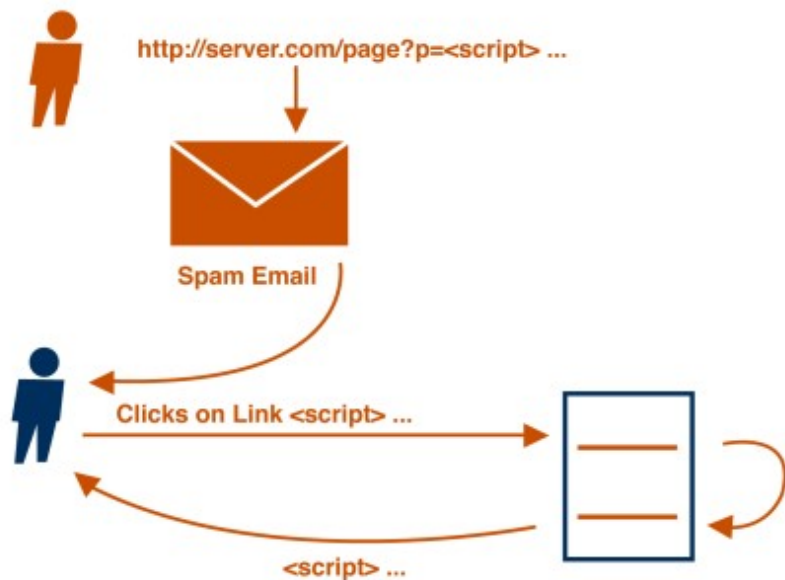


OWASP

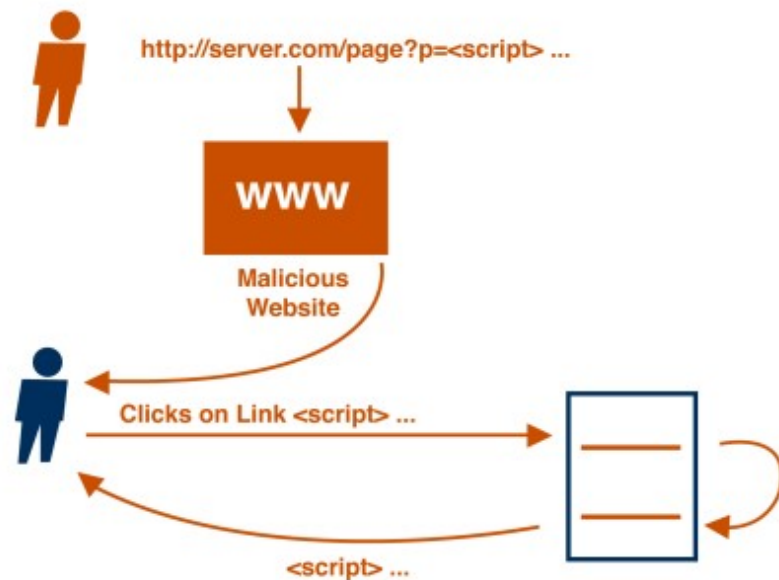
The Open Web Application Security Project

XSS Reflejado

EX: 1



EX: 2





OWASP

The Open Web Application Security Project

Ejemplo XSS Reflejado

new_buscador.php?buscada= "><img src%3Dx onerror%3Dalert("XSS-F

Precios y stock correspondientes a: Central

Ingrese aquí su búsqueda **BUSCAR**

Comprar por Sección

XSS-Reflejado

Aceptar

```
<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         $ts = strtotime($th
217         if ($ts === -1 || $
218             throw new Prop
219     }
220     } else {
221         $ts = $this->date_l
222     }
223     if ($format === null) {
224         return $ts;
225     } elseif (strpos($format, '%') !== false) {
226         return strftime($format, $ts);
227     } else {
228         return date($format, $ts);
229     }

```

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

Yes

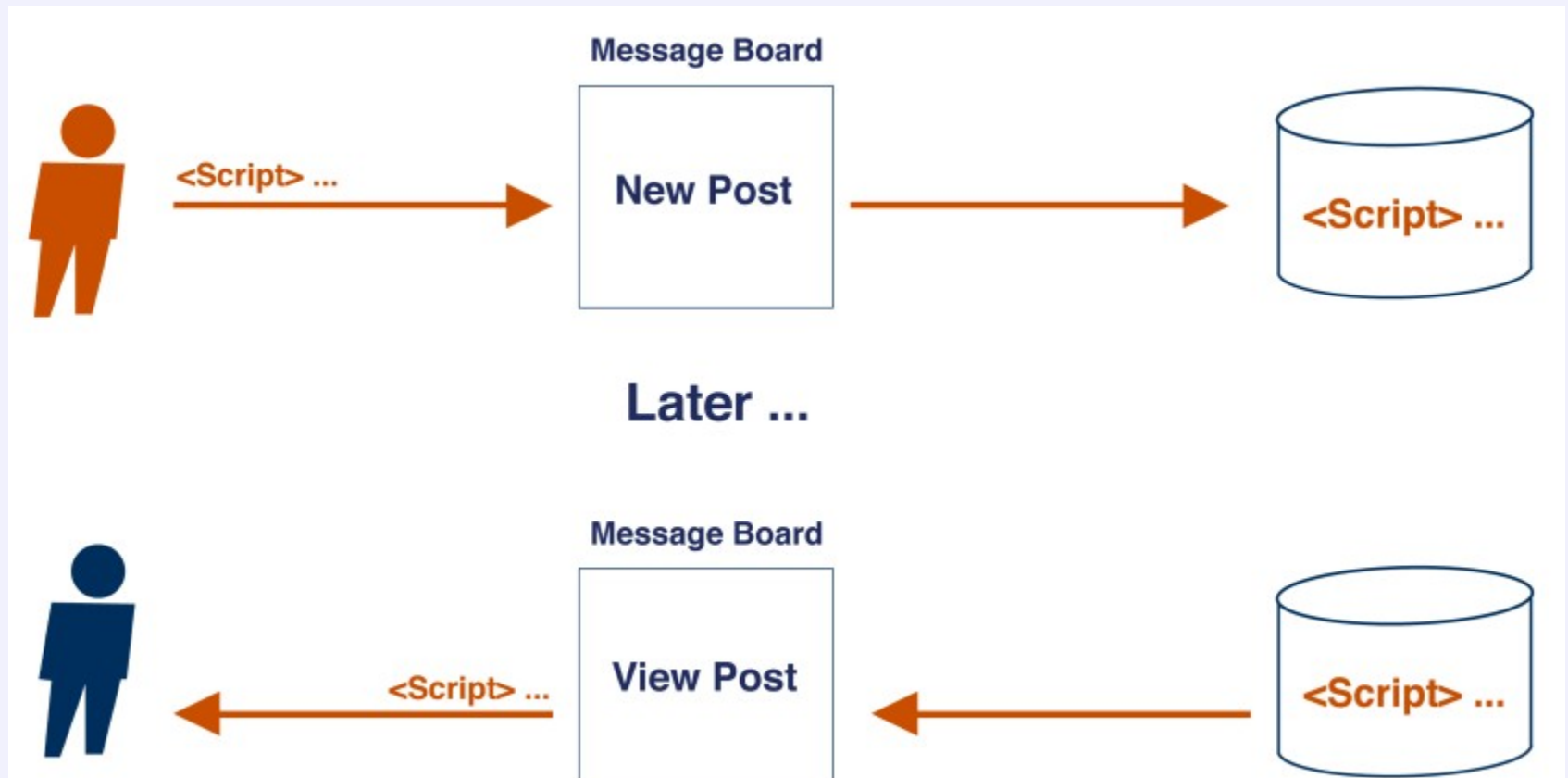




OWASP

The Open Web Application Security Project

XSS Almacenado





OWASP

The Open Web Application Security Project

Ejemplo XSS Almacenado

← → ↻ [REDACTED] /modificar_domicilio.php?idDomicilio=595899

[Chat Online](#) [Contacto](#) [Ayuda](#)

Modificar Domicilio

Pais:

Uruguay ▼ *

Departamento / Provincia:

Treinta y Tres ▼ *

Localidad / Barrio:

Treinta y Tres ▼ *

Calle:

"><img src=x onerror=alert('XSS_Persistente')" *

Nombre del domicilio:

Indicaciones:

Número:

Piso: Depto: Torre:

☐ No tengo numero de puerta

☐ Domicilio en zona franca

VOLVER

GUARDAR

CANCELAR

(*) Campo requerido



OWASP

The Open Web Application Security Project

Ejemplo XSS Almacenado

← → ↻ [Redacted URL] domicilios.php?r

Chat Online Contacto Ayuda

Seleccione donde...

Domicilio de entrega

Dirección

">

Mensaje de la página [Redacted URL] x

XSS_Persistente

☐ Evita que esta página cree cuadros de diálogo adicionales.

Aceptar

```
<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)

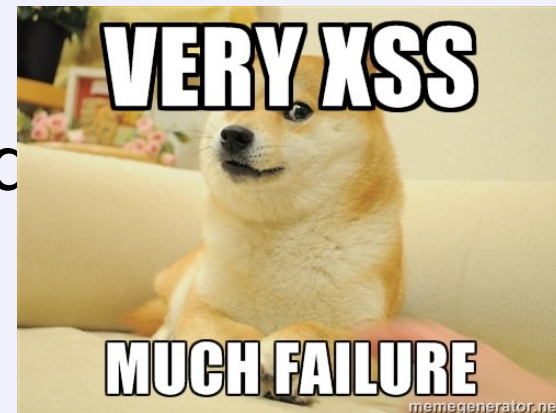


OWASP

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 sería valido?
 - Es un campo requerido?
- Encoding de la salidas.
- Recordar que todas las peticiones HTTP están bajo el control del atacante (Parámetros, POTS, GET, Headers, etc.)

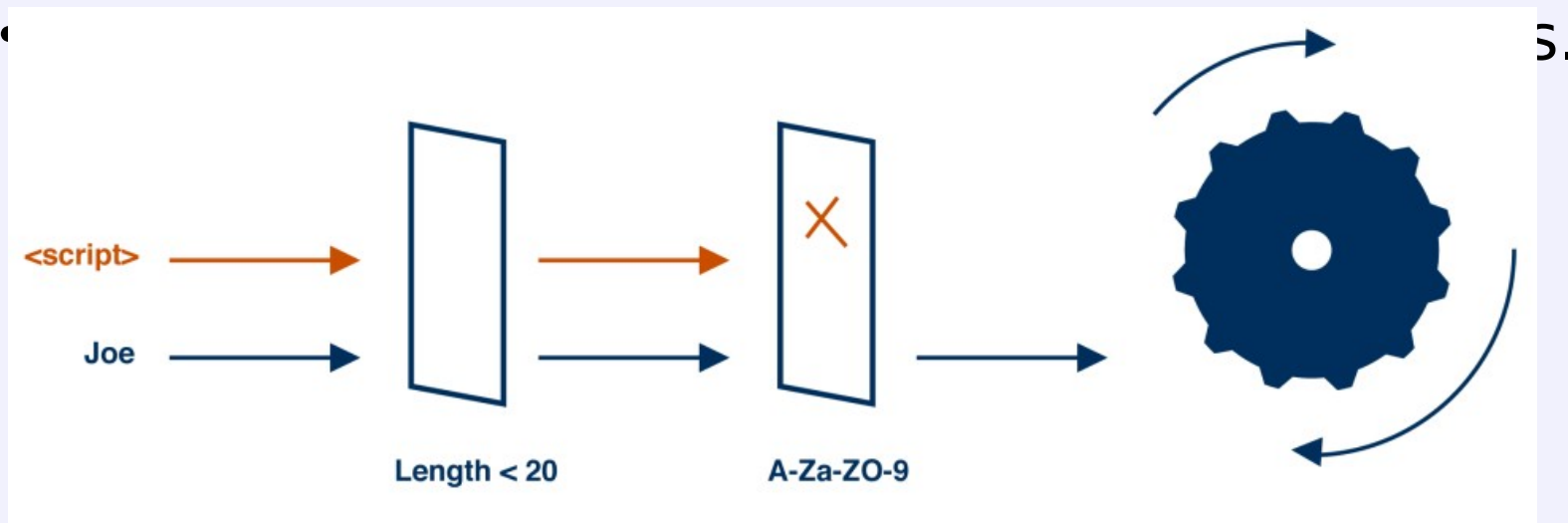


OWASP

The Open Web Application Security Project

Validación de lista negra

- Filtrar los males conocidos
- Requiere mantenimiento ya que la lista deber 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

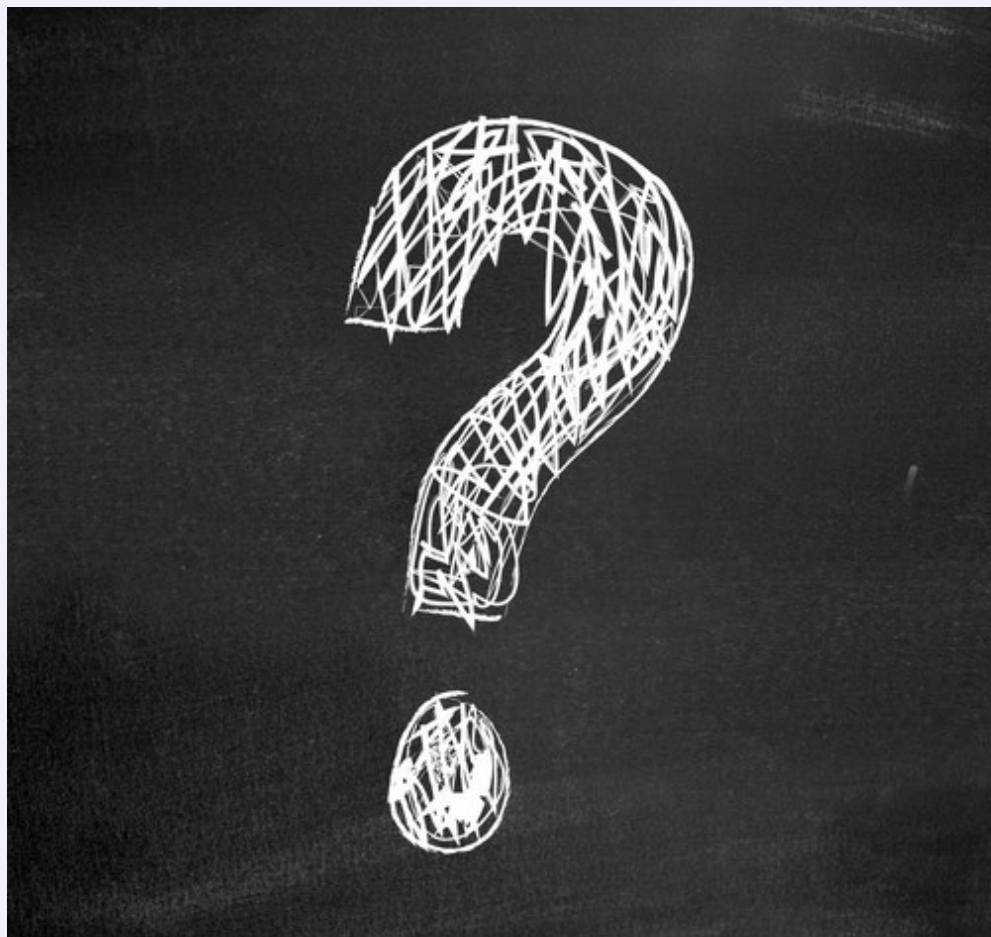
- Es altamente recomendable utilizar una biblioteca especialmente diseñada para esta tarea
- Algunas bibliotecas:
 - HtmlSanitizer (.NET) - <https://github.com/mganss/HtmlSanitizer>
 - OWASP Java HTML Sanitizer - https://www.owasp.org/index.php/OWASP_Java_HTML_Sanitizer_Project
 - -PHP Html Purifier - <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



**MUCHAS GRACIAS
POR SU ATENCIÓN**



@dcotelo13



**dcotelo@outlook.co
m**