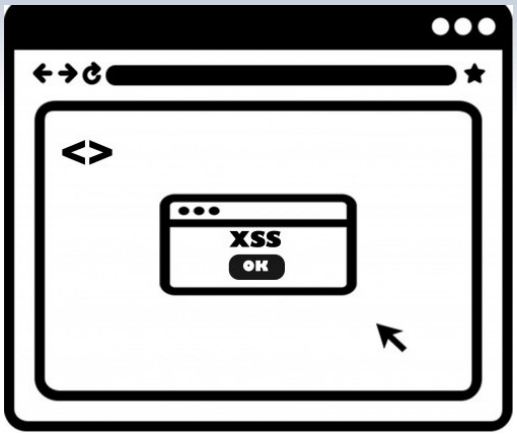


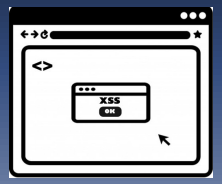
Cross Site Scripting

Enrique Alexis Peinado Rodriguez
Julio Cesar Silva Leon

Gerson André Garrido Mantillo

June 28, 2017

Seguridad Informática - Ciencia de la Computación



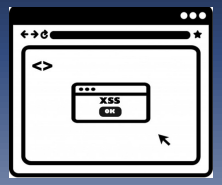
Overview

Introduction

XSS es un tipo de vulnerabilidad en seguridad informática que se encuentran típicamente en aplicaciones web benignos y de confianza .

Introduction

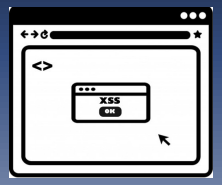
XSS es un tipo de vulnerabilidad en seguridad informática que se encuentran típicamente en aplicaciones web benignos y de confianza . Cross-Site Scripting (XSS) se producen cuando:



Introduction

XSS es un tipo de vulnerabilidad en seguridad informática que se encuentran típicamente en aplicaciones web benignos y de confianza . Cross-Site Scripting (XSS) se producen cuando:

1. Los datos que se ingresan a una aplicación Web a través de una fuente no fiable, la más frecuente es una solicitud web.
2. Los datos se incluyen en el contenido dinámico que se envia a un usuario web sin ser validado para contenido malintencionado.



Introduction

XSS es un tipo de vulnerabilidad en seguridad informática que se encuentran típicamente en aplicaciones web benignos y de confianza . Cross-Site Scripting (XSS) se producen cuando:

1. Los datos que se ingresan a una aplicación Web a través de una fuente no fiable, la más frecuente es una solicitud web.
2. Los datos se incluyen en el contenido dinámico que se envia a un usuario web sin ser validado para contenido malintencionado.

Antecedentes

Las vulnerabilidades de XSS se han reportado y explotado desde los años 1990. Sitios prominentes afectadas en el pasado incluyen los sitios de redes sociales de Twitter, Facebook, MySpace, YouTube y Orkut.

Facebook

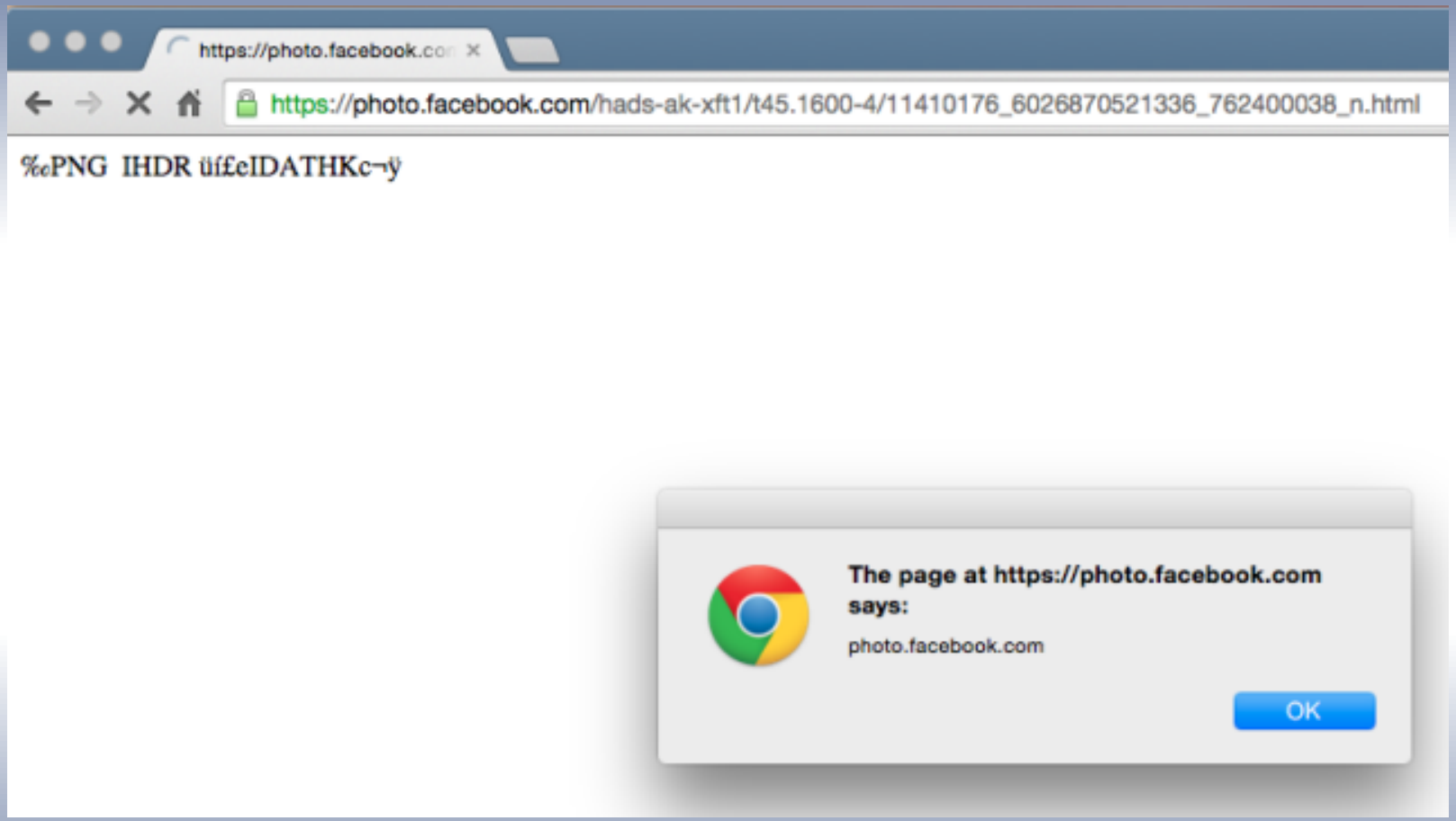
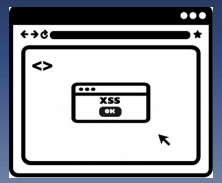


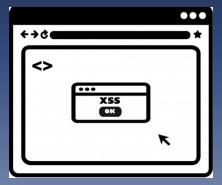
Figure: Uso de la esteganografía



¿Cómo clasificarlas?

Categorías de vulnerabilidades

- XSS almacenado (AKA persistente o tipo I)
- XSS reflejado (AKA no persistente o tipo II)
- DOM basado en XSS (AKA tipo-0)



¿Cómo clasificarlas?

Categorías de vulnerabilidades

- XSS almacenado (AKA persistente o tipo I)
- XSS reflejado (AKA no persistente o tipo II)
- DOM basado en XSS (AKA tipo-0)

Tipos de scripts entre sitios

- Server XSS
- Client XSS

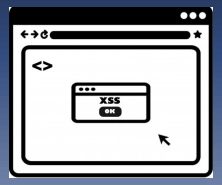
Formas de tipos de ataques

Where untrusted data is used

Data Persistence	XSS	Server	Client
	Stored	Stored Server XSS	Stored Client XSS
	Reflected	Reflected Server XSS	Reflected Client XSS

- DOM Based XSS is a subset of Client XSS (where the data source is from the DOM only)
- Stored vs. Reflected only affects the likelihood of successful attack, not the nature of vulnerability or the most effective defense

Figure: Formas de ataques

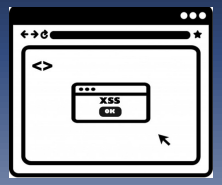


¿Como saber si soy vulnerable?

La mejor manera de encontrar fallas es realizar una revisión de seguridad del código.

- buscar todos los lugares donde exista una entrada de una solicitud HTTP pues posiblemente podría hacer su camino en la salida HTML.

Debemos tener en cuenta que una variedad de etiquetas HTML diferentes se pueden utilizar para transmitir un JavaScript malicioso.



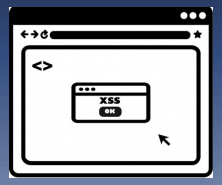
¿Qué hacer?

Existen herramientas disponibles que pueden ayudar a escanear un sitio web para estos defectos.

1. Scan My Server
2. SUCURI
3. Qualys SSL Labs, Qualys FreeScan
4. Quttera
5. Detectify
6. SiteGuarding
7. Web Inspector
8. Acunetix

Principales defensas en el OWASP

Figure: https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Chea



Primeras acciones

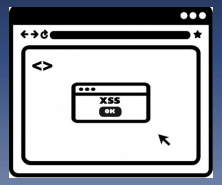
Desactivar el soporte de HTTP TRACE en todos los servidores web. Un atacante puede robar datos de cookies a través de Javascript, incluso cuando document.cookie está deshabilitado o no es compatible con el cliente.

```
TRACE /<script>foo()</script> HTTP/1.1
Host: test.lab
X-Wing: <script>bar()</script>
\r\n
```

Request

```
HTTP/1.1 200 OK
Date: Tue, 11 May 2010 18:58:16 GMT
Server: MPS
Transfer-Encoding: chunked
Content-Type: message/http
\r\n
5a
TRACE /<script>foo()</script> HTTP/1.1
Host: test.lab
X-Wing: <script>bar()</script>
\r\n
\r\n
0
\r\n
```

Response

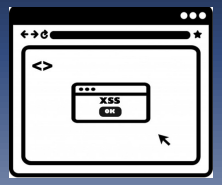


Defensas Recomendas

Servidor XSS

El servidor XSS se debe a la inclusión de datos no confiables en una respuesta HTML. La defensa más fácil y más fuerte contra el servidor XSS en la mayoria de los casos es:

- Codificación de salida del lado del servidor sensible al contexto



Defensas Recomendas

Servidor XSS

El servidor XSS se debe a la inclusión de datos no confiables en una respuesta HTML. La defensa más fácil y más fuerte contra el servidor XSS en la mayoria de los casos es:

- Codificación de salida del lado del servidor sensible al contexto

Cliente XSS

El cliente XSS se produce cuando se utilizan datos no fiables para actualizar el DOM con una llamada insegura de JavaScript. La defensa más fácil y más fuerte contra el Cliente XSS es:

- Uso de API JavaScript seguras

Credits

- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_
- http://blog.segu-info.com.ar/2016/02/cross-site-scripting-xss-en.html
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet