Cross Site Scripting

OWASP – Edmonton
December 5, 2006

Yegor Jbanov
What are we going to discuss?

- XSS Definition
- XSS-Friendly Environment
- What is the role of the web-browsers?
- XSS Types: DOM-based, non-persistent and persistent
- Discussion
**Definition**

**OWASP:** When attacker uses a web-site to send malicious code to a different user

**Wikipedia:** A type of vulnerability in web-apps which allow code injection

**My Definition:** When one web-site gains partial or complete control over another web-site. XSS is:
- Not necessarily web-site's fault
- Not necessarily browser's fault
Prerequisites & Causes

Prerequisites

- The victim web-site must accept user input
- The attacker has to know the document structure of the victim web-site

Causes

- Weak user input validation which allows passing blocks of client-side executable script, e.g. JavaScript/JScript, VBScript
- Unencoded user-provided information being rendered as part of a web-page
There are at least two known techniques that a web-browser can employ to make XSS more difficult. However, a web-browser alone cannot prevent all kinds XSS attacks.

<table>
<thead>
<tr>
<th></th>
<th>Local Objects</th>
<th>Encoded URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Opera</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Firefox/Netscape</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Because all of the most popular web-browsers implement Local Objects technique in order to perform XSS the script must be injected into the web-page (see OWASP and Wikipedia definitions).
DOM-based XSS is a kind of attack which uses the fact that a webpage receives and uses user-provided data inside the client-side script. The script may never even reach the server.

**Scope:** Directly affects only one user at a time when the user visits attacker's site

**Example:** Bugzilla used `document.location` to print current URL on the page

**Fix:** Character escaping
Type 1: Non-persistent

Non-persistent (also reflected) XSS is a kind of attack which uses the fact that a web-page is rendered by the server immediately using user-provided data without saving it.

Scope: Directly affects only one user at a time when the user visits attacker's site
Example: Common in web-site searching when the search term is shown immediately on the web-page but not stored on the server. Happened on www.bbc.co.uk
Fix: Character escaping
Persistent XSS is a kind of attack which uses the fact that a web-application allows storing user-provided data on the server without a strong validation and viewed later.

**Scope:** May directly affect all users visiting victim's site containing attacker's post

**Example:** Common in online e-mail systems and message boards, e.g. Microsoft's Hotmail e-mail system would print JavaScript stored in an e-mail message.

**Fix:** Stronger content filtering
Questions?