OWASP VAC – Cross Site Scripting

9 april 2009
Martin Visser
Overview

• Cross Site Scripting or XSS
  > Vulnerability
  > Attack
  > Countermeasures
Overview

• **Cross Site Scripting is**
  > injection of script interpreted on client
  > failure to preserve web page structure
  > a misnomer since the same origin policy in browsers

• **Cross Site Scripting can be**
  > Stored
  > Reflected
  > DOM based (less common)
Overview
Overview

- **Cross Site Scripting is**
  - injection of script interpreted on client
  - failure to preserve web page structure
  - a misnomer since the same origin policy in browsers

- **Cross Site Scripting can be**
  - Stored (script injection)
  - Reflected (direct echo)
  - DOM based (less common)
Overview - Stored XSS
Overview - Reflected XSS
Overview - Reflected XSS
Overview - Facts & Figures

- No. 1 in top 10 2007
- SANS top 25
- 32,384 registered occurrences
  > MySpace.com
  > Google.com
  > Nasa.gov
  > McAfee.com (hacker-safe ;)
  > Etc.
- Some claim 80% of sites vulnerable
XSS - Vulnerability

- Very common
- Easily found
  > XSSed.com: 20,000+ unfixed
- Underestimated
- Misunderstood
  > “Our site uses SSL”
- “First stage” in attacks
  > CSRF
  > DoS
**XSS - Vulnerability**

- **A few examples**
  - Deface your site
  - Steal your cookies
  - Phish your valuable data
  - Spread as a very efficient worm

*First 24 Hours of Worm Propagation*

WhiteHat Security 2006
Attacks with Javascript

- HTML attributes
  - `<body onload=alert('test1')>`
  - `<b onmouseover=alert('Wufff!')>click me!</b>`
  - `<img src="http://url.to.file.which/not.exist" onerror=alert(document.cookie);>`

- Encoded URI
  - `<IMG SRC=j&(#X41vascript:alert('test2')>`

- Code encoding
  - `<META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgndGVzdDMnKTwvc2NyaXB0Pg">`
XSS - Attack

- Some examples
XSS - Countermeasures

• **Use input validation**
  > Whitelist
  > Defense-in-depth strategy
  > Define trust boundaries

• **Use encoding**
  > Whitelist
  > Both input and output
  > In the appropriate context
    • HTML, URL, CSS, XML, JavaScript, HTML Attributes, VB script, etc.
XSS - Countermeasures

- **Architecture & Design**
  - Use protection in framework
  - Ensure input validation & encoding

- **Implementation**
  - OWASP prevention cheat sheet
  - OWASP ESAPI Encoding module
  - Static code analysis

- **Test**
  - Use tools like CAL9000
  - RSnake’s XSS cheat sheet

- **Operations**
  - Application firewall
Further Reading

- OWASP
- Google Code Best Practices
Staat voor resultaat