OWASP VAC
-
Cross Site Scripting

9 april 2009

Martin Visser

Overview

- **Cross Site Scripting or XSS**
  - > **Vulnerability**
  - > **Attack**
  - > **Countermeasures**

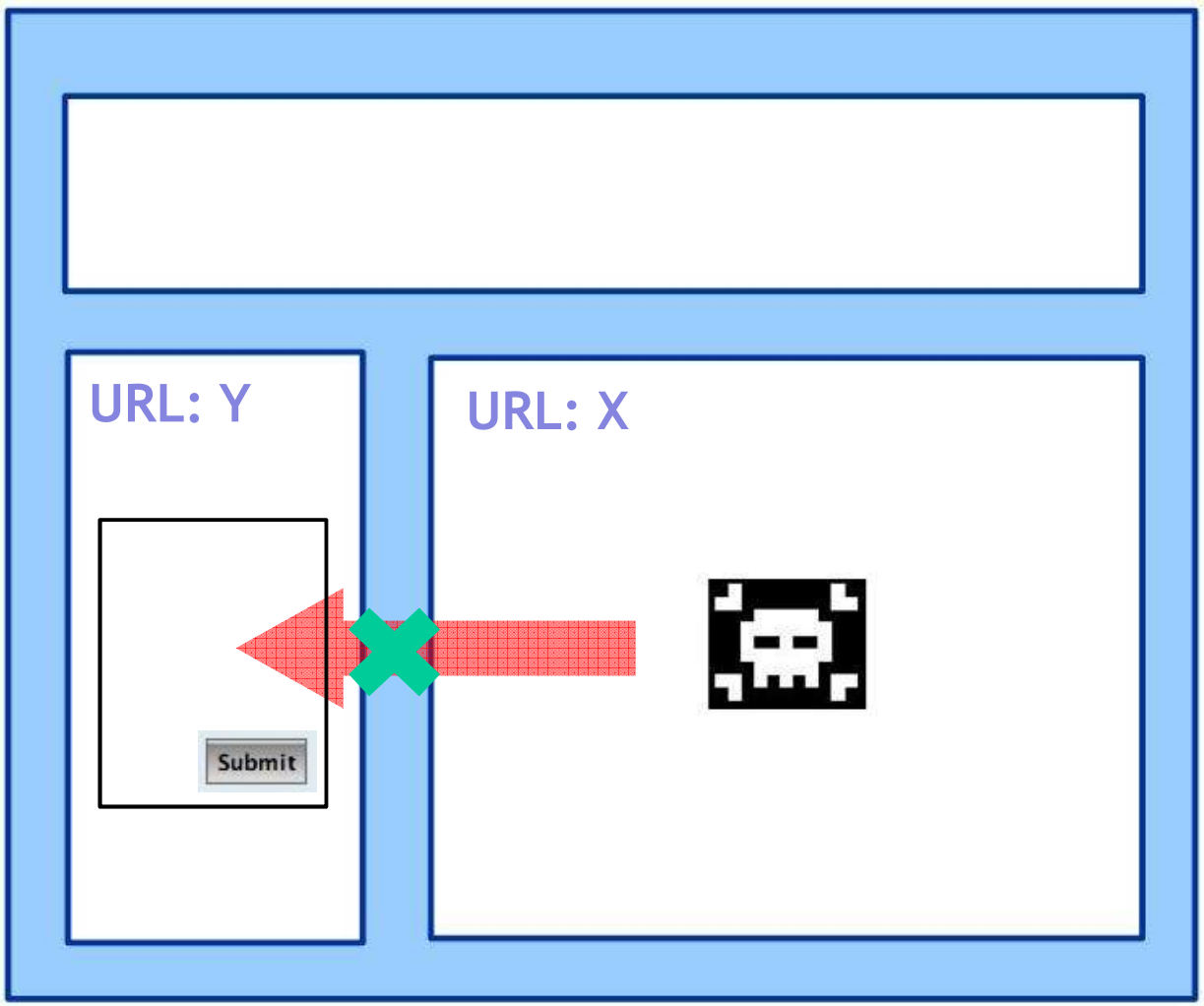
SOGETI

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)**

SOGETI

Overview

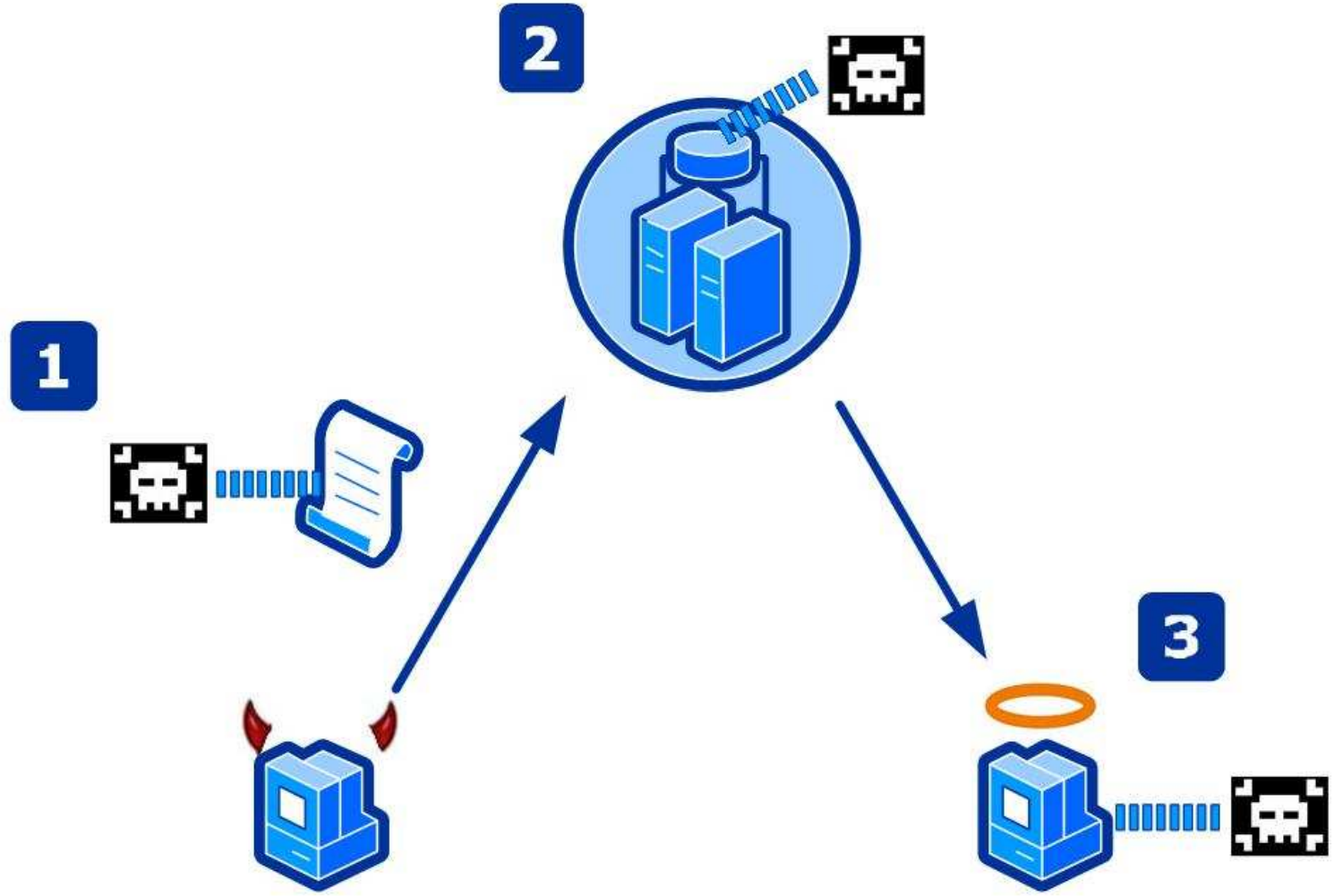


SOGETI

Overview

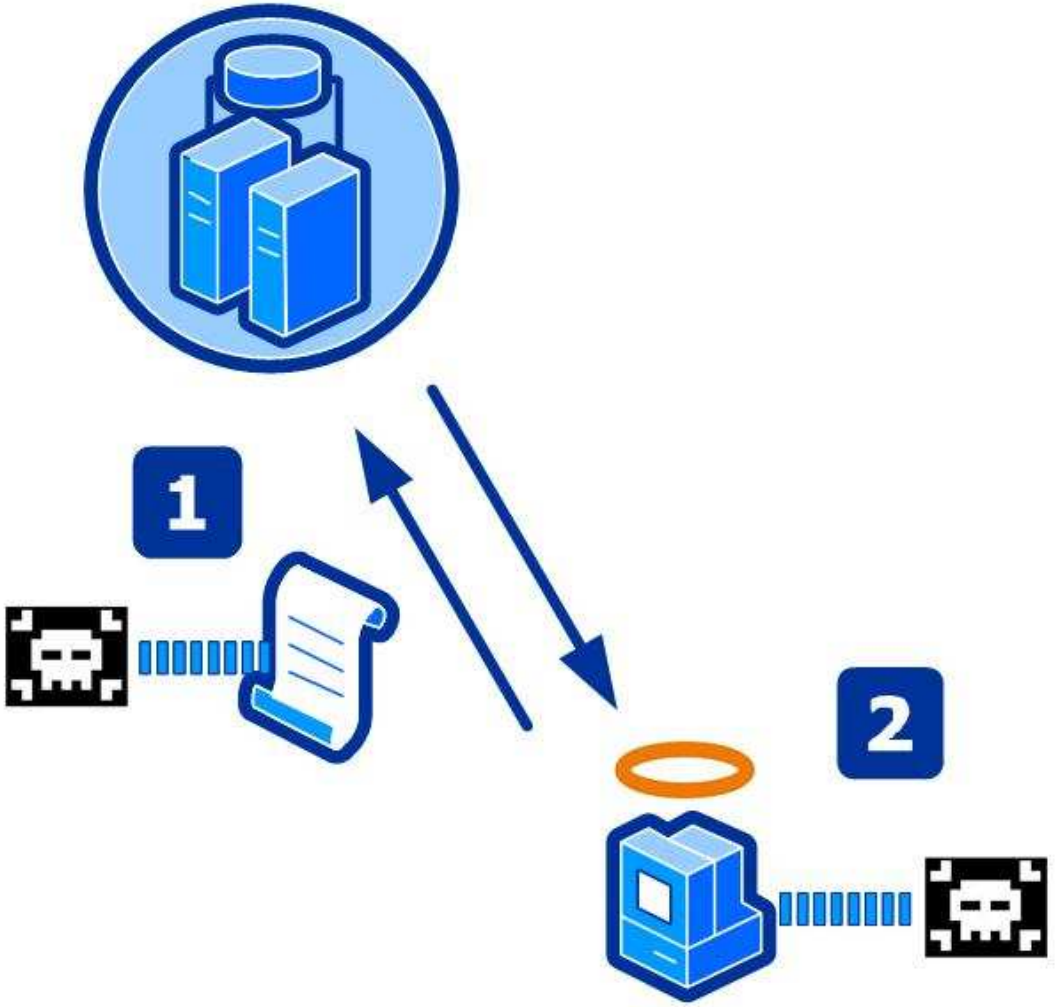
- **Cross Site Scripting is**
  - > **injection of script interpreted on client**
  - > **failure to preserve web page structure**
  - > **a misnomer since the same origin policy in browsers**
- **Cross Site Scripting can be**
  - > **Stored (script injection)**
  - > **Reflected (direct echo)**
  - > **DOM based (less common)**

Overview - Stored XSS



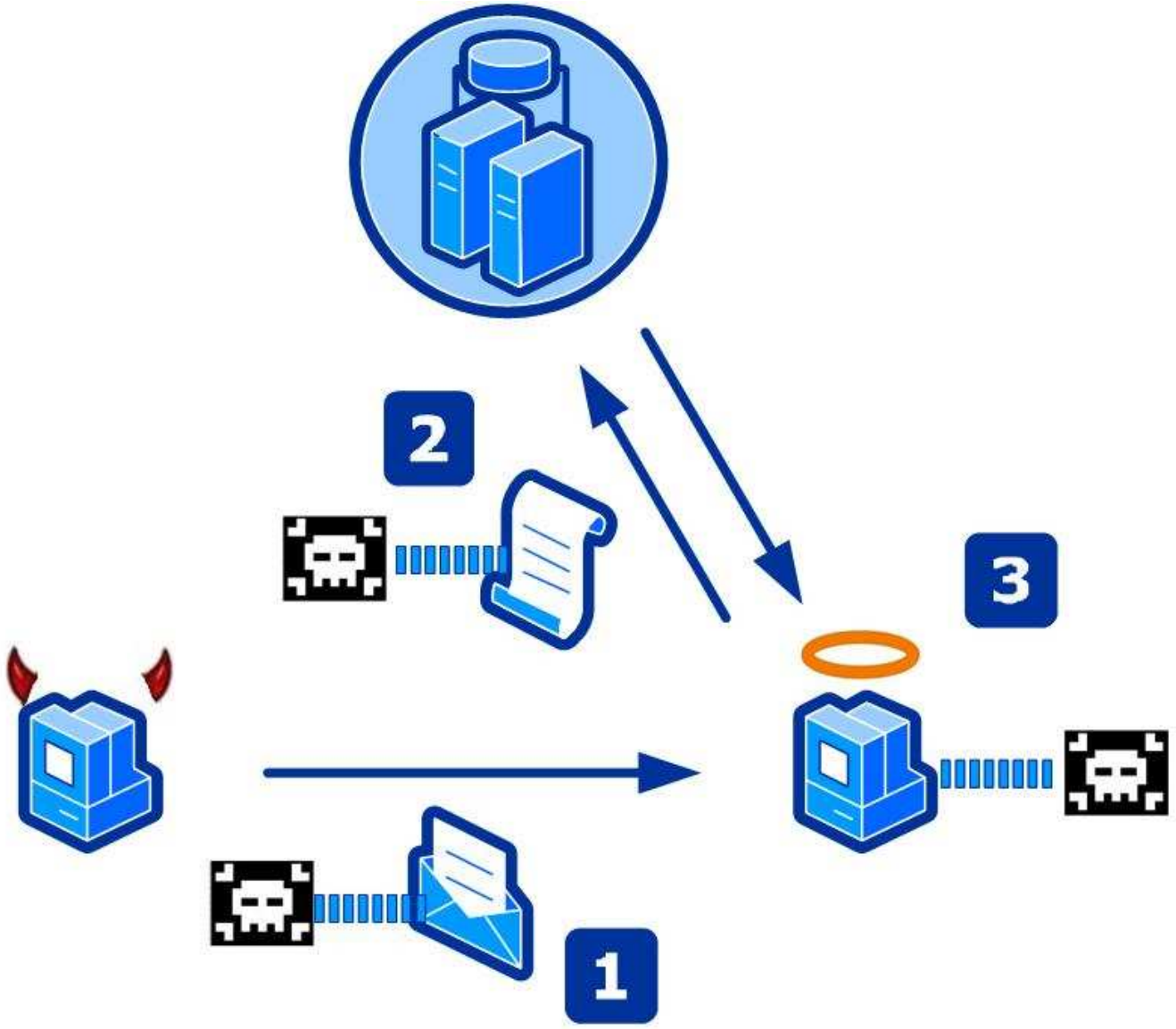
SOGETI

Overview - Reflected XSS



SOGETI

Overview - Reflected XSS



SOGETI

Overview - Facts & Figures

- **No. 1 in top 10 2007**
- **SANS top 25**
- **32.384 registered occurences**
  - > **MySpace.com**
  - > **Google.com**
  - > **Nasa.gov**
  - > **McAfee.com (hacker-safe ;)**
  - > **Etc.**
- **Some claim 80% of sites vulnerable**

SOGETI

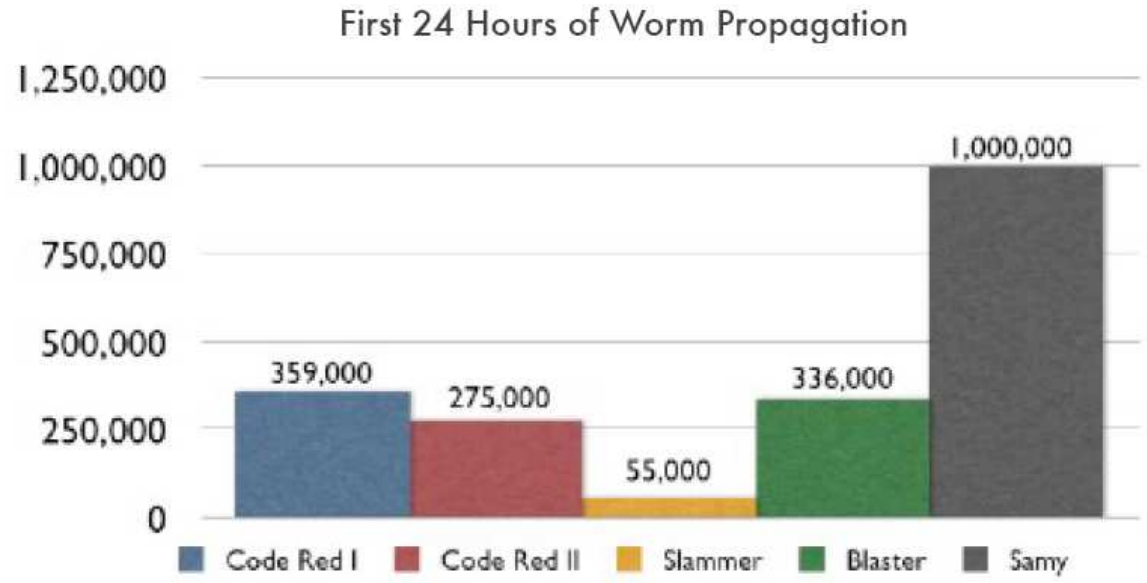
XSS - Vulnerability

- **Very common**
- **Easily found**
  - > **XSSed.com: 20.000+ unfixed**
- **Underestimated**
- **Misunderstood**
  - > **"Our site uses SSL"**
- **"First stage" in attacks**
  - > **CSRF**
  - > **DoS**

SOGETI

XSS - Vulnerability

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



WhiteHat Security 2006

SOGETI

XSS - Attack

- **Attacks with Javascript**
  - > **HTML attributes**
    - <body onload=alert('test1')>
    - <b onmouseover=alert('Wufff!')>click me!
    - <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,PHNjcmlwd D5hbGVydCgndGVzdDMnKTwvc2NyaXB0Pg">

SOGETI

XSS - Attack

- **Some examples**

SOGETI

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**

SOGETI

Further Reading

- **OWASP**
- **Google Code Best Practices**

SOGETI

Staat voor resultaat

www.sogeti.nl