

Input Validation Vulnerabilities Cross Site Scripting (XSS)

Laurie Williams
North Carolina State University
williams@csc.ncsu.edu

NC STATE UNIVERSITY

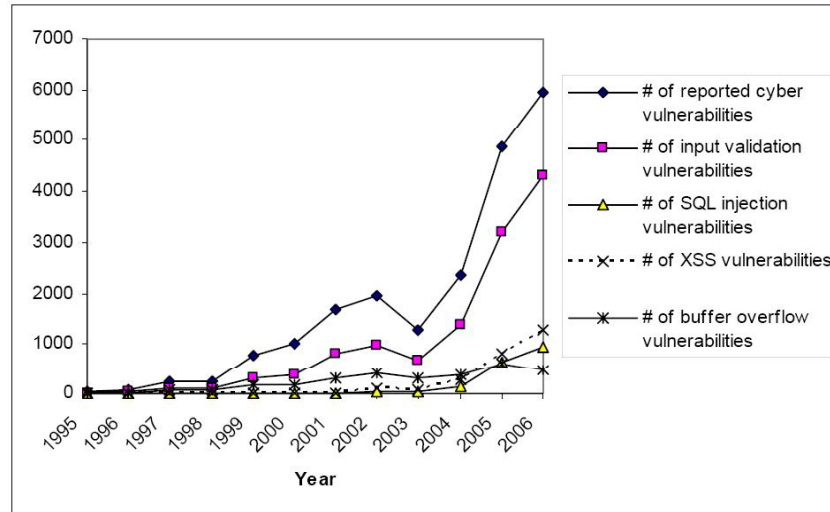
Input Validation Vulnerabilities

- **Input validation vulnerabilities (IVVs) are vulnerabilities that are caused by insufficient input validation .**
- **“Using unvalidated input as part of a directive or command to a subsystem can introduce vulnerability.”¹**
 - **Buffer Overflow**
 - **Cross Site Scripting**
 - **SQL Injection**

NC STATE UNIVERSITY

¹“Build Security In” <https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/guidelines/342.html>

Trends



NC STATE UNIVERSITY

© 2007 Laurie Williams

Data from National Vulnerability Database

Buffer Overflow

- An error caused when a program tries to store too much data in a temporary storage area. This can be exploited by hackers to execute malicious code.

NC STATE UNIVERSITY

<http://www.smoothwall.net/support/glossary.php>

Cross Site Scripting

- **Cross-site scripting is possible when**
 - **An adversary tricks a victim into clicking on a link that he crafted and presented to the victim (via a web server or email),**
 - **The link contains a URL with embedded malicious script (typically as a query string, for example “phishing”), and**
 - **The URL refers to host that echoes input back to a browser without input validation.**
- **When the victim clicks the link, he is referred to the host in the URL, the host processes the query string and echoes it to the victim's browser, and the victim's browser executes the malicious script.**
- **This is an unusual vulnerability because the system at fault, the web site not doing input validation, is not the victim of attack.**
- **The only remedy for this vulnerability is for the web site to perform adequate input validation.**

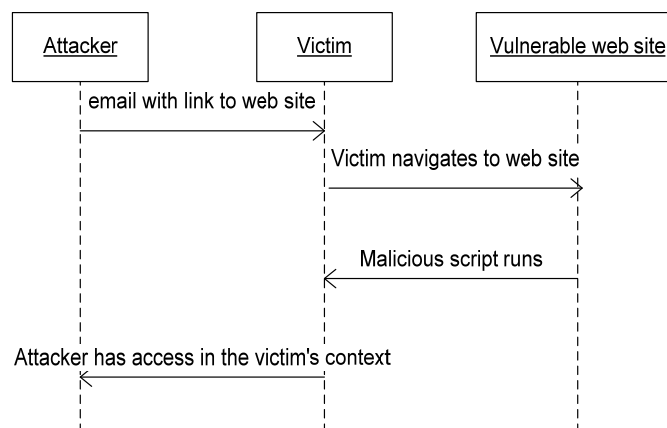
SQL Injection

- **When a program accepts unvalidated input from a user and uses that input to construct a dynamic SQL query to an SQL database, a vulnerability may exist.**
- **The usual context for this class of vulnerability is a web server that accepts input from browsers, uses that input to construct queries against a server-side database, and formats the query response to the browser. The browser user may construct crafted input that, when embedded in a string that is interpreted as an SQL query, performs database operations that are not intended.**

Validating Input

- **Black list:** a list of input types that are expressly forbidden from being used as input into a program
- **White list:** a list of input types that are expressly allowed from being used as input into a program
- Generally expressed as regular expressions
- Input validation must be server side (not in JSP)

Sequence diagram of a XSS attack



Unvalidated Input with XSS

Investments Feedback Customer Care Contact

Online Application

Personal Information

An asterix (*) indicates a required field.

* First Name (Do not use nicknames) Joe

Middle Initial p

* Last Name Hacker

* Social Security Number (format: xxx-xx-xxxx) 555-55-5555

* Birth Date (format yyyy-mm-dd) 1985-11-11

* Mother's Maiden Name (For security verification) Foo

* Address **<script>alert(document.cookie)</script>**

Apartment/Room Number 123

* City Hackville

* State (Please Select State) ▾

* Zip Code 90210

Telephone Number 555-555-5555

* Email foo@foo.com

Occupation Criminal

Annual Income 1500000

Unvalidated Input with XSS

True Value True Money

Welcome to Kelev Investments Feedback Customer Care Conta

Home

Loans

Net Banking

Credit Cards

Contact Us

Bills Online

Online Trading

Register

BILLS ONLINE

Pay your regular monthly bills (telephone, electricity, mobile phone, insurance etc.) right here - from your desktop. [Have a look](#)

Dear Joe,

Thank you. Your loan request has been registered. Please save the following confirmation number for your records. C1005658293

A loan officer will contact you within the next 48 hours. For further assistance you can reach us at 1-800-GET-LOAN.

© 2004 Kelev Investments

Unvalidated Input with XSS

Loan request lists - Microsoft Internet Explorer

Address: http://localhost:8081/kelev/php/approve_loanpage.php

KELEV Investments
True Value True Money

Welcome to Kelev Investments Feedback Customer Care Cor

Pending loan requests

#	Request ID	Requestor	Category	Lo
1	1	John McCafferty	Home	Of che
2	2	Peter Lauros	Home	Ba
3	3	Remy Martin	Car	Mi
4	4	Robert Marksman	Personal	Cc
5	5	Joe Hacker	Home	Ha

Attacker's Loan Request

Unvalidated Input with XSS

Loan request lists - Microsoft Internet Explorer

Address: http://localhost:8081/kelev/php/approve_loanpage.php

KELEV Investments
True Value True Money

Welcome to Kelev Investments Feedback Customer Care Cor

Pending loan requests

#	Request ID	Requestor	Category	Lo
1	1	John McCafferty	Home	Of che
2	2	Peter Lauros	Home	Ba
3	3	Remy Martin	Car	Mi
4	4	Robert Marksman	Personal	Cc
5	5	Joe Hacker	Home	Ha

Attacker's Loan Request

Microsoft Internet Explorer

PHPSESSID=4b1ff0cf3e0c2289d54e4f49fb3776a4

Unvalidated Input and resulted in a Cross-Site Scripting Attack and the theft of the Administrator's Cookie

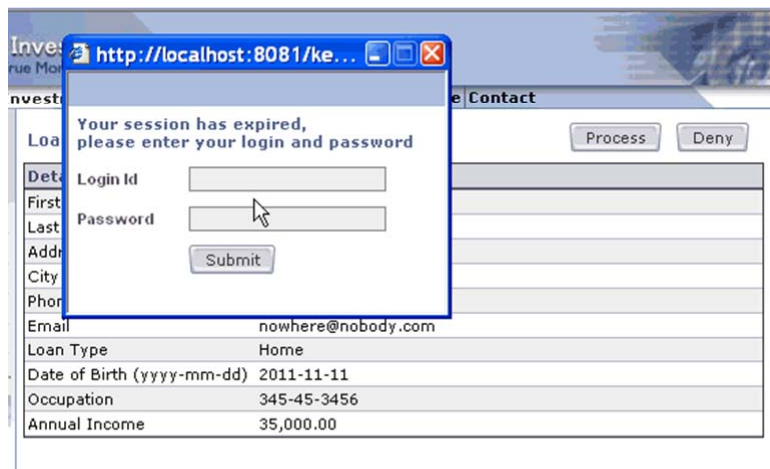
Cross-Site Scripting: Content Spoofing

- Insert un-trusted content into the web application that can be used to trick users.
- Compromise of the integrity of application code via malicious script code injected into the database
- Limited only by the attackers imagination.

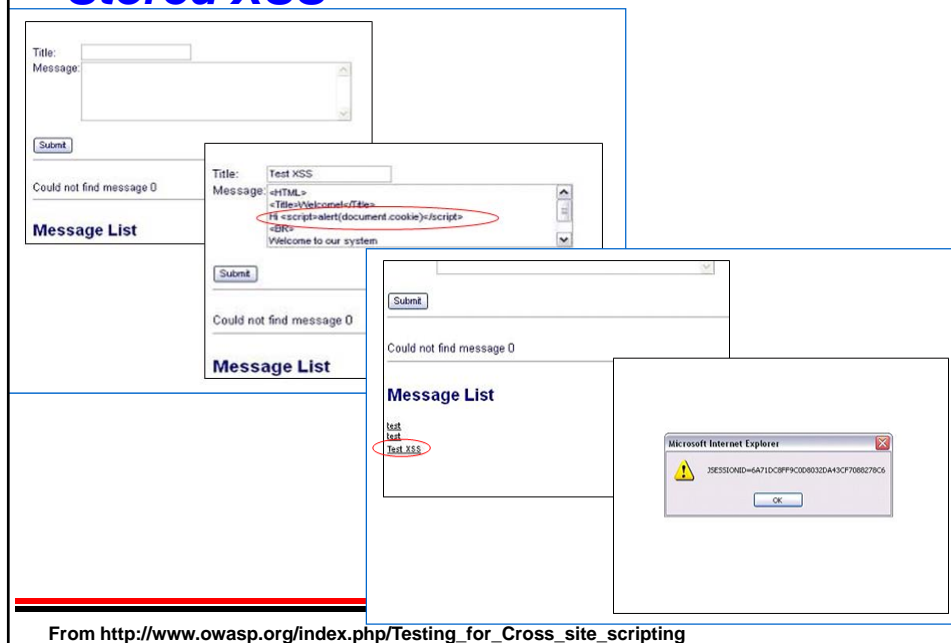
Cross-Site Scripting Exploit

- `<SCRIPT>var oWH = window.open("", "", "width=275, height=175, top=200, left=250 location=no, menubar=no, status=no, toolbar=no, scrollbars=no, resizable=no");oWH.document.write("`
- HTML FORM with POST request to `http://compromised-server/h4xor.php`
- `);</SCRIPT>`

Cross-Site Scripting: Content Spoofing



Stored XSS



Testing for XSS

- **Test for: valid HTML and script code allowed in an input field**
 - Special characters like < or >
 - `<script>alert("XSS");</script>`
 - `<script>alert(document.cookie);</script>`
 - `article.php?title=<meta%20http-equiv="refresh"%20content="0;">`
 - Causes denial of service
 - See <http://ha.ckers.org/xss.html>
 - See http://www.owasp.org/index.php/Testing_for_Cross_site_scripting