



Ohio Information Security Conference '08

# Threats and Countermeasures for Cross Site Scripting

**Blaine Wilson**



**OWASP**

The Open Web Application Security Project

# Speaker Biography



## Blaine Wilson

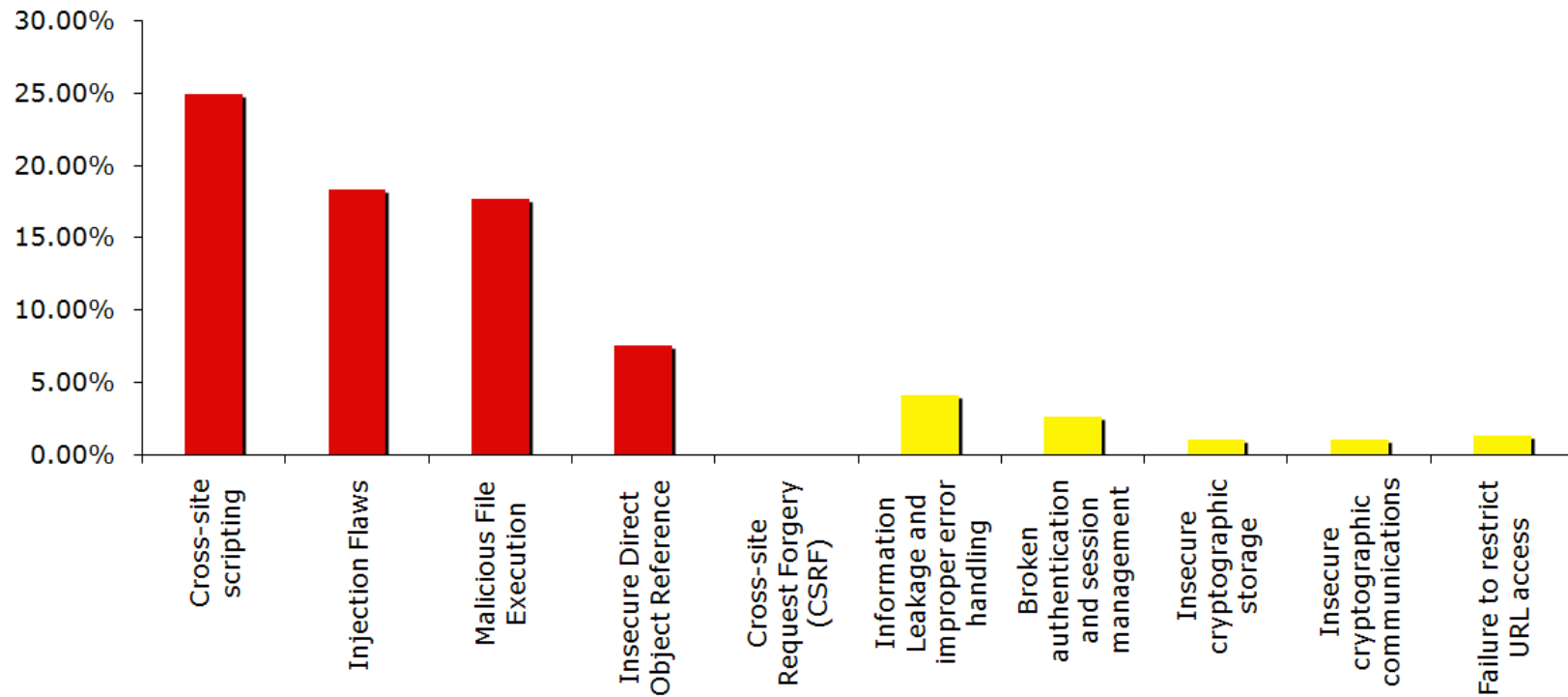
- 14 years experience in software development.
- Joined a global financial company in April 2007 to focus on security through the SDLC.
- 7 years working on performance, scalability and security of web applications for an automotive software company.
- I worked as a consultant to medical corporations for their application, data and network needs.



- Is there really an issue?
- Cross Site Scripting Described
- The Risk
- How it works
- Things you can do

# Is there really an issue?

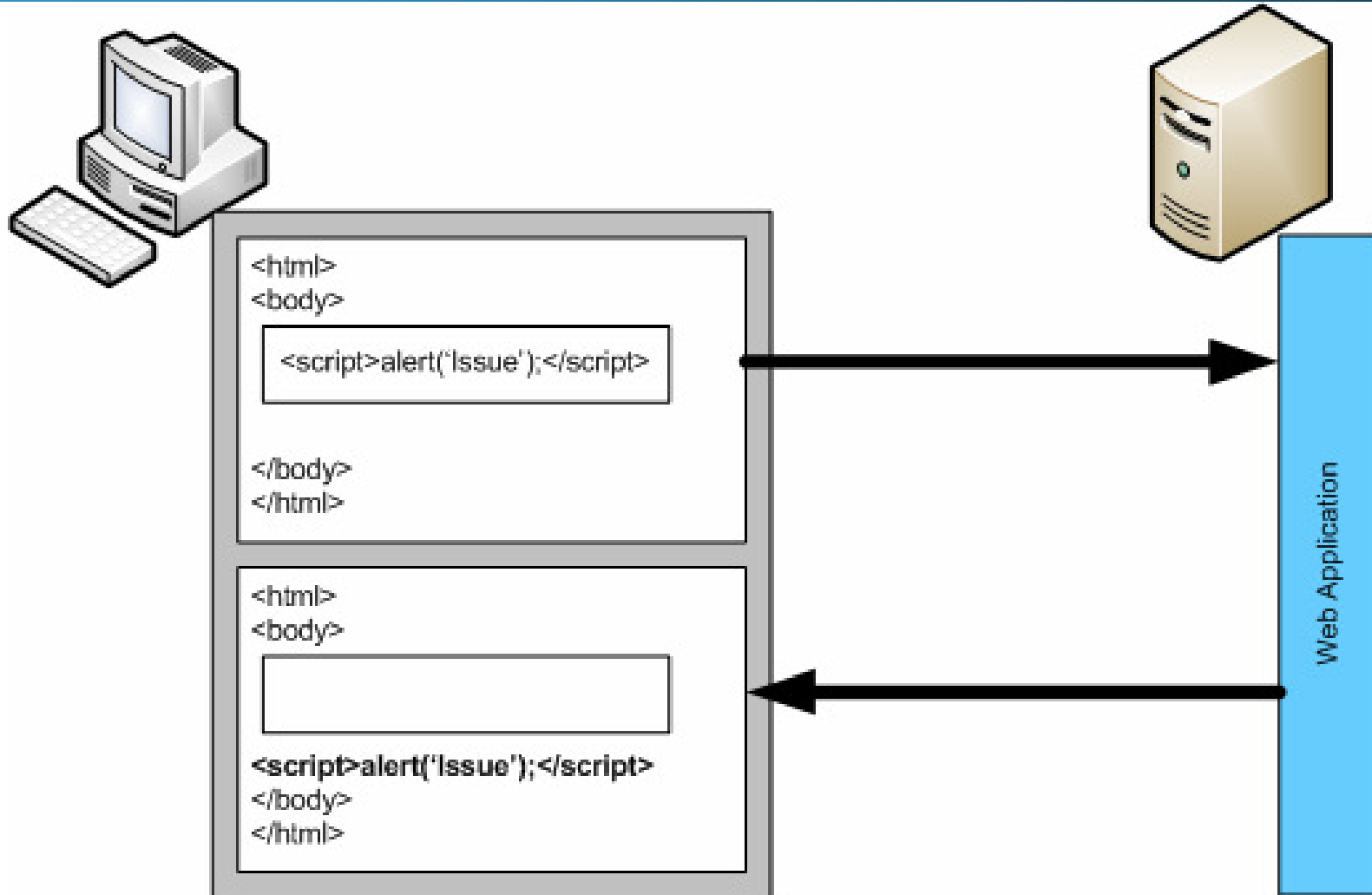
## OWASP Top Ten



# Description

- XSS flaws occur whenever an application takes data that originated from a user and sends it to a web browser without first validating or encoding that content.

# Description



# Description



# DEMO



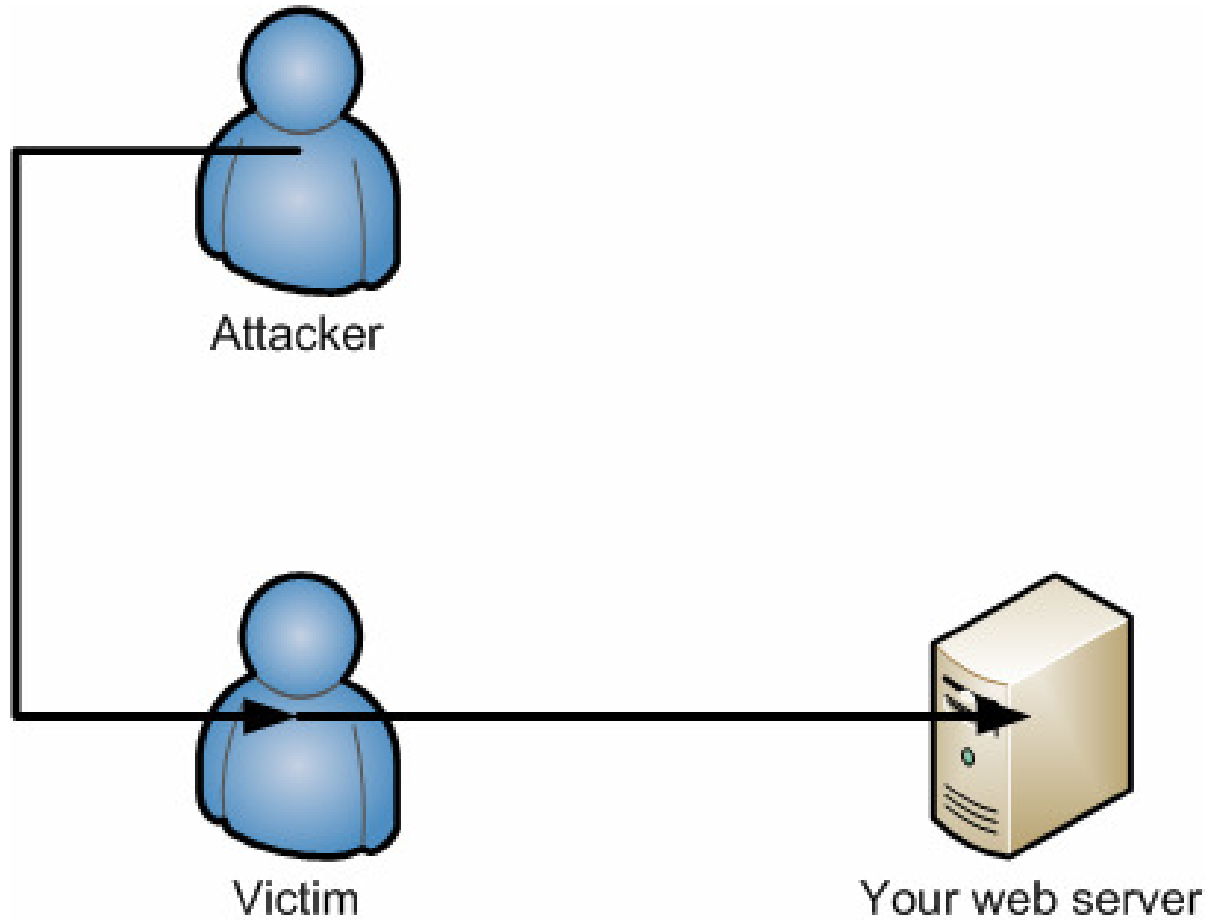
# Risk

- Installation of viruses and other malware
- Loss of sensitive data
- Identity theft

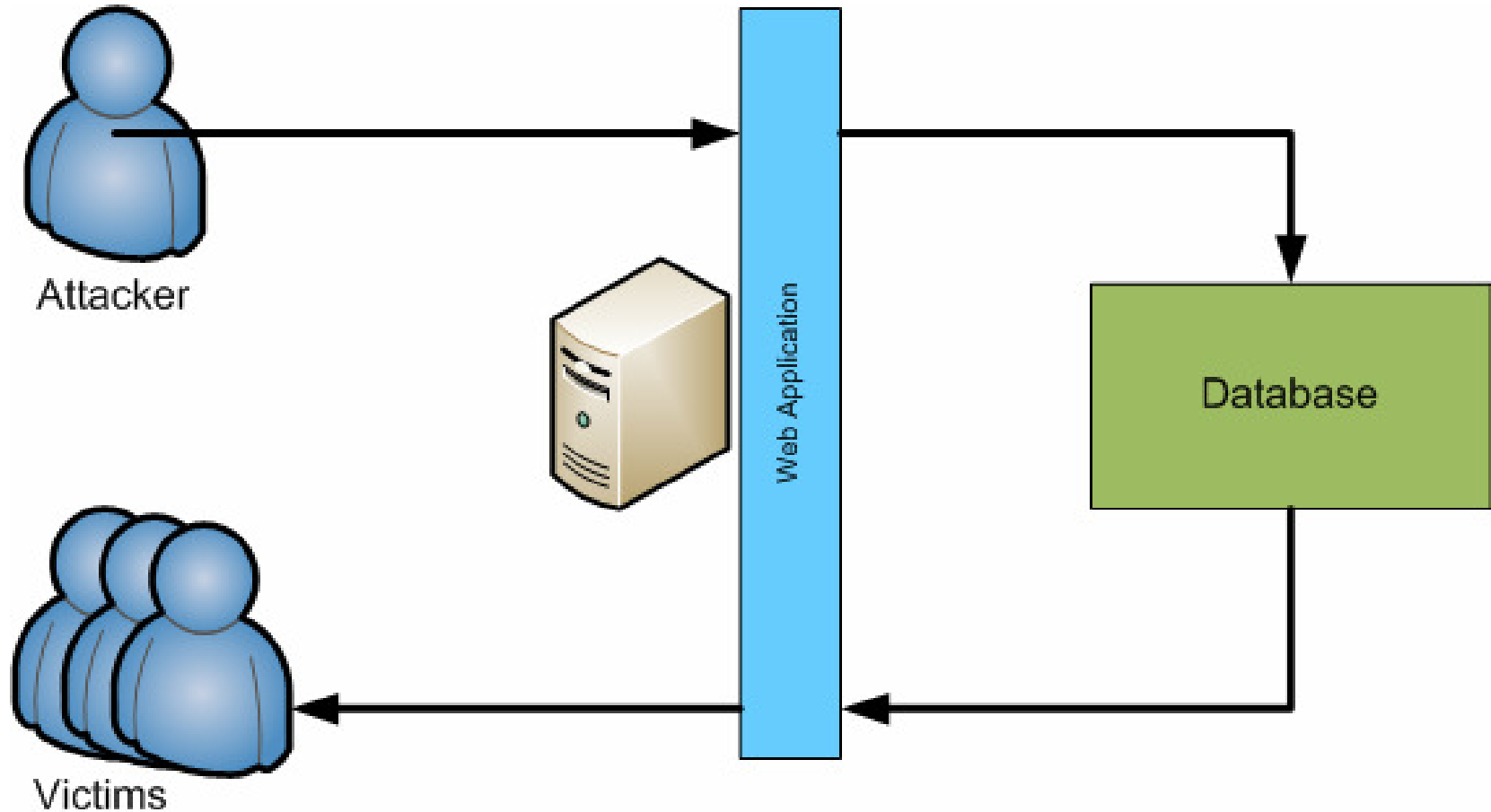
# Types

- Non-Persistent
- Persistent

# Non-Persistent



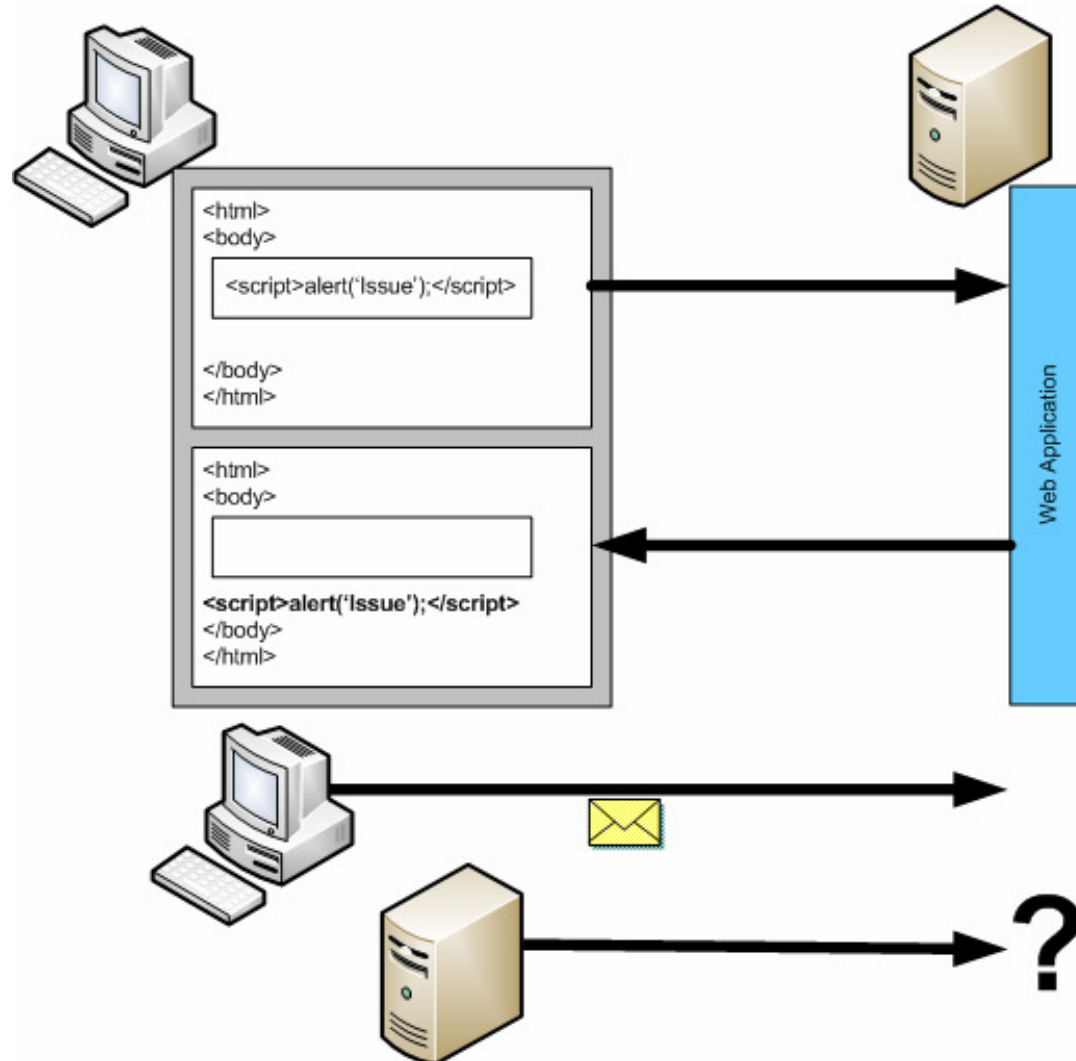
# Persistent



# What to do

- Architecture
- Input validation
- Specify the output character set
- Output encoding

# Architecture



# Input validation

- White Listing
- Black Listing
  - Understand encoding

# White Listing

- Allow known good data
- Gender
  - Male
  - Female
- ZIP Code
  - [0-9]{5}
  - [0-9]{5}-[0-9]{4}
  - What about Canada?

# Black Listing

Deny known bad data

- Watch for scripts and input
- Know the potentially dangerous HTML tags
- Understand canonicalization issues

Keyword is KNOWN

# Black Listing

## DEMO

# Potentially Dangerous HTML



O-ISC '08

Ohio Information Security Conference

- applet
- body
- embed
- frame
- script
- frameset
- html
- object
- iframe
- img
- style
- layer
- link
- ilayer
- meta



**OWASP**

The Open Web Application Security Project

# Canonicalization

What do these have in common?

■ <

■ &lt;

■ %3C

■ &#60;

■ +ADw-

# Canonicalization

## DEMO

# Output character set

- Don't let the attacker choose your character encoding.
- Figure out your character encoding and explicitly set it in your application.
  - Content-Type HTTP Header
  - meta tag http-equiv="Content-Type"

# Output character set

## DEMO

# Output Encoding

Know where your data is going

- HTML Encode data going to the screen
- Confirm data cannot break out of their containers

# Output Encoding



## DEMO





**O-ISC '08**  
Ohio Information Security Conference

---

# Questions & Answers



**OWASP**  
The Open Web Application Security Project

## OWASP - Top 10 2007-Cross Site Scripting

- [http://www.owasp.org/index.php/Top\\_10\\_2007-A1](http://www.owasp.org/index.php/Top_10_2007-A1)

## OWASP - Cross Site Scripting

- [http://www.owasp.org/index.php/Cross\\_Site\\_Scripting](http://www.owasp.org/index.php/Cross_Site_Scripting)

## Wikipedia - Cross-site scripting

- [http://en.wikipedia.org/wiki/Cross\\_site\\_scripting](http://en.wikipedia.org/wiki/Cross_site_scripting)

## Microsoft - How To: Prevent Cross-Site Scripting in ASP.NET

- <http://msdn2.microsoft.com/en-us/library/ms998274.aspx>