

*AN INTERACTIVE APPROACH  
FOR EDUCATING  
VULNERABILITIES*

Group 6

Raelle Panchoo, Vinutha Prabhakar, Jake Nunn, Ruslan Popovych,  
Sundip Patel

# Agenda

- Introduction
  - Details
- Levels of Game
  - Demo for each level
- Q & A

# Introduction

- **An Interactive Approach for Educating Vulnerabilities:** educational website which teaches users about the most common software vulnerabilities
- Composed of levels, each consisting of common web elements flawed with a unique vulnerability
- **Goal:** have the user complete all levels and finish the game

# Details

- **Objective:** Provide an informative and interactive way for users to learn about common vulnerabilities
- Website's home page will include goal of project and instructions for game

# Levels of Game

- Home Page: Contains goal and instructions for game
- Level 1: Manipulating a URL Query String
- Level 2: SQL Injecting a User and Password Form
- Level 3: Disabling/Modifying JavaScript Based Form
- Level 4: Decompiling a Flash Applet to Find Hidden Information
- End of Game: User is congratulated for completing all the levels

# Educational Concepts

- Scaffolding
- Participatory Learning

# Level 1: Query String Manipulation

- A query string sends textual data to the server since HTML is stateless
- Appended onto a URL
- Most commonly sent by an HTML `<form>` tag
- Can also be appended by Javascript and other client-side code

# Query String Basics

- Begin with a ?
- Parameter names and values follow in a name=value format
- Separated by & (delimiter)
- Visible in the Address Bar (part of the URL)
- Example: `http://foo.com/index.html?var1=yes&var2=m`

# Query String Manipulation Impacts

- Input is often overlooked as a candidate for sanitizing
- Very visible and not hard to learn
- Can be used to perform other hacks, like SQL injection
- Can be used to inject code into a page
- Can provide unauthorized privileges
- Context clues often aid hacking

LEVEL ONE:

**DEMO**

# Level 2: SQL Injection

- Quick Summary
  - SQL (Structured Query Language) designed for retrieval and management of data
  - Database Applications
    - Large multi-user applications
    - Mail programs
    - Personal Organizers
  - SQL Injection - code injection that exploits a security vulnerability in databases

# Level 2: SQL Injection Types

- Escape characters
  - Magic String 'OR"='
- Type Handling
  - ... where id=" + input + ";"
- Blind Injection
  - Time delays
    - Measuring web page load delay
  - Conditional Responses
  - Conditional errors

# Level 2: SQL Injection Defense

- Parameters in Statements
  - Don't use input directly in queries
  - Avoid dynamically generated statements
- Stored Procedures
  - Allows better restrictions to users
- Hide the errors
  - The user will not be there debugging with you, so filter out your debugging information

LEVEL TWO:

**DEMO**

# Level 3: JavaScript Form Validation

- Form Validation

- Scrubbing user input to meet requirements
- Usually performed on the server before using data for:
  - Constructing SQL statements
  - Checking credentials
  - Anything that can compromise the server

# Level 3: JavaScript Form Validation

- JavaScript

- Powerful client-side scripting language
- Commonly used by web browsers
- Typically used for:
  - Adding interactivity
  - Dynamically sending and loading data
  - Form Validation

# Level 3: JavaScript Form Validation

- JavaScript + Form Validation =
  - Can equal a potential security flaw
  - JavaScript is client-side:
    - Can be accessed and modified by user
    - Can be disabled by user altogether
    - User can obtain sensitive knowledge by viewing code

# Level 3: JavaScript Form Validation

- Solution

- Always perform server-side data validation
- Do not trust client-side

- Why Client-side Form Validation?

- Instant feedback to user
- Less information sent to server
- Web 2.0 – application look-and-feel

LEVEL THREE:

**DEMO**

# Level 4: Flash Applet Decompilation

- Flash

- Multimedia platform owned by Adobe Systems.
- Adds multimedia and interactivity to websites
- Embed objects, code and forms in an applet
- Requires a runtime plug-in installed on client

- Uses

- Embed Video and Animation to websites
- Make Games and other rich interactive applications
- Compose introductions or entire websites

# Level 4: Flash Applet Decompilation

- Embedded Objects and Code
  - Can contain sensitive information
    - Gift Codes
    - Usernames and Passwords
    - Links to other sources
  - Can extract objects
    - Videos
    - Music
    - Documents

# Level 4: Flash Applet Decompilation

- Solution

- Don't rely on applets to disguise information
- Never store sensitive data on client
- Always do server-side input validation

LEVEL FOUR:

**DEMO**

# Conclusion

- Summary
- QUESTIONS AND ANSWERS