Exploit-Me

Open Source Firefox Plug-Ins for Penetration Testing
Introduction

Nish Bhalla
Founder

Direct: 201.390.9198
Direct: 647.722.4883
Mobile: 732.614.1020
E-mail: nish@securitycompass.com
Web: www.securitycompass.com

Toronto, Canada | Shrewsbury, USA
Introduction

Rohit Sethi  CISSP
Manager

Direct:  416.848.0668
Mobile:  732.546.4473
E-mail:  rohit@securitycompass.com
Web:  www.securitycompass.com

Toronto, Canada | Shrewsbury, USA
Agenda

State of web application security

XSS – Really a Danger?

Introducing XSS-Me

Applying XSS-Me in Applications

SQL Inject Me

Public Release and Future of App
Web Application Security

- Despite advances in knowledge, web apps are still very dangerous

```php
m/register.php?id=6; DROP TABLE CUSTOMERS; XP_CMD_SHELL('TFTP')
```

- Web app vulnerabilities now out-number buffer overflows in CVE
Testing Tools

- A variety of testing tools exist
  - OWASP tools, commercial tools, other open source

- Some are very powerful
  - Problem: many are proxy-based
The Missing Piece ...

- Most tools not made for developers, QA
  - Many apps do not benefit from security testing WITHIN SDLC

- Need light-weight tools that can test quickly
But First ...

• Do we really need to care about XSS vulns
  – Aren’t they just annoying pop-up boxes?
XSS – The Real Danger

• AJAX+CSRF+XSS = Major problem

• One single XSS in an online banking app can allow malicious users to transfer funds
If you answered "no," think again. An interesting running thread over at the Russian security blog by Valery Marchuk -- SecurityLab.ru -- shows examples of several such flaws on sites belonging to -- among others -- Verisign, eEye Digital Security, Cisco Systems F-Secure, Snort.org, and the National Security Agency. Clicking on most of the links on the SecurityLabs thread demonstrates the vulnerability in each site, with the exception of a few of the older ones, which appear to have been fixed.
Repercussion of AJAX

- **XMLHttpRequest** Object in JavaScript

- Allows attackers to:
  - Send
  - Receive
  - Parse
data as if it were coming from the victim

- Used to evade most anti-CSRF
XSS-Me

- Firefox plug-in testing tool to the rescue!
XSS-Me

- Choose which fields to test on the fly
Options

- Import new XSS attack strings
  - Ships with RSnake’s cheat sheet
How it Works

• Set ‘document.vulnerable’ DOM property to true via JavaScript

• If document property is set, XSS worked

• Also checks for literal presence of string
Inner Workings of Exploit-Me

- Rendered Request
- Response
- Raw Request
if (document.wrappedJSObject.vulnerable &&
document.wrappedJSObject.vulnerable == true)
{
rv = new Result(RESULT_TYPE_ERROR, 100,
"Was able to add property to DOM, this page is
very vulnerable");
(""+attackRunner.testValue.string+""");
}
Report – Possible XSS

(document.wrappedJSObject.vulnerable)
{
    rv = new Result(RESULT_TYPE_WARNING, 100, "Seemed to add property but not value. This should be investigated further");//(""+attackRunner.testValue.string+"")
};
Report – Not vulnerable to XSS

```java
{
    rv = new Result(RESULT_TYPE_PASS, 100, "document did not get property"); // ("" + attackRunner.testValue.string + ")")
}
```
Where to Use It?

- Multiple phases of the SDLC
SQL-Inject Me

- Similar interface to XSS-Me
SQL-Inject Me

- To be released in public Beta along with XSS-Me
- Works by checking for presence of ‘error messages’ or ‘result strings’ in HTTP response
Next Steps

• Both XSS-Me and SQL Inject-Me to be released publicly on Nov. 26\textsuperscript{th}, 2007
  – Check \url{http://www.securitycompass.com} for updates

• Open Source under GPL 3
  – Contribute to make safer web apps!

• New tools such as Web Service Exploit-Me to be created early next year
What is Next For these plug-ins

- Auto Encoding
- Error management (Error Enumeration)
- Stored XSS
- Crawling a site for stored attacks (to look for results on multiple pages either through user input or automatic)
- URL Parameters
Other Exploit-Me Plug-in

- **Web Service-Me**
  - Auto-generated form on the basis of the WSDL

- **Overflow-Me**
  - Field Overflow/underflow

- **Access-Me**
  - Toggle transmission of session cookies for each request

- **Enumerate-Me**
  - User and Password Enumeration through forgotten password functionality

- **BruteForce Me**
  - Brute force/dictionary attacks against authentication
Questions / Profile

- Our consultants have serviced large (Fortune 500) and medium sized companies across most major industries
- We have worked for major security players, including Foundstone and Deloitte

- We have co-authored or contributed to several security books, including:
  - Hacking Exposed: Web Applications, 2nd Edition
  - HackNotes: Network Security
  - Buffer Overflow Attacks: Detect, Exploit & Prevent
  - Windows XP Professional Security
  - Writing Security Tools and Exploits
- We have presented at and continue to present at security conferences, including:
  - Blackhat Amsterdam; Reverse Engineering Conference 2005 in Montreal; HackInTheBox 2005 in Malaysia; ISC2's Infosec Conferences in Las Vegas, NYC, Toronto & DC; CSI NetSec; DallasCon; ToorCon; and Freenix.

- We present and contribute to open source projects:
  - Chair at OWASP Toronto, Presented at OWASP Toronto, Contributed to YASSP Project (Lead by SANS and Xerox).