Kicking Down the Cross Domain Door
Techniques for Cross Domain Exploitation

Billy K Rios (BK) and Raghav Dube
Implication of Cross Domain Attacks

Rich Content
- Cookies
- Mash-ups
- Tabbed Browsing
- Ajax
- JSON
Implication of Cross Domain Attacks

CU Online Banking - Account Balance Summary

Below is a summary of your current account balances. This information is as of 5:00 PM EST on 2/26/2007.

<table>
<thead>
<tr>
<th>Description</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous Balance</td>
<td>$99994.69</td>
</tr>
<tr>
<td>Current Withdrawals</td>
<td>(6999.62)</td>
</tr>
<tr>
<td>Current Deposits</td>
<td>4999.73</td>
</tr>
<tr>
<td><strong>Current Balance</strong></td>
<td><strong>$97994.80</strong></td>
</tr>
</tbody>
</table>
Cross Site Scripting (XSS)

- Injected Client Code
- Cookie Stealing
- Browser Hijacking
- Web Page Defacement
- Hawtness
XSS Example / Demo
Cross Site Request Forgery (XSRF)

- Applications Trust
- Parameters, Cookie, IP Space...
- Authenticated Examples
- New Hawtness
XSRF Example / Demo
**XSS meets XSRF**

- Using XSS and XSRF together!
- XSSXSSRFSSX?
- Both Have Strengths
- Both Have Weaknesses
- One Armed Boxers
XSS Proxy Fundamentals

- Anton Rager - XSS Proxy
- BeEf, XSS Shell, Backframe
- `<script>alert('xss')</script>`
- `<script src="../proxy.js">`
- Dynamic JavaScript Payloads
- Frames and Control Channels
XS-Sniper

- Typical XSS Proxy
- Rendering of HTML
- Organization of Data
- JavaScript Payloads Provided
- Source Code Snippets
Dynamic JavaScript Payload for execute.js

Captured incoming HTTP requests to the XS-Sniper Proxy
Dynamic JavaScript Payload for external.js

```javascript
sniperscope();
```

External Spotter Payload

```javascript
document.write('<body onload=spotter()>
var randomnumber=Math.floor(Math.random() *1000001);

function spotter()
var
bigframe=document.documentElement.innerHTML;

iframeHTML+='<IFRAME NAME="myFrame" iframe id="myFrame" width="50%" height="50%"
scrolling="auto" frameborder="0">
</IFRAME>');

iframeHTML+='<!FRAME NAME="myFrame2"
iframe id="myFrame2" width="0%" height="0%"
scrolling="auto" frameborder="0">
</IFRAME>');

iframeHTML+='<!FRAME NAME="myFrame3"
iframe id="myFrame3" width="50%" height="50%"
scrolling="auto" frameborder="0">
</IFRAME>');

External Spotter Payload Location

C:\Documents and Settings\BK\My Documents\Visua
XSS Proxies and Frameworks

Bilbo's Blog

Comments For Entry #5

The answer to the question of life!(Comments RSS)
I've been doing a lot of reading lately about life in general.

- myFrame2
  (invisible)
  Control Channel

- myFrame3
  (invisible)
  Cross Domain Contents

- crossDomainPostFrame
  (invisible)
  POSTs off Domain
The Attack – The Initial XSS

MyPercent20.com

- Popular Social Networking/Blogging Site
- User Base of Tens of Thousands of Users
- Allows Uploading of HTML and Other Content
BigCreditUnion.com

- Typical Online Banking Website
- Fictional Credit Union
- Built-in Vulnerabilities for Demo

Welcome to the Credit Union Website

Our site is designed to provide information that is important to you. Here you can find details on credit union accounts, mortgages, business and personal loans, and trust and investment services. CU account holders can use our site to find the nearest branch location, check account balances, and collaborate with other account holders.

Whether you are a visitor or an existing client, we hope our site answers your questions.
The Attack – BigCreditUnion.com

The Internet

Victim

MyPercent20

BigCreditUnion

Attacker
**Assumptions**

- The victim has access to the Internet
- BigCreditUnion.com has an XSS exposure
- The victim is using IE or Firefox
Steps to Exploitation

- Target Reconnaissance
- Initial XSS
- Jumping to BigCreditUnion
- Authenticated Attacks
- Unauthenticated Attacks


http://www.attacker.com/test/noresponse.js?test123
The Attack – WhatsUP Gold 2006

WhatsUP Gold 2006

• Made by Ipswitch
• Has Known XSS Vulnerabilities
• Found on Corporate Intranets
• Not Limited to WhatsUP Gold
• “Protected by Firewalls!”
The Attack – WhatsUP Gold 2006

### Top 10 Devices by Ping Response Time

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>Avg (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP ProCurve Sw...</td>
<td>pc158-atl.ipswit...</td>
<td>69.0</td>
</tr>
<tr>
<td>WAP Tokyo1</td>
<td>216.104.153.13</td>
<td>38.0</td>
</tr>
<tr>
<td>AT&amp;T Router</td>
<td>12.37.214.1</td>
<td>36.0</td>
</tr>
<tr>
<td>Juniper Firewall</td>
<td>192.168.3.1</td>
<td>35.0</td>
</tr>
<tr>
<td>Wireless Acces...</td>
<td>pc134-atl.ipswit...</td>
<td>35.0</td>
</tr>
<tr>
<td>HP 2500C+ Prin...</td>
<td>pc149-atl.ipswit...</td>
<td>35.0</td>
</tr>
<tr>
<td>Rome FTP Server</td>
<td>192.168.3.147</td>
<td>34.0</td>
</tr>
<tr>
<td>Rome File Server</td>
<td>192.168.3.130</td>
<td>34.0</td>
</tr>
<tr>
<td>Exchange Box</td>
<td>pc171-atl.ipswit...</td>
<td>34.0</td>
</tr>
<tr>
<td>Cisco 1811 Rou...</td>
<td>192.168.3.222</td>
<td>34.0</td>
</tr>
</tbody>
</table>
The Attack – WhatsUP Gold 2006

- Victim
- WhatsUP Gold
- The Internet
- Attacker
- MyPercent20
Assumptions

• The management console is only available via the Intranet
• The victim will NOT be logged into the management console
• The victim does NOT have a WhatsUP account
• The victim is using Firefox (Possible with I E)
• No unauthenticated XSS vulnerabilities
Steps to Exploitation

- Vulnerability Research
- Target Reconnaissance
- Initial XSS
- Port scanning and Fingerprinting
- Brute Forcing Credentials
- XSS follow-up
- Driving Interaction
Creds List

```javascript
var usernameList = new Array("administrator","whatsup","admin");
var passwordList = new Array("password","admin","administrator");
```
NOT LIMITED TO WhatsUP Gold!
DEMO
One More Time... This time in Slow motion
Questions and Thanks…

**PEOPLE I’ve MET**
- Danya
- Nitesh Dhanjani
- Rajat Swarup
- Sriram
- Mike Crabtree
- Old PAC-CERT Crew
- Ed Souza

**PEOPLE I haven’t MET**
- Jeremiah Grossman
- RSnake
- Anton Rager
- SPI Dynamics
- Black Hat

Houston & New York Advanced Security Centers!