Flash Security

OWASP KC Meeting
March 7, 2007
Rohini Sulatycki

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

The OWASP Foundation
http://www.owasp.org
What is Flash?

- Adobe Flash is the authoring environment
  - Rich Animation
  - Video
  - Action Script 2
  - FLA
- Flash Player is the VM that runs SWF byte codes
What is Flash Remoting?

- Flash Remoting is a technology for HTTP-based request/response data communication.
- Supported natively by Flash Player
- Uses Action Message Format (AMF) for communication
  - Modeled on SOAP
  - Uses packet format
Flash Remoting Communication
Flash Remoting Communication

Flash application
DataType: ActionScript

Convert between ActionScript and AMF

Internet
DataType: AMF

Convert between AMF and application server type

Application server
DataType: Java, C#, Visual Basic, or CFML
What is Flex 2?

- Flex is a framework for creating flash applications.
  - Components
    - Lists, Grids,..
  - Collection of technologies
    - XML
    - web services
    - HTTP
    - Flash Player
    - ActionScript

- Flex applications are `.swf` files which you can then run in Flash Player.
Shared Objects

- Similar to cookies
- Larger data storage 100KB
- Binary format
- No cross-domain access (by default)
- Not downloaded back to web server
Shared Objects

- Stored outside browser
  - Do not get cleared when browser cache is cleared
- Accessible across browsers
SOL Editors

- C:|Documents and Settings|<USERNAME>|Application|Data|Macromedia|Flash Player|#SharedObjects|<RANDOM>|<DOMAINNAME>

- When you drill down in each domain’s directory, you will eventually find a “SOL” file.

- **Sol Editors:**
  - http://sourceforge.net/projects/soleditor), a Windows-based tool and “Solve” by Darron Schall
  - http://solve.sourceforge.net), which is written in Java™
SOL Editor

![Image of SOL Editor interface]

- **File**
- **View**
- **Help**

**soundData**
- **volume**
- **mute**

**Editors**
- **Number**
- **Boolean**
- **String**
- **Object**
- **null**
- **undefined**
- **Array**
- **XML**
- **Date**
- **Pointer**

**Name:**
- *volume*

**Value:**
- *90*
Settings Manager

- Can view which sites have saved Flash shared objects
- Change the allowed disk size
- Remove these files
- Disable the feature all together

Settings Manager

Adobe Flash Player™ Settings Manager

Website Storage Settings
How much information can us.js2.yimg.com store on your computer?

Visited Websites

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Websites</th>
<th>Used</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://www.adidas.com">www.adidas.com</a></td>
<td>1 KB</td>
<td>100 KB</td>
</tr>
<tr>
<td></td>
<td>ivillage.com</td>
<td>1 KB</td>
<td>100 KB</td>
</tr>
<tr>
<td></td>
<td>i.cmpnet.com</td>
<td>3 KB</td>
<td>100 KB</td>
</tr>
<tr>
<td></td>
<td>bankofamerica.com</td>
<td>-</td>
<td>100 KB</td>
</tr>
</tbody>
</table>
- Can allow cross-domain access to shared objects

- `System.security.allowDomain(domain1, ..., domainN);`
Flash 8 Security Model
Flash 8 Security

- All resources follow sandbox model
  - Domain sandbox
    - Any two SWF files interact freely within sandbox
    - Need explicit permission to read data in another sandbox
- Local Files
  - Local-with-file-system sandbox
    - May only read files on local file system
Flash 8 Security (Contd.)

- Local-with-networking sandbox
  - Communicate with other l-w-n files
  - Send to network server using XML.send()
- Stronger typing of variables with ActionScript 2.0
- Processor safeguards
  - Detect app in infinite loop
- Quotas on memory usage
Network Access Warning

Macromedia Flash Player has stopped a potentially unsafe operation.

The following local application on your computer or network:
C:\Documents and Settings\...\network warning for local-with-flesupport.swf
is trying to communicate with this Internet-enabled location:
www.example.com

To let this application communicate with the Internet, click Settings.
You must restart the application after changing your settings.

OK
Settings...
Flash Vulnerabilities

- SWF runs client-side
- Can be decompiled
  - http://www.nowrap.de/flare.html
  - http://www.buraks.com/asv/
Vulnerabilities

- SQL Injection
- XSS
  - Decompile the action script
Vulnerabilities

 Forge HTTP Request headers

- [http://www.securityfocus.com/archive/1/441014](http://www.securityfocus.com/archive/1/441014)
- A design error exists in the implementation of the "addRequestHeader()" method. This can be exploited to overwrite arbitrary HTTP headers in an outgoing HTTP request to an arbitrary web site via the "LoadVars" class and the "send()" method.
- Allows malicious web site to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site by overwriting the "Host" header
- “Mostly” fixed in Flash 9
XSS

- Var req:LoadVars = new LoadVars();
- req.addRequestHeader("Expect", "<script>alert('gotcha')</script>");
- Req.send(http://www.targetsite.com/,_blank","GET");
Memory Access Error

- An attacker can create a malformed .swf file that when opened by certain versions of Macromedia Flash Player, will result in the execution of arbitrary commands.
- Can take complete control of the affected system.
- Fixed in Flash Player 9
With the new security model Flash appears to be moving in the right direction. However, the extremely high adoption rates of Flash and its ubiquity can create a situation where new vulnerabilities can create more damage than those seen previously.