

# XSS攻防与前端防御

0Kee Team

王珂、任言



**WE ARE**  
**0KEE TEAM !**

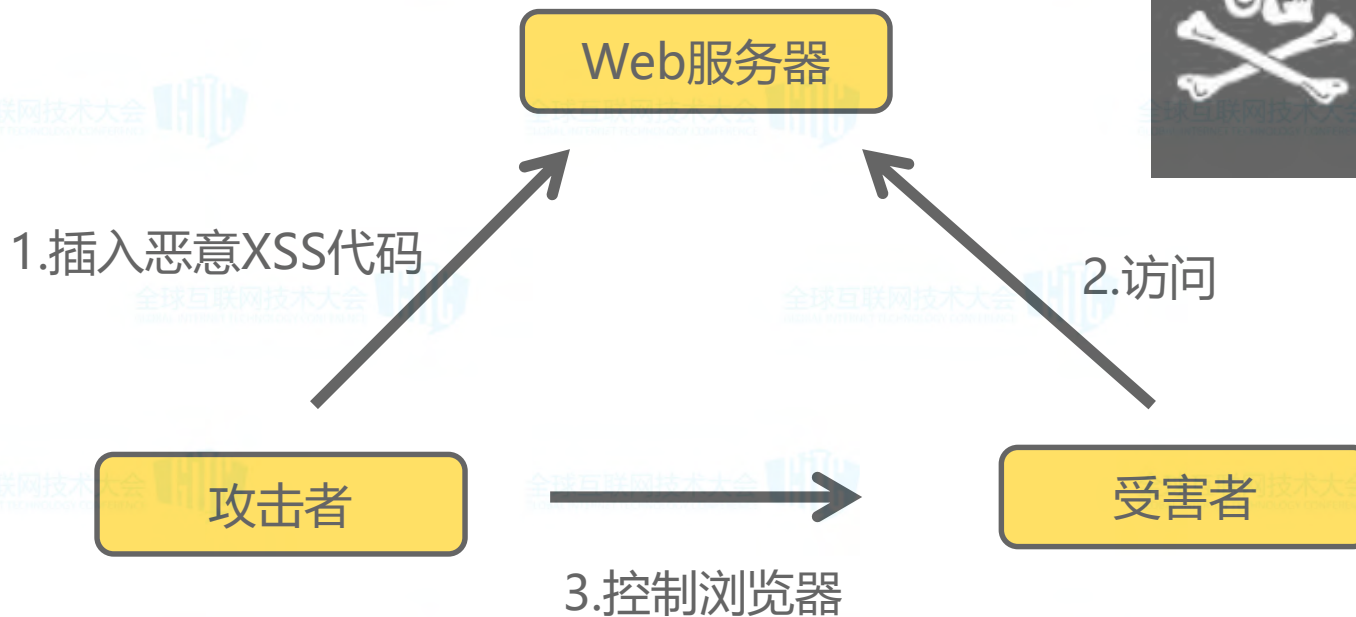


- Cross-site scripting
- 黑客控制你的浏览器

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>XSS 原理</title>
</head>
<body>
欢迎登录,王老师!
</body>
</html>
```

正常输入

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>XSS 原理</title>
</head>
<body>
欢迎登录,<script>alert(1)</script>!
</body>
</html>
```





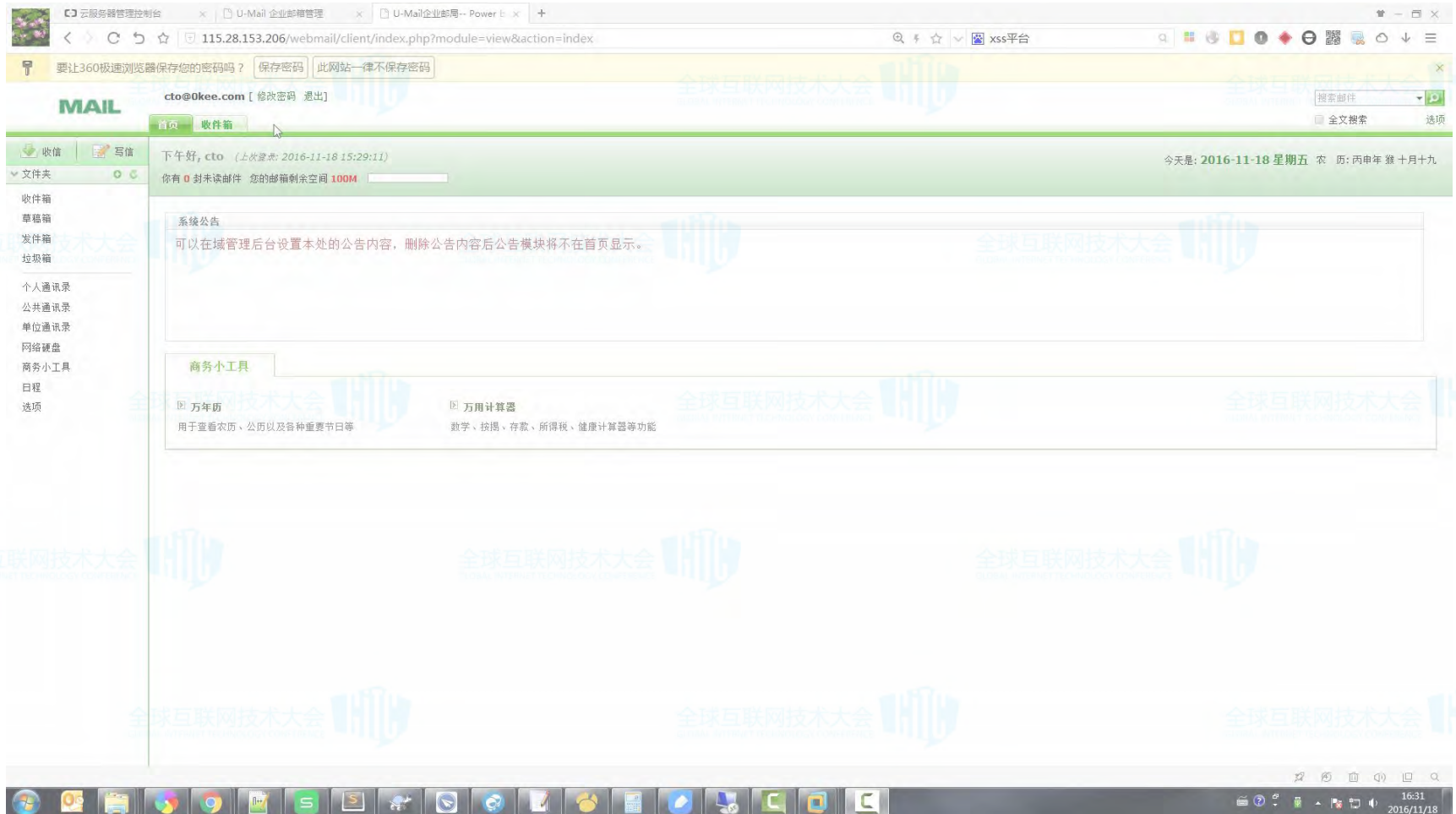
- 网站内的JS能做什么

- 权限

- 执行本~~X~~地命令

- 读取本~~X~~地文件

- XSS 获取cookie
  - QQ、网易等邮箱都曾被XSS
  - GMail的XSS黑市一万美刀
  - 演示





## XSS + CSRF



<https://0kee.360.cn/h...> x [123.59.209.245:3000/...](123.59.209.245:3000/) x [tce.corp.qihoo.net/do...](http://tce.corp.qihoo.net/do...) x [403 Forbidden](#) x <https://0kee.360.cn/h...> x [html转义](#) x [Escape加密/UnEscape](#) x [Apache Tomcat/6.0.41](#) x [My Forum - your boar...](#) x

[域名重定向](#) [bbs.0kee.com/forums/list.page](#)





此网页为 [英文](#) 网页，是否需要翻译？ [使用有道翻译](#) [使用谷歌翻译](#)

[\[Log\]](#)

## My Forum - your board description




[Search](#) [Recent Topics](#) [Hottest Topics](#) [Member Listing](#) [Back to home page](#)  
[Moderation Log](#) [My Profile](#) [My Bookmarks](#) [Private Messages](#) [Logout \[marryfaye\]](#)

You last visited on: 16/11/2016 13:51:31  
 The time now is: 16/11/2016 15:00:20  
[Forum Index](#)

Forums		Read new messages since my last visit		
		Topics	Messages	Last Message
<b>Category Test</b>				
 555 ssss Moderators		0	No messages	No messages
 Test Forum This is a test forum		3	4	16/05/2015 01:19:59 marryfaye →D
 2222		2	2	17/05/2015 17:16:35 marryfaye →D
<b>3333</b>				
 ss ssss Moderators		1	2	16/05/2015 01:36:50 marryfaye →D
<b>nnn</b>				

### Who is online

Our users have posted a total of 7 messages  
 We have 3 registered users  
 The newest registered user is marryfaye  
 There are 4 online users: 1 registered, 3 guest(s) [ [Administrator](#) ] [ Moderator ]  
 Most users ever online was 6 on 16/05/2015 02:19:02  
 Connected users: marryfaye

 New Messages
  No new messages
  Blocked Forum

Powered by JForum 2.1.9 © JForum Team

## • 新浪微博蠕虫

```
20. function random_msg(){
21.     link = 'http://163.fm/PxZHoxn?id=' +
22.     //使用短地址服务, 构造XSS传播连接
23.     //http://weibo.com/pub/star/g/yyyyd%2
24.     //隐藏自己的恶意js脚本
25.     var msgs = [ //话题列表
26.         '郭美美事件的一些未注意到的细节:',
27.         '建党大业中穿帮的地方:',
28.         '让女人心动的100句诗歌:',
29.         '3D肉团团高清普通话版种子:',
30.         '这是传说中的神仙眷侣啊:',
31.         '惊爆!范冰冰艳照真流出了:',
32.         '杨幂被爆多次被潜规则:',
33.         '傻仔拿锤子去抢银行:',
34.         '可以监听别人手机的软件:',
35.         '个税起征点有望提到4000:'];
36.     var msg = msgs[Math.floor(Math.random
37.     //随机选取话题,加上之前的传播连接作为微
38.     msg = encodeURIComponent(msg); //对内
39.     return msg;
40. }
```



碉堡了!我在#微游戏#抢到iPhone 5啦! 马上去  
抢: <http://t.cn/zYEyWm>



27分钟前 来自微游戏

删除 | 转发 | 收藏 | 评论



: 碉堡了!我在#微游戏#抢到iPhone 5啦! 马上去抢: <http://t.cn/zYEyXi>



28分钟前 来自微游戏

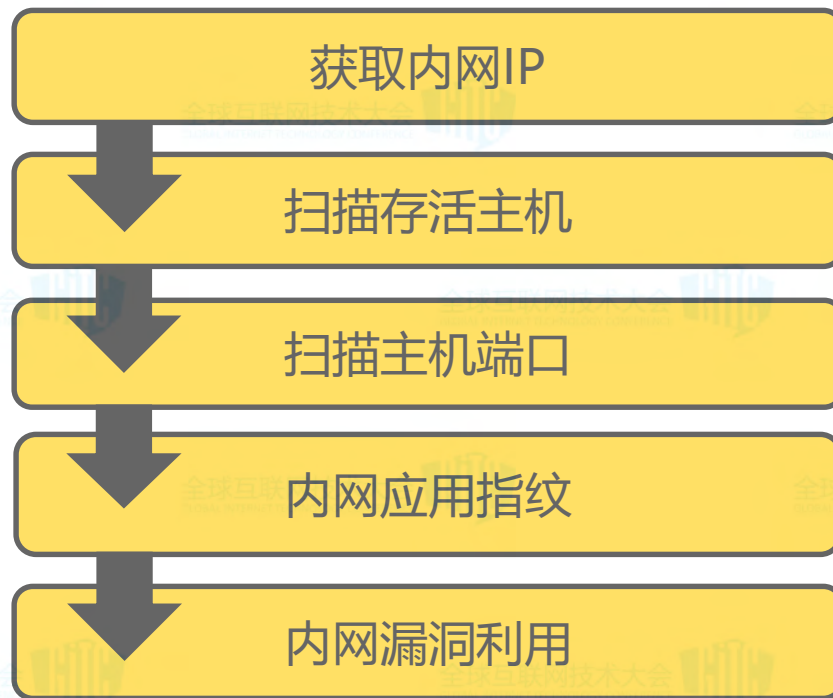
转发 | 收藏 | 评论(1)



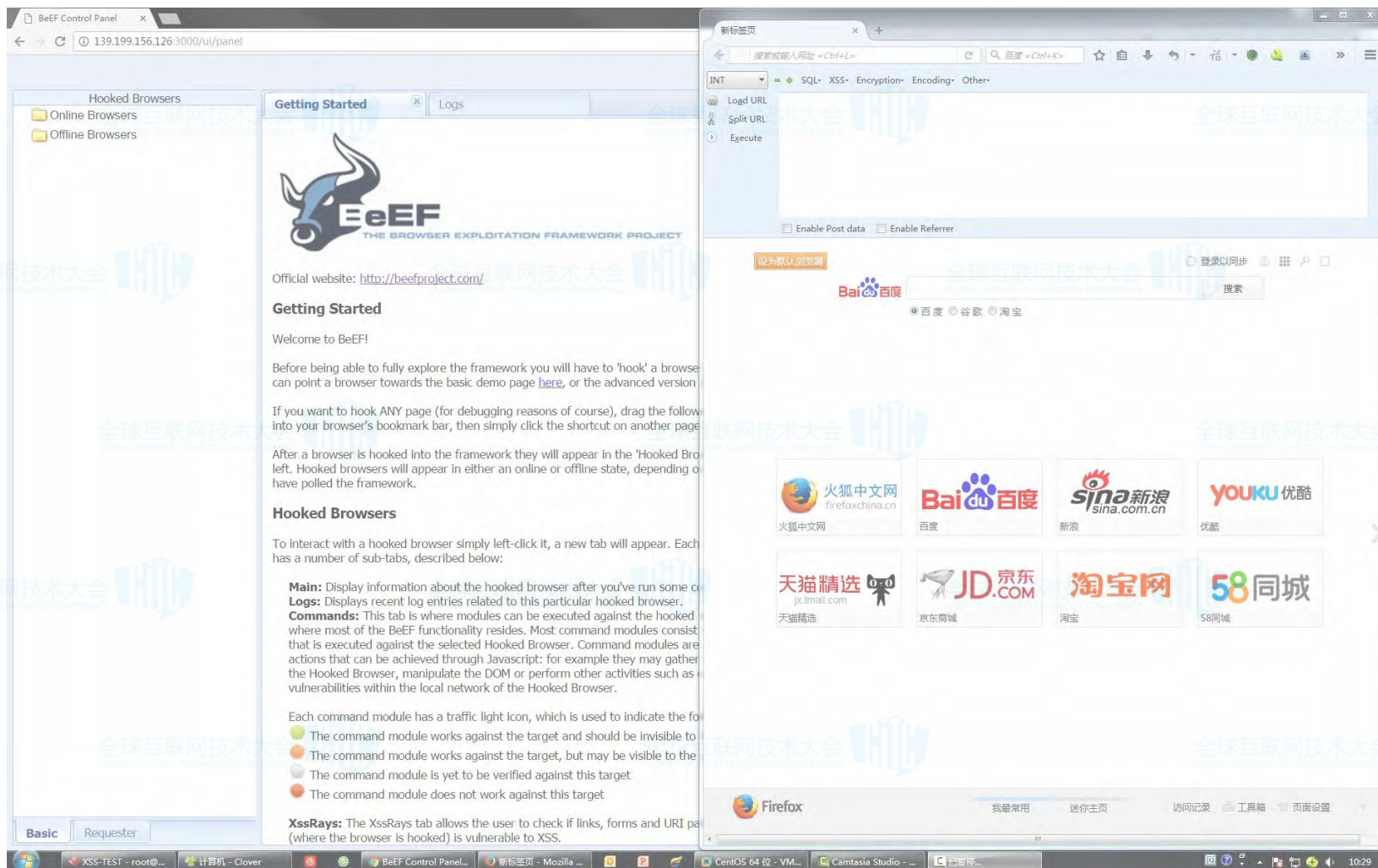
碉堡了!我在#微游戏#抢到iPhone 5啦! 马上去抢: <http://t.cn/zYEyXV>



- XSS攻击内网









BeEF 0.4.7.0-alpha | Submit Bug | Logout

Getting Started | Logs | Current Browser

Details | Commands | Rider | XssRays | Ipec | Network | WebRTC

**Module Tree**

- Search
- Identity LAR Subnets
- Ping Sweep (Java)
- Port Scanner
- Fingerprint Routers
- Ping Sweep
- Ping Sweep (FF)
- Persistence (6)
  - Man-In-The-Browser
  - Wordpress Add Adminis
  - Confirm Close Tab
  - Create Foreground IFra
  - Create Pop Under
  - Hijack Opener Window
- Phonegap (16)
  - Alert User
  - Beep
  - Check Connection
  - Detect PhoneGap
  - Geolocation
  - Globalization Status
  - Keychain
  - List Contacts
  - List Files
  - List Plugins
  - Persist resume
  - Persistence
  - Prompt User
  - Start Recording Audio
  - Stop Recording Audio
  - Upload File
- Social Engineering (23)
  - Text to Voice
  - Clickjacking
  - Clippy
  - Fake Evernote Web Cli
  - Fake Flash Update
  - Fake LastPass
  - Fake Notification Bar
  - Fake Notification Bar (C
  - Fake Notification Bar (F
  - Fake Notification Bar (IE
  - Google Phishing
  - Lcamtuf Download
  - Pretty Theft
  - Replace Videos (Fake f
  - Simple Hijacker

**Module Results History**

id	date	label
0	2016-11-15 06:05	command 1
1	2016-11-15 07:37	command 2
2	2016-11-15 07:38	command 3

**Command results**

id	data	time
1	data: result=Chrome IFrame Created .. awaiting messages	Tue Nov 15 2016 20:38:30 GMT+0800 (中国标准时间)
2	data: result=Username field changed to: te	Tue Nov 15 2016 20:38:34 GMT+0800 (中国标准时间)
3	data: result=Username field changed to: test	Tue Nov 15 2016 20:38:34 GMT+0800 (中国标准时间)
4	data: result=Username field changed to: test	Tue Nov 15 2016 20:38:34 GMT+0800 (中国标准时间)
5	data: result=Username field changed to: test	Tue Nov 15 2016 20:38:34 GMT+0800 (中国标准时间)
6	data: result=Password field changed to: a	Tue Nov 15 2016 20:38:35 GMT+0800 (中国标准时间)
7	data: result=Password field changed to: aa	Tue Nov 15 2016 20:38:35 GMT+0800 (中国标准时间)
8	data: result=Password field changed to: aaa	Tue Nov 15 2016 20:38:36 GMT+0800 (中国标准时间)
9	data: result=Password field changed to: aaaa	Tue Nov 15 2016 20:38:36 GMT+0800 (中国标准时间)
10	data: result=Password field changed to: aaaaa	Tue Nov 15 2016 20:38:36 GMT+0800 (中国标准时间)
11	data: result=Password field changed to: aaaaaa	Tue Nov 15 2016 20:38:36 GMT+0800 (中国标准时间)
12	data: result=Password field changed to: aaaaaa123	Tue Nov 15 2016 20:38:37 GMT+0800 (中国标准时间)
13	data: result=Password field changed to: aaaaaa123	Tue Nov 15 2016 20:38:37 GMT+0800 (中国标准时间)
14	data: result=Password field changed to: aaaaaa123	Tue Nov 15 2016 20:38:37 GMT+0800 (中国标准时间)

Re-execute command

Sign In LastPass

Email: test

Password: .....

☐ Remember Email

☐ Remember Password

☐ Show Vault After Login

Login Cancel

New here? Create an Account

## • XSS可以用来做什么

普通用户

Cookies、隐私数据、IP、日志、相片、邮件、CSRF...

客户端攻击

浏览器特权域、插件、APP、Webview...

键盘记录

Rootkit

Cookies、LocalStorage...

蠕虫攻击

水坑攻击

钓鱼、劫持

管理员

后台地址、页面源码、管理员信息、CSRF...

内网渗透

端口扫描、ST2利用、路由器...

方案	优势	劣势	场景
XSS-Filter	遏制反射型XSS	对存储型无能为力； 某些浏览器不支持	非企业级防御方案

JSFuck is an esoteric and educational programming style based on the atom JavaScript. It uses only six different characters to write and execute code.

It does not depend on a browser, so you can even run it on Node.js.

Use the form below to convert your own script. Uncheck "eval source" to get plain string.



Eval Source

```
[ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( [ ! [ ] ] + [ ] [ ] ) [ + ! + [ ] + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] +  
( ! ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + ! + [ ] ] [ ( [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( [ ! [ ] ] + [ ] [ ] ) ) [ + ! +  
[ ] + [ + [ ] ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] + ( ! ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] )  
[ + ! + [ ] ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ ( ! [ ] + [ ] ) [ + [ ] ] + ( [ ! [ ] ] + [ ] [ ] ) [ + ! + [ ] + [ + [ ] ] ] + ( !  
[ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] + ( ! ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + ! +  
[ ] + [ + [ ] ] ] + ( [ ] [ ] + [ ] ) [ + ! + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] + ( ! ! [ ] + [ ] ) [ + ! +  
[ ] ] + ( [ ] [ ] + [ ] ) [ + [ ] ] + ( [ ! [ ] + [ ] ) [ + [ ] ] + ( [ ! [ ] ] + [ ] [ ] ) [ + ! + [ ] + [ + [ ] ] ] + ( ! [ ] + [ ] ) [ ! +  
[ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] + ( ! ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + ! + [ ] ] + [ ] ) [ ! + [ ] + ! +  
[ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] + ( ! ! [ ] + [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( [ ! [ ] ] + [ ] [ ] ) [ + ! + [ ] + [ + [ ] ] ] + ( ! [ ] +  
[ ] ) [ ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] + ( ! ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + ! + [ ] ] ] + ( ! + [ ] +
```

1227 chars

[Run This](#)

Links

www.jsfuck.com 显示：

1

☐ 禁止此页再显示对话框。

确定

方案	优势	劣势	场景
XSS-Filter	遏制反射型XSS	对存储型无能为力； 某些浏览器不支持	非企业级防御方案
关键字过滤流量	通用性好	非常容易被绕过； 不适用于所有类型	WAF、网站程序通用防护模块（基础防御，一定要有）



方案	优势	劣势	场景
XSS-Filter	遏制反射型XSS	对存储型无能为力； 某些浏览器不支持	非企业级防御方案
关键字过滤流量	通用性好	非常容易被绕过； 不适用于所有类型	WAF、网站程序通用防护模块（基础防御，一定要有）
Http-Only	保护Cookie效果好	只能针对Cookie	任何网站都可用

方案	优势	劣势	场景
XSS-Filter	遏制反射型XSS	对存储型无能为力； 某些浏览器不支持	非企业级防御方案
关键字过滤流量	通用性好	非常容易被绕过； 不适用于所有类型	WAF、网站程序通用防护模块（基础防御，一定要有）
Http-Only	保护Cookie效果好	只能针对Cookie	任何网站都可用
CSP	可有效拦截几乎任何类型的XSS攻击	配置不方便； 部署不方便； 高误报；	任何网站都可用（前提是保证开发不打人的情况下）

方案	优势	劣势	场景
XSS-Filter	遏制反射型XSS	对存储型无能为力； 某些浏览器不支持	非企业级防御方案
关键字过滤流量	通用性好	非常容易被绕过； 不适用于所有类型	WAF、网站程序通用防护模块（基础防御，一定要有）
Http-Only	保护Cookie效果好	只能针对Cookie	任何网站都可用
CSP	可有效拦截几乎任何类型的XSS攻击	配置不方便； 部署不方便； 高误报；	任何网站都可用（前提是保证开发不打人的情况下）
?	具备CSP的特质； 配置方便； 部署方便； 低误报；	?	任何网站都可以用（并且保证开发不打人）

- 护心镜是javascript，以js对抗js
- 监控页面的恶意行为，可实时阻断并告警

```
5 <html>
6 <head>
7 <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
8 <title>文章管理</title>
9 <link href="images/css.css" rel="stylesheet" type="text/css">
10 <script type="text/javascript">
11 var hxj_config = {
12     project_key: "7220ba8d3ddddd",
13     domain_white: ["localhost", "127.0.0.1"],
14     enable_plugin: {"cookie": 1, "xstester": 1, "password": 1, "fish": 1, "script": 1, "webshell": 1},
15 };
16 </script>
17 <script type="text/javascript" src="http://res.0kee.com/hxj.min.js"></script>
18 <script src="../include/js/jquery.js" type="text/javascript"></script>
19 <script type="text/javascript">
20 function doAction(a, id, v){
21     if(a=='validate'){
```

- 二维码



- 如何降低误报？
- 如何降低成本？
- 如何主动发现？

- 可对大部分类型的XSS起到防护作用。
- 可发现系统漏洞，并进行预警。
- 部署较为灵活。

护心镜

护心镜

https://0kee.360.cn/hxj/user/#/create

护心镜

首页 介绍 演示 帮助 关于我们

创建新项目

我的项目 25

告警处理 63204

个人信息

退出

业务名称:

报警接口: https://0kee.360.cn/hxj/alert  
接口格式说明

域名白名单: 一行一个域名  
不知道填哪些域名?

使用位置: 后台  
默认采用推荐 配置

危险处理: 弹窗选择  
不管是放行还是弹窗, 都是受监控的

插件: ☒ Cookie保护 ☒ XSS感知 ☐ 反表单劫持 ☐ 反钓鱼  
☒ 第三方资源探测 ☒ webspell上传探测

提交

护心镜

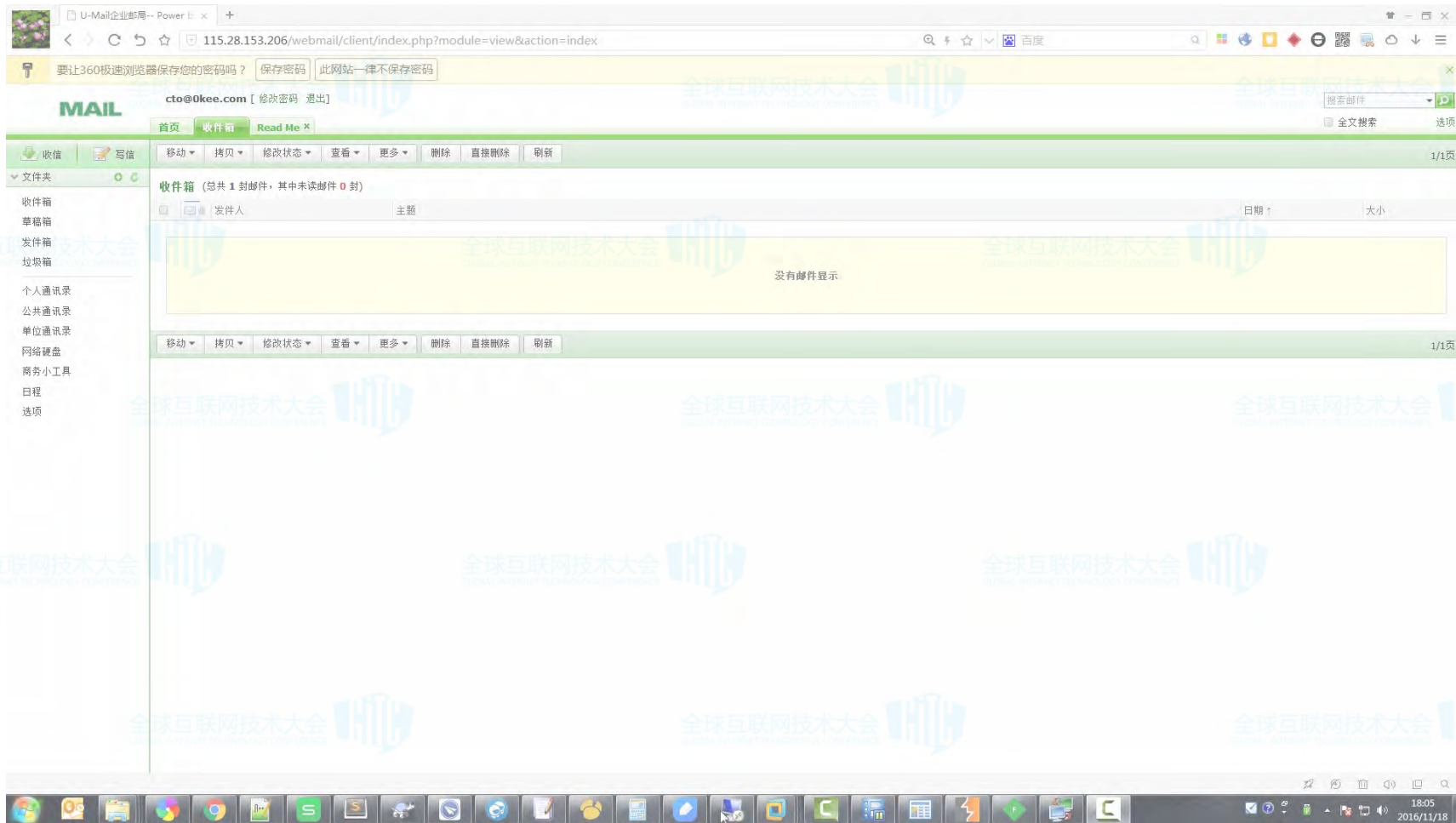
开放工具  
XSSSniper

关于我们  
OKEE TEAM  
加入QQ群

友情链接  
360安全应急响应中心  
Unicorn Team  
360安全播报  
补天响应平台

安全检测  
360爬虫猎手  
360网站安全检测  
360网站卫士

Copyright ©2015 0kee Team 京ICP备15044466号



```
1  /*函数劫持*/
2  var _alert = var a = new MutationObserver(function(d) {
3  alert = funct d.forEach(function(f) {
4      console.l    var e = f.addedNodes;    //e为加入到DOM树中的元素列表
5      _alert(s)    for (var g = 0; g < e.length; g++) {
6  }              var j = e[g];
7  /*对象/属性劫 Hookjs.log("Cteate tagName:"+j.tagName);
8  Object.defineProperty
9  1      Object.defineProperty(document, "cookie", {
10 Object._ 2      get: function() {
11 Object._ 3      console.log("获取cookie");
4          b = someMethodGetCookie();
5          return b
6      },
7      set: function(b) {
8      console.log("写入cookie");
9      someMethodSetCookie(b);
10     }
11     })
```



```
Hookjs.prototype.hook_createElement = function(d) {  
    var a = ["C_SCRIPT", "C_IFRAME", "C_IMAGE", "SCRIPT.SRC:", "C_INPUT_TYPE_PWD", "C_I  
    document.createElement = function(d) {  
        Hookjs.log("Creating Tag:" + d);  
        if (d.toLowerCase == "script") {  
            Hookjs.Report(a[0]); //记录C_SCRIPT 即创建SCRIPT标签  
        } else if (d.toLowerCase() == "iframe" || d.toLowerCase() == "frame") {  
            Hookjs.Report_w(a[1]); //记录C_IFRAME 即创建IFRAME标签  
        } else if (d.toLowerCase() == "image") {  
            Hookjs.Report(a[2]); //记录C_IMAGE 即创建IMAGE标签  
        }  
    }  
    var c = Hookjs.document.createElement.call(document, d);
```

```
hxj_config.report_action = [  
    ["Danger_Image_Call", "C_IMAGE", "IMG.SRC:", "GET_COOKIE", "URL_2L"],  
    ["Danger_URL3_Call", "URL_3:", "GET_COOKIE", "URL_2L"],  
    ["Danger_Frame_Call", "C_IFRAME", "GET_COOKIE", "M_IFRAME_SRC", "URL_2L"],  
    ["Js_Call", "C_SCRIPT_3", "SCRIPT.SRC:"],  
    ["FISH", "C_INPUT_TYPE_PWD", "C_INPUT", "URL_3:"],  
    ["GETS_PWD", "GET_PWD", "URL_3:"],  
    ["XSS_TEST", "XSS_TEST:"],  
    ["CSRF_WEBSHELL", "CSRF_WEBSHELL", "CSRF_WEBSHELL:"]  
];
```

- 自身变量安全：闭包
- 保护全局变量：护心镜所调用的全局变量

```
Hookjs.defConstProp = Hookjs.isWebkit ?  
    function(obj, key, val) {  
        Object.defineProperty(obj, key, {  
            value: val,  
            configurable: false,  
            writable: false,  
            enumerable: true  
        });  
    } :  
    function(obj, key, val) {  
        obj[key] = val;  
    };  
Hookjs.defConstProp(window, "alert", alert);
```

- 总结：保证护心镜所使用的变量、函数、对象不被外部js篡改。

- 保护回调函数

- 保护原型链函数

方案	优势	劣势	场景
XSS-Filter	遏制反射型XSS	对存储型无能为力； 某些浏览器不支持	非企业级防御方案
关键字过滤流量	通用性好	非常容易被绕过； 不适用于所有类型	WAF、网站程序通用防护模块（基础防御，一定要有）
Http-Only	保护Cookie效果好	只能针对Cookie	任何网站都可用
CSP	可有效拦截几乎任何类型的XSS攻击	配置不方便； 部署不方便； 高误报；	任何网站都可用（前提是保证开发不打人的情况下）
护心镜	具备CSP的特质； 配置方便； 部署方便； 低误报；	兼容性	任何网站都可以用 （并且保证开发不打人）

谢谢！

北京朝阳区酒仙桥路6号院2号楼 100015

Building 2, 6 Haoyuan, Jiuxianqiao Road, Chaoyang District, Beijing, P.R.C. 100015

Tel +86 10 5682 2690 Fax +86 10 5682 2000

