XSS攻防与前端防御

0Kee Team

王珂、任言

WE ARE

0KEE TEAM !

XSS

- Cross-site scripting
- 黑客控制你的浏览器

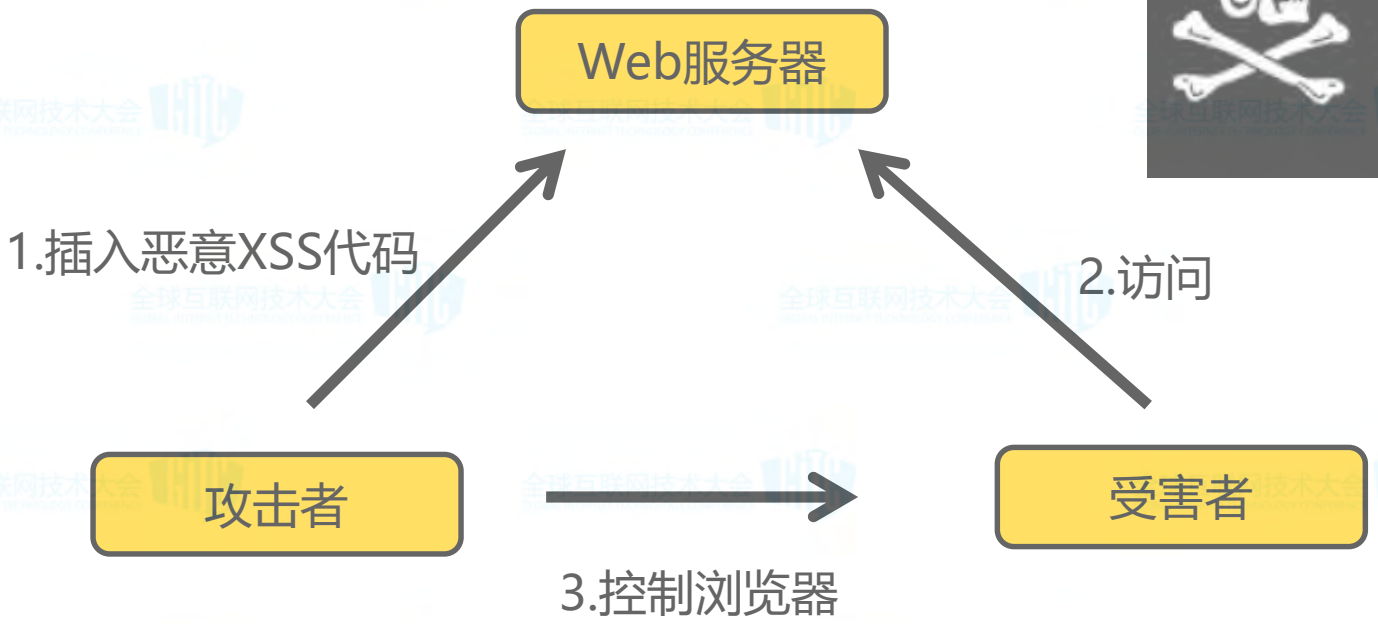
XSS

```
<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>
```

XSS

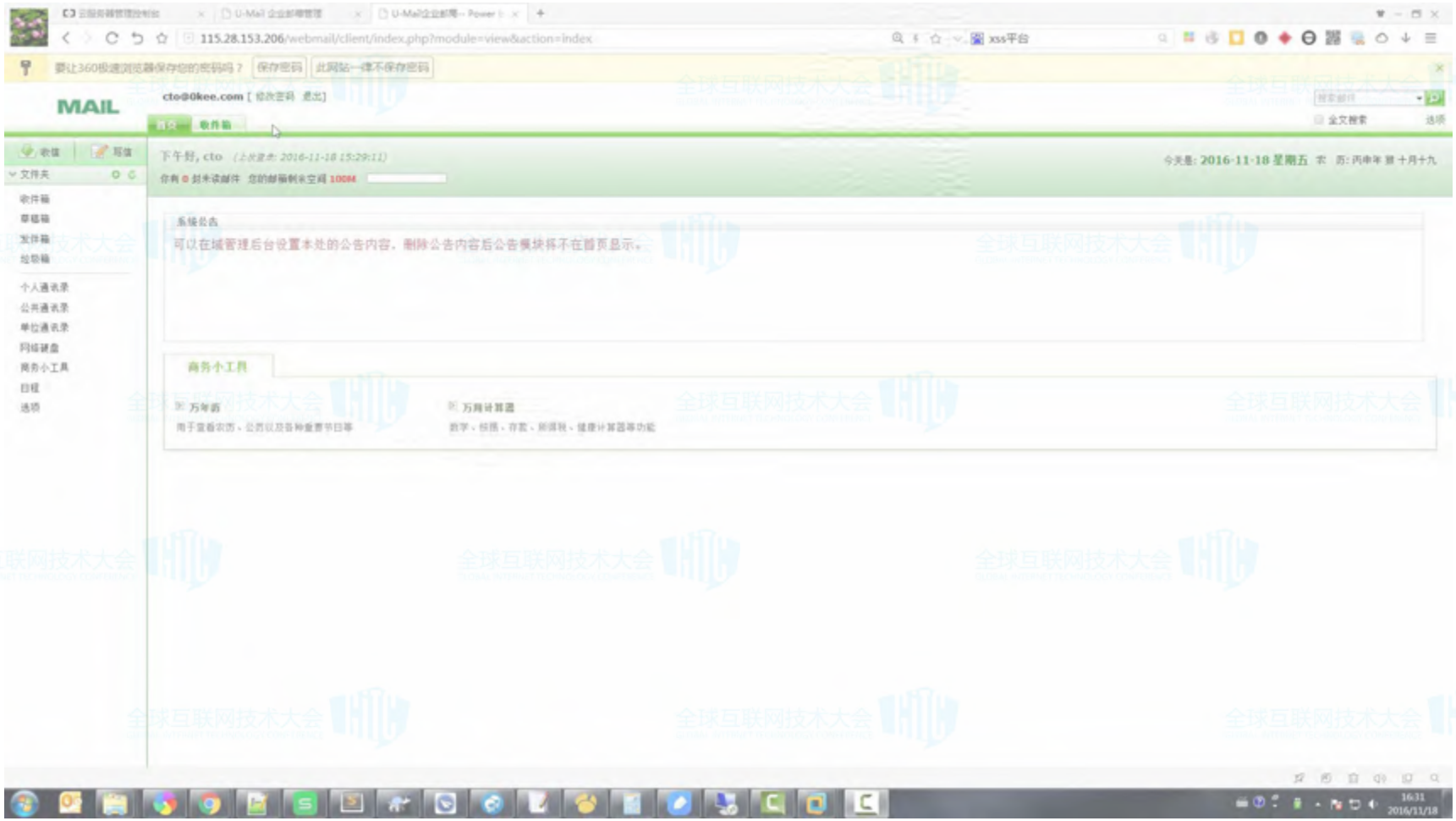


- 网站内的JS能做什么
  - 权限
    - 执行本地命令
    - 读取本地文件

XSS攻击邮箱

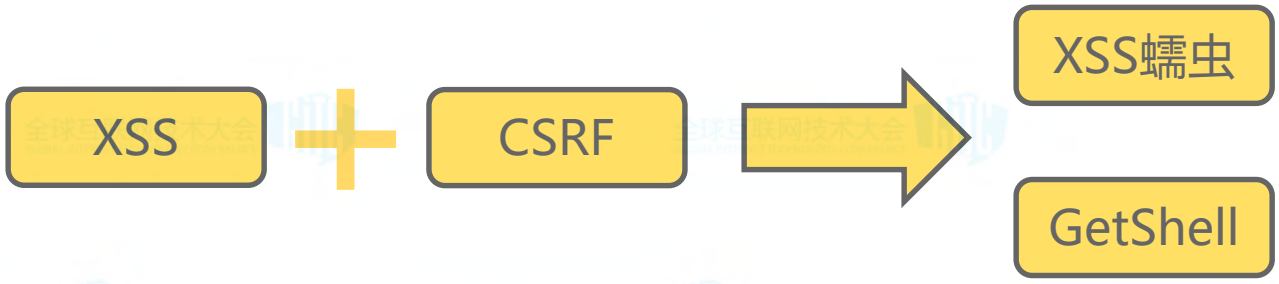
- XSS 获取cookie
  - QQ、网易等邮箱都曾被XSS
  - GMail的XSS黑市一万美刀
  - 演示

XSS攻击邮箱

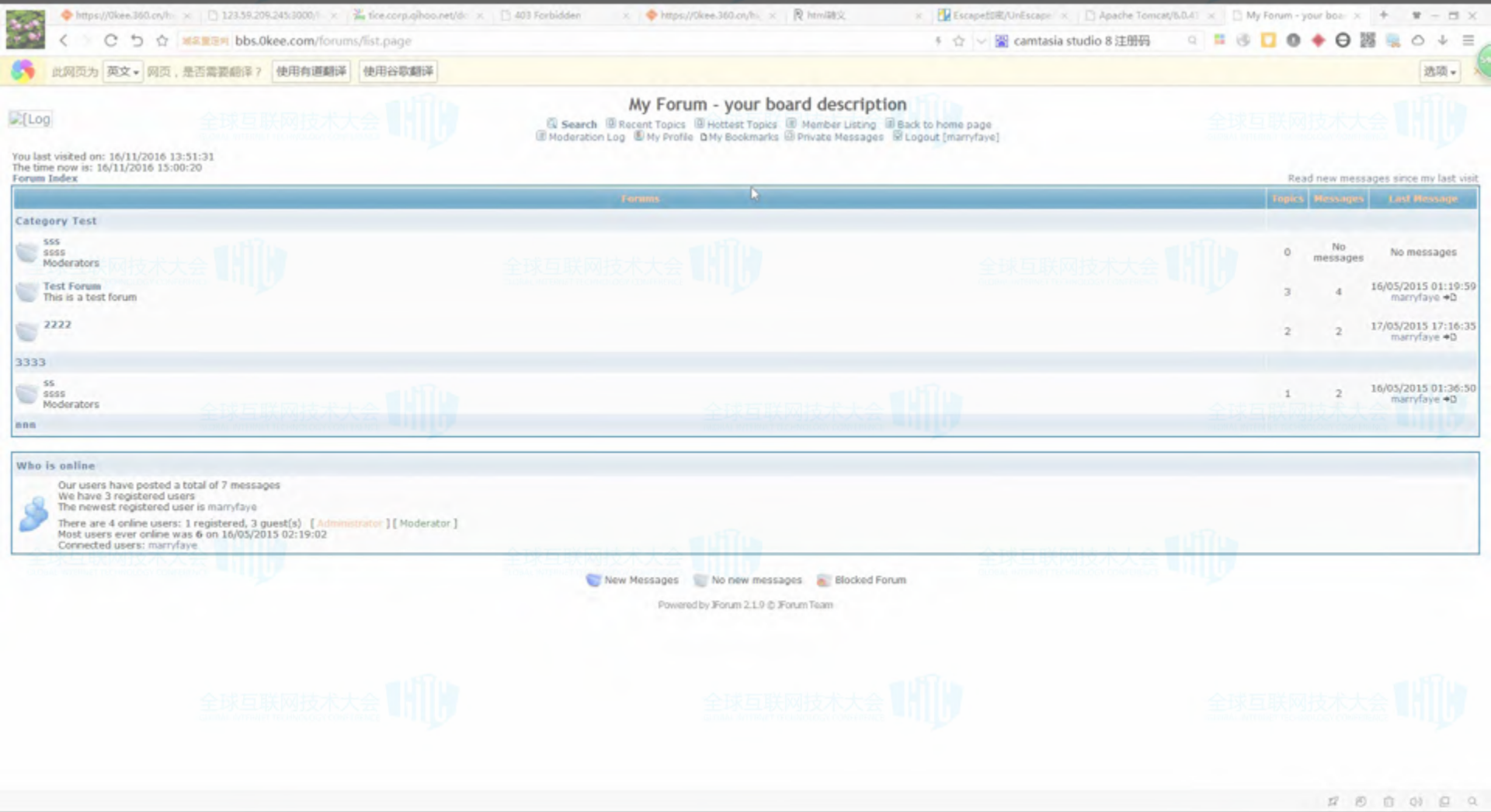

115.28.153.206/webmail/client/index.php?module=view&action=index
xss平台
MAIL
cto@0kee.com
下午好, cto
今天是: 2016-11-18 星期五
系统公告
可以在域管理后台设置本处的公告内容，删除公告内容后公告模块将不在首页显示。
商务小工具
万年历
万用计算器

XSS利用

XSS + CSRF



XSS利用


bbs.0kee.com/forums/list.page
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
Read new messages since my last visit
Forums
Topics
Messages
Last Message
Category Test
sss
ssss
Moderators
0
No messages
No messages
Test Forum
This is a test forum
3
4
16/05/2015 01:19:59
marryfaye
2222
2
2
17/05/2015 17:16:35
marryfaye
3333
ss
ssss
Moderators
1
2
16/05/2015 01:36:50
marryfaye
aaa
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

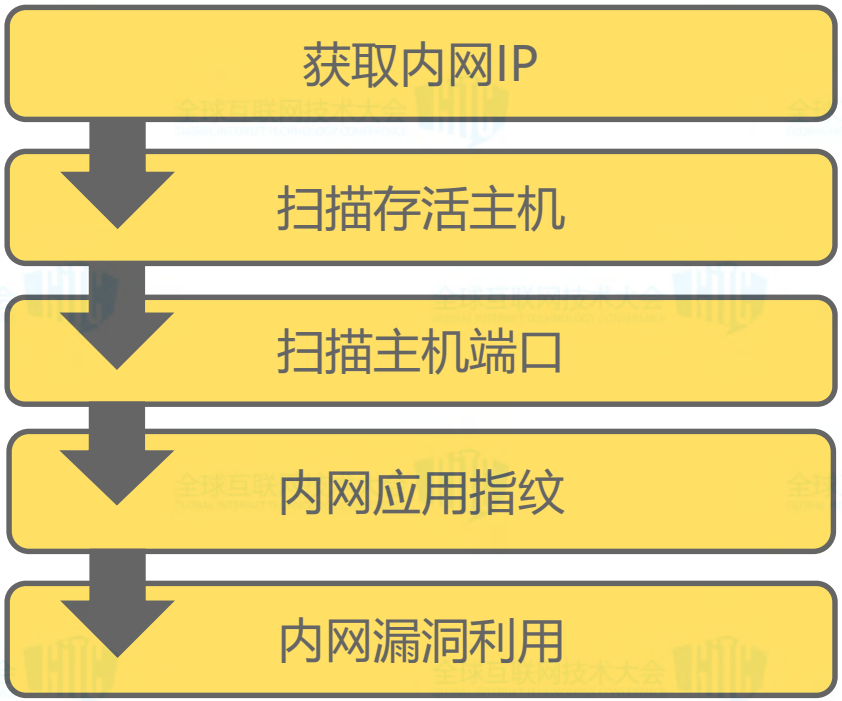
XSS事件

- 新浪微博蠕虫

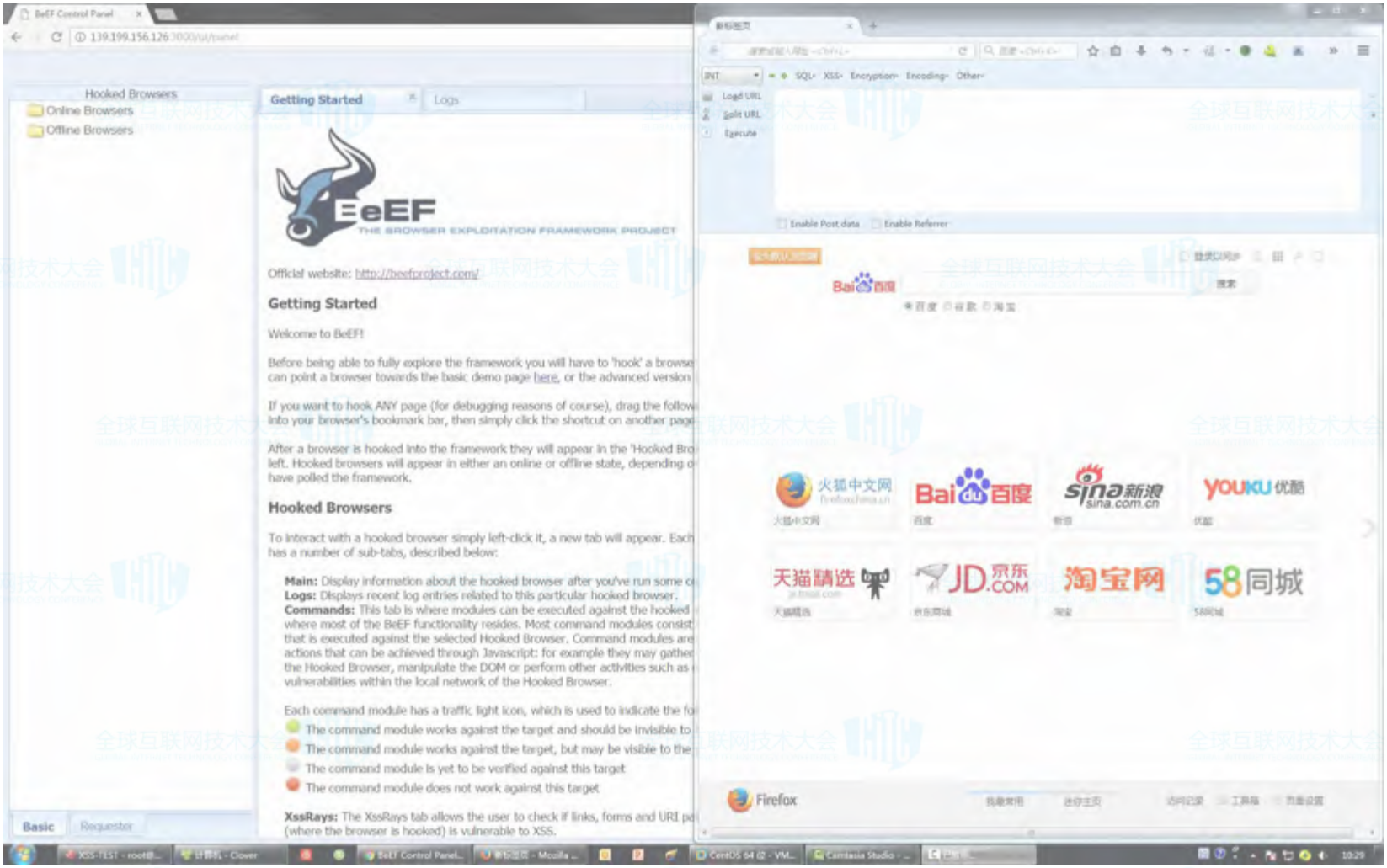
```
function random_msg(){
    link = ' http://163.fm/PxZHoxn?id=' +
    //使用短地址服务，构造XSS传播连接
    //http://weibo.com/pub/star/g/xyyyd%2
    //隐藏自己的恶意js脚本
    var msgs = [ //话题列表
        '郭美美事件的一些未注意到的细节: ',
        '建党大业中穿帮的地方: ',
        '让女人心动的100句诗歌: ',
        '3D肉团团高清普通话版种子: ',
        '这是传说中的神仙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

XSS利用

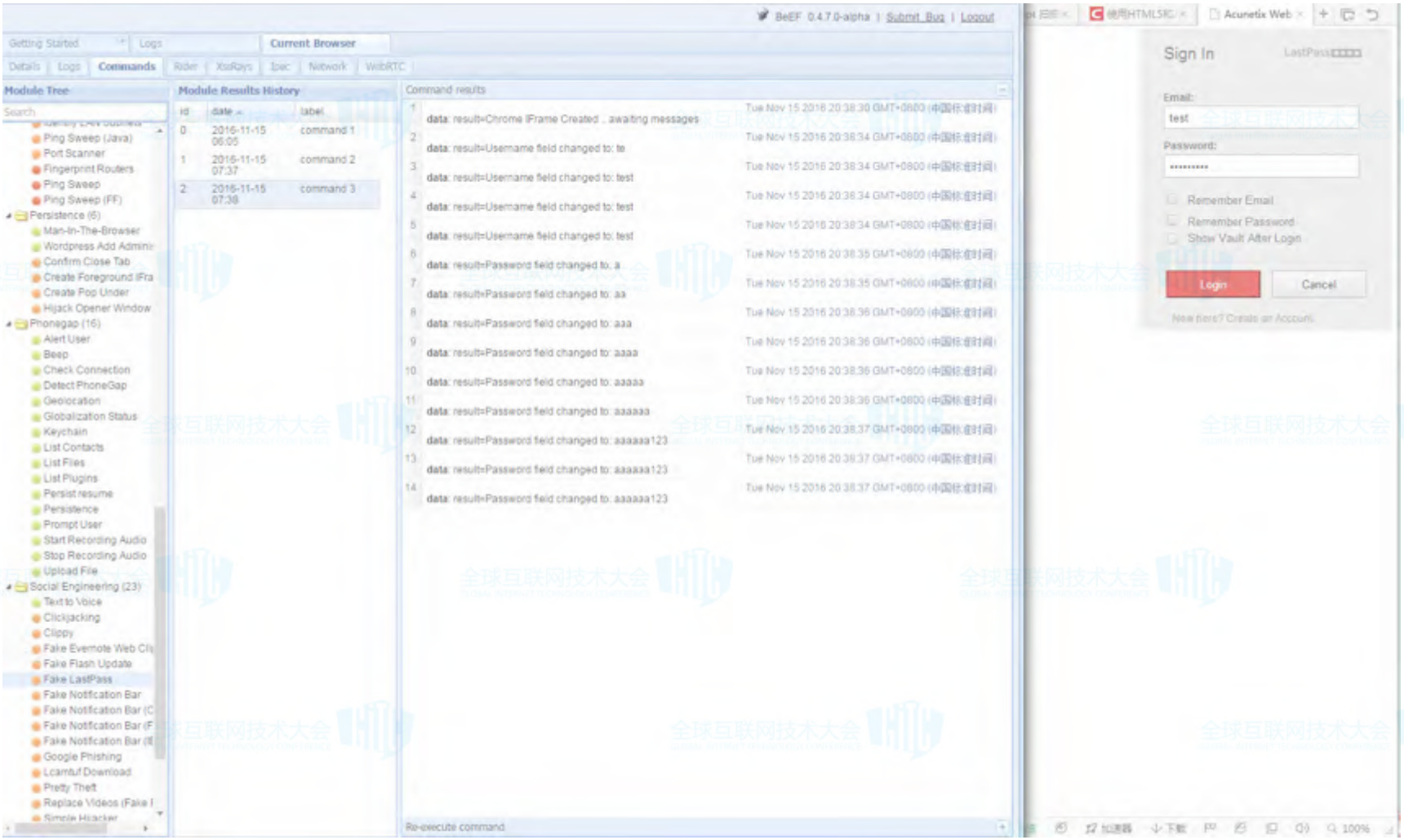
- XSS攻击内网



XSS利用


BeEF Control Panel
Hooked Browsers
Online Browsers
Offline Browsers
Getting Started
Logs
BeEF
THE BROWSER EXPLOITATION FRAMEWORK PROJECT
Official website: http://beefproject.com/
Getting Started
Welcome to BeEF!
Hooked Browsers
Basic
Requester
Firefox

XSS钓鱼


BeEF 0.4.7.0-alpha | Submit Bug | Logout
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
WebRTC
Module Tree
Module Results History
Command results
Ping Sweep (Java)
Port Scanner
Fingerprint Routers
Ping Sweep
Ping Sweep (FF)
Persistence (6)
Man-In-The-Browser
Wordpress Add Admin
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 (I
Google Phishing
Lcamtuf Download
Pretty Theft
Replace Videos (Fake I
Simple Hijacker
Re-execute command
Acunetix Web
Sign In
Email:
test
Password:
Remember Email
Remember Password
Show Vault After Login
Login
Cancel

XSS利用

- 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...

蠕虫攻击

水坑攻击

键盘记录

Rootkit

钓鱼、劫持

Cookies、Localstorage...

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...

XSS防御

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

关键字过滤的弊端

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

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 g
plain string.

alert(1) Encode Eval Source


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

1227 chars Run This

Links

XSS防御

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）

XSS防御

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

XSS防御

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）

XSS防御

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）

前端主动防御方案--护心镜

- 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

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>文章管理</title>
<link href="images/css.css" rel="stylesheet" type="text/css">
<script type="text/javascript">
var hxj_config = {
    project_key: "                    7220ba8d3ddddd",
    domain_white: ["localhost","127.0.0.1"],
    enable_plugin:{"cookie":1,"xsstester":1,"password":1,"fish":1,"script":1,"webshell":1},

};
</script>
<script type="text/javascript" src="http://res.0kee.com/hxj.min.js"></script>
<script src="../include/js/jquery.js" type="text/javascript" ></script>
<script type="text/javascript">
function doAction(a,id,v){
    if(a=='validate'){
```

- 二维码

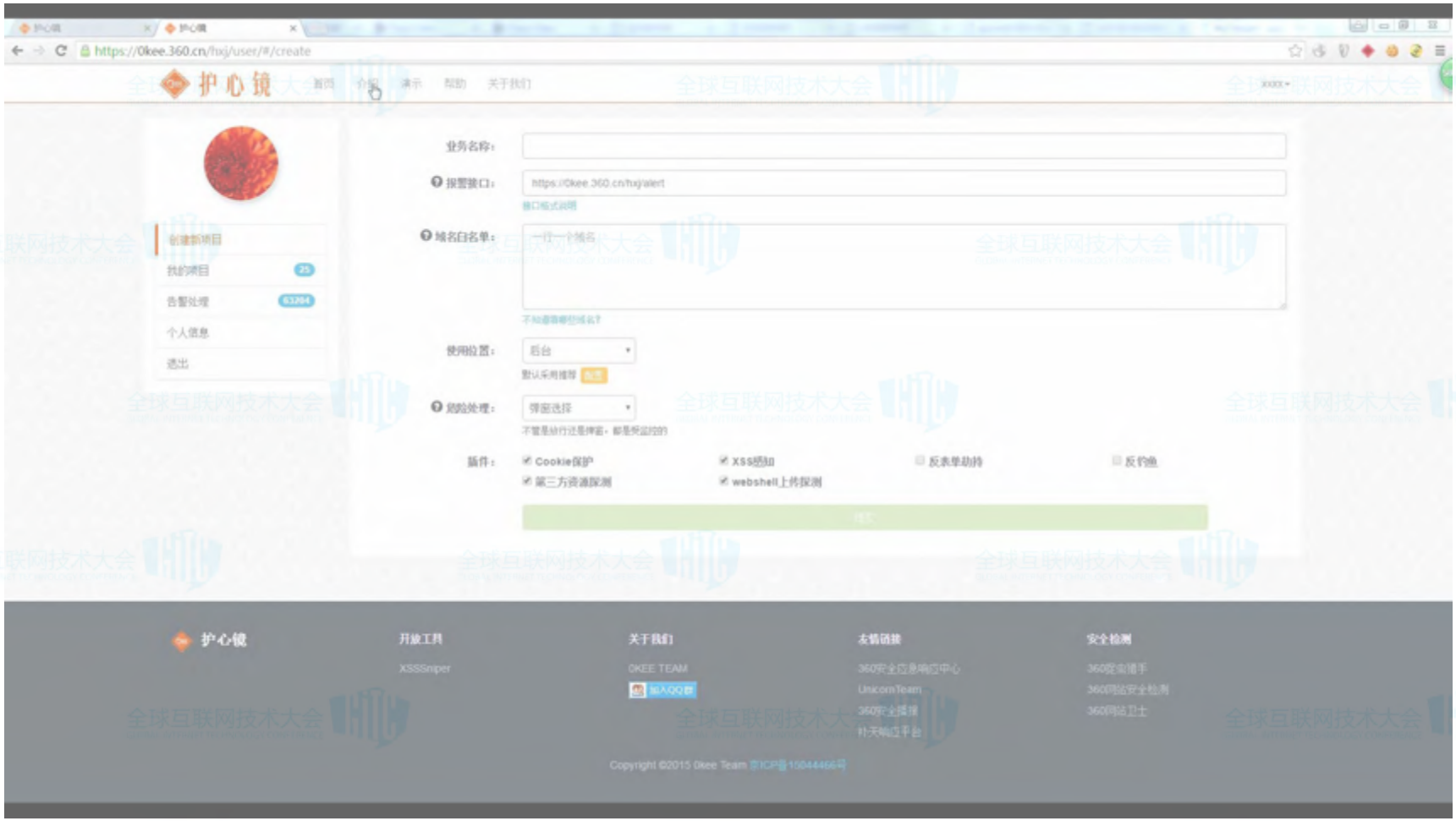
XSS防御

- 如何降低误报？
- 如何降低成本？
- 如何主动发现？

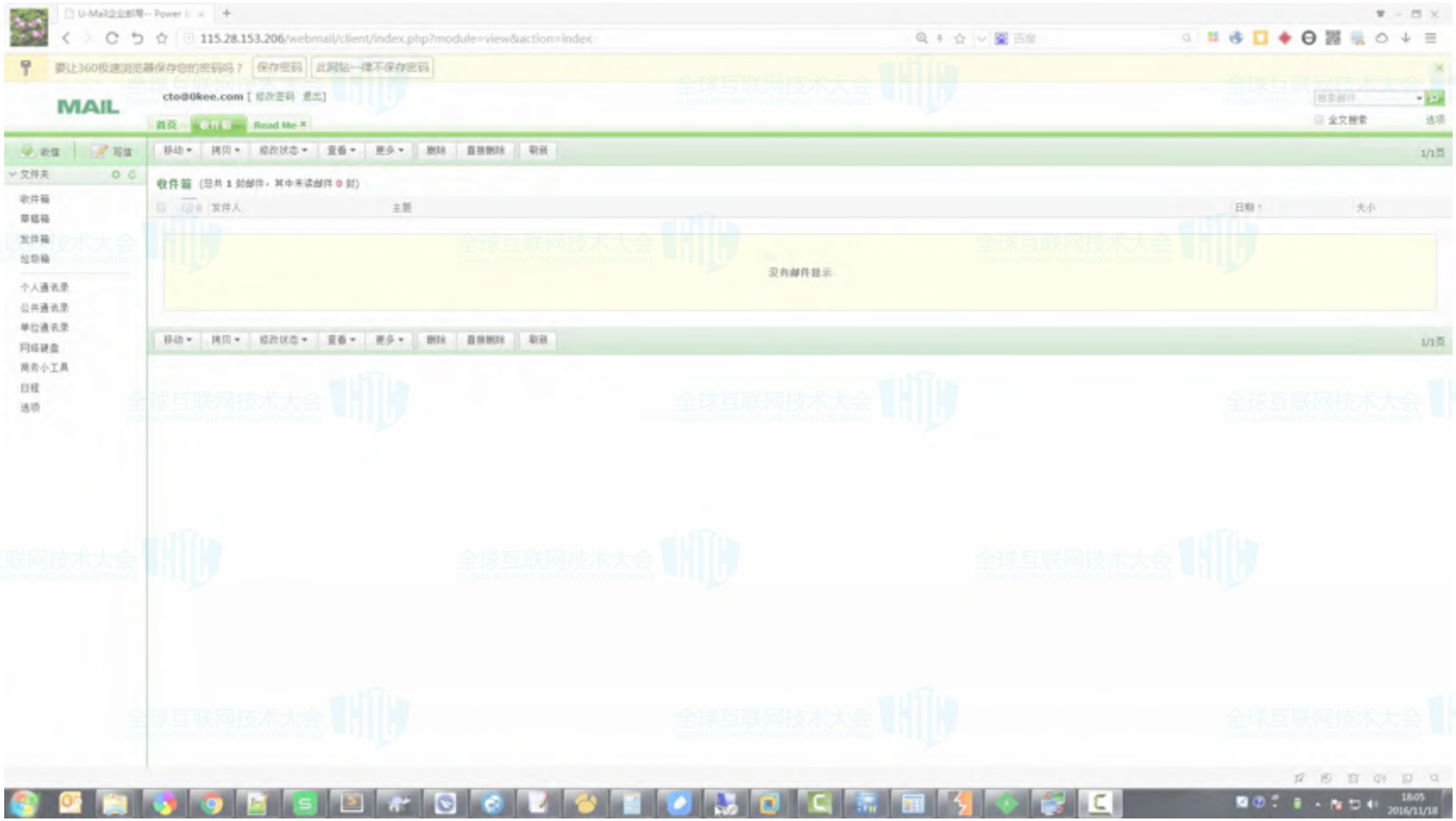
护心镜优势

- 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。

护心镜配置


https://0kee.360.cn/hxj/user/#/create
护心镜
首页
个人
演示
帮助
关于我们
创建新项目
我的项目
告警处理
个人信息
退出
业务名称：
报警接口：
域名白名单：
使用位置：
后台
启动处理：
插件：
Cookie保护
XSS防御
反表单劫持
反钓鱼
第三方资源探测
webshell上传探测
护心镜
开放工具
XSSSniper
关于我们
0KEE TEAM
友情链接
安全检测
Copyright ©2015 0kee Team

护心镜实例


115.28.153.206/webmail/client/index.php?module=view&action=index
MAIL
cto@0kee.com
Read Me
收件箱
没有邮件显示

技术实现

```
/*函数劫持*/
var _alert =
alert = funct
    console.l
    _alert(s)
}
/*对象/属性劫
Object.define
Object._
Object._
```

```
var a = new MutationObserver(function(d) {
    d.forEach(function(f) {
        var e = f.addedNodes;
        for (var g = 0; g < e.length; g++) {
            var j = e[g];
            Hookjs.log("Cteate tagName:"+j.tagName);
```

```
Object.defineProperty(document, "cookie", {
    get: function() {
        console.log("获取cookie");
        b = someMethodGetCookie();
        return b
    },
    set: function(b) {
        console.log("写入cookie");
        someMethodSetCookie(b);
    }
})
```

技术实现：事件与告警

```
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:"]
];
```

反卸载技术的对抗--保护自己

- 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。**

反卸载技术的对抗--保护回调函数

- 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

360
www.360.cn