GOPS2016
Beijing

全球运维大会

2016

DevOps 2.0：重塑运维价值

会议时间：12月16日 - 12月17日

会议地点：北京国际会议中心

主办单位：高效运维社区 GreatOPS Community　开放运维联盟 OOPSA Open OPS Alliance

XSS攻击与企业级的解决方案

王珂、任言

WE ARE

0KEE TEAM !

XSS

- Cross-Site Scripting
- 控制你的浏览器

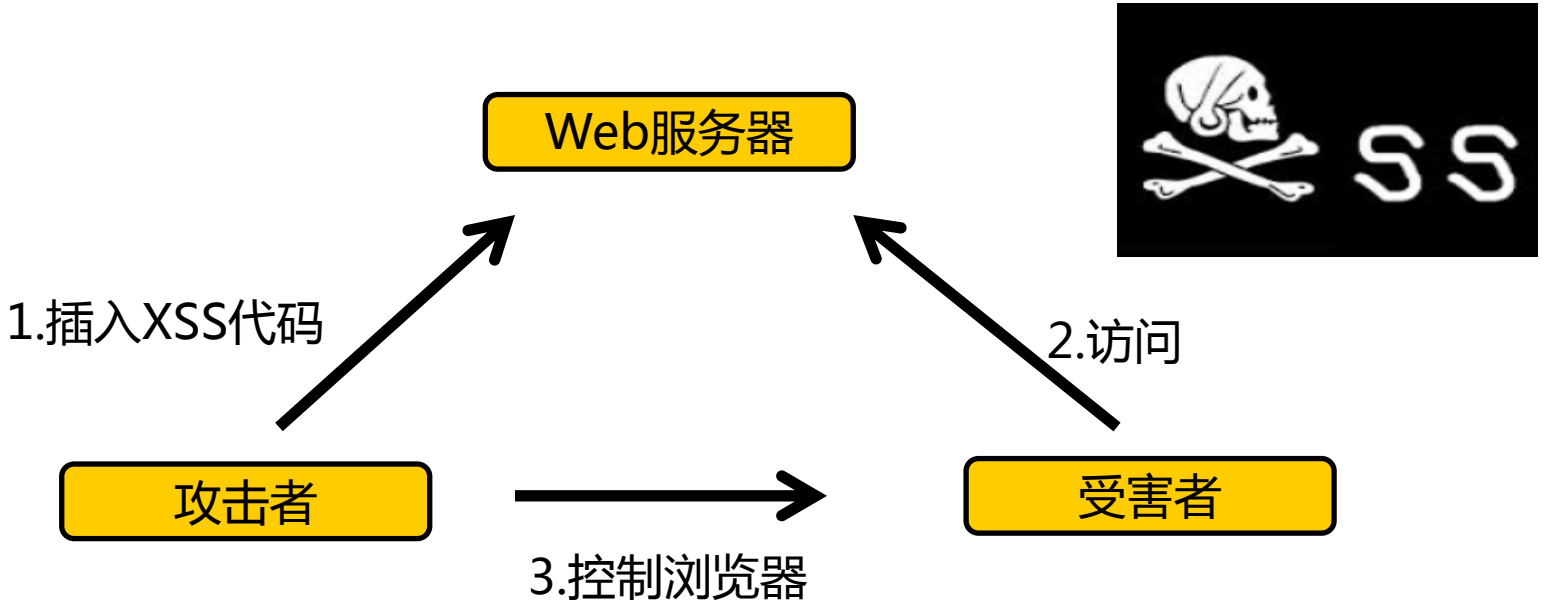
XSS

```
<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
- But，攻击花样多，覆盖面广

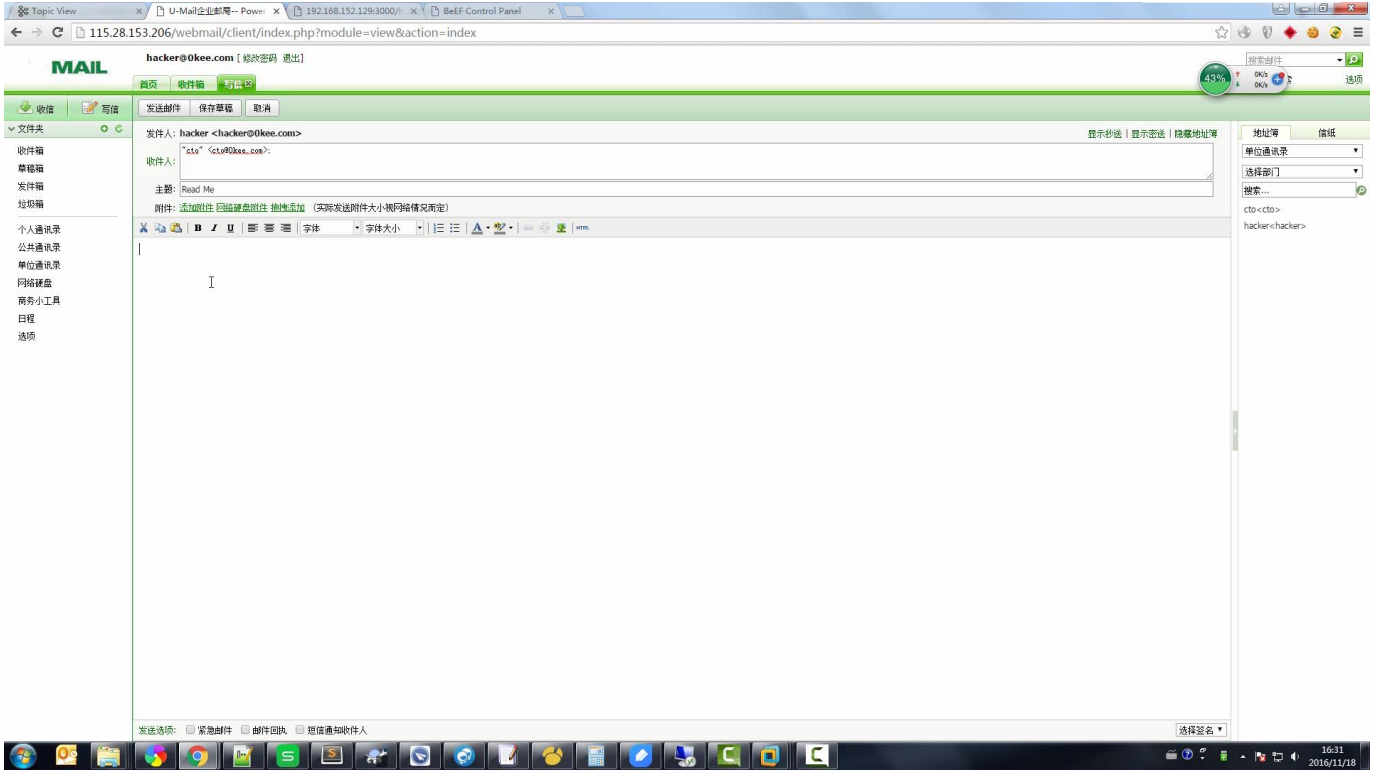
XSS利用-获取Cookie

XSS利用-攻击邮箱

XSS攻击邮箱

- QQ、网易等邮箱都曾被XSS
- GMail的XSS黑市售价高昂

XSS利用-攻击邮箱


Topic View
U-Mail企业邮局-- Powe
192.168.152.129:3000/h
BeEF Control Panel
115.28.153.206/webmail/client/index.php?module=view&action=index
MAIL
hacker@0kee.com [修改密码 退出]
首页
收件箱
写信
发送邮件
保存草稿
取消
文件夹
收件箱
草稿箱
发件箱
垃圾箱
个人通讯录
公共通讯录
单位通讯录
网络硬盘
商务小工具
日程
选项
发件人: hacker <hacker@0kee.com>
收件人:
"cto" <cto@0kee.com>;
主题:
Read Me
附件: 添加附件 网络硬盘附件 抽屉添加 (实际发送附件大小视网络情况而定)
显示抄送 | 显示密送 | 隐藏地址簿
地址簿
信纸
单位通讯录
选择部门
搜索...
cto<cto>
hacker<hacker>
发送选项:
紧急邮件
邮件回执
短信通知收件人
选择签名
43%
16:31
2016/11/18

XSS利用-结合CSRF

XSS利用-蠕虫

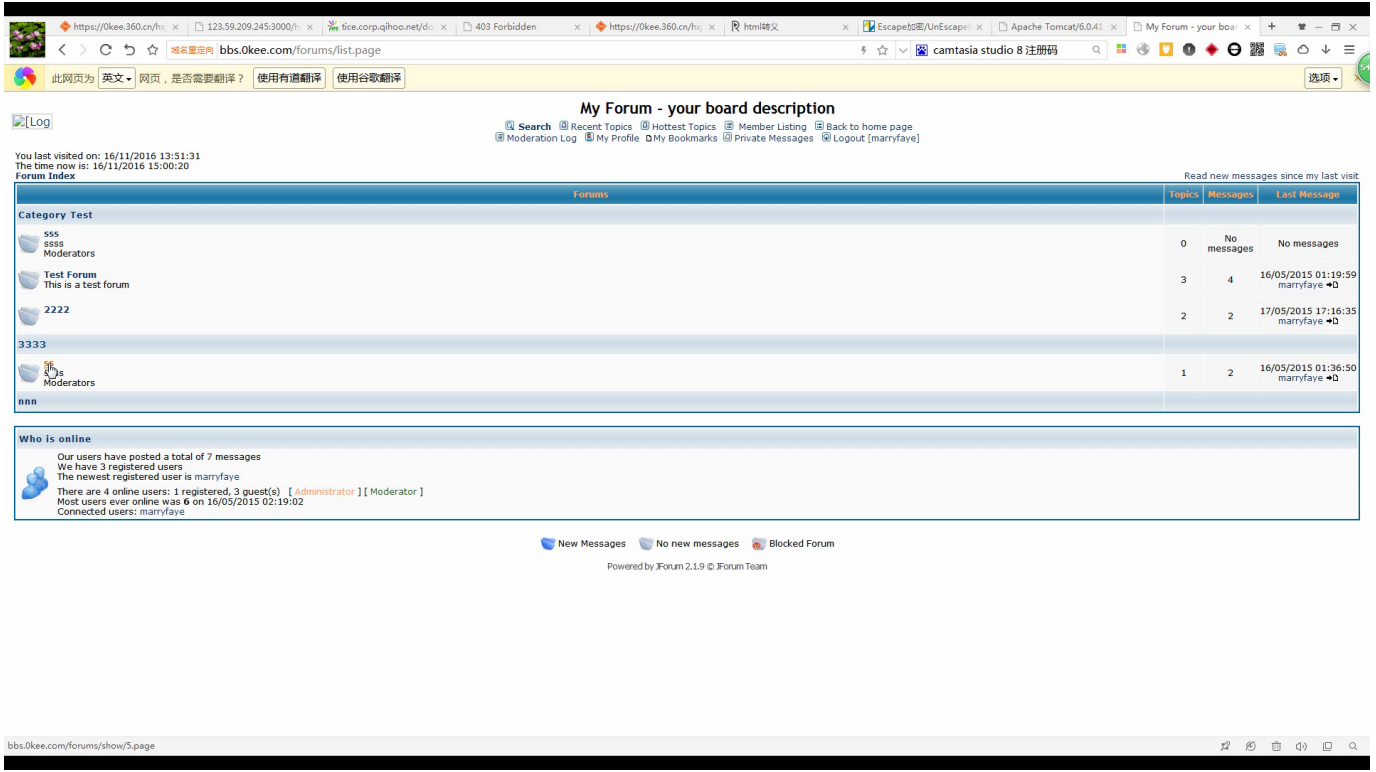
XSS利用-蠕虫

- 新浪微博蠕虫

```
function random_msg(){
    link = ' http://163.fm/PxZHoxn?id=' + new Date()
    //使用短地址服务，构造XSS传播连接
    //http://weibo.com/pub/star/g/xyyyd%22%3E%3Cscri
    //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()*msgs.ler
        //随机选取话题，加上之前的传播连接作为微博内容
    msg = encodeURIComponent(msg); //对内容进行Url编码
    return msg;
}
```

XSS利用-GetShell

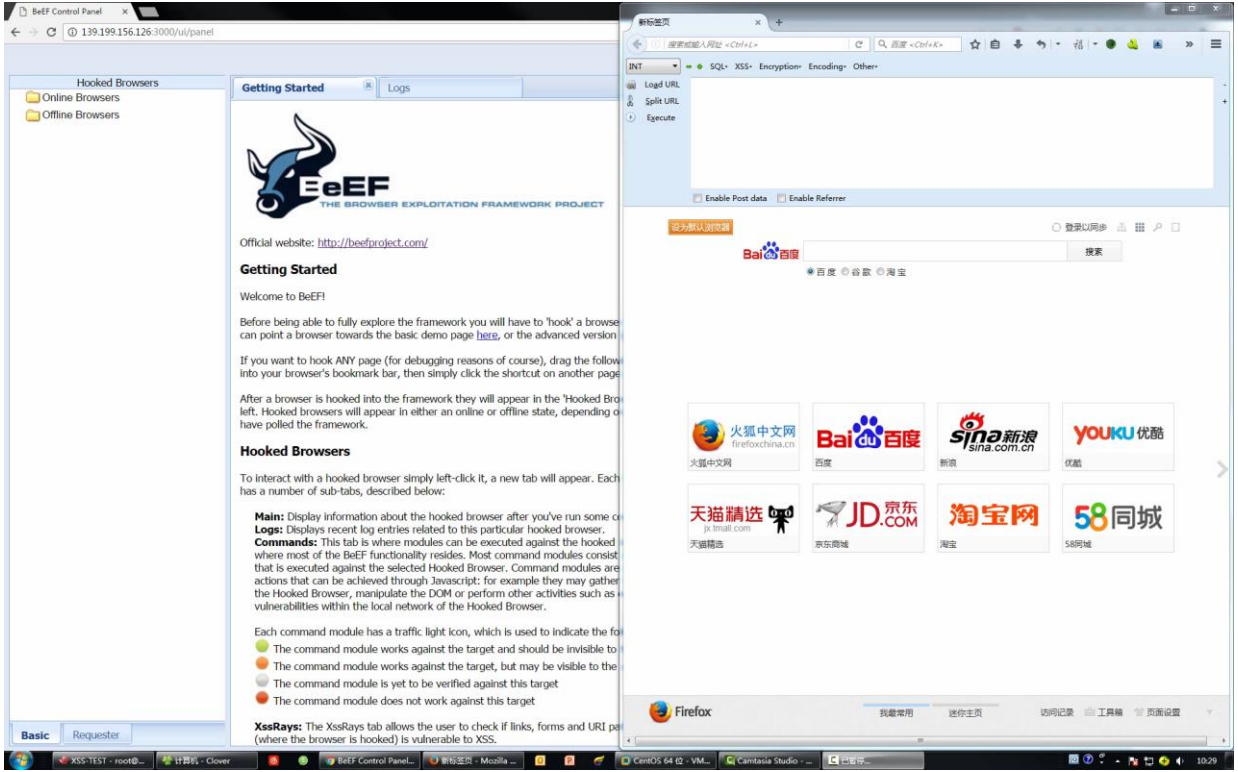
XSS利用-GetShell



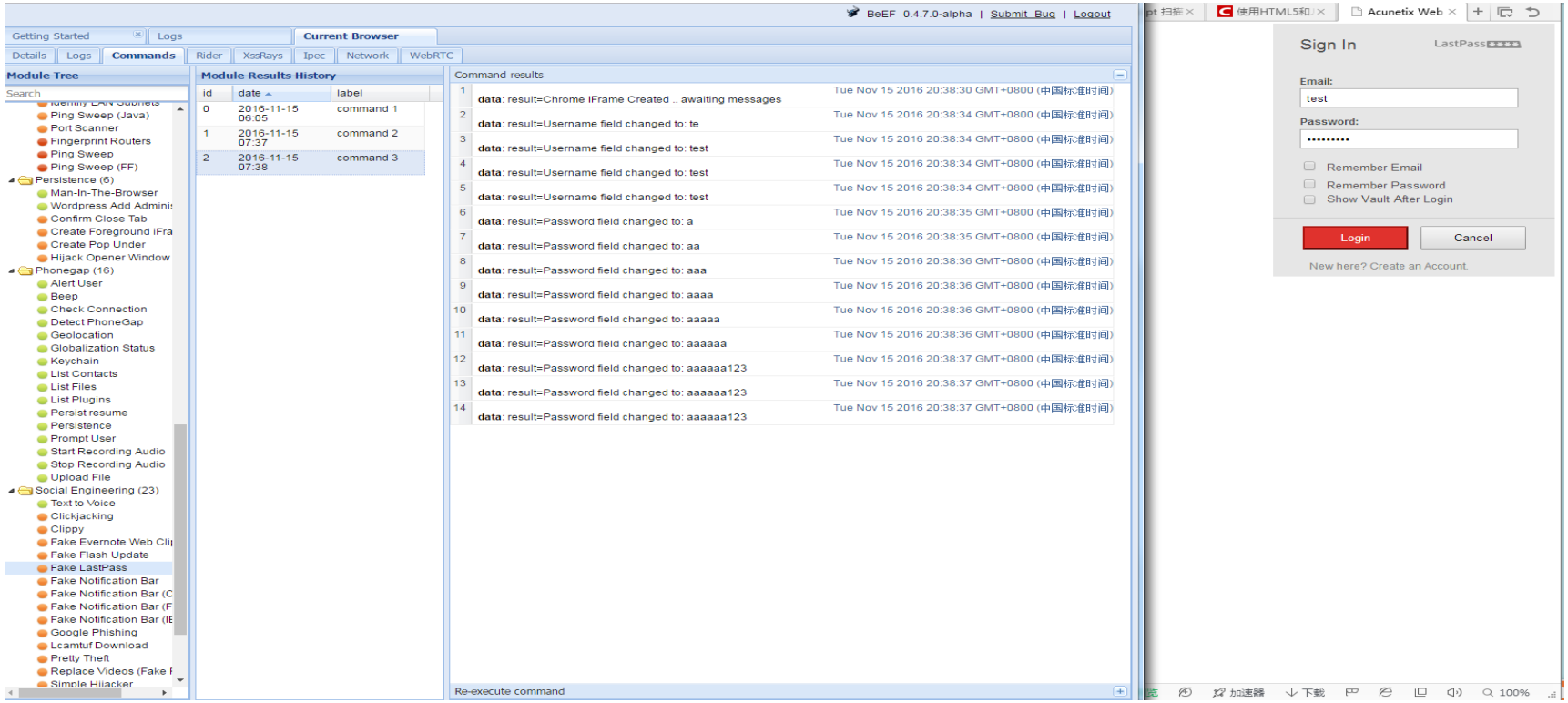
XSS利用-攻击内网

- XSS攻击内网

XSS利用-攻击内网


BeEF Control Panel
139.199.156.126:3000/ui/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
Main: Display information about the hooked browser after you've run some
Logs: Displays recent log entries related to this particular hooked browser.
Commands: This tab is where modules can be executed against the hooked
The command module works against the target and should be invisible to
The command module works against the target, but may be visible to the
The command module is yet to be verified against this target
The command module does not work against this target
XssRays: The XssRays tab allows the user to check if links, forms and URI
Basic
Requester
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
Firefox

XSS利用-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
Search
Ping Sweep (Java)
Port Scanner
Fingerprint Routers
Ping Sweep
Ping Sweep (FF)
Persistence (6)
Man-In-The-Browser
Wordpress Add Admini
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
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
data: result=Chrome IFrame Created .. awaiting messages
data: result=Username field changed to: te
data: result=Username field changed to: test
data: result=Username field changed to: test
data: result=Username field changed to: test
data: result=Password field changed to: a
data: result=Password field changed to: aa
data: result=Password field changed to: aaa
data: result=Password field changed to: aaaa
data: result=Password field changed to: aaaaa
data: result=Password field changed to: aaaaaa
data: result=Password field changed to: aaaaaa123
data: result=Password field changed to: aaaaaa123
data: result=Password field changed to: aaaaaa123
Tue Nov 15 2016 20:38:30 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:34 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:34 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:34 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:34 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:35 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:35 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:36 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:36 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:36 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:36 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:37 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:37 GMT+0800 (中国标准时间)
Tue Nov 15 2016 20:38:37 GMT+0800 (中国标准时间)
Re-execute command
Acunetix Web
Sign In
LastPass
Email:
test
Password:
Remember Email
Remember Password
Show Vault After Login
Login
Cancel
New here? Create an Account.

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

Cookies、Localstorage...

钓鱼、劫持

内网渗透

管理员

后台地址、页面源码、管理员信息、CSRF...

端口扫描、ST2利用、路由器...

XSS防御

XSS防御

方案	优势	劣势	场景

XSS防御

方案	优势	劣势	场景
安全编程	根本解决	容易遗漏； 第三方不可控	必须
WAF	通用性好	易绕过； 不适用于所有类型； 成本高	安全能力跟不上业务发展

XSS防御

方案	优势	劣势	场景
安全编程	根本解决	容易遗漏； 第三方不可控	必须
WAF	通用性好	易绕过； 不适用于所有类型； 成本高	安全能力跟不上业务发展
Http-Only	保护cookie	只能保护Cookie	具有身份认证的网站

XSS防御

方案	优势	劣势	场景
安全编程	根本解决	容易遗漏； 第三方不可控	必须
WAF	通用性好	易绕过； 不适用于所有类型； 成本高	安全能力跟不上业务发展
Http-Only	保护cookie	只能保护Cookie	具有身份认证的网站
CSP	有效拦截	配置不方便； 部署不方便； 高误报	设计之初最佳; 网站结构清晰

XSS防御

方案	优势	劣势	场景
安全编程	根本解决	容易遗漏； 第三方不可控	必须
WAF	通用性好	易绕过； 不适用于所有类型； 成本高	安全能力跟不上业务发展
Http-Only	保护cookie	只能保护Cookie	具有身份认证的网站
CSP	有效拦截	配置不方便； 部署不方便； 高误报	设计之初最佳; 网站结构清晰
？	配置方便； 部署方便； 低误报	？	任何网站

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=>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: "[redacted]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'){
```

护心镜8大功能


防御未知
脚本加载
盗取
Cookie
钓鱼
密码窃取
XSS测试
WebShell
上传
XSS平台
Http-Only
模拟
护心镜

技术实现

```
/*函数劫持*/
var _alert = alert;
alert = function(s){
    console.log(Call
    _alert(s);
}
/*对象/属性劫持*/
Object.defineProperty

Object.__define
Object.__define
```

```
var a = new MutationObserver(function(d) {
    d.forEach(function(f) {
        var e = f.addedNodes;    //e为加入到DOM树中的元素列表
        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:"]
];
```

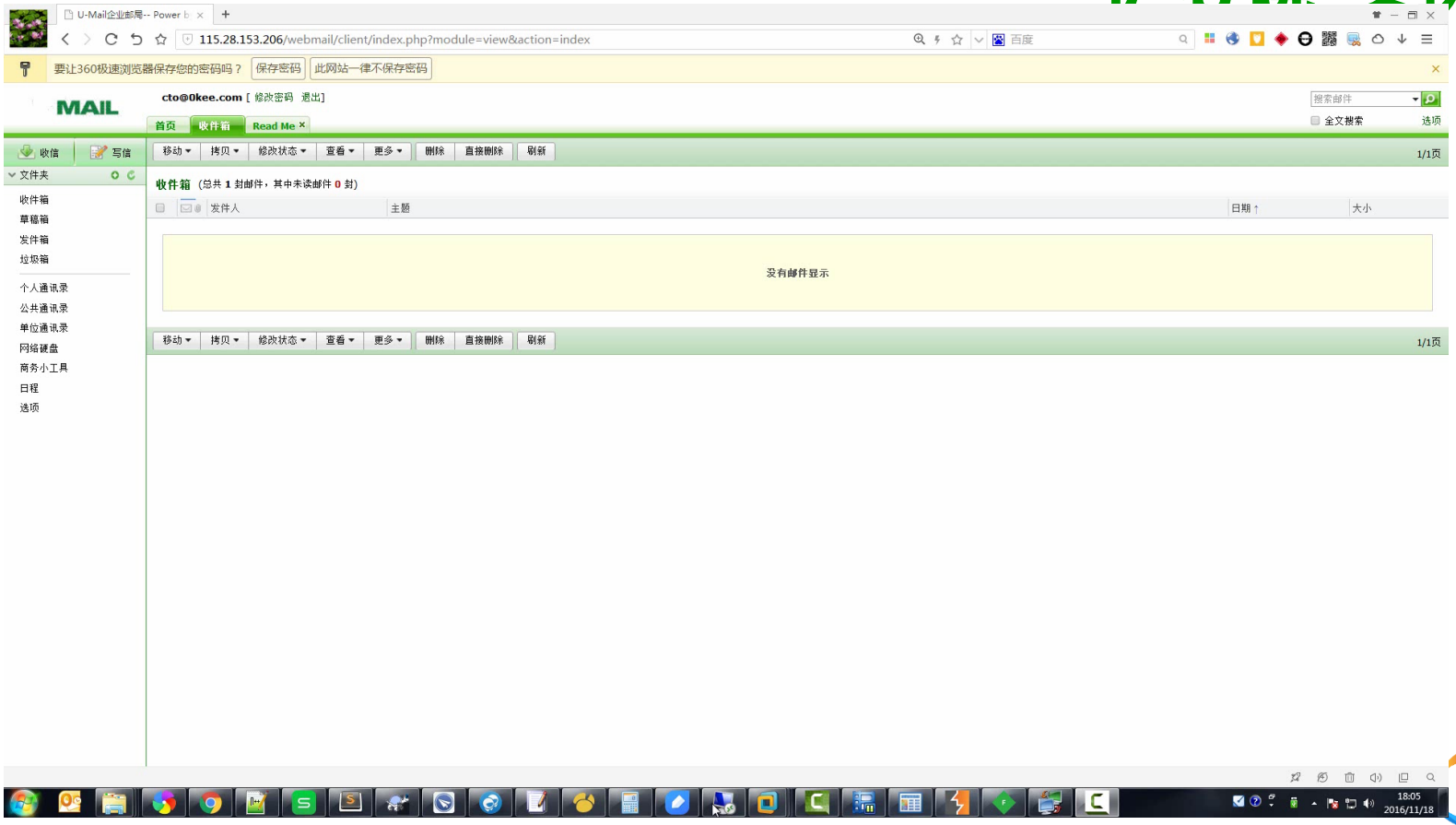
反卸载技术的对抗--保护自己

- 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);
```

- **保证护心镜所使用的变量、函数、对象不被外部js篡改。**

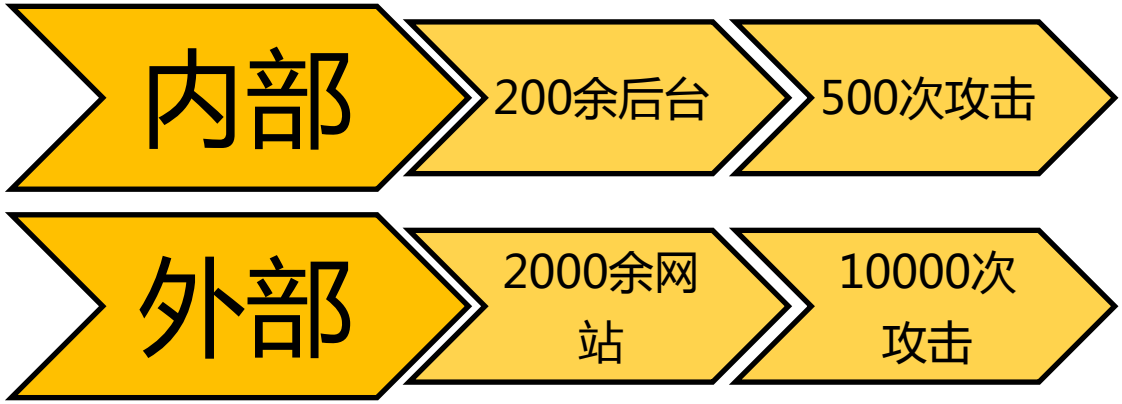
护心镜-实例


U-Mail企业邮局-- Power b
115.28.153.206/webmail/client/index.php?module=view&action=index
百度
要让360极速浏览器保存您的密码吗？
保存密码
此网站一律不保存密码
MAIL
cto@0kee.com [修改密码 退出]
搜索邮件
全文搜索
选项
首页
收件箱
Read Me
收信
写信
移动
拷贝
修改状态
查看
更多
删除
直接删除
刷新
1/1页
文件夹
收件箱
草稿箱
发件箱
垃圾箱
个人通讯录
公共通讯录
单位通讯录
网络硬盘
商务小工具
日程
选项
收件箱 （总共 1 封邮件，其中未读邮件 0 封）
发件人
主题
日期
大小
没有邮件显示
移动
拷贝
修改状态
查看
更多
删除
直接删除
刷新
1/1页
18:05
2016/11/18

护心镜-平台


护心镜
首页
介绍
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
项目名称 创建时间 告警次数 危险处理 插件 域名白名单 代码 操作
xxx 2016-11-21 16:19:21 0 选择 Cookie保护 XSS感知 反表单劫持 反钓鱼 webshell上传探测 第三方资源探测 xx 查看 删除 修改
xxxxx 2016-11-21 16:18:33 0 选择 Cookie保护 XSS感知 webshell上传探测 第三方资源探测 查看 删除 修改
Test 2016-11-16 16:02:09 20 选择 Cookie保护 XSS感知 反表单劫持 反钓鱼 webshell上传探测 第三方资源探测 cnzz.com baidu.com 360.cn 查看 删除 修改
用户画像系统 2016-11-04 12:26:40 5 放行 Cookie保护 XSS感知 反钓鱼 第三方资源探测 qihoo.com qihoo.net qhimg.com 360.cn 查看 删除 修改
邮箱XSS演示 2016-10-20 10:55:15 12 选择 Cookie保护 mail.domain.com 0kee.com qq.com 查看 删除 修改
btime 2016-09-07 16:12:32 0 放行 Cookie保护 第三方资源探测 btime.cn 360.cn qhimg.com baidu.com cnzz.com 查看 删除 修改
360好药后台 2016-08-25 11:59:20 53106 放行 Cookie保护 XSS感知 webshell上传探测 第三方资源探测 360haoyao.com s.360img.cn 360img.cn 51mdq.com 360jk.com 查看 删除 修改
花椒DMG后台 2016-08-04 18:43:45 317 放行 Cookie保护 XSS感知 反表单劫持 反钓鱼 webshell上传探测 第三方资源探测 qihoo.net huajiao.com qlogo.cn 360.cn qhimg.com 查看 删除 修改
猎网平台 2016-08-04 15:43:06 147 放行 Cookie保护 XSS感知 反表单劫持 反钓鱼 webshell上传探测 第三方资源探测 3001.net 360.cn qhimg.com 查看 删除 修改
ssp.360.cn 2016-07-27 10:47:51 0 放行 Cookie保护 XSS感知 反表单劫持 反钓鱼 webshell上传探测 第三方资源探测 360.cn mediav.com 查看 删除 修改
360商城后台（supplier.mall.360.com） 2016-07-05 16:54:11 4 放行 Cookie保护 XSS感知 反表单劫持 反钓鱼 webshell上传探测 第三方资源探测 360.cn 360.com qhimg.com useso.com 查看 删除 修改
随便填 2016-05-23 19:06:22 0 放行 Cookie保护 XSS感知 反表单劫持 反钓鱼 第三方资源探测 qiku.com 360.cn qhimg.com 360shouji.com google-analytics.com 查看 删除 修改

护心镜-实践



XSS防御总结

方案	优势	劣势	场景
安全编程	根本解决	容易遗漏； 第三方不可控	必须
Http-Only	保护cookie	只能保护Cookie	具有身份认证的网站
WAF	通用性好	易绕过； 不适用于所有类型； 成本高	安全能力跟不上业务发展
CSP	有效拦截	配置不方便； 部署不方便； 高误报	设计之初最佳; 网站结构清晰
护心镜	配置方便； 部署方便； 低误报	兼容性	任何网站

护心镜邀请码

DevOpsDays 即将首次登陆中国

DevOps 之父 Patrick Debois 与您相约
DevOpsDays 北京站 2017年3月18日

门票早鸟价仅限前100名，请从速哟

http://2017-beijing.devopsdayschina.org/

想第一时间看到
高效运维社区公众号
的好文章吗？

请打开高效运维社区公众号，点击右上角小人，如右侧所示设置就好

Thanks

高效运维社区

开放运维联盟

荣誉出品