



全球运维大会

2016

DevOps 2.0: 重塑运维价值



北京站

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：



XSS攻击与企业级的解决方案

王珂、任言



OKeep Team

WE ARE

OKEEP TEAM !





- Cross-Site Scripting
- 控制你的浏览器

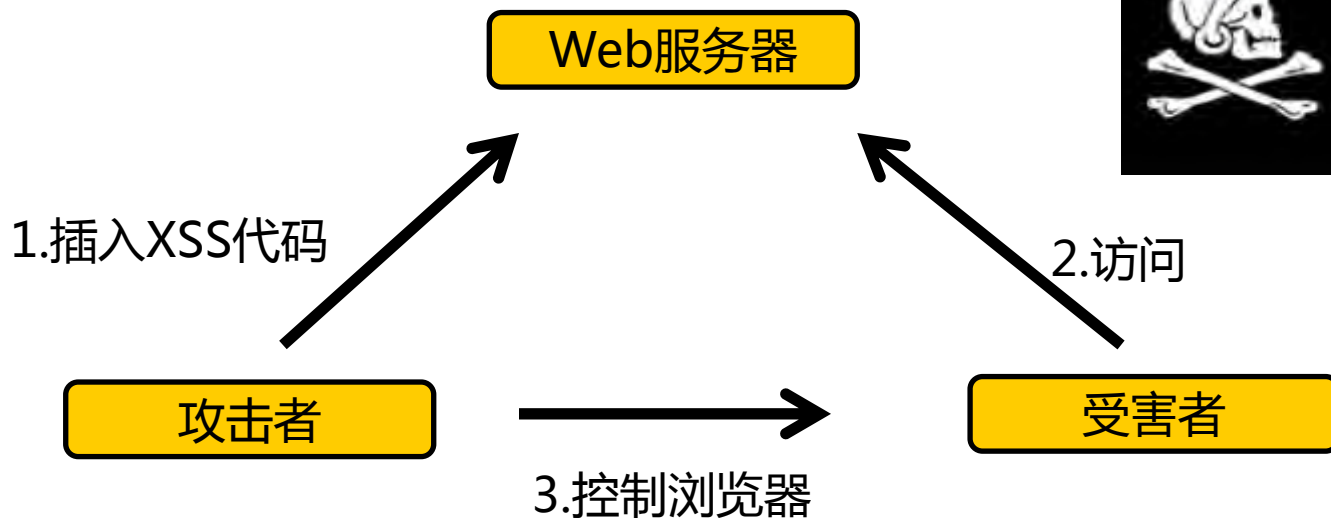
XSS

```
<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

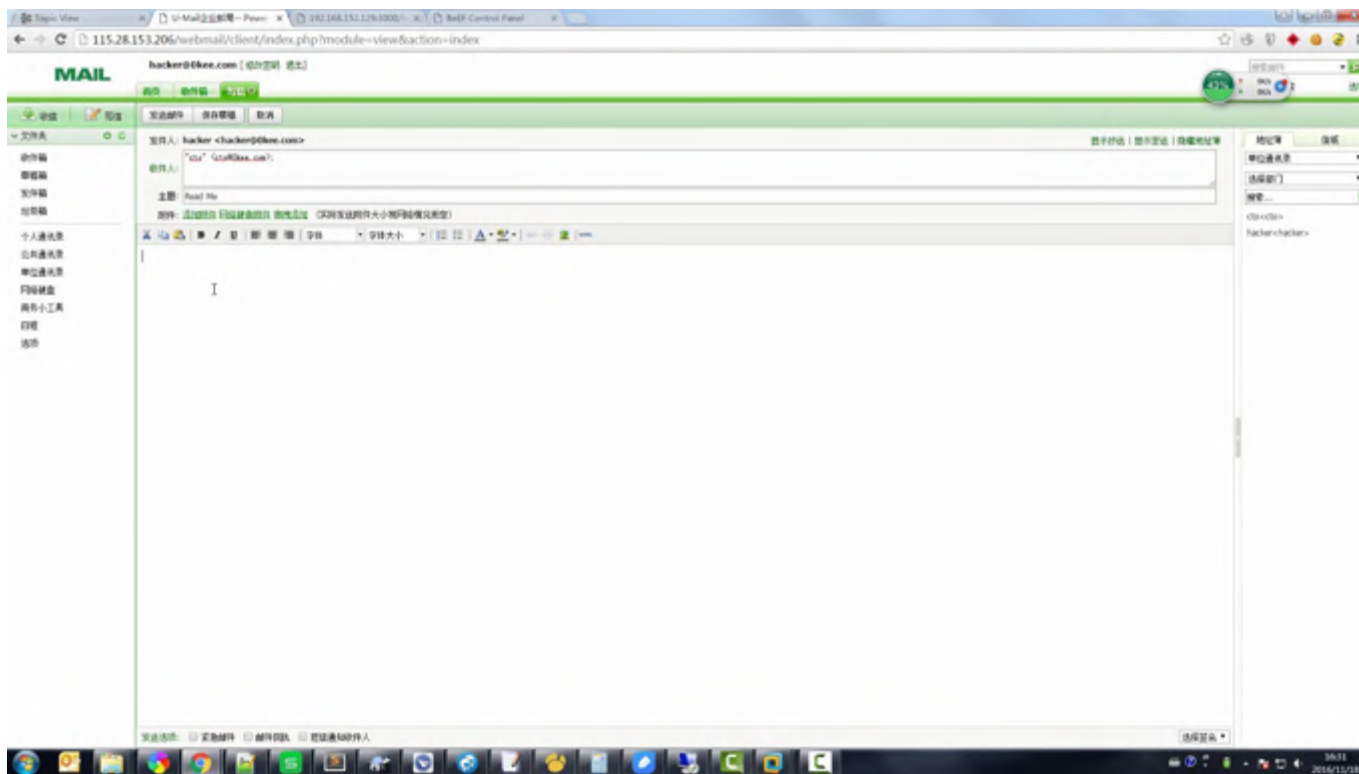
XSS利用-获取Cookie



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



XSS利用-结合CSRF



XSS利用-蠕虫



• 新浪微博蠕虫

```
20. function random_msg(){
21.     link = ' http://163.fm/Px2Hoxn?id=' + new Date()
22.     //使用短地址服务, 构造XSS传播连接
23.     //http://weibo.com/pub/star/g/xyyd%22%3E%3Cscxi
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肉团高清图普通话版种子:',
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.         '杨幂被曝多次潜规则:',
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()*msgs.length)];
37.     //随机选取话题, 加上之前的传播连接作为微博内容
38.     msg = encodeURIComponent(msg); //对内容进行Uri编码
39.     return msg;
40. }
```



XSS利用-GetShell



XSS利用-GetShell

The screenshot shows a web browser window displaying a forum page titled "My Forum - your board description". The browser's address bar shows the URL "https://bbs.0kee.com/forums/list.page". The forum page includes a navigation menu with links for Search, Recent Topics, Hottest Topics, Member Listing, Back to home page, Moderation Log, My Profile, My Bookmarks, Private Messages, and Logout. A table lists forum categories with columns for Topics, Messages, and Last Message. Below the table is a "Who is online" section with statistics on registered users, online users, and most users ever online.

Category Text	Topics	Messages	Last Message
sss sss Moderators	0	No messages	No messages
Test Forum This is a test forum	3	4	16/05/2015 01:10:59 marryfaye ↻
2222	2	2	17/05/2015 17:16:35 marryfaye ↻
3333			
sss Moderators	1	2	16/05/2015 01:36:50 marryfaye ↻

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: 3 registered, 3 guest(s) [Administrator] [Moderator]
Most users ever online was 6 on 16/05/2015 02:19:02
Connected users: marryfaye

Powered by Forum 2.1.0 © Forum Team

- XSS攻击内网

获取内网IP

扫描存活主机

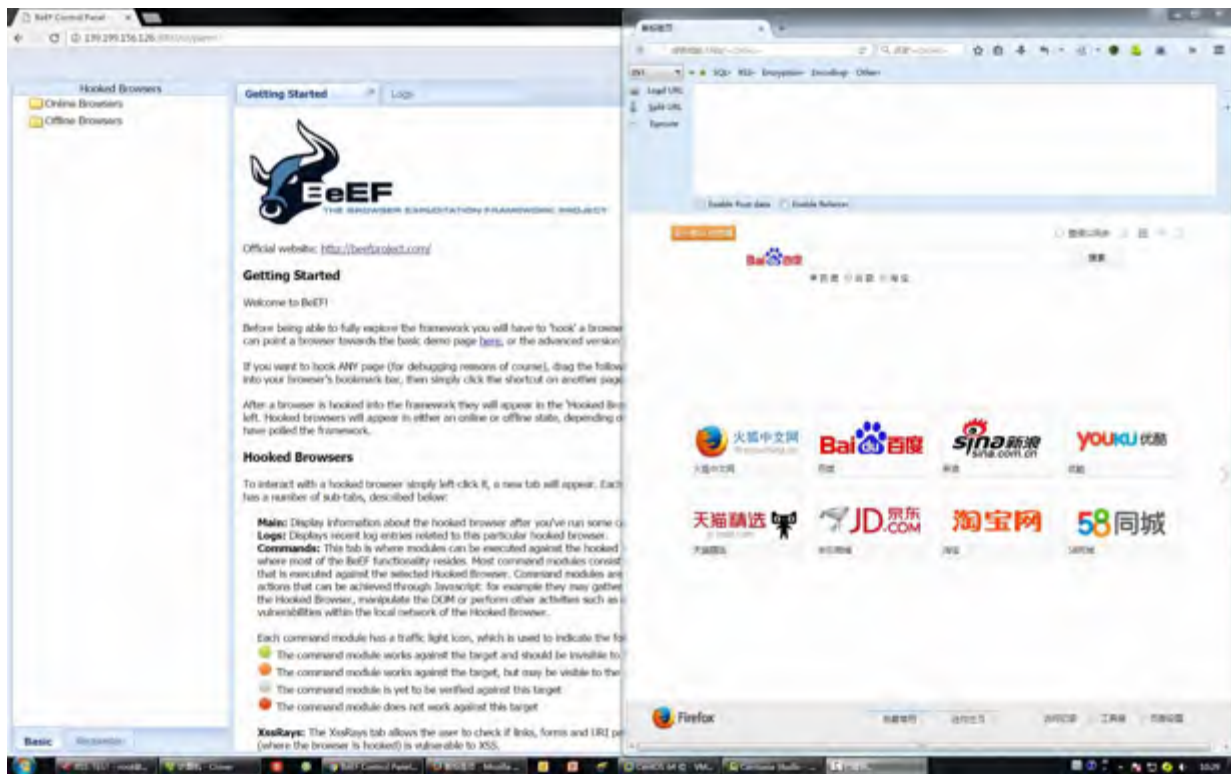
扫描主机端口

识别应用指纹

内网漏洞利用



XSS利用-攻击内网



XSS利用-钓鱼

The screenshot displays the Burp Suite interface on the left and a browser window on the right. The Burp Suite interface shows the 'Module Results History' table with the following data:

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

The 'Command results' pane shows the following log entries:

```
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 20:38:35 GMT+0800 (中国标准时间)
5 data: result=Username field changed to: test Tue Nov 15 2016 20:38:35 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 20:38:36 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 20:38:37 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)
```

The browser window on the right shows a 'Sign In' page for LastPass. The 'Email' field contains 'test' and the 'Password' field contains 'aaaaaa'. The 'Login' button is highlighted in red.

• 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...



No XSS!



正在等待扩展程序“Res_Discover”...

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

护心镜8大功能



技术实现

```
1  /*函数劫持*/
2  var _alert = alert;
3  alert = function(s){
4      console.log(Call
5          _alert(s);
6  }
7  /*对象/属性劫持*/
8  Object.defineProperty
9
10 Object.__define 1
11 Object.__define 2
3
4
5
6
7
8
9
10
11 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

```
hookjs.prototype.hook_createElement = function() {  
  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:"]  
];
```

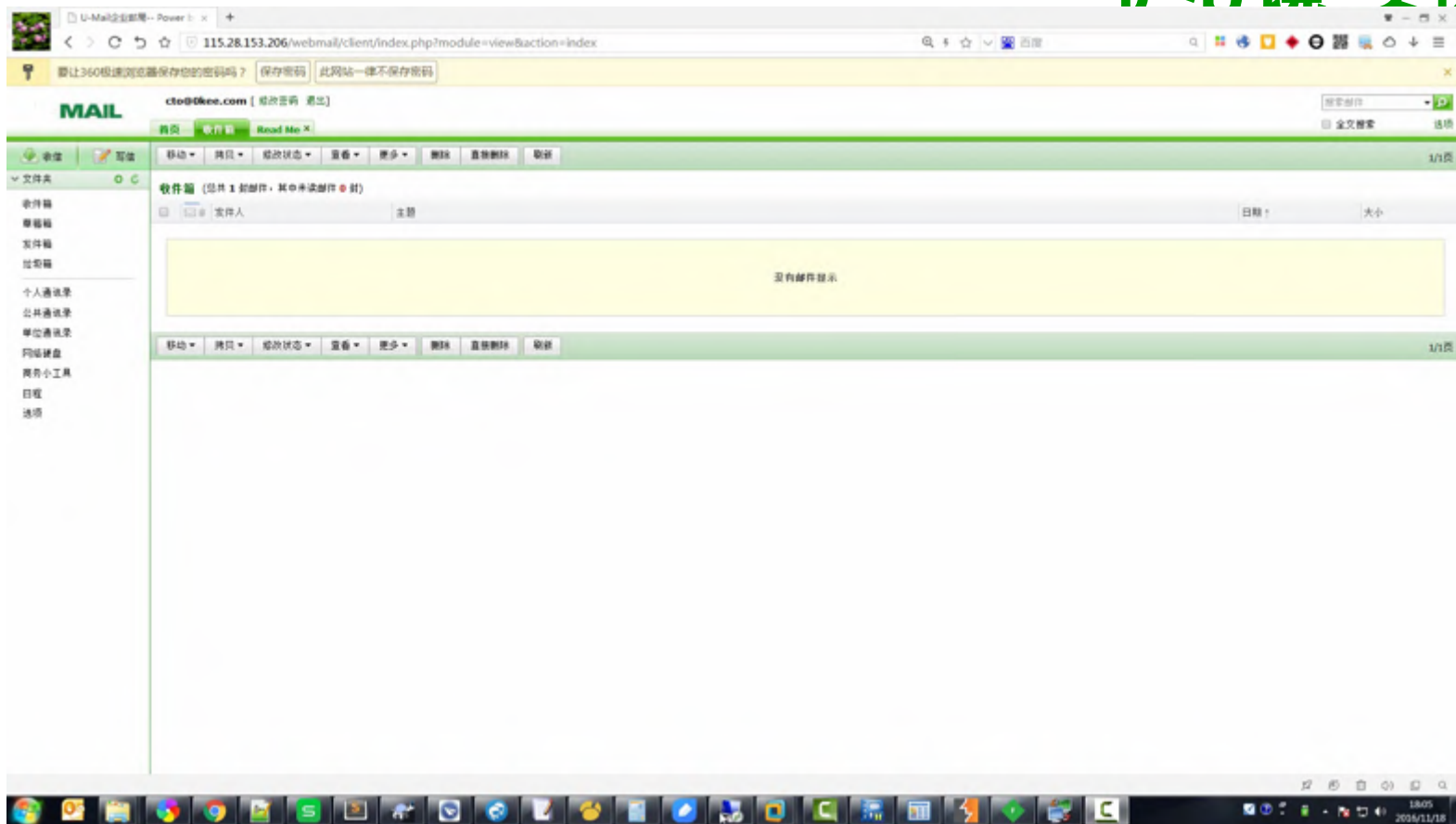
反卸载技术的对抗--保护自己

- 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



护心镜-平台



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

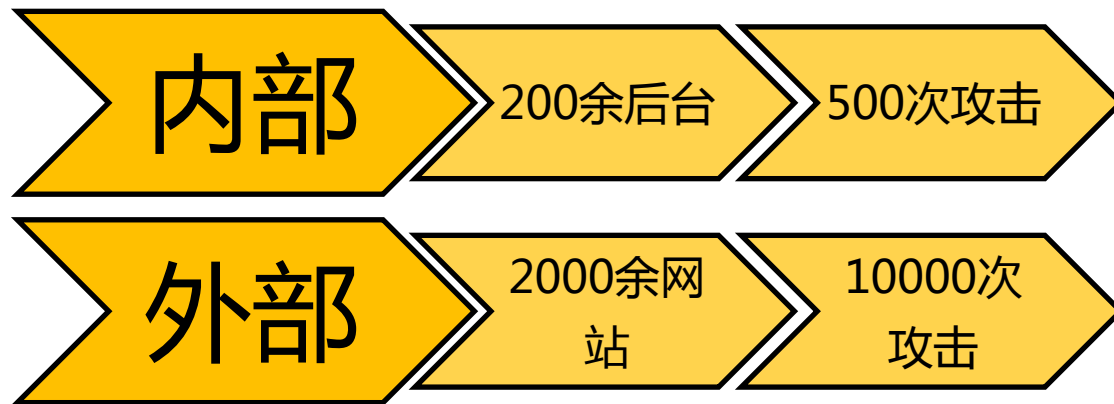
个人信息

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 16:10:21	0	选择	Cookie保护 XSS感知 反表单劫持 反钓鱼 weishell上告拦截 第三方资源拦截	xx	查看	删除 操作
xxxxx	2016-11-21 16:18:33	0	选择	Cookie保护 XSS感知 weishell上告拦截 第三方资源拦截		查看	删除 操作
Test	2016-11-16 16:02:09	20	选择	Cookie保护 XSS感知 反表单劫持 反钓鱼 weishell上告拦截 第三方资源拦截	cnzz.com baidu.com 360.cn	查看	删除 操作
用户画像系统	2016-11-04 12:26:40	5	放行	Cookie保护 XSS感知 反钓鱼 第三方资源拦截	qhoo.com qihoo.net qhimg.com 360.cn	查看	删除 操作
邮箱XSS演示	2016-10-20 10:55:15	12	选择	Cookie保护	mail.domain.com dkae.com qq.com	查看	删除 操作
btimg	2016-09-07 16:12:32	0	放行	Cookie保护 第三方资源拦截	btimg.cn 360.cn qhimg.com baidu.com cnzz.com	查看	删除 操作
360好药后台	2016-08-25 11:59:20	53100	放行	Cookie保护 XSS感知 weishell上告拦截 第三方资源拦截	360haoyao.com s.360img.cn 360img.cn 51mdq.com 360jk.com	查看	删除 操作
花糖OMG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 weishell上告拦截 第三方资源拦截	qhoo.net huajiao.com glogo.cn 360.cn qhimg.com	查看	删除 操作
铺网平台	2016-08-04 15:43:06	147	放行	Cookie保护 XSS感知 反表单劫持 反钓鱼 weishell上告拦截 第三方资源拦截	3001.net 360.cn qhimg.com	查看	删除 操作
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 weishell上告拦截 第三方资源拦截	360.cn mediav.com	查看	删除 操作
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 weishell上告拦截 第三方资源拦截	360.cn 360.com qhimg.com useso.com	查看	删除 操作
精微谱	2016-05-23 19:06:22	0	放行	Cookie保护 XSS感知 反表单劫持 反钓鱼 第三方资源拦截	qiku.com 360.cn qhimg.com 360shouji.com google-analytics.com	查看	删除 操作



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



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

