

Neglected UI-Redressing



OWASP 中国

The Open Web Application Security Project

About Me



- 谢雄钦 ID: be_n
- Before 360
- Now 阿里巴巴
- web 安全、RIM 安全、html5 以及 web 框架

Agenda



OWASP 中国
The Open Web Application Security Project

- UI-Redressing介绍
- Clickjacking
- Dragjacking
- Cursorjacking
- UI-Redressing of HTML5
- Malicious use of UI-Redressing
- 防御对策

客户端攻击形式的演变



OWASP 中国
The Open Web Application Security Project

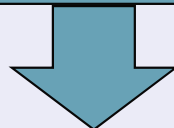
远程溢出, 代码执行



跨站脚本执行(XSS)



跨站伪造请求(CSRF)



HTML5、UI-Redressing、RMI

视觉欺骗



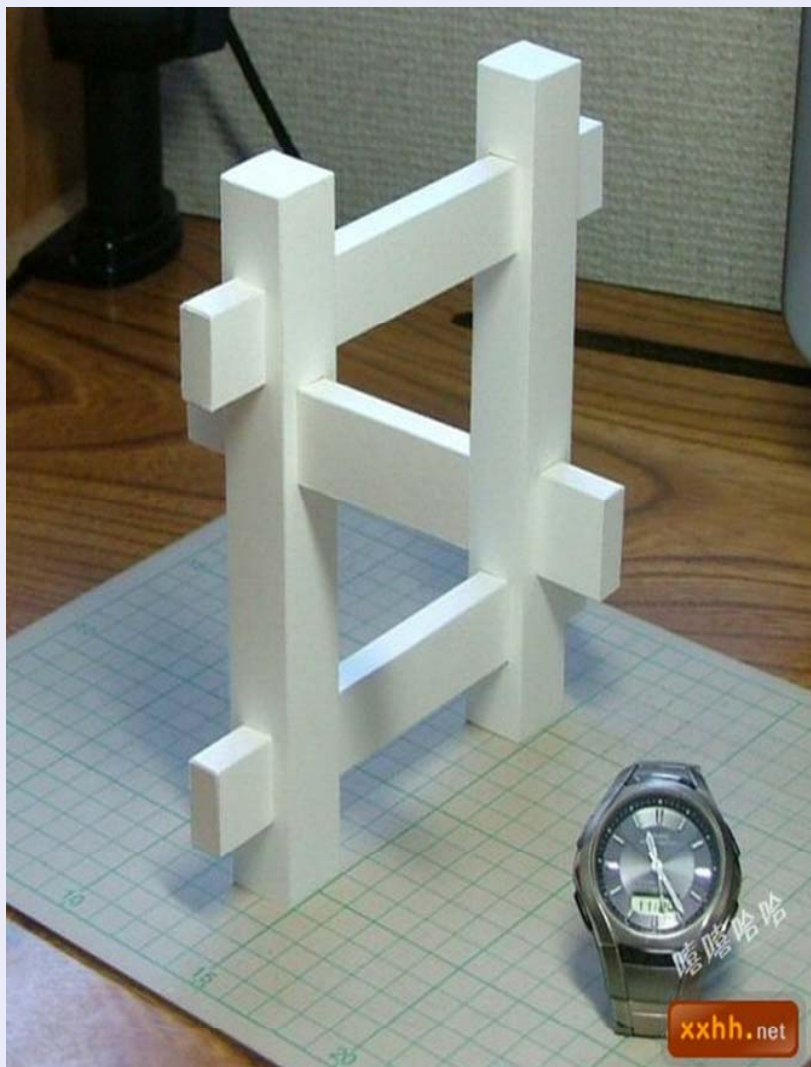
OWASP 中国
The Open Web Application Security Project



视觉欺骗



OWASP 中国
The Open Web Application Security Project





简单定义：界面伪装



1. Clickjacking(点击劫持)



OWASP 中国
The Open Web Application Security Project





- Position: absolute、fixed、relative
- opacity
- Z-index
- 定位: #-锚点

tips:

一种绕过同源策略检测iframe中是否存在某个标签的方法



<http://mall.aliapp.com/follow.html>

<http://mall.aliapp.com/clickjacking2.html>



OWASP 中国

The Open Web Application Security Project

腾讯微博clickjacking dem x

clickjacking2.html

内网系统-...



Full Disclosure Ma...



Attack and Defens...



平台架构 - 首页



Taobao VipViewer...



技术

腾讯微博 Beta

首页

微频道

找人

微群

应用

实验室



我收听的人

我的听众

我推荐的人

特别收听

clickjacking attack

筛选:

全部

互听

认证

排序:

按收听时间

显示:

详细

听众153人



明月心

2194



开始游戏

名单

更多

6

Wordpress clickjacking to shell



OWASP 中国
The Open Web Application Security Project

WordPress Install Plugin Webpage

http://wordpress/wp-admin/plugin-install.php?tab=plugin-information&plugin=wp-gallery-remote&T

BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SE SEORG.org Music

Description Installation Screenshots Changelog Faq Other Notes

Description

Warning: This plugin has **not been tested** with your current version of WordPress.

WP-Gallery-Remote includes albums and images from any Gallery installation using Gallery's Gallery Remote Protocol. Images are display as thumbnails in you posts and pages. Thereby you can choose between a plain output of the thumbnails and a CSS and Javascript based carousel mode. Have a look at the screenshots to see how that looks like. If the [Lightbox Plugin](#) is available and activated, clicking on a thumbnail opens the respective image using the lightbox effect. If the plugin is not available or activated, the image is shown in a new browser window.

Features

- displays images and albums of any Gallery installation which has enabled the Gallery-Remote-Protocol
- support for multiple wpgr tags in one post/page (v1.1)
- support for multiple Gallery installations (v1.2)
- two output types: plain and carousel (v1.2)
- Lightbox integration
- supports caching of fetched album and image meta data (can be enabled/disabled globally and per post/page)
- include/exclude filter to only show some images from an album

Install Now

FYI

Version: 1.5.1

Author: [Christian Bartels](#)

Last Updated: 1012 days ago

Requires WordPress Version: 2.5 or higher

Compatible up to: 2.6

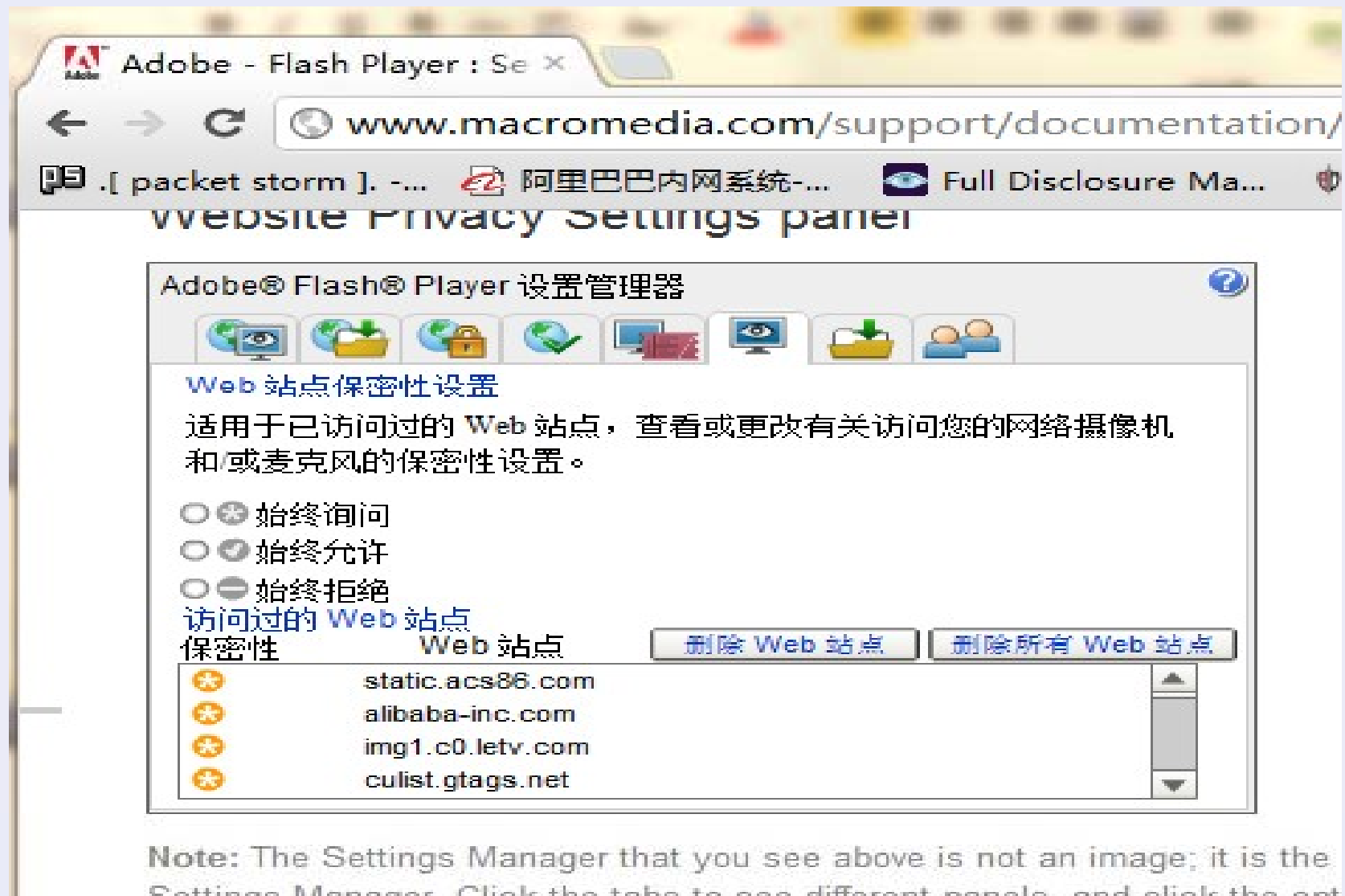
Downloaded: 12,338 times

[WordPress.org Plugin Page »](#)

[Plugin Homepage »](#)

Average Rating

★★★★☆
(based on 6 ratings)





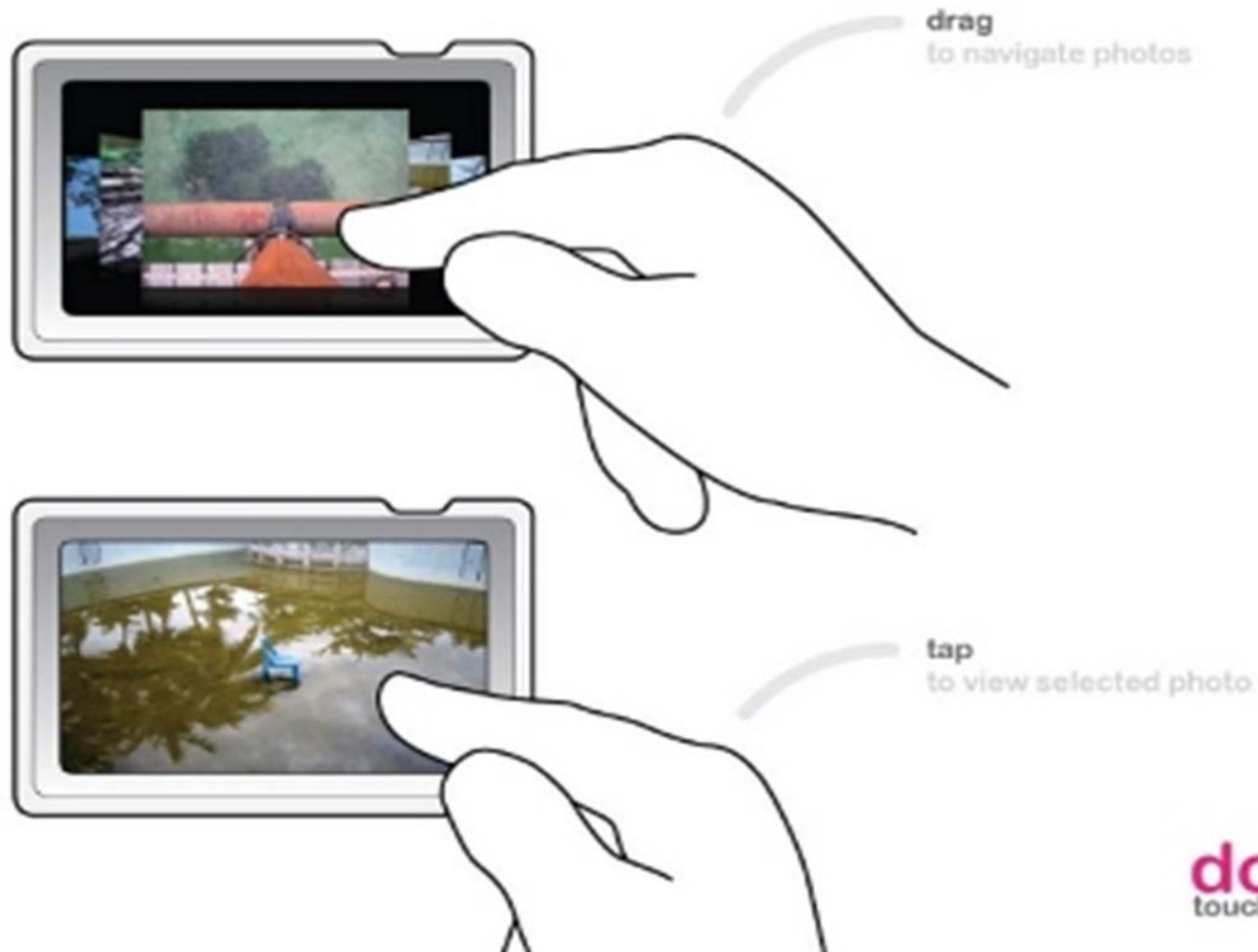
利用条件:

1. 允许接收GET方式放松过来的表单提交
2. 表单的action为当前的URL

2. Drag&Drop jacking



OWASP 中国
The Open Web Application Security Project





可见即可拖

浏览器中可以拖放对象一直在不断的增加, 而且允许页面上任何控件成为放置目标, 随着HTML5的发展, 支持拖放操作的API函数也会相应增多而且功能强大

HTML 5中的拖放事件

拖动时 依次触发:	Dragstart
	Drag
	Dragend
放置时 依次触发:	Dragenter
	Dragover
	Dragleave 或 Drop



跨域操作

拖放不受同源策略限制，用户可以把一个域的内容拖放到另外一个不同的域，而这样的操作是“点击劫持”无法做到的。



如果能抽取网页中的内容，我们可以：

1. 页面中的所有URL（URL中也许包含敏感信息）
2. Hidden隐藏的内容
3. 一些重要的元素(csrf-token)



- 拖动到的目标区域要求：
需要开启designMode或者contentEditable模式
- 利用浏览器的一些特性：
Chrome和firefox的“view-source”协议头



鼠标劫持

<http://mall.aliapp.com/cursor-jacking1.html>

<http://mall.aliapp.com/cursor-jacking2.html>



OWASP 中国
The Open Web Application Security Project

- Html5 fullscreen

<http://mall.aliapp.com/flashfullscreen.html>

<http://mall.aliapp.com/fullscreen.html>



OWASP 中国
The Open Web Application Security Project

- Webkit x-webkit-speech

<http://mall.aliapp.com/webkitspeech.html>

can you bypass?

360 搜索⁺



OWASP 中国
The Open Web Application Security Project

- 广告联盟欺骗
- 钓鱼攻击
- 数据伪造
-



← → ↺ bangpai.taobao.com/group/thread/1163074-2674412

5月
15

淘宝漏洞曝光，卖家技术太牛了不得不佩服

点击生活 post in 电子商务 at 16:21 评论(0) 阅读(691)

大 | 中 |

价 格: **60.00** 元

物流运费: 快递:5.00元 EMS:5.00元 平邮:5.00元

30天售出: 0件

评 价: 暂无评价

宝贝类型: 全新 | 27次浏览

尺 码:

主要颜色:

购买数量: 件 (库存597件)

[立刻购买](#)

[加入购物车](#)

支付: 快捷支付 网银支付

服务:

举报中心

和我联系

动态评分 与同行比

描述相符:5.0	高于 100.00%
服务态度:5.0	高于 100.00%
发货速度:5.0	高于 100.00%

好评率:100.00% 宝贝数:340

创店时间:2011-02-24



[进入店铺](#)

[收藏店铺](#)



物流运费：北京 | 至 福建福州 - 卖

30天售出：580件

评价：暂无评价

宝贝类型：全新 | 249次浏览

NEW

我的应用 - 我的钱包 - 淘足迹 - 分享给好友 - 消息

Resources Network Sources Timeline

`<em class="J_TDealCount">0`

58

14 × 16 pixels



业 找有银行下，如何支付 找有银行下，如何支付 支付保障，父

宝贝详情

评价详情(20)

成交记录 (580件)

主图来源: 自主实拍图

品牌: Lee

裤长: 长裤

腰型: 中腰

适合季节: 通用型

价格区间: 501-1000元

5. Clickjacking protection



OWASP 中国
The Open Web Application Security Project

- 38% if (top != self)
- 22.5% if (top.location != self.location)
- 13.5% if (top.location != location)
- 8% if (parent.frames.length > 0)
- 5.5% if (window != top)
- 5.5% if (window.top !== window.self)
- 2% if (window.self != window.top)
- 2% if (parent && parent != window)
- 2% if (parent && parent.frames && parent.frames.length>0)
- 2%
if((self.parent&&!(self.parent===self))&&(self.parent.frames.length!=0))

最常见：

```
if (top.location != location)
top.location = self.location ;
```



1. 二次frame（不能针对 `top.location`，只能针对 `parent.location`）
2. 利用 `onbeforeunload` 事件
3. xss（ie的xss filter，chrome的xss auditor）
4. 构造referer绕过js referer检查
5. `iframe security`属性（仅IE支持）
6. `iframe sandbox`属性（HTML5）
7. 浏览器designmode

The Best Javascript framebusting



OWASP 中国
The Open Web Application Security Project

```
<style>
html {display:none;}
</style>
<script>
if(self==top){
    document.documentElement.style.display='block
';
}else{
    top.location=self.location;
}
</script>
```

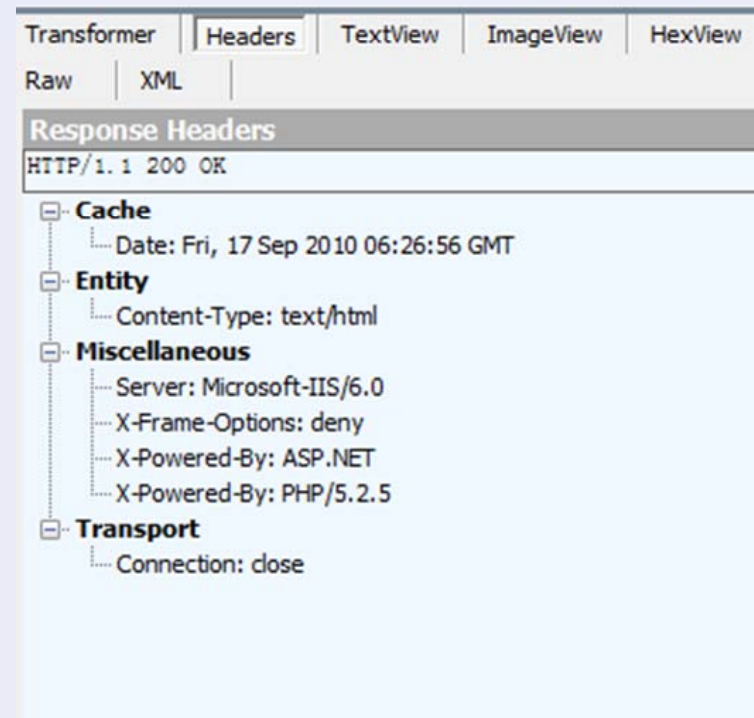


DENY

这个页面不能被任何
IFRAME包含。

SAMEORIGIN

这个页面只能被“同源
页面”IFRAME 包含。



支持X-Frame-Options的浏览器



OWASP 中国
The Open Web Application Security Project

-  IE8+
-  Opera 10+
-  Safari 4+
-  Chrome 5.0+
-  Firefox 3.6.9+

X-Frame-Options_test



此内容无法在框架中显示

X-Frame-Options_test



OWASP 中国
The Open Web Application Security Project



Thank you !