Neglected UI-Redressing

OWASP 中国

The Open Web Application Security Project

About Me

OWASP 中国
The Open Web Application Security Project

- 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

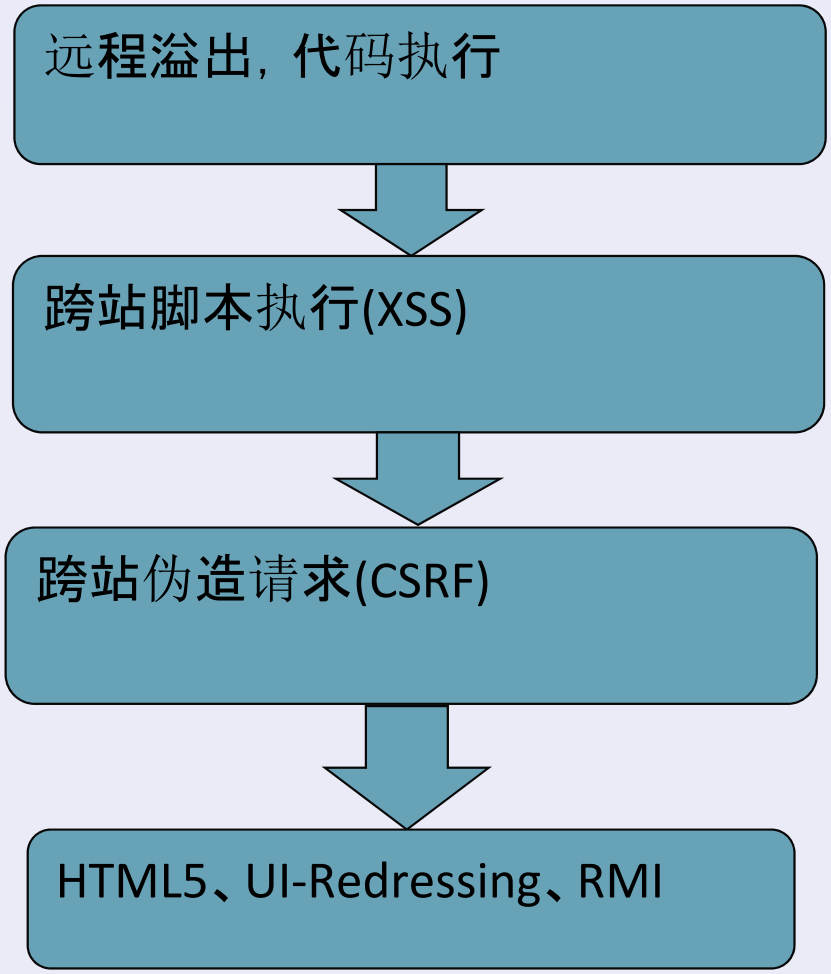
Agenda

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

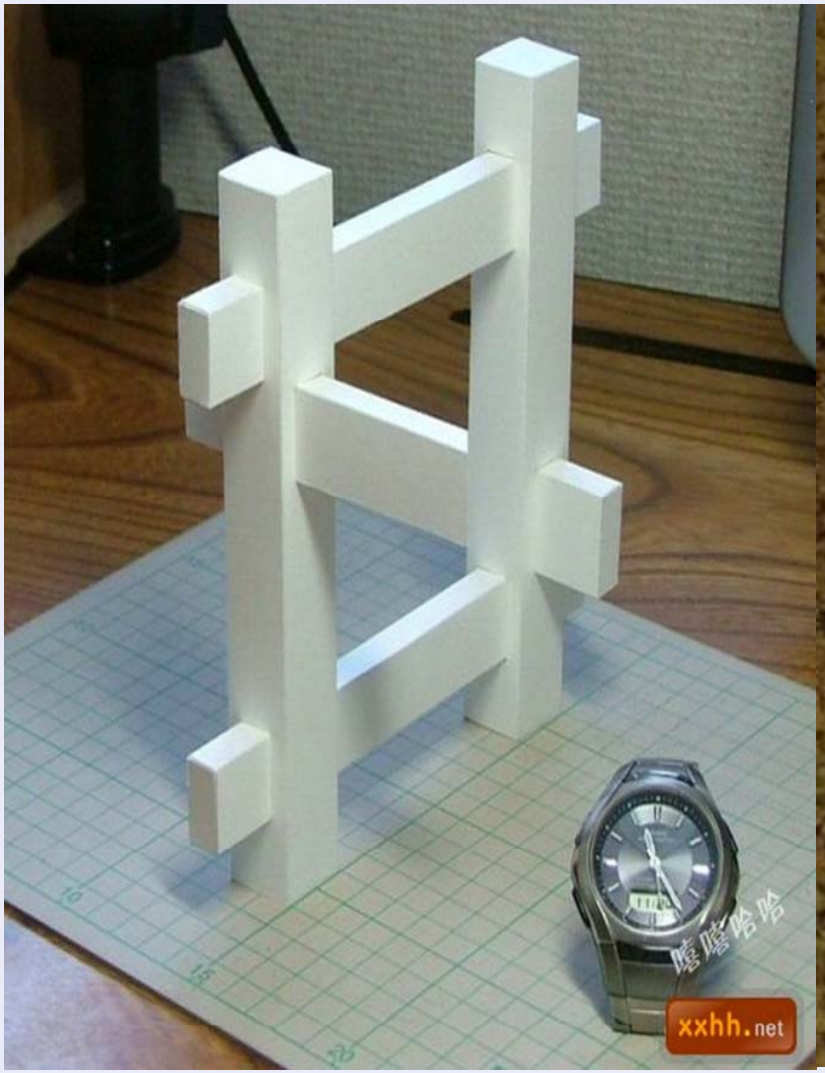
客户端攻击形式的演变

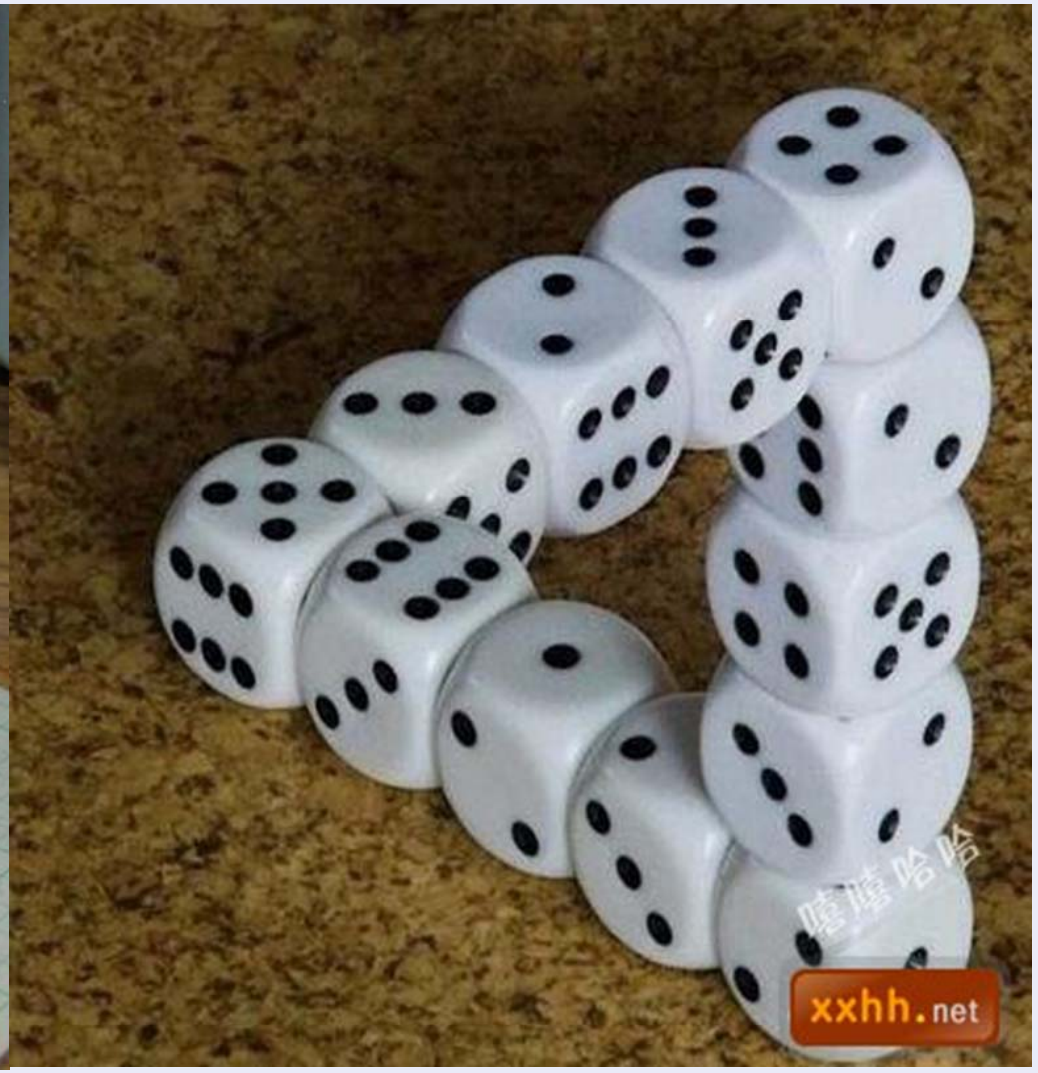
OWASP 中国
The Open Web Application Security Project



视觉欺骗

视觉欺骗





简单定义：界面伪装

1. Clickjacking(点击劫持)

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

tips：

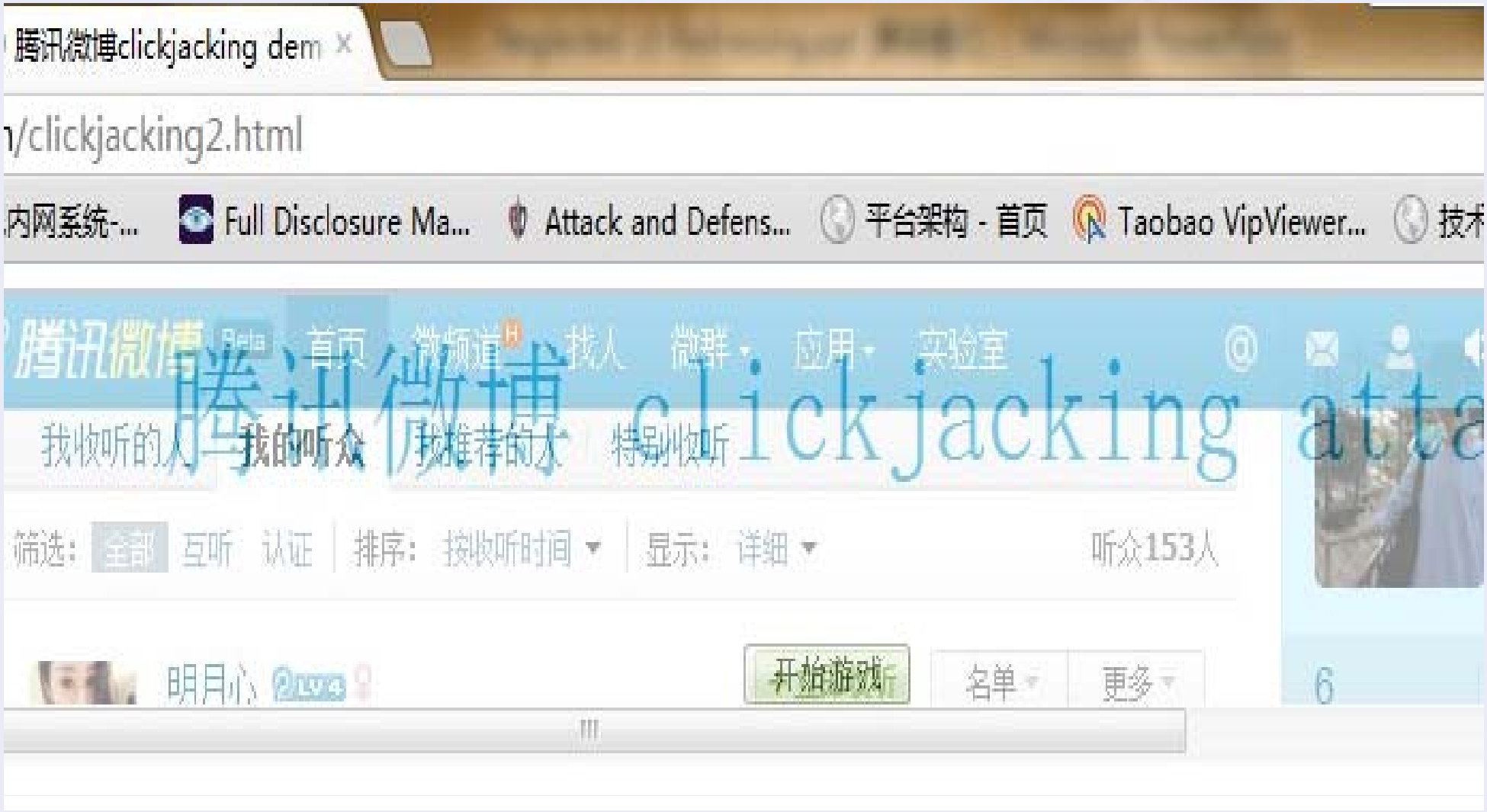
一种绕过同源策略检测iframe中是否存在某个标签的方法

Demo

OWASP 中国
The Open Web Application Security Project

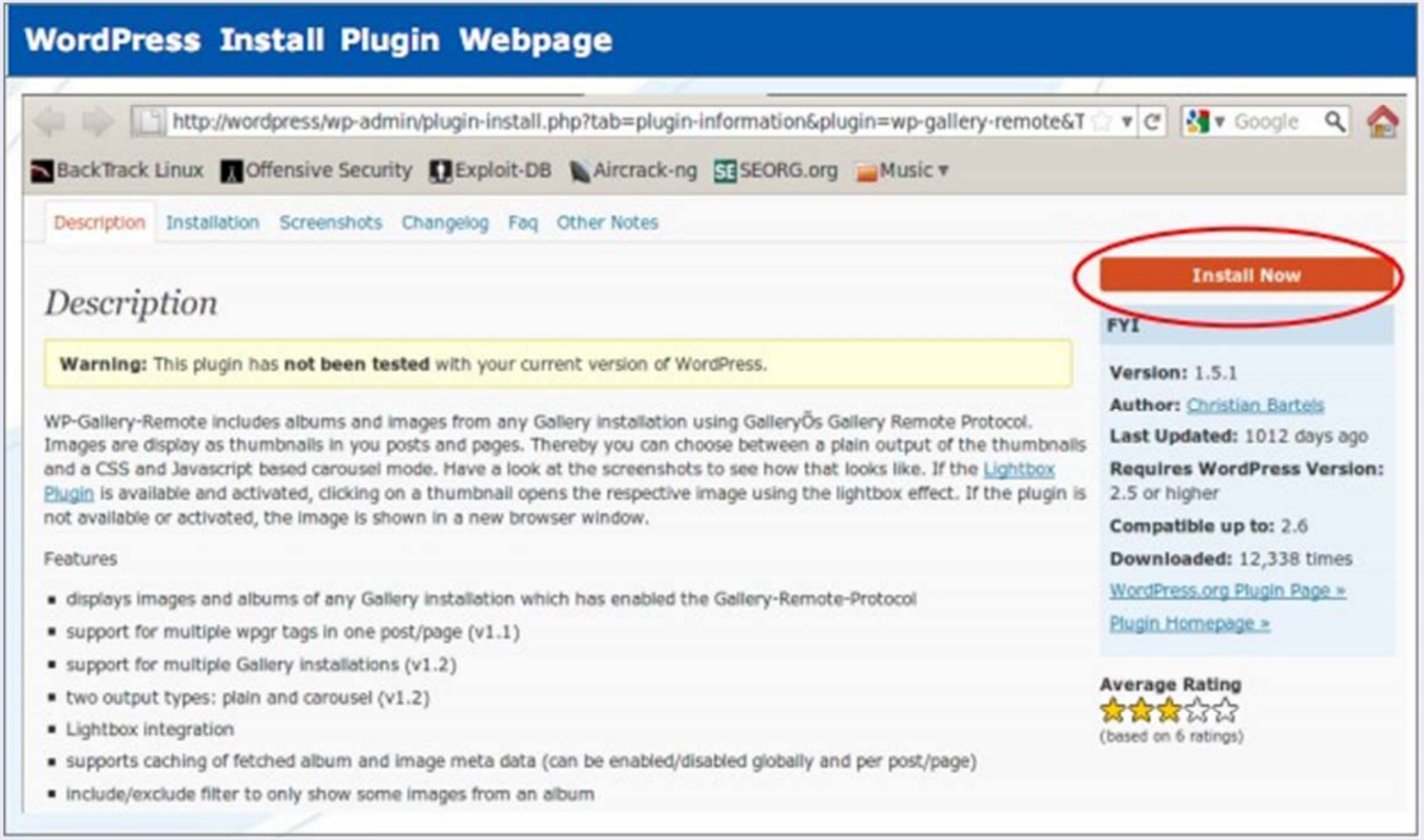
http://mall.aliapp.com/follow.html

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


腾讯微博clickjacking dem
/clickjacking2.html
内网系统-...
Full Disclosure Ma...
Attack and Defens...
平台架构 - 首页
Taobao VipViewer...
腾讯微博
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
腾讯微博 clickjacking atta
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
开始游戏
名单
更多
6

Wordpress clickjacking to shell

OWASP 中国
The Open Web Application Security Project



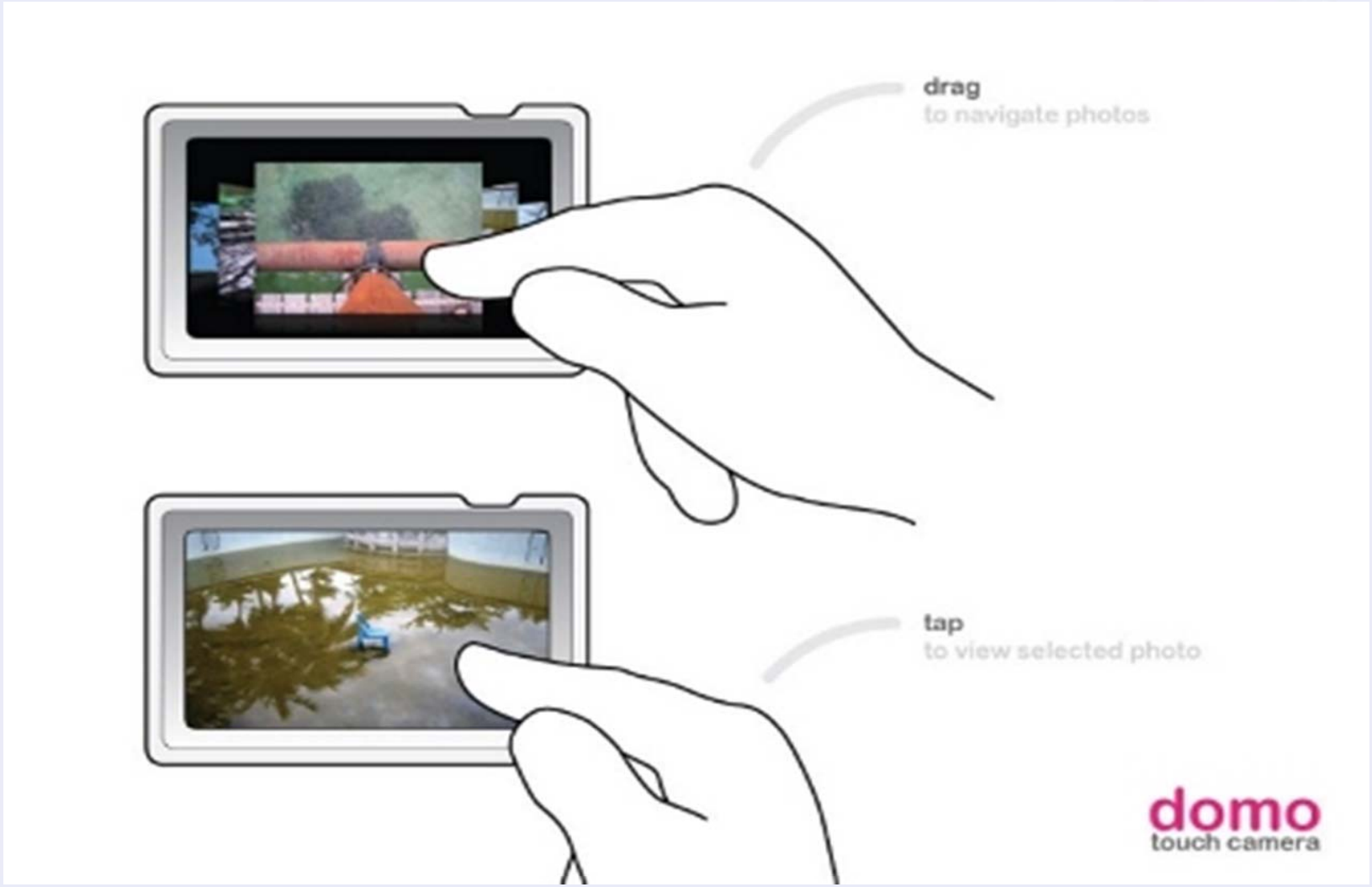
webcam-clickjacking

OWASP 中国
The Open Web Application Security Project

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

OWASP 中国
The Open Web Application Security Project

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

Cursorjacking

OWASP 中国
The Open Web Application Security Project

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

- Webkit x-webkit-speech

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

can you bypass?

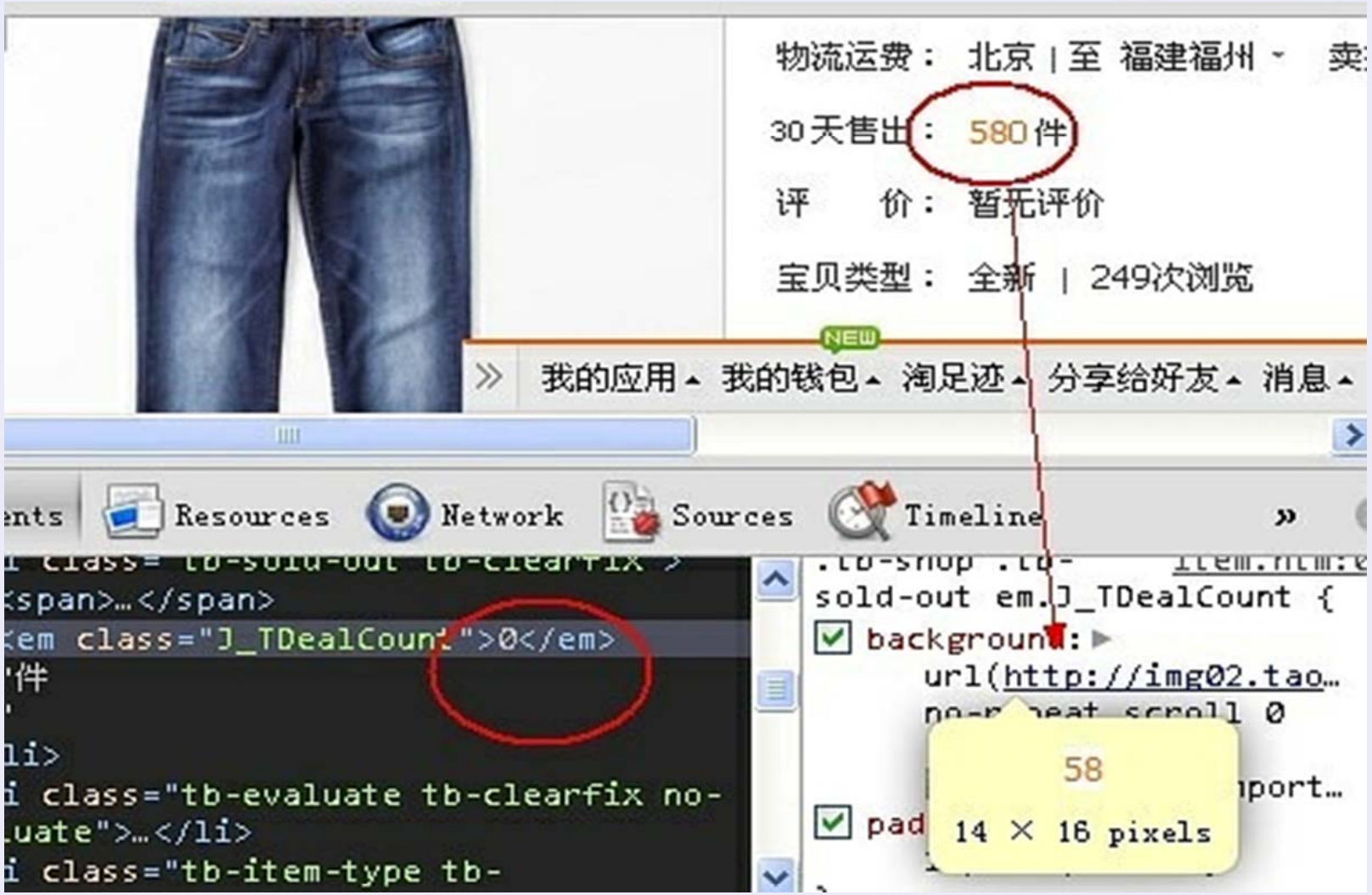
Malicious use of UI-Redressing

OWASP 中国
The Open Web Application Security Project

- 广告联盟欺骗
- 钓鱼攻击
- 数据伪造
- ……

OWASP 中国
The Open Web Application Security Project

OWASP 中国
The Open Web Application Security Project




宝贝详情
评价详情(0)
成交记录 (0件)
主图来源: 自主实拍图
品牌: Lee
裤长: 长裤
腰型: 中腰

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 ;
```

Busting Frame busting

OWASP 中国
The Open Web Application Security Project

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，chorme的xss audior）
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

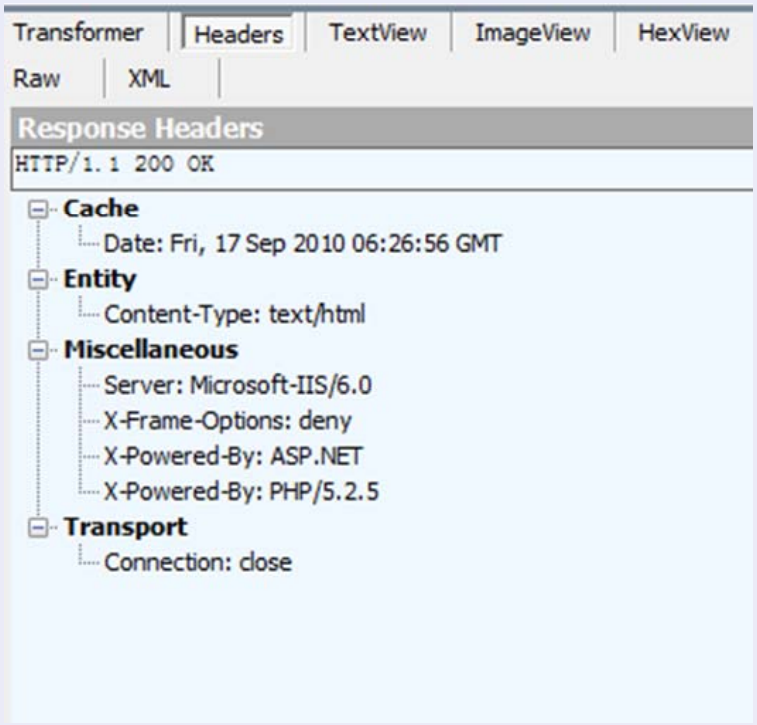
```
<style>
html {display:none;}
</style>
<script>
if(self==top){
        document.documentElement.style.display='block
';
}else{
        top.location=self.location;
}
</script>
```

X-FRAME-OPTIONS

OWASP 中国
The Open Web Application Security Project

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+

Thank you！