

Web安全技术

Web Security

2.3 ClickJacking

刘奇旭

liuqixu@iie.ac.cn

中科院信工所 第六研究室



中国科学院大学
University of Chinese Academy of Sciences

一章一问

□ Clickjacking的表现形式及防御思路

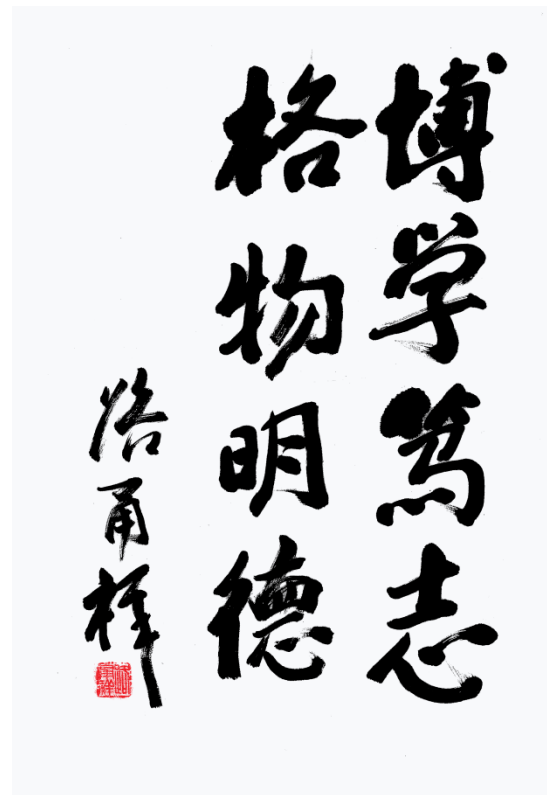


本章大纲

□ 概述

□ 攻击类型

□ 防御方法



CLICKJACKING

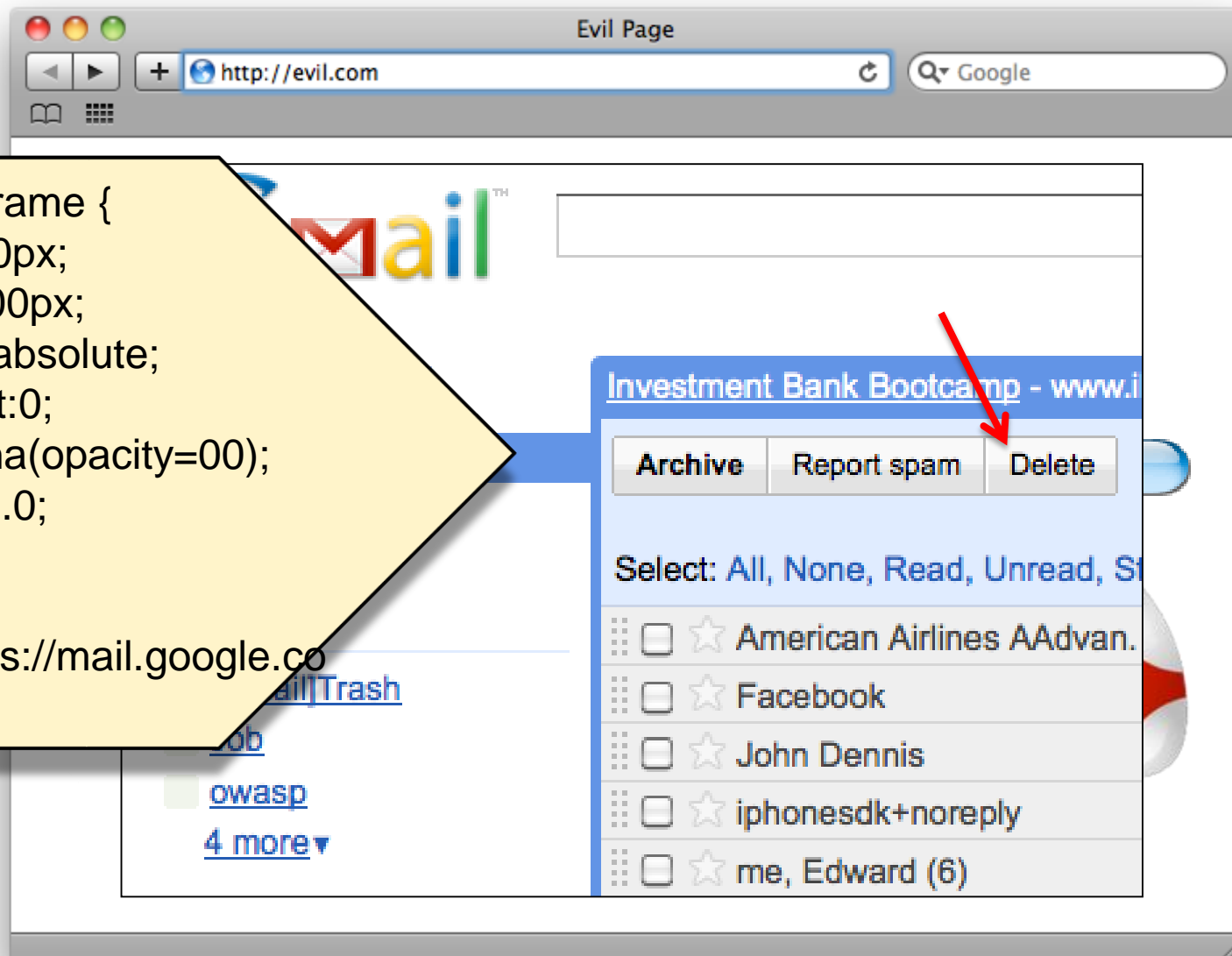
- ❑ Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.
- ❑ Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.



CLICKJACKING



CLICKJACKING



CLICKJACKING



CLICKJACKING

- ❑ ClickJacking称为**点击劫持攻击**，又称为**UI-覆盖攻击**。2008年由互联网安全专家罗伯特·汉森和耶利米·格劳斯曼首次提出。
- ❑ 点击劫持从根本上来说是对人类感知的攻击。在用户不知情的情况下，利用与用户产生的交互界面，诱使用户触发一些动作，达到攻击者想要实现的其它目的。



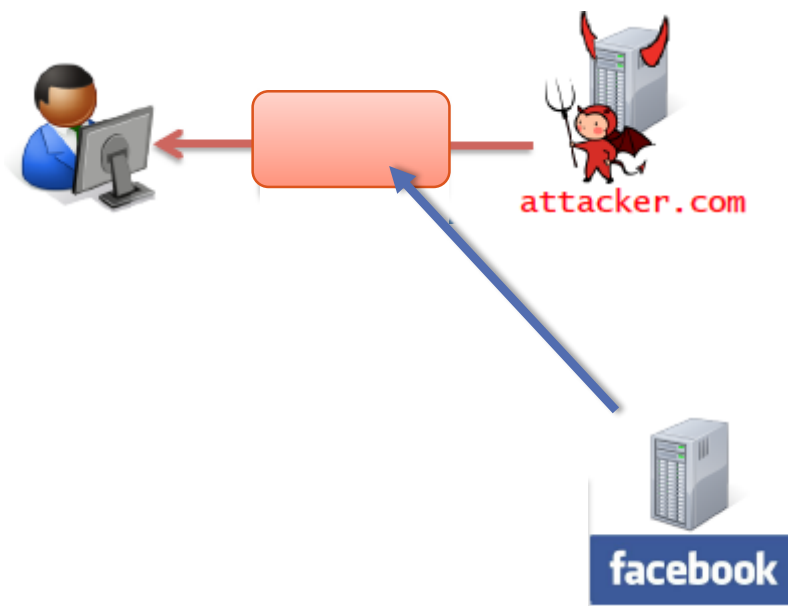
CLICKJACKING危害

- ❑ ClickJacking是一种恶意攻击技术，用于跟踪网络用户，获取其私密信息，对IE、Safari、Firefox、Opera、Adobe Flash等平台构成威胁。
- ❑ Iframe一个银行转账页面，可窃取银行账户口令，造成财产损失。
- ❑ 可能莫名其妙发出了不该发的消息，粉了不认识的人，点了一个带有黑产性质的广告，恶意刷流量。



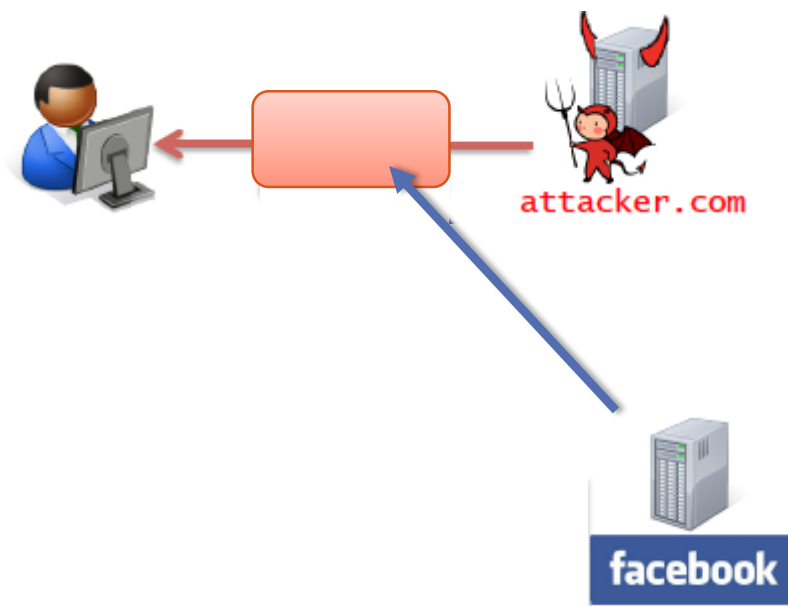
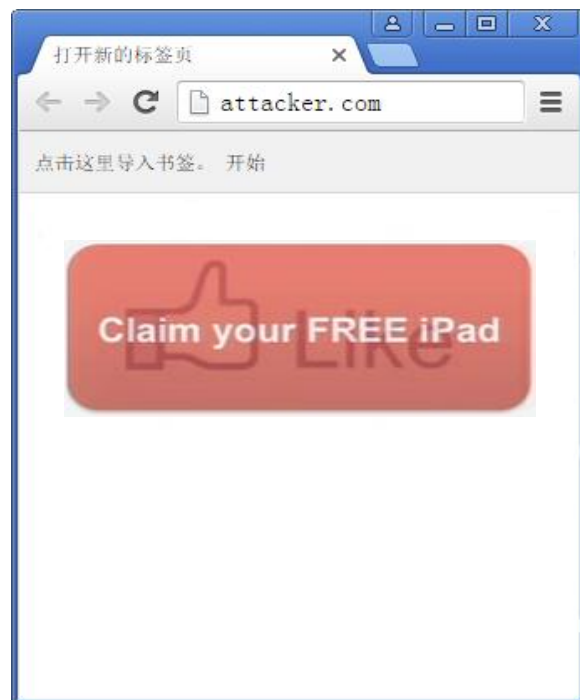
攻击原理解析

- ClickJacking是一种视觉欺骗手段，利用HTML中<iframe>标签等手段嵌套一个透明不可见的页面，让用户在不知情的情况下，点击攻击者想要欺骗用户点击的另一个置于原网页上面的透明页面。



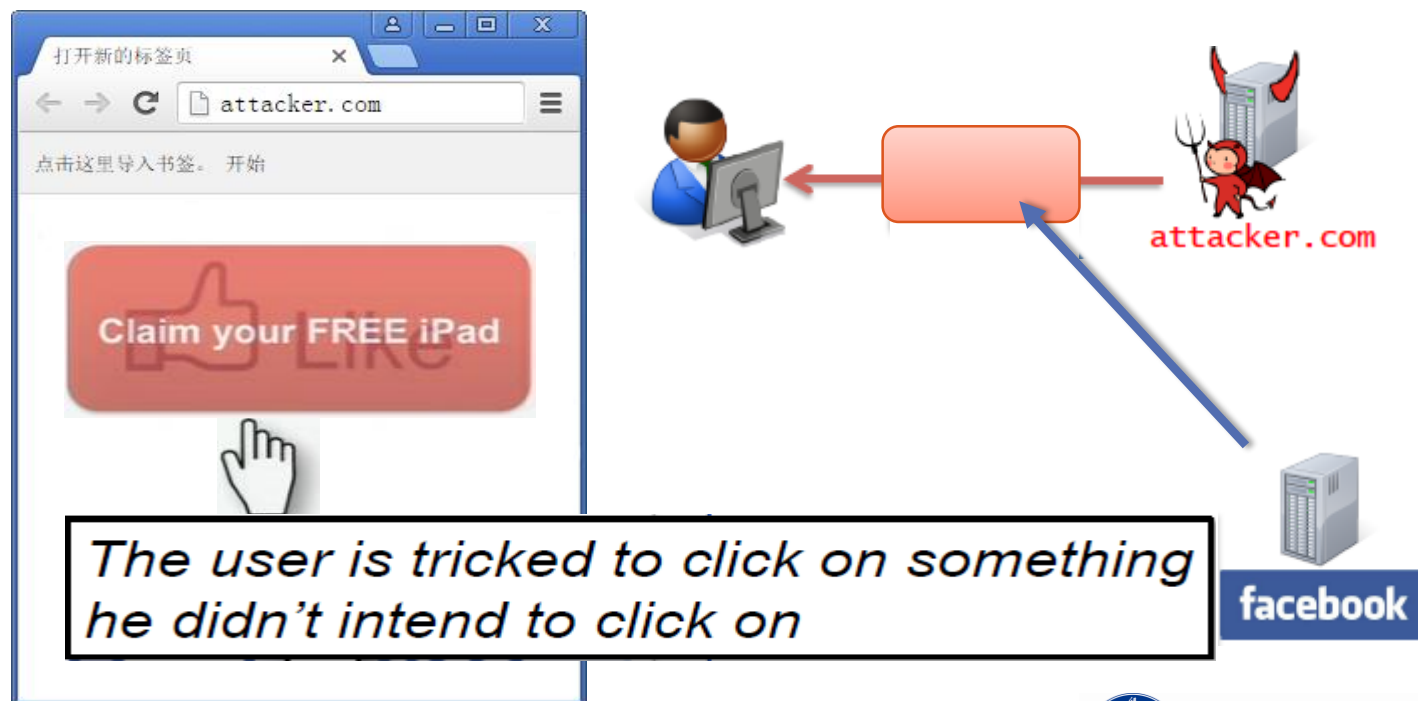
攻击原理解析

- ClickJacking是一种视觉欺骗手段，利用HTML中<iframe>标签等手段嵌套一个透明不可见的页面，让用户在不知情的情况下，点击攻击者想要欺骗用户点击的另一个置于原网页上面的透明页面。



攻击原理解析

- ClickJacking是一种视觉欺骗手段，利用HTML中<iframe>标签等手段嵌套一个透明不可见的页面，让用户在不知情的情况下，点击攻击者想要欺骗用户点击的另一个置于原网页上面的透明页面。



CLICKJACKING概述

- ClickJacking利用视觉欺骗手段，诱导用户点击被攻击者嵌入的恶意页面。
- 用户在浏览web页面时中了ClickJacking后，可能带来财产损失，账号窃取，隐私泄露，恶意吸费等。
- 实施ClickJacking，主要利用浏览器或HTML的一些特性，如：
iframe**标签透明**，image**图片浮动**等，将恶意页面覆盖原来的页面，对用户发起攻击。

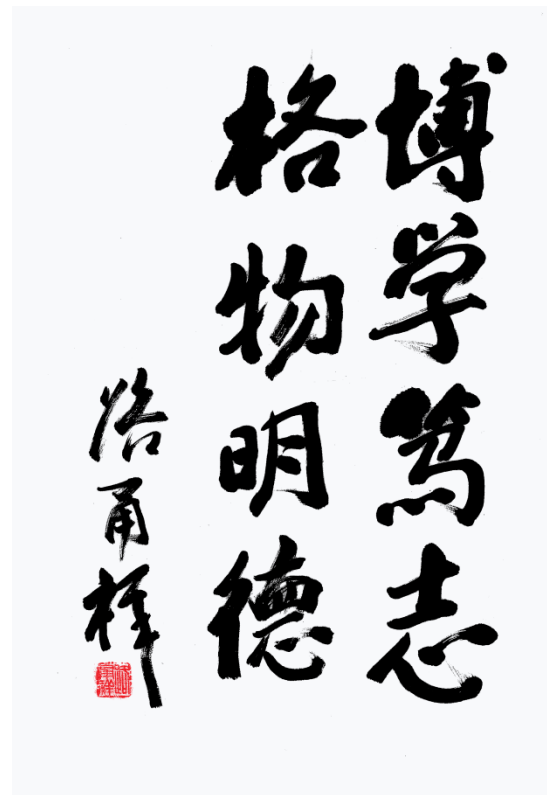


本章大纲

□ 概述

□ 攻击类型

□ 防御方法



图片覆盖劫持

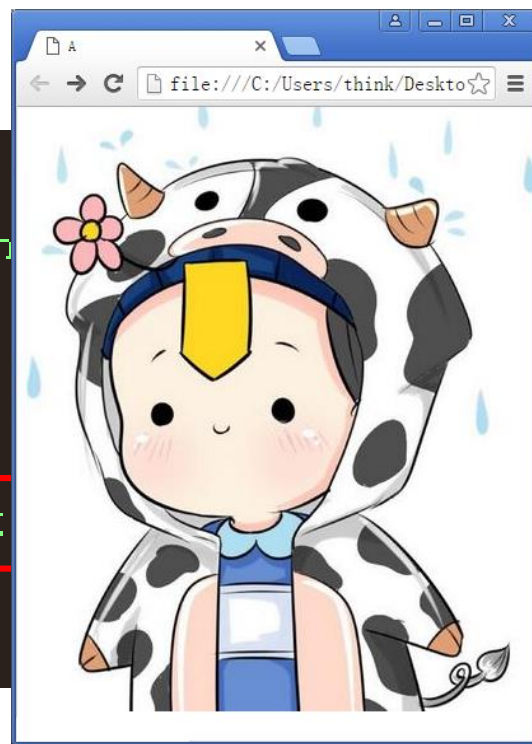
- ❑ 图片覆盖攻击（Cross Site Image Overlaying），攻击者使用一张或多张图片，利用图片的style或者能够控制的CSS，将图片覆盖在网页上，形成点击劫持。
- ❑ 当然图片本身所带的信息可能就带有欺骗的含义，这样不需要用户点击，也能达到欺骗的目的。
- ❑ 这种攻击很容易出现在网站本身的页面。



图片覆盖劫持

- 示例：在可以输入HTML内容的地方加上一张图片，该图片覆盖在指定的位置。

```
<html>
<head>
<meta http-equiv="content-type" content="text/html">
<title>A</title>
</head>
<body>
  <a href="B.html">
    This is B.
    
</body>
</html>
```

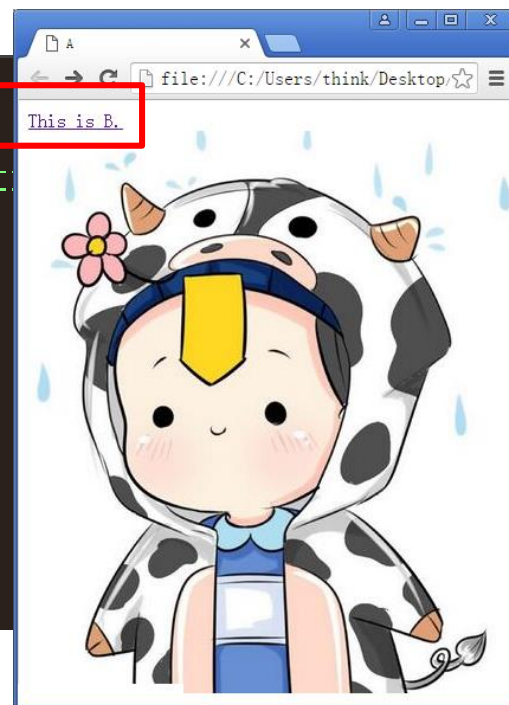


图片覆盖劫持防御

- 在防御图片覆盖攻击时，需要检查用户提交的HTML代码中，img标签的style属性是否可能导致浮动。

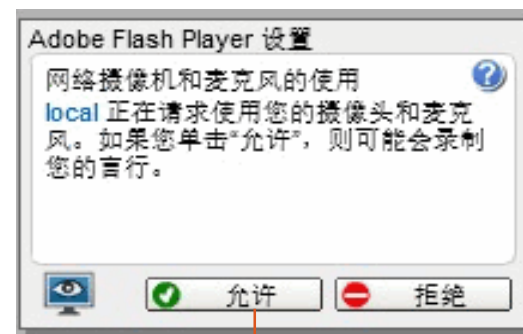
```
<html>
<head>
<meta http-equiv="content-type" content="text/html">
<title>A</title>
</head>
<body>
  <a href="B.html">
    This is B.
    
  </a>
</body>
</html>
```

禁用浮动



FLASH点击劫持

- 攻击者通过Flash构造点击劫持，在完成一系列复杂动作后，最终控制用户的摄像头。目前Adobe已修复此漏洞。



Real Cursor

Fake Cursor

<http://feross.org/webcam-spy/>

浏览器拖拽劫持

- ❑ 目前很多浏览器开始支持Drag&Drop的API。拖拽使得用户体验佳，操作方便。浏览器支持的拖拽对象有超链接、文字、窗口等。
- ❑ 浏览器拖拽不受同源策略限制。
- ❑ 拖拽劫持诱使用户从隐藏的iframe中拖拽出攻击者希望得到的数据，然后放到攻击者能够控制的另外一个页面中，从而窃取数据。
- ❑ 在JavaScript的支持下，拖拽劫持攻击更加隐蔽，能够突破传统ClickJacking的一些局限，造成更大的破坏。



浏览器拖拽劫持

- ❑ 国内的安全研究者xisigr 曾构造了一个针对窃取Gmail数据的拖拽劫持的网页小游戏，在小球和海豹的顶部都有隐藏的iframe。
- ❑ 当用户拖拽小球时，实际上选中了隐藏的iframe里的数据；在放下小球时，把数据也放在了隐藏的textarea中，从而完成一次数据窃取的过程。

隐藏的
IFrame

Gmail数据



触屏劫持

- ❑ 2010年9月，智能手机上的“触屏劫持”攻击被斯坦福的安全研究者公布，将其称为TapJacking。
- ❑ 以苹果公司的iPhone为代表，智能手机为人们提供了更先进的操控方式：触屏。从手机OS的角度来看，触屏实际上是一个事件，手机OS捕捉这些事件，并执行相应的动作，如：touchstart, touchend, touchmove, touchcancel。
- ❑ 手机屏幕范围有限，一些浏览器为了节约屏幕空间，甚至隐藏浏览器地址栏，导致手机上的视觉欺骗更加容易实施。



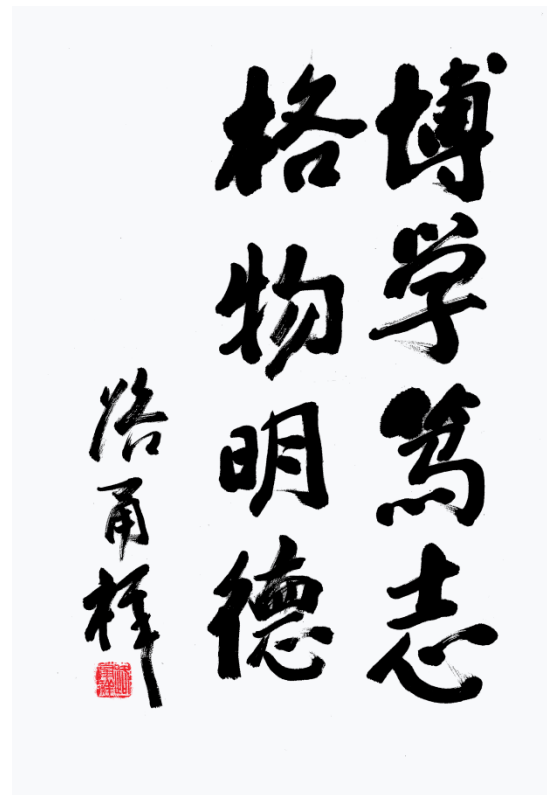
触屏劫持

- ❑ 智能手机用户以为自己在登录某个账号，实际上却按到了一个隐藏页面的按钮上，用户名和密码信息就这样被悄悄窃取。



本章大纲

- 概述
- 攻击类型
- 防御方法



X-FRAME-OPTIONS

❑ X-FRAME-OPTIONS是微软提出的一个http头，用来防御利用iframe嵌套的点击劫持攻击。在IE8、Firefox3.6、Chrome4以上的版本均能很好的支持。

❑ X-FRAME-OPTIONS属性值

DENY // 拒绝任何域加载

SAMEORIGIN // 允许同源域加载到iframe或frame

ALLOW-FROM **URI** // 允许指定的Uri嵌入到iframe或frame



X-FRAME-OPTIONS

□ APACHE配置X-FRAME-OPTIONS

- 在站点配置文件httpd.conf中添加如下配置，限制只有站点内的页面才可以嵌入iframe。

Header always append X-Frame-Options SAMEORIGIN

- 如果同一apache服务器上有多多个站点，只想针对一个站点进行配置，可以修改.htaccess文件，添加如下内容：

Header append X-FRAME-OPTIONS "SAMEORIGIN"



X-FRAME-OPTIONS

□ NGINX 配置X-FRAME-OPTIONS

□ 到 nginx/conf文件夹下，修改nginx.conf，添加如下内容并重启：

`add_header X-Frame-Options "SAMEORIGIN";`

```
server {  
    listen      80;  
    server_name localhost;  
    server_tokens off;  
    add_header X-Frame-Options "SAMEORIGIN";  
}
```



X-FRAME-OPTIONS

□ IIS配置X-FRAME-OPTIONS

□ 在web站点的web.config中配置如下：

```
<add name="X-Frame-Options" value="SAMEORIGIN" />
```

```
<system.webServer>  
...  
<httpProtocol>  
  <customHeaders>  
    <add name="X-Frame-Options" value="SAMEORIGIN" />  
  </customHeaders>  
</httpProtocol>  
...  
</system.webServer>
```



FRAME BUSTING

❑ 针对传统的点击劫持，一般是通过禁止跨域的iframe来防范；通常可以写一段**JavaScript**代码，以禁止iframe的嵌套。这种方法叫做Frame Busting。

❑ 例如下列代码：

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



FRAME BUSTING

□ 常见的Frame Busting有以下方式:

```
if (top !== self)
if (top.location !== self.location)
if (top.location !== location)
if (parent.frames.length > 0)
if (window !== top)
if (window.top !== window.self)
if (window.self !== window.top)
if (parent && parent !== window)
if (parent && parent.frames && parent.frames.length>0)
if((self.parent&&!(self.parent===self))&&(self.parent.frames.length!=0))
top.location = self.location
top.location.href = document.location.href
top.location.href = self.location.href
top.location.replace(self.location)
top.location.href = window.location.href
```



FRAME BUSTING (续)

□ 常见的Frame Busting有以下方式:

```
top.location.href = window.location.href
top.location.href = "URL"
document.write('')
top.location = location
top.location.replace(document.location)
top.location.replace('URL')
top.location.href = document.location
top.location.replace(window.location.href)
top.location.href = location.href
self.parent.location = document.location
parent.location.href = self.document.location
top.location.href = self.location
top.location = window.location
top.location.replace(window.location.pathname)
windowwindow.top.location = window.self.location
setTimeout(function(){document.body.innerHTML='';},1);
```





安装浏览器插件


- ❑ NoScript是一个免费和开源的，为Mozilla Firefox和Mozilla Application Suite网页浏览器（诸如Flock、SeaMonkey等）所开发的扩展（Add-ons）。
- ❑ NoScript允许JavaScript, Java, Flash, Sliverlight以及其它插件和脚本内容基于白名单被选择性的执行。
- ❑ NoScript在很大程度上能增强浏览器的安全性，对XSS, CSRF和Clickjacking可以起到防护作用。

选项 (Q)...


- ✓ 显示被阻止脚本的信息
- ✓ 在浏览器底部显示信息
- 脚本被阻止时提示声音

 全局允许 JavaScript (危险)


 *Temporarily allow all this page*


 不可信任

 允许 feedsky.com


 临时允许 feedsky.com

 禁止 googlesyndication.com

 允许 baidu.com

 临时允许 baidu.com

 允许 appinn.com

 临时允许 appinn.com

HTML5防御

- 在HTML 5中，专门为iframe定义了一个新的属性，叫做sandbox；使用sandbox这一个属性后，<iframe>标签加载的内容将被视为一个独立的“源”，其中的脚本将被禁止执行，表单被禁止提交，插件被禁止加载，指向其他浏览器对象的连接也会被禁止。



HTML5防御

语法

```
<iframe sandbox="value">
```

属性值

值	描述
""	应用以下所有的限制。
allow-same-origin	允许 <code>iframe</code> 内容被视为与包含文档有相同的来源。
allow-top-navigation	允许 <code>iframe</code> 内容从包含文档导航（加载）内容。
allow-forms	允许表单提交。
allow-scripts	允许脚本执行。



小结

- ❑ ClickJacking攻击形式包含图片覆盖劫持、Flash点击劫持、浏览器拖拽劫持、触屏劫持。
- ❑ X-FRAME-OPTIONS和Frame Busting是应对ClickJacking攻击的常用防御方式，在Apache、Nginx、IIS web 服务器上均可配置X-Frame-Options。
- ❑ HTML 5中加入了一些新的安全元素属性，如：sandbox，可以防止ClickJacking带来的恶意攻击。



延伸阅读

Clickjacking Revisited A Perceptual View of UI Security

*Devdatta Akhawe, Warren He, Zhiwei Li, Reza Moazzezi, Dawn Song
UC Berkeley*

USENIX
Security 2012

Clickjacking: Attacks and Defenses

Lin-Shung Huang
Carnegie Mellon University
linshung.huang@sv.cmu.edu

Alex Moshchuk
Microsoft Research
alexmos@microsoft.com

Helen J. Wang
Microsoft Research
helenw@microsoft.com

Stuart Schechter
Microsoft Research
stuart.schechter@microsoft.com

Collin Jackson
Carnegie Mellon University
collin.jackson@sv.cmu.edu

Busting Frame Busting: a Study of Clickjacking Vulnerabilities on Popular Sites

Gustav Rydstedt, Elie Bursztein, Dan Boneh
Stanford University
{rydstedt, elie, dabo}@stanford.edu

Collin Jackson
Carnegie Mellon University
collin.jackson@sv.cmu.edu

June 7, 2010

Clickjacking Defense Cheat Sheet

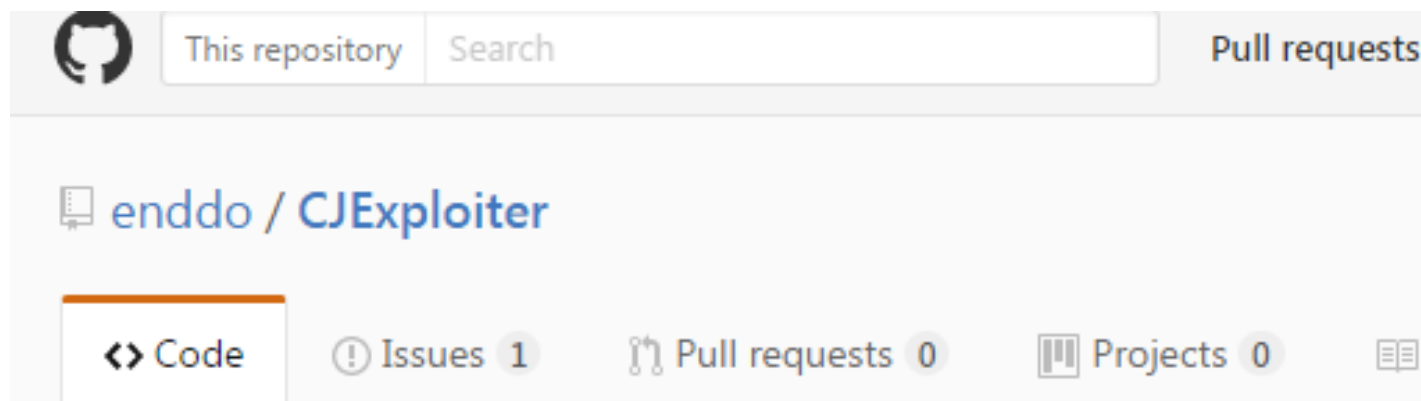


https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet



延伸阅读

□ <https://github.com/enddo/CJExploiter>



Drag and Drop ClickJacking exploit development assistance tool.

CJExploiter是一个支持拖放的点击劫持漏洞利用辅助工具。首先在本地用浏览器打开“index.html”，输入目标的URL并点击“View Site”。你可以自定义JS，最后点击“Exploit it”，你就能得到PoC了。



后续课程内容

- 第二部分：Web客户端安全
- 详细讲解XSS跨站、跨站点请求伪造、点击劫持等前端安全。
- 2.1 OWASP Top Ten
- 2.2 XSS与CSRF
- 2.3 ClickJacking
- 2.4 浏览器与扩展安全
- 2.5 案例分析





[2017秋]Web Security

扫一扫二维码，加入该群。

谢谢大家

刘奇旭

liuqixu@iie.ac.cn

中科院信工所 第六研究室



中国科学院大学
University of Chinese Academy of Sciences