第 5 章

IFrame 框架钓鱼攻击与防护

【本章重点】 熟悉 IFrame 攻击的定义及产生原理，了解钓鱼网站的传播途径和钓鱼方式。

【本章难点】 掌握 IFrame 框架钓鱼总体防护方法。

5.1 IFrame 框架钓鱼攻击背景与相关技术分析

5.1.1 IFrame 攻击的定义

所谓 IFrame 框架钓鱼攻击，是指在 HTML 代码中嵌入 IFrame 攻击，IFrame 是可用于在 HTML 页面中嵌入一些文件（如文档、视频等）的一项技术。对 IFrame 最简单的解释就是“IFrame 是一个可以在当前页面中显示其他页面内容的技术”。

5.1.2 IFrame 攻击产生的原理

Web 应用程序的安全始终是一个重要的议题，因为网站是恶意攻击者的第一目标。黑客利用网站传播他们的恶意软件、蠕虫、垃圾邮件及其他等。OWASP 概括了 Web 应用程序中最具危险的安全漏洞，且仍在不断积极地发现可能出现的新的弱点以及新的 Web 攻击手段。黑客总是在不断寻找新的方法欺骗用户，因此从渗透测试的角度看，我们需要看到每一个可能被用来入侵的漏洞和弱点。

IFrame 利用 HTML 支持这种功能应用，而进行的攻击。

IFrame 的安全威胁作为一个重要议题被讨论，因为 IFrame 的用法很常见，许多知名的社交网站都会使用到它。使用 IFrame 的方法如下：

例 1：

```
<iframesrc="http://www.2cto.com"></iframe>
```

该例说明在当前网页中显示其他站点。

例 2：

```
<iframesrc='http://www.2cto.com /' width='500' height='600' style=
'visibility: hidden;'></iframe>
```

IFrame 中定义了宽度和高度，但是由于框架的可见度被隐藏了，所以不能显示。由于这两个属性占用面积，所以一般情况下攻击者不使用它。

现在,它完全可以从用户的视线中隐藏了,但是 IFrame 仍然能够正常运行。而我们知道,在同一个浏览器内显示的内容是共享 Session 的,所以你在一个网站中已经认证的身份信息,在另一个钓鱼网站轻松就能获得。

5.1.3 钓鱼网站传播途径

互联网上活跃的钓鱼网站传播途径主要有 8 种:

(1) 通过 QQ、MSN、阿里旺旺等客户端聊天工具发送传播钓鱼网站链接。

(2) 在搜索引擎、中小网站投放广告,吸引用户单击钓鱼网站链接,此种手段被假医药网站、假机票网站常用。

(3) 通过 E-mail、论坛、博客、SNS 网站批量发布钓鱼网站链接。

(4) 通过微博、Twitter 中的短链接散布钓鱼网站链接。

(5) 通过仿冒邮件,例如冒充"银行密码重置邮件",欺骗用户进入钓鱼网站。

(6) 感染病毒后弹出模仿 QQ、阿里旺旺等聊天工具窗口,用户单击后进入钓鱼网站。

(7) 恶意导航网站、恶意下载网站弹出仿真悬浮窗口,用户单击后进入钓鱼网站。

(8) 伪装成用户输入网址时易发生的错误,如 gogle.com、sinz.com 等,一旦用户写错,就误入钓鱼网站。

如果网站开发人员不懂 Web 安全常识,那么许多网站都可能是一个潜在的钓鱼网站(被钓鱼网站 IFrame 注入利用)。

5.2 IFrame 框架钓鱼攻击经典案例重现

5.2.1 试验 1: testaspnet 网站有框架钓鱼风险

缺陷标题: testaspnet 网站>comments 评论区>评论框中,存在通过框架钓鱼的风险

测试平台与浏览器: Windows 7 + IE9 或 Firefox 浏览器

测试步骤:

(1) 用 IE 浏览器打开网站 http://testaspnet.vulnweb.com/。

(2) 在主页中单击 comments。

(3) 在 comments 输入框中输入<iframesrc=http://baidu.com>,如图 5-1 所示。

(4) 单击 Send comment 按钮。

(5) 查看结果页面。

期望结果: 用户能够正常评论,不存在通过框架钓鱼风险。

实际结果: 存在通过框架钓鱼风险,覆盖了其他评论,并且页面显示错乱,如图 5-2 所示。

【攻击分析】

对于禁止自己的网页或网站被 Frame 或者 IFrame 框架(阻止钓鱼风险),目前国内

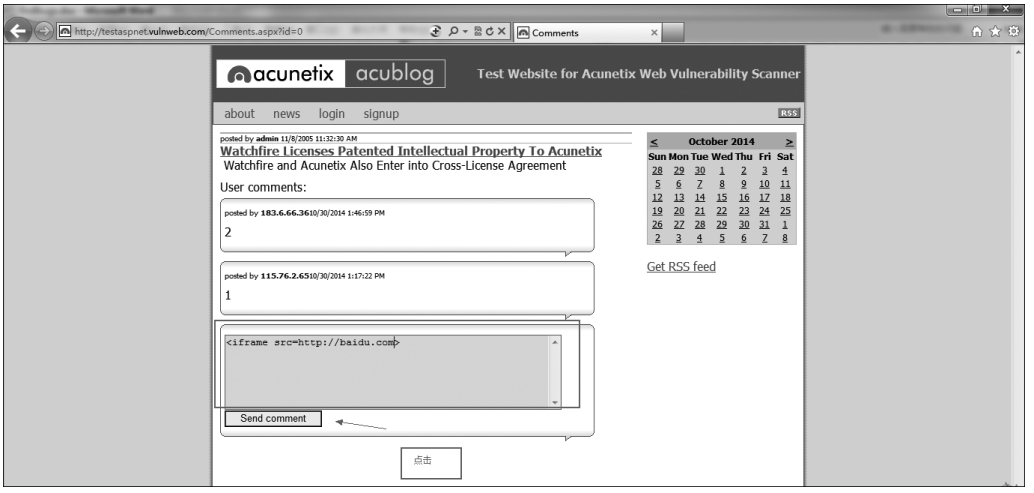

图 5-1　输入脚本代码

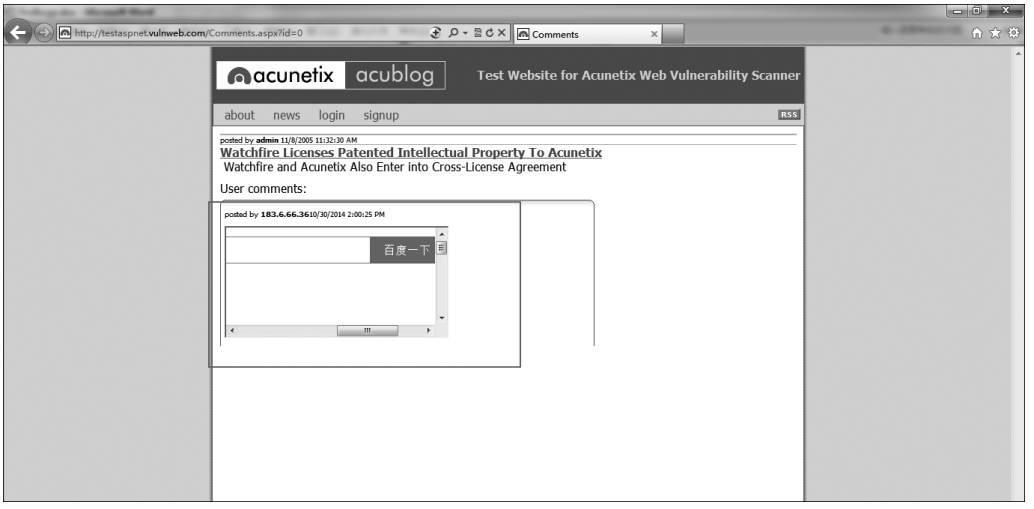

图 5-2　存在通过框架钓鱼风险

使用的方法有以下三种：

(1) 使用 meta 元标签

```
<html>
<head>
<meta http-equiv="Windows-Target" contect="_top">
</head>
<body></body>
</html>
```

(2) 使用 JavaScript 脚本

```
function location_top(){
```

```
  if(top.location!=self.location){
top.location=self.location;
    return false;
  }
  return true;
}
location_top();    //调用
```

这个方法用得比较多，但是网上的高手也想到了破解的办法，那就是在父框架中加入脚本 var location＝document.location 或者 var location＝""。记住：前台的验证经常会被绕行或被其他方式取代而不起作用。

(3) 使用加固 HTTP 安全响应头：这里介绍的响应头是 X-Frame-Options，这个属性可以解决使用 JavaScript 判断会被 var location 破解的问题，IE8、Firefox3.6、Chrome4 以上的版本均能很好地支持，以 Java EE 软件开发为例，补充 Java 后台代码如下：

```
//to prevent all framing of this content
response.addHeader( "X-FRAME-OPTIONS", "DENY" );
//to allow framing of this content only by this site
response.addHeader( "X-FRAME-OPTIONS", "SAMEORIGIN" );
```

就可以进行服务器端的验证，攻击者是无法绕过服务器端验证的，从而确保网站不会被框架钓鱼利用，此种解决方法是目前最安全的解决方案。

5.2.2 试验 2: testasp 网站有框架钓鱼风险

缺陷标题：在国外网站 Acunetix acuforum 查询时可以通过框架钓鱼

测试平台与浏览器：Windows 7＋Google 浏览器＋Firefox 浏览器＋IE11 浏览器

测试步骤：

(1) 打开国外网站：http://testasp.vulnweb.com。

(2) 单击 search 按钮。

(3) 在输入框中输入＜iframe src＝http://baidu.com＞，单击 search posts 按钮，如图 5-3 所示。

期望结果：页面提示警告信息。

实际结果：页面成功通过框架钓鱼，出现了百度搜索网站的内容，如图 5-4 所示。

【攻击分析】

对于一些安全要求较高的网站，往往不希望自己的网页被另外非授权网站框架包含，因为这是危险的，不法分子总是想尽办法以“钓鱼”的方式牟利。常见的钓鱼方式有：

(1) 黑客通过钓鱼网站设下陷阱，大量收集用户个人隐私信息，并贩卖个人信息或敲诈用户。

(2) 黑客通过钓鱼网站收集、记录用户网上银行账号、密码，盗取用户的网银资金。

(3) 黑客假冒网上购物、在线支付网站，欺骗用户直接将钱打入黑客账户。

(4) 通过假冒产品和广告宣传获取用户信任，骗取用户金钱。

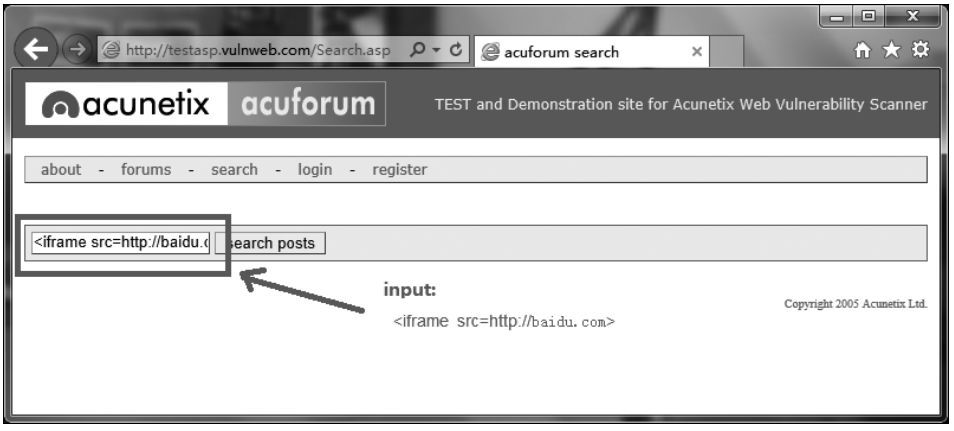

图 5-3　在输入框中输入框架攻击

图 5-4　在网站框架上百度

(5) 恶意团购网站或购物网站,假借“限时抢购”“秒杀”“团购”等噱头,让用户不假思索地提供个人信息和银行账号,这些黑心网站主可直接获取用户输入的个人资料和网银账号密码信息,进而获利。

钓鱼网类型主要有两种:一种是主动的钓鱼网站,就是高仿网站,专门用于钓鱼,如中国工商银行的官网是 www.icbc.com,钓鱼网站可能仅修改部分,例如修改为 www.lcbc.com,钓鱼网站表面上看,内容与官网完全一样,甚至弹出的公告和你平常见到的页面一样。这样,当你在钓鱼网站用自己的银行账户与密码登录后,你的银行账户与密码就存储到钓鱼网站数据库中了,你的银行账户就不再安全。

另一种是网站本身不是专门的钓鱼网站,但由于被其他网站利用,成了钓鱼网站。一

个网站如果能被框架，就有被别人网站钓鱼的风险。现在许多钓鱼攻击都是这种情况，合法网站被不法分子利用。

5.3 IFrame框架钓鱼攻击的正确防护方法

5.3.1 IFrame框架钓鱼总体防护思想

（1）所有能输入的框，攻击者都可以填写框架钓鱼语法，进行攻击测试，所以要禁止用户输入形如下面的IFrame代码段：

```
<iframesrc=XXX.XXX.XXX>
```

（2）不仅要防护自己的网站不能被框架到其他网站中，也要防护自己的网站不能框架别人的网站。

5.3.2 能引起IFrame框架钓鱼的错误代码段

如果一个网站的填充域（任意可供用户输入的地方）没有阻止用户输入IFrame标签字样，那么就有可能受到IFrame框架钓鱼风险，这种是框架其他网站（内框架）。

如果一个网站没有设置禁止被其他网站框架，那么就有被框架在其他网站中的风险（外框架）。

这里不提供错误的代码，如果没有按5.3.3节的正确代码进行防护，就可能出现IFrame框架钓鱼风险。

5.3.3 能防护IFrame框架钓鱼的正确代码段

以Java EE软件开发为例，补充Java后台代码如下：

```
//to prevent all framing of this content
response.addHeader( "X-FRAME-OPTIONS", "DENY" );
//to allow framing of this content only by this site
response.addHeader( "X-FRAME-OPTIONS", "SAMEORIGIN" );
```

就可以进行服务器端的验证，攻击者是无法绕过服务器端验证的，从而确保网站不会被框架钓鱼利用，此种解决方法是目前最安全的解决方案。

5.4 IFrame框架钓鱼攻击动手实践与扩展训练

5.4.1 Web安全知识运用训练

请找出以下网站的IFrame框架攻击安全缺陷：

（1）testfire网站：http://demo.testfire.net

（2）testphp网站：http://testphp.vulnweb.com

（3）testasp网站：http://testasp.vulnweb.com

(4) testaspnet 网站：http://testaspnet.vulnweb.com

(5) zero 网站：http://zero.webappsecurity.com

(6) crackme 网站：http://crackme.cenzic.com

(7) webscantest 网站：http://www.webscantest.com

(8) nmap 网站：http://scanme.nmap.org

5.4.2 安全夺旗 CTF 训练

请从安全夺旗 CTF 提供的各个应用中找出 IFrame 框架攻击安全缺陷：

(1) A little something to get you started 应用：https://ctf.hacker101.com/ctf/launch/1

(2) Micro-CMS v1 应用：https://ctf.hacker101.com/ctf/launch/2

(3) Micro-CMS v2 应用：https://ctf.hacker101.com/ctf/launch/3

(4) Pastebin 应用：https://ctf.hacker101.com/ctf/launch/4

(5) Photo Gallery 应用：https://ctf.hacker101.com/ctf/launch/5

(6) Cody's First Blog 应用：https://ctf.hacker101.com/ctf/launch/6

(7) Postbook 应用：https://ctf.hacker101.com/ctf/launch/7

(8) Ticketastic：Demo Instance 应用：https://ctf.hacker101.com/ctf/launch/8

(9) Ticketastic：Live Instance 应用：https://ctf.hacker101.com/ctf/launch/9

(10) Petshop Pro 应用：https://ctf.hacker101.com/ctf/launch/10

(11) Model E1337-Rolling Code Lock 应用：https://ctf.hacker101.com/ctf/launch/11

(12) TempImage 应用：https://ctf.hacker101.com/ctf/launch/12

(13) H1 Thermostat 应用：https://ctf.hacker101.com/ctf/launch/13

(14) Model E1337 v2-Hardened Rolling Code Lock 应用：https://ctf.hacker101.com/ctf/launch/14

(15) Intentional Exercise 应用：https://ctf.hacker101.com/ctf/launch/15

(16) Hello World! 应用：https://ctf.hacker101.com/ctf/launch/16

提醒 1：可以在 http://collegecontest.roqisoft.com/awardshow.html 中查阅历年全国高校大学生在这些网站中发现的更多安全相关的缺陷。

提醒 2：本章中讲解的安全技术，因为对系统的破坏性很大，为避免产生法律纠纷，请不要乱用。请在自己设计的网站上测试；或者你已得到授权允许做安全测试，才可以用各种安全测试技术或安全测试工具进行安全测试(本章动手实践与扩展训练中所举的样例网站，都是公开可以做各种安全测试的)。