实验5 软件探索测试训练

实验目的

探索测试(Exploratory Testing)是指通常用于没有产品说明书的测试,这需要把软件当作产品说明书来看待,分步骤逐项探索软件特性,记录软件执行情况,详细描述功能,综合利用静态和动态技术进行测试。探索测试人员只靠智能、洞察力和经验来对 Bug 的位置进行判断,所以探索测试又被称为自由形式测试。探索性强调测试人员的主观能动性,抛弃繁杂的测试计划和测试用例设计过程,强调在碰到问题时及时改变测试策略。

经过前面四大主题的经典软件缺陷寻找过程,相信每位读者都想体验一下自己的真正实力。探索测试是一个测试工程师个人实力与技术修养的体现。本实验将带领各位读者共同领略各位工程师与大学生竞赛中获奖选手的技术风采。

5.1 实验#1:oricity 网站 JavaScript 前端控制被绕行

缺陷标题 oricity 网站→好友分组,通过更改 URL 可以添加超过最大个数的好友分组。

测试平台与浏览器 Windows 7+IE 11 或 Chrome。

测试步骤

(1) 打开 oricity 网站 http://www.oricity.com/。

(2) 使用正确的账户登录。

(3) 单击账户名称,进入“我的城市空间”页面。

(4) 单击“好友分组”,添加好友分组到最大个数 10 个,此时“添加”按钮变成灰色,为不可添加状态,选择一个分组,单击“修改组资料”。

(5) 在 URL 后面加上 ?action=add,按 Enter 键。

(6) 在添加页面输入组名,单击“确定”按钮。

期望结果 不能添加分组。

实际结果 第 11 个分组添加成功，如图 5-1 所示。

图 5-1 添加了 11 个分组

专家点评

当 10 个分组添加完成之后，“新建组”按钮变灰，不可再单击添加，也就是前端 JS 判断正确，但是当编辑分组，更改 URL 为添加页面的 URL 补上 ?action＝add 时，却可以添加成功，说明后端服务器程序并没有验证是否已达到最大限制，这是标准的安全技术问题。

A7-Missing Function Level Access Control 在 2013 年 Web 安全排名第 7 位。功能级访问控制缺失，大部分 Web 应用在界面上进行了应用级访问控制，但是应用服务器端也要进行相应的访问控制。如果请求没有服务器端验证，攻击者就能够构造请求访问未授权的功能。

5.2 实验＃2：oricity 网站上传文件大小限制问题

缺陷标题 oricity 网站→个人中心→我的相册中图片上传，可上传超过限制大小的图片。

测试平台与浏览器 Windows 7＋Chrome。

测试步骤

（1）打开 oricity 网站 http://www.oricity.com/。

（2）登录，单击[××的城市空间]，在“我的相册”目录下找到“图片上传”。

（3）选择超过限制的图片并上传，如图 5-2 所示。

（4）查看上传结果。

期望结果 上传失败，并提示。

图 5-2　可以上传超过限制的图片

实际结果　能上传，并能打开。

专家点评

文件上传部分经常出现安全问题：一种是文件大小限制不工作，或能被轻易攻击导致文件大小限制不工作；另一种是文件类型没做限制，导致能上传病毒文件至服务器中，破坏服务器中的源程序或其他有用文件。

对于文件上传，一般需要考虑以下测试。

1. 功能测试

(1) 选择符合要求的文件，上传，上传成功。

(2) 上传成功的文件名称显示，显示正常(根据需求)。

(3) 查看/下载上传成功的文件，上传的文件可查看或下载。

(4) 删除上传成功的文件，可删除。

(5) 替换上传成功的文件，可替换。

(6) 上传文件是否支持中文名称，根据需求而定。

(7) 文件路径是否可手动输入，根据需求而定。

(8) 手动输入正确的文件路径，上传，上传成功。

(9) 手动输入错误的文件路径，上传，提示不能上传。

2. 文件大小测试

(1) 符合格式，总大小稍小于限制大小的文件，上传成功。

(2) 符合格式，总大小等于限制的大小的文件，上传成功。

(3) 符合格式，总大小稍大于限制大小的文件，在上传时提示附件过大，不能上传。

(4) 大小为 0KB 的 TXT 文档，不能上传。

3. 文件名称测试

(1) 文件名称过长。Windows 2000 标准为 255 个字符(指在英文的字符下),如果是中文则不超过 127 个汉字,否则提示过长。

(2) 文件名称达到最大长度(中文、英文或混在一起)上传后显示名称,页面排版,页面显示正常。

(3) 文件名称中包含特殊字符,根据需求而定。

(4) 文件名全为中文,根据需求而定。

(5) 文件名全为英文,根据需求而定。

(6) 文件名为中英文混合,根据需求而定。

4. 文件格式测试

(1) 上传正确格式,上传成功。

(2) 上传不允许的格式,提示不能上传。

(3) 上传 RAR、ZIP 等打包文件(多文件压缩),根据需求而定。

5. 安全性测试

(1) 上传可执行文件(EXE 文件),根据需求而定。

(2) 上传常见的木马文件,提示不能上传。

(3) 上传时服务器空间已满,有提示。

6. 性能测试

(1) 上传时网速很慢(限速),当超过一定时间,有提示。

(2) 上传过程断网,有提示上传是否成功。

(3) 上传过程服务器停止工作,有提示上传是否成功。

(4) 上传过程服务器的资源利用率,在正常范围。

7. 界面测试

(1) 页面美观性,易用性(键盘和鼠标的操作、Tab 跳转的顺序是否正确)。

(2) 按钮文字是否正确。

(3) 正确/错误的提示文字是否正确。

(4) 说明性文字是否正确。

8. 冲突或边界测试

(1) 有多个上传框时,上传相同名称的文件。

(2) 上传一个正在打开的文件。

(3) 文件路径是手动输入的是否限制长度。

(4) 上传文件过程中是否有取消正在上传文件的功能。

(5) 保存时有没有已经选择好但没有上传的文件,需要提示上传。

(6) 选择好但是未上传的文件是否可以取消选择,需要可以取消选择。

5.3 实验#3:oricity 网站权限控制错 403 Forbidden

缺陷标题 oricity 网站→都市论坛→帮助网页出现 403 Forbidden。

测试平台与浏览器 Windows 7+Firefox。

测试步骤

(1) 打开 oricity 网站 http://www.oricity.com/。

(2) 进入都市论坛,单击“帮助”,查看页面。

期望结果　页面正确显示。

实际结果　页面出现 403 Forbidden,如图 5-3 所示。

图 5-3　页面出现 403 Forbidden

专家点评

单击“帮助”,应该出现关于该网站的一些帮助信息,但是这里出现 403 Forbidden,还显示网站内部代码,这是不应该的。这也是典型的 Web 安全功能性访问控制出错的案例。

在 Web 安全测试中,权限控制出错的例子非常多。

例如,用户 A 在电子书籍网站购买了 3 本电子书,然后用户 A 单击书名就能阅读这些电子书,每本电子书都有 bookid,用户 A 通过篡改 URL,把 bookid 换成其他 id,就有可能免费看别人购买的电子书籍。

又如,普通用户 A 拿到了管理员的 URL,试图去运行,结果发现自己也能操作管理员界面。

以上两个例子是缺少功能性安全访问控制。也有出现过分安全保护导致正常用户无法访问所需要的页面或功能。本实验就是过分保护导致的错误。

5.4　实验＃4：oricity 网站有内部测试网页

缺陷标题　oricity 网站→活动详情页面,在 URL 后面添加/test.php 出现测试页面。

测试平台与浏览器　Windows 7(64 bit)＋Chrome 或 IE 11。

测试步骤

(1) 打开 oricity 网站 http://www.oricity.com/。

(2) 单击任一活动。

(3) 修改 URL 为 http://www.oricity.com/event/test.php,按 Enter 键。

期望结果 不存在测试页面。

实际结果 存在测试页面,并能访问,如图 5-4 所示。

图 5-4 网站存在测试页面

专家点评

软件开发人员经常为调试代码或功能需要增加许多内部测试页或打印一些 Log 日志信息,但这些测试页或内部调试信息在发布的产品上需要删除掉;如果的确有用途,那需要进行相应的身份认证,不能侥幸地认为 URL 没公布出去别人应该不知道。实际上,Web 安全扫描工具或渗透工具能用网络爬虫技术遍历所有的 URL。

某些 Web 应用包含一些“隐藏”的 URL,这些 URL 不显示在网页链接中,但管理员可以直接输入 URL 访问到这些“隐藏”页面。如果不对这些 URL 做访问限制,攻击者仍然有机会打开它们。

这类攻击常见的情形如下。

(1) 某商品网站举行内部促销活动,待定内部员工可以通过访问一个未公开的 URL 链接登录公司网站,购买特价商品,此 URL 通过某员工泄露后,导致大量外部用户登录购买。

(2) 某公司网站包含一个未公开的内部员工论坛(http://example.com/bbs),攻击者经过一些简单的尝试就能找到这个论坛的入口地址,从而发各种垃圾帖子或进行各种攻击。

5.5 实验#5:NBA 网站 files 目录能被遍历

缺陷标题 NBA 网站 files 目录能被遍历。

测试平台与浏览器 Windows 7+Chrome 或 Firefox。

测试步骤

(1) 打开 NBA 网站 http://www.nba.com。

（2）在 URL 后面补上 files，形如 http://www.nba.com/files。

期望结果　不会显示 files 目录结构。

实际结果　显示 files 目录结构，并且继续向后遍历目录，如图 5-5 所示。

图 5-5　files 目录能被遍历

专家点评

对于一个安全的 Web 服务器来说，对 Web 内容进行恰当的访问控制是极为关键的。目录遍历是 HTTP 存在的一个安全漏洞，它使得攻击者能够访问受限制的目录，并在 Web 服务器的根目录以外执行命令。

Web 服务器主要提供两个级别的安全机制。

（1）访问控制列表，即常说的 ACL。

（2）根目录访问。

访问控制列表是用于授权过程的，它是一个 Web 服务器的管理员用来说明什么用户或用户组能够在服务器上访问、修改和执行某些文件的列表，同时也包含了其他一些访问权限内容。

根目录是服务器文件系统中的一个特定目录，它往往是一个限制，用户无法访问位于这个目录之上的任何内容。

例如，Windows 的 IIS 默认的根目录是 C:\Inetpub\wwwroot，那么用户一旦通过了 ACL 的检查，就可以访问 C:\Inetpub\wwwroot\news 目录以及其他位于这个根目录以下的所有目录和文件，但无法访问 C:\Windows 目录。

根目录的存在能够防止用户访问服务器上的一些关键性文件，如在 Windows 平台上的 cmd.exe 或是 Linux/UNIX 平台上的口令文件。

这个漏洞可能存在于 Web 服务器软件本身，也可能存在于 Web 应用程序的代码之中。

要执行一个目录遍历攻击，攻击者所需要的只是一个 Web 浏览器，并且有一些关于系统的默认文件和目录所存在的位置的知识即可。

如果网站存在这个漏洞，那么攻击者可以用它来做些什么？

利用这个漏洞，攻击者能够走出服务器的根目录，从而访问文件系统的其他部分，如攻击者能够看到一些受限制的文件，或者能够执行一些造成整个系统崩溃的指令。

依赖于 Web 站点的访问设置，攻击者能够仿冒站点的其他用户来执行操作，而这就依赖系统对 Web 站点的用户是如何授权的。

在包含动态页面的 Web 应用中，输入往往是通过 GET 或是 POST 的请求方法从浏览器获得，http://test.webarticles.com/show.asp? view=oldarchive.html 是一个 GET 的 HTTP URL 请求示例。利用这个 URL，浏览器向服务器发送了对动态页面 show.asp 的请求，并且伴有值为 oldarchive.html 的 view 参数，当请求在 Web 服务器端执行时，show.asp 会从服务器的文件系统中取得 oldarchive.html 文件，并将其返回客户端的浏览器。那么，攻击者就可以假定 show.asp 能够从文件系统中获取文件并编制如下 URL——http://test.XXX.com/show.asp?view=../../../../../Windows/system.ini。那么，这就能够从文件系统中获取 system.ini 文件并返回给用户。攻击者不得不去猜测需要往上多少层才能找到 Windows 目录，但可想而知，这其实并不困难，经过若干次的尝试后总会找到的。

除了 Web 应用的代码以外，Web 服务器本身也有可能无法抵御目录遍历攻击。这有可能存在于 Web 服务器软件或是一些存放在服务器上的示例脚本中。

在最近的 Web 服务器软件中，这个问题已经得到了解决。但是，网上的很多 Web 服务器仍然使用老版本的 IIS 和 Apache，它们可能仍然无法抵御这类攻击。即使使用了已经解决这个漏洞的版本的 Web 服务器软件，仍然可能会有一些对黑客来说是很明显的存有敏感默认脚本的目录。

例如，http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\这个 URL 请求使用了 IIS 的脚本目录来移动目录并执行指令它会返回 C:\目录下所有文件的列表，是通过调用 cmd.exe 然后再用 dir c:\来实现的，%5c 是 Web 服务器的转换符，用来代表一些常见字符，这里表示的是\。

新版本的 Web 服务器软件会检查这些转换符并限制它们通过，但一些老版本的服务器软件仍然存在这个问题。

另外，本实验直接访问 files 目录，是因为对 Web 开发比较熟练，一般 Web 开发的目录结构都会有类似 images、photo、js、css、html 之类的目录，所有的目录结构都要做保护处理，不能让人直接访问，否则网站源代码、一些隐私信息都有可能泄露。

5.6 实验#6：NBA 网站有内部测试网页

缺陷标题 NBA 网站检测到测试脚本问题。

测试平台与浏览器 Windows 7 (64 bit)+IE 11 或 Chrome。

测试步骤

(1) 打开 NBA 网站 http://www.nba.com/test.html。

(2) 观察页面信息，并查看页面源代码。

期望结果 不显示测试脚本信息。

实际结果 显示测试脚本信息，如图 5-6 所示。

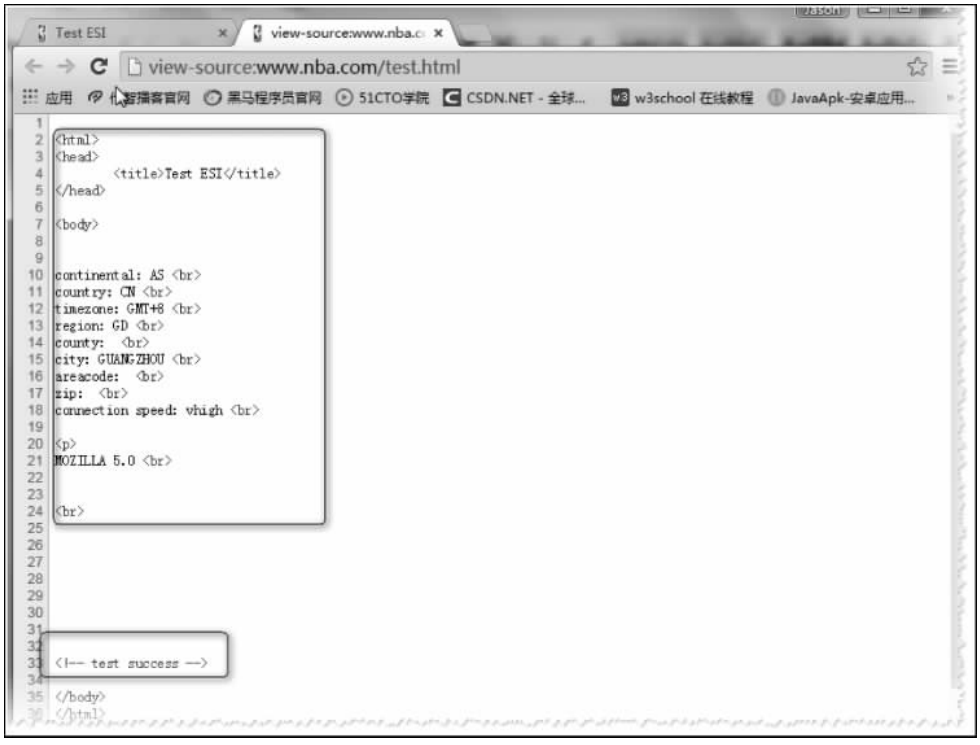

图 5-6　显示测试脚本信息

专家点评

参见 5.4 节实验＃4 的专家点评。

5.7　实验＃7：NBA 网站 Servlet 信息泄露

缺陷标题　NBA 网站存在 Servlet 信息泄露问题。

测试平台与浏览器　Windows 7 (64 bit)＋IE 11、Firefox 或 Chrome。

测试步骤

(1) 打开 NBA 网站 http://www.nba.com/axis/fingerprint.jsp。

(2) 分别在 IE、Firefox、Chrome 浏览器上观察页面信息。

期望结果　不显示 Apache AXIS 样本 Servlet 具体信息。

实际结果　显示 Apache AXIS 样本 Servlet 具体信息，如图 5-7 所示。

专家点评

参见 5.4 节实验＃4 的专家点评。

本例中的 URL 能直接访问到服务器指纹的详细信息，给攻击者更多的空间去研究如何更深入地攻击网站。

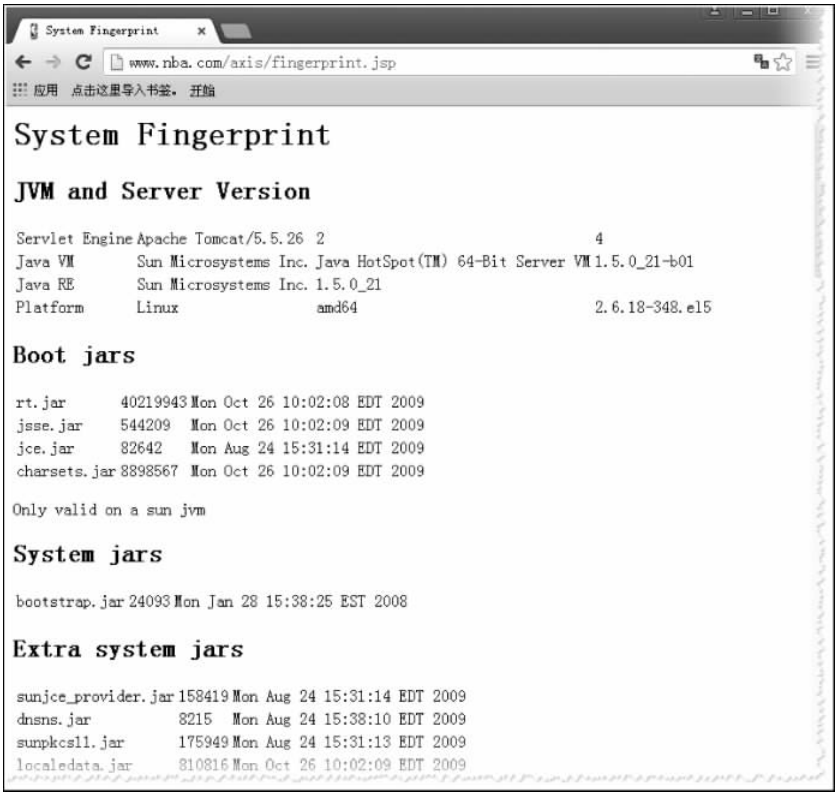

图 5-7 显示 Apache AXIS 样本 Servlet 具体信息

5.8 实验#8：南大小百合 BBS 存在 CSRF 攻击漏洞

缺陷标题 南大小百合 BBS 存在 CSRF 攻击漏洞。

测试平台与浏览器 Windows 7＋Chrome 或 Firefox。

测试步骤

(1) 打开南大小百合 BBS http://bbs.nju.edu.cn。

(2) 登录进入 BBS，尝试发几个帖子，并且观察删除帖子的链接。

主题 Test BBS 111：http://bbs.nju.edu.cn/vd64377/bbsdel?board＝D_Computer&file＝M.1444972425.A。

主题 BBS test 2222：http://bbs.nju.edu.cn/vd64377/bbsdel?board＝D_Computer&file＝M.1444972485.A。

主题 CSRF BBS 333：http://bbs.nju.edu.cn/vd64377/bbsdel?board＝D_Computer&file＝M.1444972604.A。

(3) 尝试直接在浏览器中删除帖子链接。

期望结果 不会直接删除帖子。

实际结果 没有任何提示信息，帖子能被删除，如图 5-8 所示。

D_Computer(计算机系)

本版域名: http://bbs.nju.edu.cn/g/D_Computer, 版主: Amati pizzacake, 版内在线: 43人.　　↑,订阅本版

版主寄语: 淡泊以明志 宁静而致远

序号	状态	作者	日期	标题	人气
Bo0	置顶	elong99	Sep 24 09:39	○ 关于本科生海外交流项目的一些要求 (459字节)	4960
Bo0	置顶	CSJob	Aug 28 10:13	○ 2016届毕业生招聘信息汇总【10.16更新】 (170.3K)	1497
11992	N	Nettle	Oct 15 12:30	○ 计算机系图书阅览室图书整理志愿活动总结 (1858字节)	1010
11993	N	tututututu	Oct 15 12:38	Re: 计算机系图书阅览室图书整理志愿活动总结 (8字节)	24
11994	N	dong9301q	Oct 15 12:40	Re: 计算机系图书阅览室图书整理志愿活动总结 (26字节)	16
11995	N	15851672701	Oct 15 12:48	Re: 计算机系图书阅览室图书整理志愿活动总结 (115字节)	21
11996	N	hf119119	Oct 15 16:37	○ 兼职组稿招聘 (486字节)	86
11997	N	nettis	Oct 15 16:59	Re: 计算机系图书阅览室图书整理志愿活动总结 (22字节)	21
11998	N	microflash	Oct 15 17:06	○ [转载] 江苏金陵科技校园招聘暨JCTF2015，两万元大奖等你拿 (1220字节)	109
11999	N	13450	Oct 15 21:02	Re: 计算机系图书阅览室图书整理志愿活动总结 (10字节)	21
12000	N	yaleyoga	Oct 16 08:35	Re: 计算机系图书阅览室图书整理志愿活动总结 (90字节)	6
12001	N	1316	Oct 16 08:58	Re: 计算机系图书阅览室图书整理志愿活动总结 (72字节)	6
12002	N	cs2012	Oct 16 09:16	Re: 计算机系图书阅览室图书整理志愿活动总结 (34字节)	7
12003	N	SHSJ	Oct 16 11:01	○ [转载] 三星电子Tizen技术开放日讲座（南京大学） (1157字节)	12
12004		kuro	Oct 16 11:14	○ 关于计算机学院萌萌哒小正太 (86字节)	132
12005	N	SMElman	Oct 16 11:16	○ 【实习】北京鼎丰基金招聘程序实习生 (3.5K)	16
12006	N	jamesliu	Oct 16 12:03	Re: 关于计算机学院萌萌哒小正太 (261字节)	11
12007		LoseAGain	Oct 16 12:28	○ 摩根士丹利信息技术部简历接收即将截止，请抓紧投递 (2.9K)	12
12008		tsingcoo	Oct 16 12:48	Re: 计算机系图书阅览室图书整理志愿活动总结 (2字节)	3
12009		roywang	Oct 16 13:13	○ Test bbs 11111 (12字节)	4
12010		roywang	Oct 16 13:14	○ BBS test 2222 (11字节)	3
12011		roywang	Oct 16 13:16	○ CSRF BBS 333 (10字节)	4

[添加边框] 发表文章 上载区 刷新 上一页 主题模式 进版画面 文摘区 精华区 下载精华区 版内查询 精华区查询 清除未读

跳转到 第 篇

图 5-8　南大小百合 BBS 有 CSRF 攻击漏洞

专家点评

南大小百合 BBS 删除帖子的 URL 没有做 CSRF 保护，导致恶意用户可以伪造删帖的 URL 让合法用户去单击，合法用户在不知情的情况下，删除了帖子。

分析并执行这个 URL，可以发现以下问题。

(1) URL 上缺少 CSRF 安全 Token 保护，导致 URL 很容易伪造。

(2) 删除时没有弹出警示确认信息，例如“您真的要删除这个帖子吗?”，使得合法用户在不知情的情况下被不法分子利用，单击链接，删除了内容。

CSRF 的思想可以追溯到 20 世纪 80 年代。1988 年，Norm Hardy 发现这个应用级别的信任问题，并把它称为混淆代理人(Confused Deputy)。2001 年，Peter Watkins 第一次将其命名为 CSRF，并将其列在 Bugtraq 缺陷列表中，从此 CSRF 开始进入人们的视线。从 2007 年开始，开放式 Web 应用程序安全项目(Open Web Application Security Project，OWASP)组织将其排在 Web 安全攻击的前十名。

CSRF 就像一个狡猾的猎人在自己的狩猎区布置了一个个陷阱。上网用户就像一个个猎物，在自己不知情的情况下被其引诱，触发了陷阱，导致了用户的信息暴露、财产丢失。因为其极为隐蔽，并且利用的是互联网 Web 认证自身存在的漏洞，所以很难被发现并且破坏性大。

现在大部分 Web 应用使用 Cookie/Session 来标识用户的身份并保持会话状态，这种设

计在建立之初就没有考虑可能带来的安全性问题。换句话说，假设站点使用 Cookie/Session 的隐式身份验证，当用户完成身份验证时，浏览器将获得一个用于识别用户身份的 Cookie/Session，只要用户不关闭浏览器或退出 Web 应用，用户访问这个网站的后续操作都不需要重新进行登录认证，浏览器会为每个请求都“智能”地带上网站已认证成功的 Cookie/Session 来识别自己。

当第三方网页生成对当前站点域的请求时，该请求也将会获取当前站点已认证的 Cookie/Session，便于后续操作。这种类型的认证称为隐式认证。

隐式认证带来的问题就是一旦用户登录某网站，然后单击某链接进入该网站下的任意一个网页，那么他在此网站中已经认证过的身份就有可能被非法利用，在用户不知情的情况下执行了一些非法操作。而这种 Web 身份认证自身存在的缺陷普通用户很少知道，这给 CSRF 攻击提供了便利。

5.9 实验＃9：新浪微博存在 CSRF 攻击漏洞

缺陷标题 新浪微博存在 CSRF 攻击漏洞。

测试平台与浏览器 Windows 7＋Chrome 或 Firefox。

测试步骤

(1) 打开新浪微博 http://weibo.com。

(2) 登录进入新浪微博，查看退出的链接 http://weibo.com/logout.php?backurl=%2F。

(3) 在浏览器中直接运行退出链接。

期望结果 不会直接登录。

实际结果 没有任何提示信息，直接退出新浪微博，如图 5-9 所示。导致新浪微博能任意伪造退出链接，让任何一个用户单击后退出系统。

图 5-9 新浪微博有 CSRF 攻击漏洞

专家点评

每个登录新浪微博的用户，所使用退出系统的 URL 完全一致，并不做身份检查，都是 http://weibo.com/logout.php?backurl=%2F，所以这个 URL 能让任意用户在不知情的情况下单击后退出系统。

有的测试人员或开发人员对于这样的 Bug 不理解，认为这并没有什么缺陷。但是这的确是让安全界头痛的一个 Web 安全问题——CSRF 攻击，这个问题稍一延伸大家就不会陌生。

例如以下情况。

(1) 因为自己不小心扫了一个二维码，结果自己被误拉入一个群。

(2) 因为自己误扫了一个二维码，结果自己微信账户的零钱没有了。

(3) 因为自己误点了一个链接，结果自己银行卡的钱被转走了。

无论是二维码还是链接，都是去执行一个操作，如果关键的操作不进行 CSRF 防护，那么这些 URL 很容易被伪造，给用户在不知情的情况下带来重大损失。

这需要各大应用提供商提高自己应用的安全等级，防护住各种安全漏洞，以免让用户处于威胁与不安之中。目前对 CSRF 防护比较优秀的解决方案就是 URL 中带有 CSRFToken 参数。这个参数的值是攻击者无法预知的，服务器校验时，只要 URL 不带 CSRFToken 或者 CSRFToken 带得不对，就不执行用户的请求，这样就能彻底杜绝 CSRF 攻击。

5.10　实验＃10：testphp 网站目录列表暴露

缺陷标题　testphp 网站存在目录列表信息暴露问题。

测试平台与浏览器　Windows 7(64 bit)＋IE 11 或 Firefox。

测试步骤

(1) 打开 testphp 网站 http://testphp.vulnweb.com/Flash/。

(2) 分别在 IE、Firefox 浏览器上观察页面信息。

期望结果　不显示目录列表信息。

实际结果　显示目录列表信息，如图 5-10 所示。

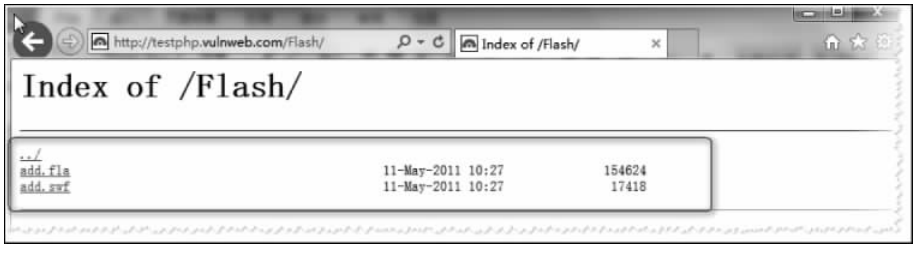

图 5-10　显示目录列表信息

专家点评

如果目录结构能被轻松遍历，那么网站的源码、数据库设计、日志等都能被下载研究，这

对一个网站或应用来说是灾难性的。

5.11 实验＃11：智慧绍兴-电子刻字选择颜色下拉列表出现英文

缺陷标题 智慧绍兴→到此一游→电子刻字页面单击“电子刻字”，选择颜色下拉列表为 red、yellow、blue、white、black。

测试平台与浏览器 Windows 10＋Chrome 或 Firefox。

测试步骤

（1）打开智慧绍兴网站 http://www.roqisoft.com/zhsx。

（2）单击导航条中的“到此一游”。

（3）单击“电子刻字”→“体验电子刻字”。

期望结果 选择颜色下拉列表中应该为中文红色、黄色、蓝色、白色、黑色。

实际结果 选择颜色下拉列表为 red、yellow、blue、white、black，如图 5-11 所示。

图 5-11 颜色下拉列表为英文

专家点评

对于中文网站，所有的文字应该显示为中文。但是，开发者经常主界面上都是中文，当出现提示、下拉列表等项的时候，忘记将选项改成中文。

类似地，对于国际网站测试，许多网站支持多种语言切换，主界面一般看上去都能切换到相应的语言，但是当出错、输入无效、输入不满足要求时，就可能出现英文提示，测试工程师需要注意验证。

5.12　实验＃12：oricity 网站错误提示使用英文

缺陷标题　oricity 网站→已经结束的活动页面，单击任意链接出现“Access Reject，请登录后浏览...”。

测试平台与浏览器　Windows 7＋IE 11 或 Firefox 或 Chrome。

测试步骤

(1) 打开 oricity 网站 http://www.oricity.com/。

(2) 在“已经结束的活动”栏目中，单击任意活动去查看活动详情信息，例如，单击“OC No.330 羽球活动(迈歌 发起)”活动。

期望结果　提示登录后才能查看，或者跳转到登录页面(活动需要登录才能查看)。

实际结果　提示“Access Reject，请登录后浏览...”，如图 5-12 所示。

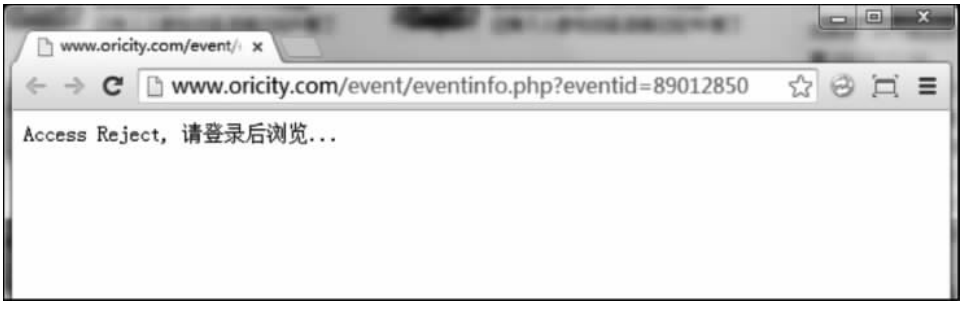

图 5-12　出现 Access Reject 英文提示错误

专家点评

导致 Access Reject 错误的原因有多种，可能是程序设计中权限分配有问题，或者认证服务器失败等。“已经结束的活动”板块设置的权限是登录后才能查看，在未登录的状态下访问此板块的活动信息，那么应该跳转到登录页，而不是直接出现 Access Reject。

另外，这是一个中文的站点，即使是出错页，也应该出现中文的错误提示，用英文的提示也不合适。

5.13　实验＃13：openclass 软件开发在线公开课问题

缺陷标题　言若金叶在线免费公开课“软件开发方向”页面无法显示。

测试平台与浏览器　Windows XP＋IE 8 或 Firefox。

测试步骤

(1) 打开言若金叶在线免费公开课网站 http://openclass.roqisoft.com。

（2）单击“软件测试方向”，观察页面。

（3）单击“软件开发方向”，观察页面。

期望结果 既能看到软件测试方向也能看到软件开发方向的公开课。

实际结果 只能看到软件测试方向的在线免费公开课页面，单击“软件开发方向”后页面无反应，如图 5-13 所示。

图 5-13 单击“软件开发方向”后页面无反应

专家点评

“软件开发方向”的链接是一个典型的空链接，不会跳转到任何页面。

出现空链接的原因如下。

网页开发是一个一个页面编写代码的，当时在做链接时，这个页面可能没做出来，所以当时就留下一个空链接在这里，最后忘记改成真实的链接了。

也有可能当时接口的 URL 没定义好，先放一个空链接在这里。

5.14 实验＃14：books《生命的足迹经典版》样张下载问题

缺陷标题 言若金叶软件研究中心-资源下载→找到书籍《生命的足迹》页面，书籍电子版下载无法打开。

测试平台与浏览器 Windows 10＋IE 11 或 Chrome。

测试步骤

（1）打开言若金叶软件研究中心-资源下载网站 http://books.roqisoft.com/download。

（2）单击“中英双语励志书籍”导航链接，出现的页面如图 5-14 所示。

（3）单击“书籍样张电子版下载阅读”链接。

期望结果 能够正常打开电子版下载阅读。

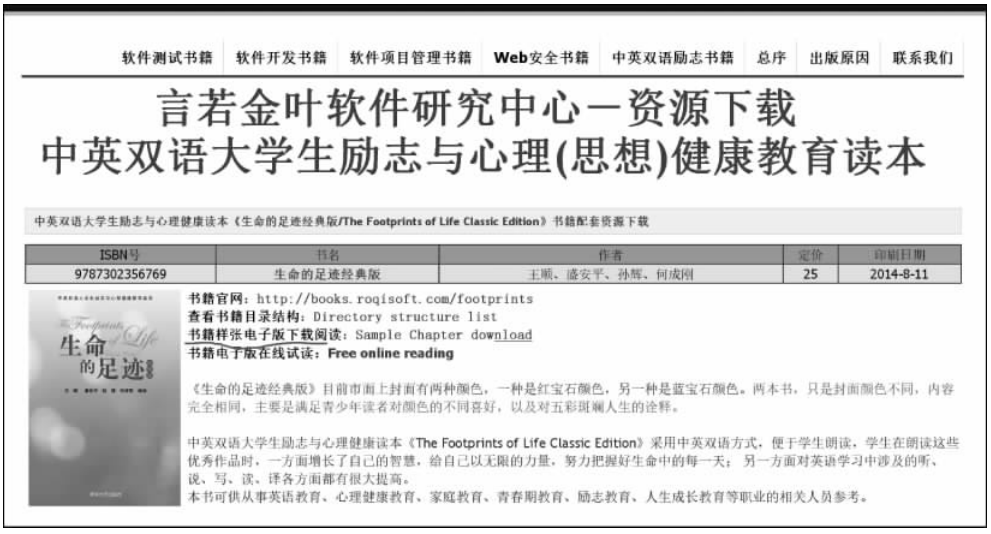

图 5-14　中英双语励志书籍

实际结果　无法正常打开网页，出现 404 错误，如图 5-15 所示。

图 5-15　出现 404 错误

专家点评

书籍样张链接接口指向清华大学出版社，出现找不到样张的原因，可能是原先这个样张链接是可以下载的，也是清华大学出版社提供的，但是后来清华大学出版社网站改版，系统中的链接或内部编号升级，导致找不到对应的样张。

这要求网站如果有第三方的图片、网页、文档等链接，必须及时更新，为避免第三方网站引用的图片、文档等被删除、转移目录等，可以把这些图片、文档放到自己的网站目录下引用，减少对第三方网站的依赖。

5.15　实验＃15：InfoSec 网络空间安全公告问题

缺陷标题　网络空间安全-信息安全技术网→公告，出现 404 错误。

测试平台与浏览器　Windows 7＋Chrome 54.0。

测试步骤

（1）打开网络空间安全-信息安全技术网 http://www.roqisoft.com/infosec/。

（2）单击“公告”，如图 5-16 所示。

图 5-16 “公告”页面

期望结果 能够查看公告详情。

实际结果 出现 404 错误，参见图 3-2。

专家点评

参见 3.1 节实验＃1 的专家点评。

探索测试也经常会找到一些功能或界面上的问题。

5.16 实验＃16：InfoSec 网络空间安全图片问题

缺陷标题 网络空间安全-信息安全技术网图片无法正常显示。

测试平台与浏览器 Windows 7＋Chrome 54.0。

测试步骤

（1）打开网络空间安全-信息安全技术网 http://www.roqisoft.com/infosec/。

（2）单击“也许这样理解 HTTPS 更容易”链接，在新的页面检查网页元素。网页 URL 为 http://www.roqisoft.com/infosec/?post＝21。

期望结果 网页上所有元素显示正常。

实际结果 图片无法显示，如图 5-17 所示。

专家点评

参见 2.13 节实验＃13 的专家点评。

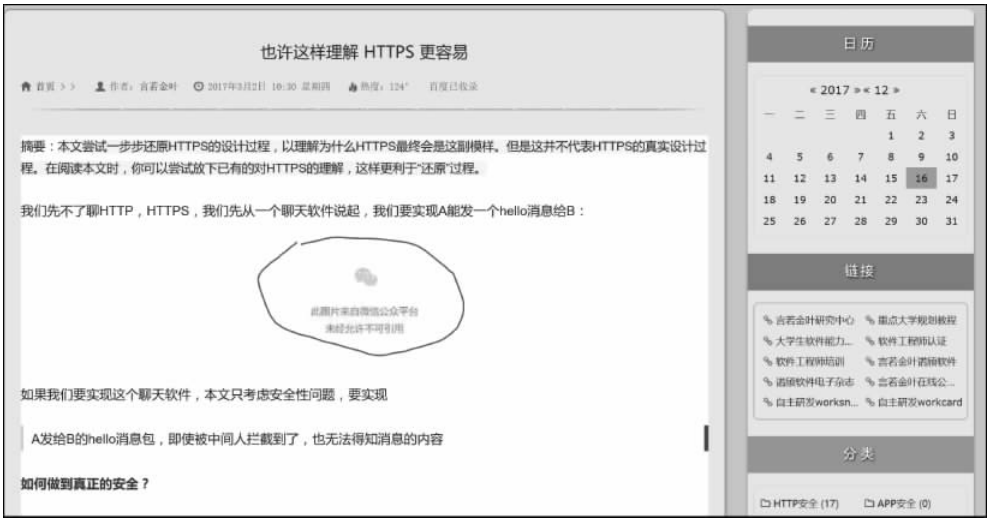

图 5-17　图片无法显示

5.17　实验＃17：testphp 网站出现错误暴露服务器信息

缺陷标题　testphp 网站出现禁止错误，并显示服务器信息。

测试平台与浏览器　Windows 10＋IE 11 或 Chrome 45.0。

测试步骤

（1）打开 testphp 网站 http://testphp.vulnweb.com/。

（2）在地址栏中追加 cgi-bin，按 Enter 键，如图 5-18 所示。

图 5-18　在地址栏中追加 cgi-bin

期望结果 页面不存在，出现一个友好的界面。

实际结果 出现 Forbidden(禁止)错误，并显示服务器信息，结果如图 5-19 所示。

图 5-19 出现 Forbidden(禁止)错误并显示服务器信息

专家点评

如果是禁止访问，应该出现一个友好的页面，而且不能出现具体的服务器信息。

每当 Apache2 网站服务器返回错误页时(如 404 页面无法找到，403 禁止访问页面)，它会在页面底部显示网站服务器签名(如 Apache 版本号和操作系统信息)。同时，当 Apache2 网站服务器为 PHP 页面服务时，它也会显示 PHP 的版本信息。

1. 关闭 Apache 服务器 banner

在/home/apache/conf/httpd.conf 文件中添加如下两行即可。

```
ServerSignature Off
ServerTokens Prod
```

2. 关闭 tomcat 版本的服务器

(1) 找到 tomcat6 主目录中的 lib 目录，找到 tomcat-coyote.jar。

(2) 修改 tomcat-coyote.jar\org\apache\coyote\ajp\Constants.class 和 tomcat-coyote.jar\org\apache\coyote\http11\Constants.class。

ajp\Constants.class 中：

```
SERVER_BYTES = ByteChunk.convertToBytes("Server: Apache-Coyote/1.1\r\n");
```

http11\Constants.class 中：

```
public static final byte[] SERVER_BYTES = ByteChunk.convertToBytes("Server: Apache-Coyote/
1.1\r\n");
```

将 server:Apache-Coyote/1.1 修改为 unknown 即可。

(3) 修改完毕将新的 class 类重新打包至 tomcat-coyote.jar 中。

(4) 上传至服务器，重启 tomcat 服务即可。

5.18 实验＃18：智慧绍兴-积分管理页随机数问题

缺陷标题 智慧绍兴→我的空间→积分管理，单击“赞”图标后观察 URL，随机数有问题。

测试平台与浏览器　Windows 10＋Chrome 或 Firefox。

测试步骤

（1）打开智慧绍兴网站 http://www.roqisoft.com/zhsx，用 zxr/test123 登录。

（2）单击导航条中的“我的空间”→“积分管理”。

（3）单击“赞”图标，观察浏览器地址栏的 URL 变化，特别是随机数。

期望结果　随机数每次会变，并且每次都不一样。

实际结果　随机数不断地拼在 URL 中，最终导致 URL 过长而不能正常解析，如图 5-20 所示。

图 5-20　随机数不断地拼在 URL 中

专家点评

URL 后面添加随机数通常用于防止客户端（浏览器）缓存页面。也就是保证每次显示这个网页，会从服务器端获取最新的数据来展示，而不是直接显示已经缓存过的旧页面。

浏览器缓存是基于 URL 进行的，如果页面允许缓存，则在一定时间内（缓存时效时间前）再次访问相同的 URL，浏览器不会再次发送请求到服务器端，而是直接从缓存中获取指定资源。URL 后面添加随机数后，URL 就不同了，可以看作唯一的 URL（随机数恰好相同的概率非常低，可以忽略不计），这样浏览器的缓存就不会匹配出 URL，每次都会从服务器获取最新的文件。

初学网页开发的人员经常会犯不带随机数的错误，导致明明自己保存的数据已经写到数据库中，却不能显示出来。但是，对于 URL 随机数的拼装也是有讲究的，那就是如果原先的 URL 中没有类似 random 的随机数参数，那就要带上；如果已经有了，就要替换 random 参数中的值，而不是继续往后拼装 random 参数。

本例 XXX/scoremgr.php? rnd＝568531182? rnd＝1087411872 是赞了两次出现了两个 rnd 参数，如果赞 3 次就会出现 3 个 rnd 参数，依此类推。但是，浏览器 URL 能接收的字符数是有限的，如果不停地单击，就会导致页面不再刷新展示。这是一个隐藏比较深的缺陷，一般具有网页开发相关技术背景的人才能发现这样的潜在问题。

5.19 实验＃19：智慧绍兴-我的好友列表翻页问题

缺陷标题 智慧绍兴→我的好友，好友太多，不支持翻页。

测试平台与浏览器 Windows 10＋Chrome 或 Firefox。

测试步骤

(1) 打开智慧绍兴网站 http://www.roqisoft.com/zhsx，用 zxr/test123 登录。

(2) 单击导航条中的“我的空间”→“我的好友”。

(3) 加一些人为好友，观察页面情况。

期望结果 页面能正常显示，如果好友太多，可以翻页显示。

实际结果 页面好友太多，没有翻页功能，如图 5-21 所示。

图 5-21 好友展示不支持翻页

专家点评

当只有一个好友时，界面是美观的；当站点只有10个用户时，好友推荐也是美观的；但是当人数呈几何增长时，则要考虑网页能不能正常显示、翻页。

通过“我的好友”网页测试发现，当网站注册人数增多时，“我的好友列表”“等待我批准的好友列表”“我的好友请求，等待他人批准列表”“好友推荐”这几项都需要支持翻页功能，否则，这个页面最后就无法使用与查看。所以，程序员在设计网站时一定要有前瞻性，要能看到当网站数据增大到不同数量级时网站与网页的设计与维护。

5.20　实验＃20：智慧绍兴-手写刻字图片与画布问题

缺陷标题　智慧绍兴→到此一游→手写刻字，图片与画布在不同计算机中展示不同。

测试平台与浏览器　Windows 10＋Chrome或Firefox/Windows 7＋Chrome。

测试步骤

（1）打开智慧绍兴网站 http://www.roqisoft.com/zhsx。

（2）单击导航条中的“到此一游”→“手写刻字”，然后单击“体验手写刻字”。

（3）在不同的机器上选择图片，体验手写刻字。

期望结果　选择的图片与底色的画布能完美配合在一起。

实际结果　不同机器上选择的图片与底色的画布不能完美配合，有的出现空白画布，正常的如图5-22所示，不美观的情形如图5-23所示。

图5-22　图片与画布满屏，方便手写刻字（Windows 10＋Chrome）

图 5-23 图片与画布没满屏，部分画布区域空白(Windows 7＋Chrome)

专家点评

当程序员在设计手写刻字时，是基于自己的计算机进行测试、调试的，不同图片的拉伸与画布的配合在程序员自己的计算机上是正确的。但是换到另一台计算机，可能就有问题，这主要是用不同的浏览器解析，不同计算机的屏幕显示分辨率设计不一样，导致许多意想不到的结果。这就要求测试人员在测试时要留意跨平台和跨浏览器的测试结果。

拓展训练

找出以下网站的探索缺陷(测试人员在这些网站时，也可以换成自己的账户测试)。

(1) 百度搜索：www. baidu. com。

(2) 微软搜索：www. bing. com。

(3) QQ 空间：http://user. qzone. qq. com/470701012/infocenter。

(4) 新浪微博：http://weibo. com/roywang123。

(5) 腾讯微博：http://t. qq. com/roywang123。

(6) 豆丁文库：http://www. docin. com/roywang123。

(7) 新浪爱问知识共享：http://iask. sina. com. cn/u/1853705661/ish。

(8) 百度网盘知识共享：http://pan. baidu. com/share/home? uk＝2952985194。

提醒：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探索相关的缺陷。

读书笔记

读书笔记　　*Name*：　　*Date*：

励志名句：*God helps those who help themselves*.

自助者天助之。