乌云漏洞整理

整理者：李欣宜
文档源码地址：https://github.com/Lixinyi-DUT/Project-Wuhu
整理自乌云漏洞平台

第一周

(2015/6/29-2015/7/3)

6/29 中国移动某 IP 依旧可心脏滴血（可泄露用户服务密码等信息）

http://www.wooyun.org/bugs/wooyun-2015-0122764

提交时间 2015/6/25
确认时间 2015/6/29
漏洞 hash 183e27ad5344f8c03dfa1cb97a16be59
漏洞类型 系统/服务补丁不及时
简要描述 中国移动某 IP 存在 OpenSSL 漏洞 -（可泄露用户服务密码等信息）

heartbleed bug
心脏出血漏洞是出现在加密库 OpenSSL 1.0.1 (实现 SSL 与 TLS 协议) 上的程序错误，可允许攻击者读取服务器的内存信息，客户端和服务器都可能因为这个漏洞受到攻击。该漏洞得名于 TLS 协议 (Transport Layer Security) 和于 DTLS 协议 (Datagram Transport Layer Security) 中已成为标准的机制心跳扩展 (heartbeat extension)，它提供了一种测试和保持安全通信链路的方式，而无需每次都重新协商连接，但这种扩展没有进对输入行有效验证，即边界检查 (bounds check)，导致了缓冲区过读 (buffer over-read)，因此引发信息泄露。受影响的 OpenSSL 版本为 1.0.1 至 1.0.1f（含），而较早的版本和较新的版本均没有受到影响。

漏洞影响 约有 17% 通过认证机构认证的互联网安全网络服务器被认为容易受到攻击，导致服务器私钥和用户会话 cookie 及密码被盗。

补救措施 OpenSSL 版本 1.0.1g 增加了一些边界检查，以防止过度读取缓冲。例如，已添加了下列测试，以丢弃将引发心脏出血漏洞的心跳请求，阻止回复继续构建：

```
if (1 + 2 + payload + 16 > s->s3->rrec.length) return 0;
```

存在缺陷的服务器应及时升级系统和服务补丁，疑似受到攻击的这些应用服务的用户也被建议及时更换密码等信息，并获取系统的更新。一些网站推出了测试，检测给定的网站上是否存在心脏出血漏洞，比如Critical Watch 免费在线心脏出血测试器，Lookout Mobile Security 心脏出血探测器 (一个用于 Android 设备的应用程序，可确定设备使用的 OpenSSL 版本，并指出是否启用了有缺陷的心跳特性) 和Qualys (SSL 实验室的 SSL 服务器测试，不仅能查找心脏出血漏洞，还能找到其他位于 SSL/TLS 实现中的错误) 等。

6/30 TCL 某站后台弱口令导致整站 webshell 部分 VIP 会员信息泄露

http://www.wooyun.org/bugs/wooyun-2010-0123296

提交时间 2015/6/28
漏洞类型 后台弱口令
漏洞细节 图片见该漏洞的报告地址，这里不再给出

1. 进入网站http://tvp.multimedia.tcl.com/sysadmin/login.aspx
2. 使用弱口令 admin/toprand 登录

3. 修改上传设置，在图片类型中增加 asp 和 aspx 类型
4. 将测试文件上传 Shell，可以得到服务器的安全信息
5. 删除后发现 VIP 用户信息泄露

weak password
漏洞简述 弱口令通常是指容易被人猜测或者被破解工具破解的口令，一般仅包含简单的数字和字母。
weak password dictionary
可以通过弱口令字典以一定概率扫描获得。口令强度可以用微软提供的密码检查器进行评估。
补救措施 修改弱口令，升级后台系统。

7/1 华融证券某站补丁不及时导致 getshell（可内网渗透）

http://www.wooyun.org/bugs/wooyun-2015-0111837

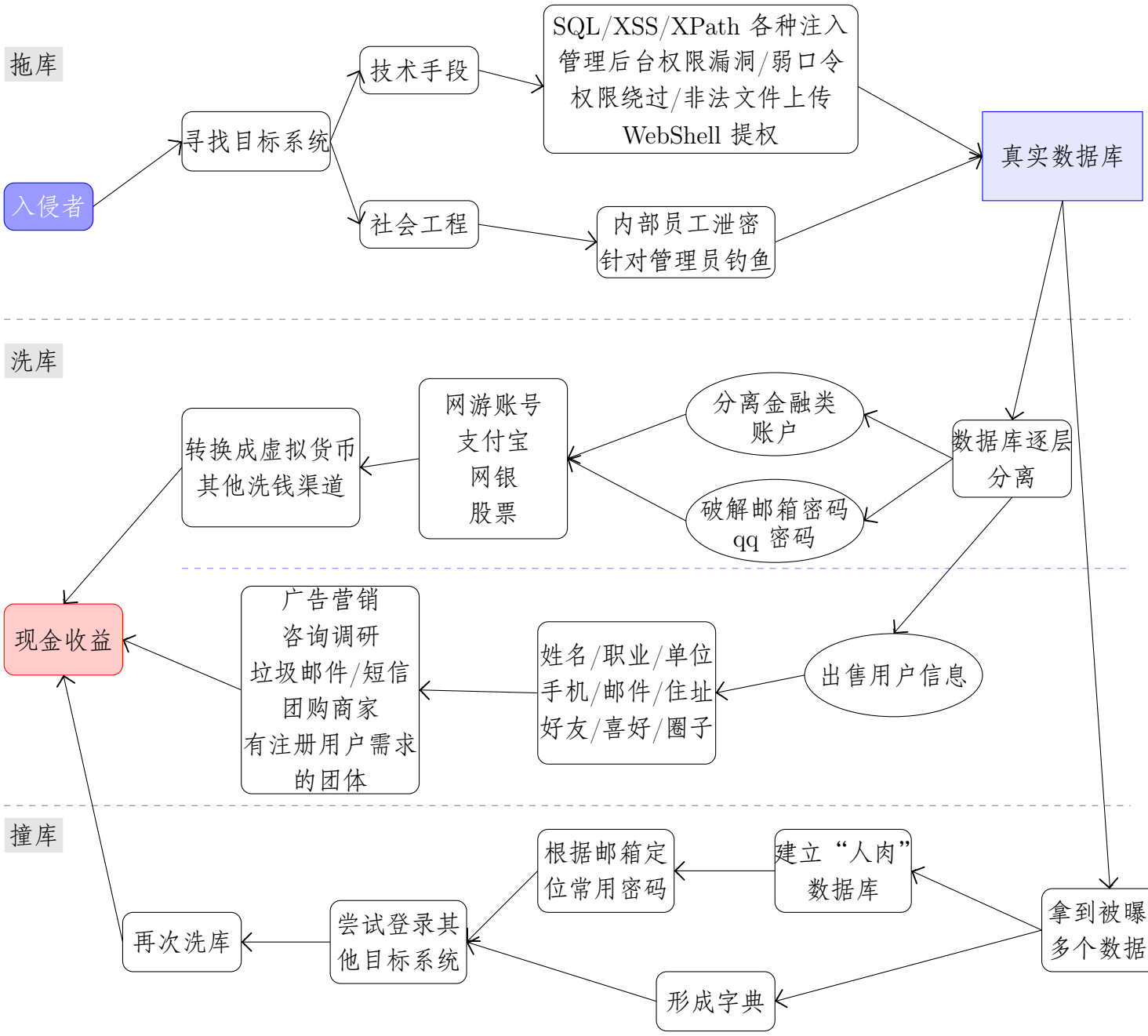
提交时间 2015/5/12
公开时间 2015/6/29
漏洞类型 成功的入侵事件
漏洞细节 站点：http://oa.hrsec.com.cn/login/Login.jsp?logintype=1
使用泛微 oa 找到弱口令进入，上传测试文件后，直接 getshell，获得了 root 权限。
漏洞简述 泛微 oa 系统存在着很大的缺陷，使用定制泛微 oa 的厂家的信息安全也因此受到了很大的威胁。不及时打补丁的使用厂家尤甚，SQL 注入和弱口令都可能使没有合法权限的入侵者进入系统后台，由于任意文件上传威胁的存在，攻击者可以上传制作好的测试脚本获得 root 权限。
WebShell 是以 asp、php、jsp 或者 cgi 等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。
入侵者通常会将这些 asp 或 php 后门文件与网站服务器 WEB 目录下正常的网页文件混在一起，然后就可以使用浏览器来访问这些 asp 或者 php 后门，得到一个命令执行环境，以达到控制网站服务器的目的，这就是 WebShell 攻击。
这种攻击也可以通过Pecker Scanner 工具进行检测。
补救措施 及时更新系统补丁，遵循最低权限原则。

7/2 趣分期撞库漏洞（成功 98 个）

http://www.wooyun.org/bugs/wooyun-2015-0114565

提交时间 2015/5/18
公开时间 2015/7/2
漏洞类型 设计缺陷/逻辑错误
漏洞细节 撞库接口：http://www.qufenqi.com/login 频繁测试受到限制时换 IP 列表继续测试
漏洞简述 拖库攻击指入侵有价值的网络站点，把注册用户的资料数据库全部盗走的行为。取得大量的用户数据之后，黑客会通过一系列的技术手段和黑色产业链将有价值的用户数据变现，这通常也被称作洗库。最后黑客将得到的数据在其它网站上进行尝试登陆，叫做撞库，因为很多用户喜欢使用统一的用户名密码。
为了应对这种攻击，有时企业会在登录页面加上验证码，然而识别图像验证码的脚本并不难获得，所以收效甚微。与之类似，对于 IP 和输入密码错误次数限制也是出于同样的考虑，但还是难以防止有针对性的恶意攻击。
补救措施 ① 对于用户来说，尽量不要在不同的网站使用统一的用户名和密码，如果有使用，那么一旦发现其中某个网站的信息泄露，立即更换其他站点使用的密码。② 对于应用的运营商，除了增强

数据库常规的安全手段，也可以从多维度入手防止撞库扫号，比如增加手机验证码验证，或者使用 Flash Cookies 代替 Cookies。



7/3 上海虹桥火车站 Wi-Fi 认证设计不当导致绕过漏洞

http://www.wooyun.org/bugs/wooyun-2015-0112807

提交时间 2015/5/8
公开时间 2015/6/26
漏洞类型 设计缺陷/逻辑错误
漏洞细节 填手机号，发送验证码之后，抓包。可以看到返回信息中直接包含了验证码。这样也就绕开了短信接收验证码然后再输入验证的过程，无法进行身份验证。
漏洞简述 Wi-Fi Portal 认证是开放 WLAN 中验证用户身份的一种方式，我校的无线网络 DLUT 也是使用的这种认证机制。在机场、火车站、咖啡厅等公共场所的 WLAN 一般应用挑战/应答认证对接入者身份进行验证，比如短信接收验证码。这种认证中，用户填写的个人信息请求通过 POST 方法传

Challenge-Response authenticat
POST method

给服务器，而这个POST 请求的数据包中就含有用户的个人信息，在 Web 条件下，可以通过 IE 或者 Chrome 自带的抓包工具获得，我曾经利用过这个方法写了一个实现 DLUT 后台自动登录的应用，也是利用了 DLUT 数据包明文传输的缺陷。

补救措施 数据包中的验证码加密，或者在认证中心建立可靠的数据库管理这些验证码，而避免验证信息在数据包中传递。

第二周

(2015/7/6-2015/7/10)

7/6 联想手机 VIBE UI 部分版本设计缺陷绕过锁屏读所有联系人

http://www.wooyun.org/bugs/wooyun-2015-0105688

提交时间 2015/4/3
公开时间 2015/7/6
漏洞类型 设计错误/逻辑缺陷
漏洞细节 ① 机型：A355e ② VUBE UI的版本：A355e_S020_20141229 ③ 向测试手机拨打电话，然后这个时候往上滑动，进入自定义短信回复界面 ④ 进入短信回复界面以后，在联系人框那里随便输入一个数字，比如一般手机号开头都是 1，这样就可以读到所有联系人了。
漏洞简述 iOS7也曾经出现过可以绕过锁屏的安全漏洞，而 Android系统由于各个厂家的定制 UI，对安全问题的重视程度不一，也经常存在同样的问题。Android应用单词锁屏也存在这个漏洞，下拉状态栏可以直接进入其他应用而绕过锁屏，强迫自己背单词不玩手机的目的也就无法达到。
这种漏洞存在的原因很多，在 Android 4.3中`com.android.settings.ChooseLockGeneric`是负责更改系统的解锁方式的类，再解锁确认后它的成员`mPasswordConfirmed`被设置为`True`，这个成员没有私有保护，从外部启动`ChooseLockGeneric`再设置这个参数，设定密码策略为`PASSWORD_QUALITY_UNSPECIFIED`(对密码没有要求)，系统就会自动清除锁屏密码，更多其他方法可以自行查阅。
补救措施 ① 把逻辑设置为自定义回复短信的时候需要输入解锁密码 ② 学习华为的最新系统，把在通话界面实现自定义回复短信的功能用另外的模块实现，在这个模块中只有短信内容框别的什么都没有。③ 参考 Android原生系统，对`mPasswordConfirmed`进行保护。

7/7 墨迹天气可以重置任意用户密码

http://www.wooyun.org/bugs/wooyun-2015-0115443

提交时间 2015/5/22
公开时间 2015/7/6

漏洞类型 网络设计缺陷/逻辑错误

漏洞细节 ① 找回密码页面http://uc.mojichina.com/findpwd/byphone#填写手机号和验证码，点下一步 ② 网页自动跳转到页面http://uc.mojichina.com/findpwd/verifysms ③在同一个浏览器中再打开网页http://uc.mojichina.com/findpwd/resetpwdbyphone#，就直接进入重置密码界面了，不需要短信验证码的确认。

URL redirection

漏洞简述 这是程序设计的严重缺陷，致使边界绕过，也类似URL 重定向跳转漏洞。在一个页面认证完成之前就可以通过重定向跳转到本应该完成认证后出现的页面，这是认证设计上完全可以避免的漏洞。

7/8 苏宁易购服务器支持 EXP 密码套件可 SSL FREAK 攻击解密通信流量（含 poc）

http://www.wooyun.org/bugs/wooyun-2015-0106650

提交时间 2015/4/8

公开时间 2015/7/8

漏洞类型 默认配置不当

漏洞细节 苏宁易购服务器因支持 EXP 密码套件，遭受 SSL FREAK 攻击，中间人可在线解密通信流量（获取到登陆凭证等敏感信息）

- 服务器会接受 EXP-DES-CBC-SHA(SSLv3、TLSv1)、EXP-RC2-CBC-MD5(SSLv3、TLSv1)、EXP-RC4-MD5(SSLv3、TLSv1)这三种出口级密码套件 (EXP 密码) 。

export-grade cipher suite

- 以登陆页面https://passport.suning.com/ids/login为例，中间人在受此漏洞影响的客户端（如还未打补丁的 IE、Chrome、Safari、Opera on Mac OS 等）访问页面时，如果有中间人发起 FREAK 攻击，将 client hello消息中的密码套件改为 EXP 类别，那么服务器会选择使用 EXP 级别的密码套件进行通信，发送 512bit RSA 公钥给客户端。

man in the middle

Rivest-Shamir-Adleman public key

- 客户端用这个 512bit 的公钥加密预主密钥，服务器收到后用私钥解密出预主密钥，两方依据此秘密信息同时计算出后续通信的密钥。

pre-master secret

- 而对于中间人来说，如果其可以分解服务器发送的 512bit 的公钥，那么即可计算出私钥，从而也同样可以得到预主密钥，进而算出通信的密钥，解密客户端和服务器的通信内容。

- 对于suning.com服务器来说，目前支持 EXP 密码套件的主机有 18 台，每台有一个固定的 512bit 的公钥，那么对于攻击者来说，只要分解其中的一个公钥，不管每次客户端 DNS 查询到的是哪台主机，中间人都可以连接到已分解公钥的那台主机进行通信获取发送给客户端的必要信息，从而成功建立与客户端和服务器的通信。

Factoring Attack on RSA-EXPORT Keys

漏洞简述 这个漏洞编号为 CVE-2015-0204，人们把它命名为FREAK。攻击者可以拦截服务器与易受攻击的客户端间的 HTTP连接，并迫使他们使用弱加密。这里有一个比较八卦的说法：90 年代美国政府要求出口货物使用弱加密的“出口级”加密方式，这种加密方式可以便于情报机构和特殊机构破解利用，而美国本土的产品使用更加强的加密方式。后来这一出于这一政治需求的间谍手段被废弃，但这种弱加密的出口级加密方式依然存在并且被攻击者作为了 FREAK 漏洞。常见的流程类似于本案例中的攻击，修改存在缺陷的客户端发出的 Hello消息把要求标准 RSA 加密改为请求“出口级的 RSA 加密”，出于OpenSSL/Secure 传输的漏洞，客户端会接受服务器发来的 512 比特的弱加密的 RSA 公钥，由于较 90 年代来说，计算机的计算性能大大提高，得到弱加密的 RSA 公钥以后可以计算出私钥

weaken encryption

并对客户端发出的信息进行修改。

补救措施 服务器停止支持 EXP 级别的密码套件，如果一定要支持，那么在通信时实时生成 512bit 的公钥，或者提前生成一批密钥，在使用过一段时间后更换。总之，要保证密钥使用的周期不超过 512bit 密钥分解需要的时间。

参考资料 ① The FREAK bug in TLS/SSL - what you need to know: https://nakedsecurity.sophos.com/2015/03/04/the-freak-bug-in-tlsssl-what-you-need-to-know/

② “历史遗留”漏洞：浅析新型 SSL/TLS 漏洞 FREAK: http://sec.chinabyte.com/216/13280716.shtml

③ Tracking the FREAK Attack：https://freakattack.com/ (可以在线测试浏览器是否受到 FREAK 威胁)

④ 'FREAK' —New SSL/TLS Vulnerability Explained：http://thehackernews.com/2015/03/freak-openssl.html

7/9 w3cschool.cc 菜鸟教程任意代码执行

http://www.wooyun.org/bugs/wooyun-2015-0112029

提交时间 2015/5/25

公开时间 2015/7/9

漏洞类型 命令执行

漏洞细节 漏洞出在在线执行代码工具http://tool.w3cschool.cc/languages/online.php?language=python, 可以执行任意代码，比如 `os.system()`函数。这里的语言仅测试 python，由于对敏感函数没有过滤直接执行，可以写一个脚本在这个在线编译平台上获取 shell 权限。

漏洞简述 根据这个报告，我们来看一下其他几个我比较熟悉的在线编译平台的表现（依然仅限 python）

① Codepad在线编译器，执行结果:`Disallowed system call: SYS_fork`，显然对敏感操作进行了保护。

② DataJoy旨在建立方便数据科学研究的在线编译、分享平台，支持 python 和 R 语言，执行结果：`0`，由于该网站主题是利用 python 语言解决数据分析问题，所以对 `os`模块进行了保护。

③ CodeSkulptor莱斯大学 (Rice University) 为课程 python 交互设计导论用 js 制作的在线编译平台 (需翻墙)，内置自制的特色交互模块 `SimpleGUI Module`，由于课程性质的缘故，阉割了很多无关模块，包括 `os`，所以并没有受到影响。

补救措施 对敏感函数进行过滤

7/10 人人投某漏洞可刷无限瓶饮料过夏天

http://www.wooyun.org/bugs/wooyun-2015-0116144

提交时间 2015/5/25

公开时间 2015/7/9

漏洞类型 设计缺陷/逻辑错误

漏洞细节 只要注册成功，就送饮料。http://wap.renrentou.com/friendgodeuser/success?dns=534230，因为没有对 dns 进行过滤，所以这个参数`dns=`后面可以任意修改，获得不同的兑换码，然后去自动贩卖机兑换。

漏洞简述 厂家虽然已经表示忽略，但是页面已经打不开了，不能继续利用这个漏洞了。嘴上说着不要，实际早已傲娇地修复了漏洞。类似的漏洞还存在于软院的旧学院网，以及新学院网的部分功能http://ssdut.dlut.edu.cn/info/1116/3946.htm 这个参数也是可以任意篡改实现任意跳转的，所幸我院

对安全的要求不高，没有从验证从指定入口进入的限制，否则这也是十分危险的。
补救措施 执行 dns 参数过滤，对 url 重定向进行认证。

第三周

(2015/7/13-2015/7/18)

7/13 QQ 邮箱 Android 客户端存在存储型跨站脚本攻击漏洞

http://www.wooyun.org/bugs/wooyun-2015-0107526

提交时间 2015/4/22
确认时间 2014/7/12
漏洞类型 远程代码执行
漏洞细节 ① 我们首先自己搭建一个原始的服务器，存在很多 XSS 漏洞的邮件服务器。对 QQ 手机邮箱进行 XSS 测试，发现 QQ 邮箱进行测试后发现存在 XSS 漏洞。测试后发现 QQ 邮箱客户端对 script,img，iframe 等危险标记没有过滤，导致 XSS 漏洞。② 先用自己的邮件服务器发一个所有其他测试邮箱都能收到的邮件。邮件中插入恶意代码

```
<script>alert(/3/)</script>
<img src=1 onerror=alert(888) >
```

发送我们的邮件到自己的邮箱、qq 邮箱、163 邮箱、搜狐邮箱、新浪邮箱等。③ 把我们各种邮箱在 QQ 邮箱客户上绑定。④ 测试发现，QQ 邮箱测试不能执行 XSS 代码，可能 QQ 的邮件在自己的邮件服务器上做了过滤，导致不能执行。其余邮箱都能执行。

漏洞简述 XSS (Cross-Site Scripting) 又称跨站脚本，通常存在于 Web 应用，攻击者可以在 Web 页面注入客户端脚本 (Client-side scripting) (HTML 代码)，通常用于绕过获得控制权限，比如利用同源政策 (same-origin policy)，浏览器允许包含第一个页面的脚本进入第二个页面。恶意用户在公共区域提交恶意表单，其他用户访问时嵌入 Web 页面的恶意脚本将执行，获取用户的个人信息。
威胁缓解 ① 根据语境输出输入的编码和转义 ② 对不受信任的 HTML 输入慎重认证 ③ 注意 Cookie 安全 ④ 禁用脚本 ⑤ 紧急防御技术，包括内容安全政策、js 沙盒和自动转义模板 ⑥ 扫描服务
相关内容 BeEF (Brower Exploitation Framework) 是个开源的渗透测试工具，可用于模拟 XSS 攻击。http://beefproject.com/

7/14 中科新业网络哨兵跳过验证修改管理员密码

http://www.wooyun.org/bugs/wooyun-2015-0107127

提交时间 2015/4/10
确认时间 2015/7/14
漏洞类型 权限控制绕过
漏洞细节 中科新业网络哨兵跳过验证随意修改管理员密码，可进入后台任意查看审计信息。V4,V5 版本均存在问题。部分审计服务器暴露于公网，可被搜索引擎收录。①先点击忘记密码，找到对应版本密码找回页面地址，然后直接提交 post 请求：例如地址`https://**.**.**/ucenter/stgl/pwd_question.php` ②提交

```
https://**.**.**/ucenter/stgl/pwd_question_s.phpnewpwd=admin123
&newpwd1=admin123&uid=admin&passwd=&questions=&answer=&step=4&act=forget&lang=1
```

即可直接将 admin 用户密码修改为 admin123，无视密码提示问题。
补救措施 加校验，不信任任何用户提交的数据

7/15 搜狐焦点旗下搜狐家居可劫持任意账号（flash 劫持案例）

http://www.wooyun.org/bugs/wooyun-2015-0116384

提交时间 2015/5/26
公开时间 2015/7/15
漏洞类型 CSRF
漏洞细节 ①http://mpsohu.com/web/personal/get 上传身份证处未过滤，且文件上传到了 itc 信任域下，查看源码得到 flash 链接：http://sucimg.itc.cn/avatarimg/b9242b2cbe19450a9347accbc8dcc639_1432645407636 ②接下来构造 POC 进行操作，这里用修改资料证明，得到请求包和 POC ③用 flash 跨域理论上是可以模拟出用户的任何操作的，即使是在某些有 token 的情况下
漏洞简述 很多上传文件的后端逻辑在实现时，仅仅验证了文件后缀名和 Content-Type，没有对上传文件的内容进行验证。object 标签在包含 flash 文件时没有对嵌入的文件后缀进行判断。也就是说，只要文件内容包含了正常的 flash 文件代码，就能够被 object 标签成功加载并执行。而 ActionScript 中又提供了多种 API 能够让 Flash 发送网络请求。flash 跨域数据劫持正是利用了目标网站的文件上传逻辑没有验证文件内容、上传的文件没有做域隔离处理、服务端没有强制设置 Content-Disposition 响应头，以及访问上传的文件没有 session 限制，构造一个 poc swf 文件能够对外发送 http 请求，将之前写好的 swf 文件后缀修改为 jpg 并上传，服务端没有检查文件内容，文件上传成功。通过之前构造的 html 页面，使用 object 包含上面的链接，swf 文件能够被正常的执行，当其他用户访问该页面，会以该用户的身份打开指定的页面，造成跨域数据劫持，此时 Anti-CSRF 已经形同虚设，可以获取 CSRF Token，访问特权页面，进行特权操作。
补救措施 ①涉及用户操作的请勿在 crossdomain 里配置 ②上传文件到信任域时验证文件内容