



探寻业务安全中的极(基)点

--江南天安猎户实验室.张洪骏





初探电商

电商安全现状

业务安全漏洞分析

如何应对业务安全漏洞





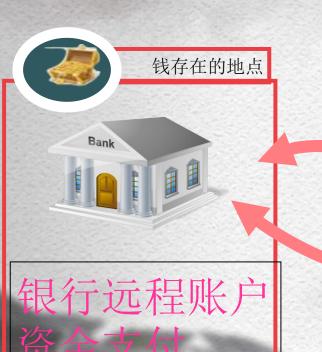
电子商务是基于计算机技术、

网络技术、通信技术和应用软件开发基础上的新兴的、充满生气的经济活动。

电子商务主要基于Internet开展,Internet的特点就是随时随地、方便易用、即时互动并且结合多媒体传递,这些为电子商务的信息流、商流(如电子合同)、物流信息的交互与共享、全天候跨区域与低成本处理提供了很好的技术支撑。因此,电子商务无论是在中国还是在全球,都在快速的发展。











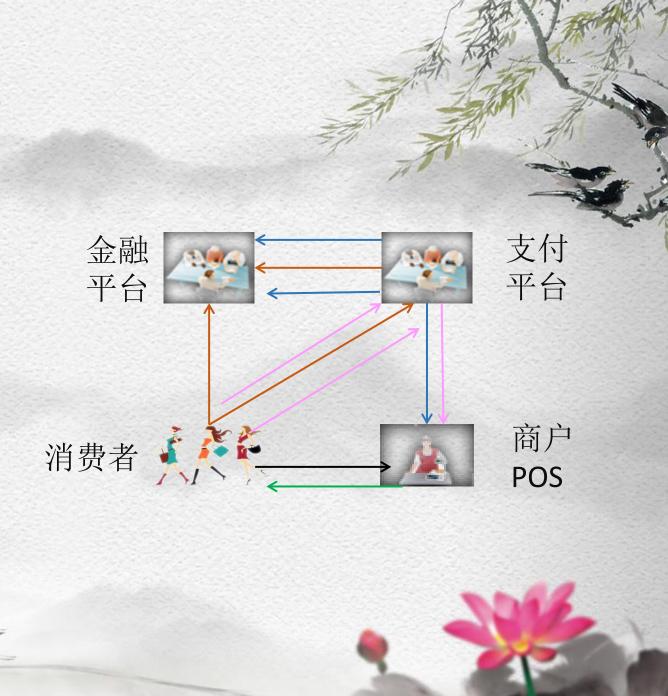






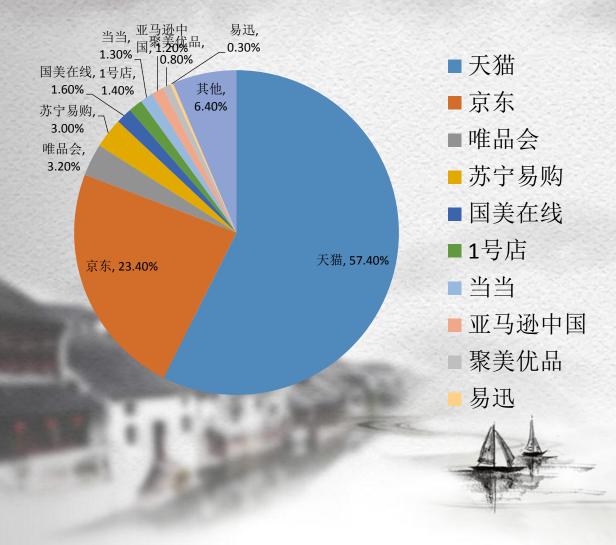
预授权交易流程:电子交易实体间的关系

- (1)创建账户
- (2)注册会员
- (3)账户绑定
- (4)浏览商品提交订单
- (5)预授权请求
- (6)预授权请求
- (7)预授权凭证
- (8)提供商品或服务
- (9)支付请求
- (10)转发支付请求
- (11)支付凭证





2015年,中国 B2C 网络零售市场.市场份额



市场规模: 2015 年,中国网络零售市场交易规模 38285 亿元,同比增长 35.7%。



电商安全现状

业务安全漏洞分析

如何应对业务安全漏洞





电子商务现状

2014年全年,360网站安全检测平台共扫描各类网站164.2万个,其中存在安全漏洞的网站61.7万个。从行业来看,电子商务类网站存在高危漏洞的比例最高,达到26%,银行类网站安全性相对较高。-

-----《2014年中国网站安全报告》

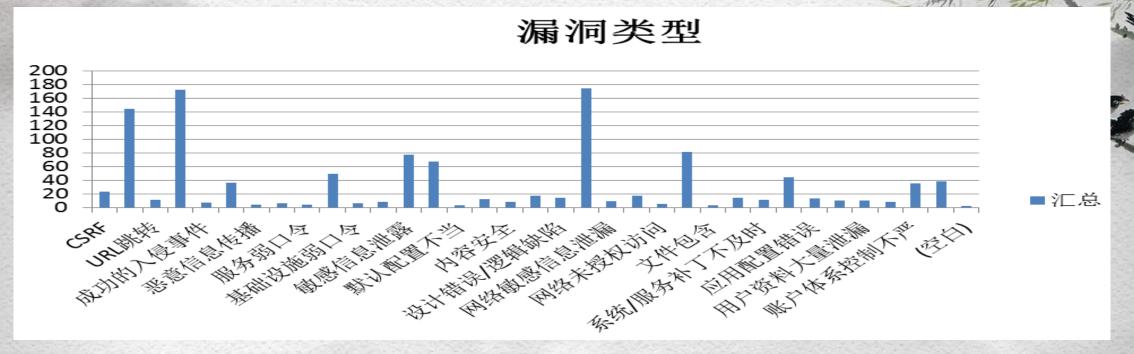
中国平均每天有24.5个电商网站遭受入侵和攻击,在针对电商网站实施的侵害中,利用网站安全漏洞入侵占绝大多数 ,占比97%;另外3%为针对电商网站的CC攻击等攻击行为。

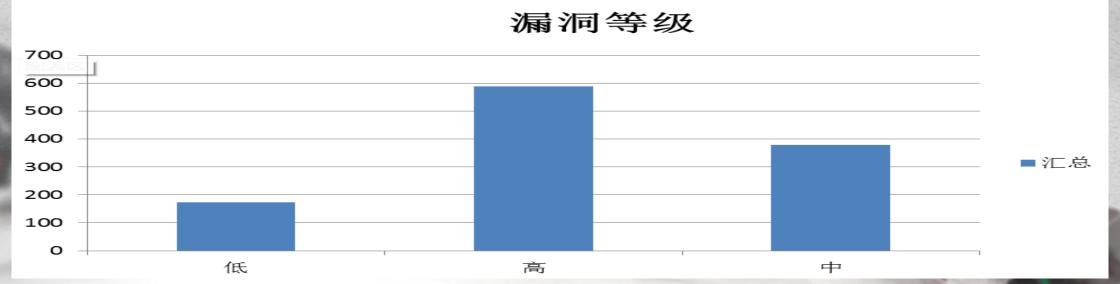


-----《2013年中国电商行业网站安全检测报告》



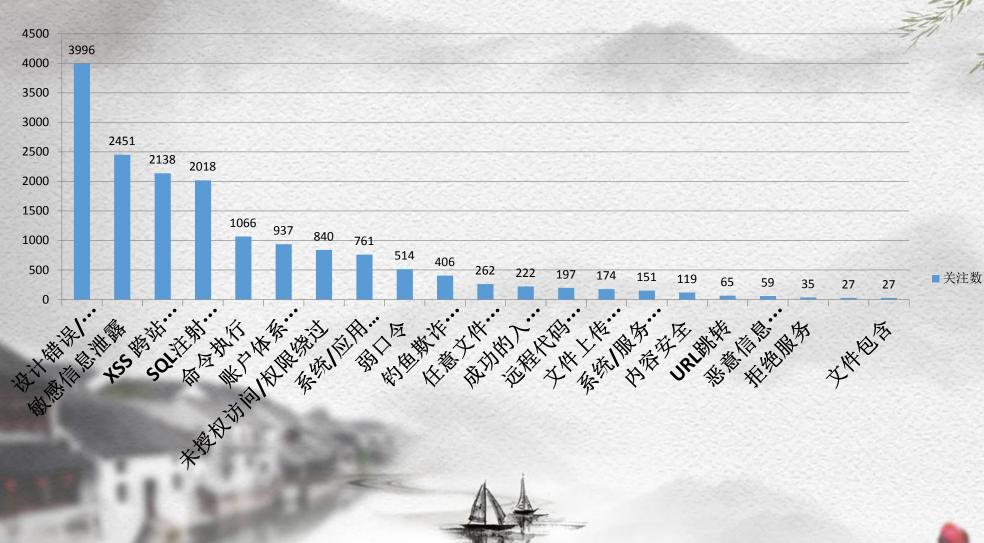




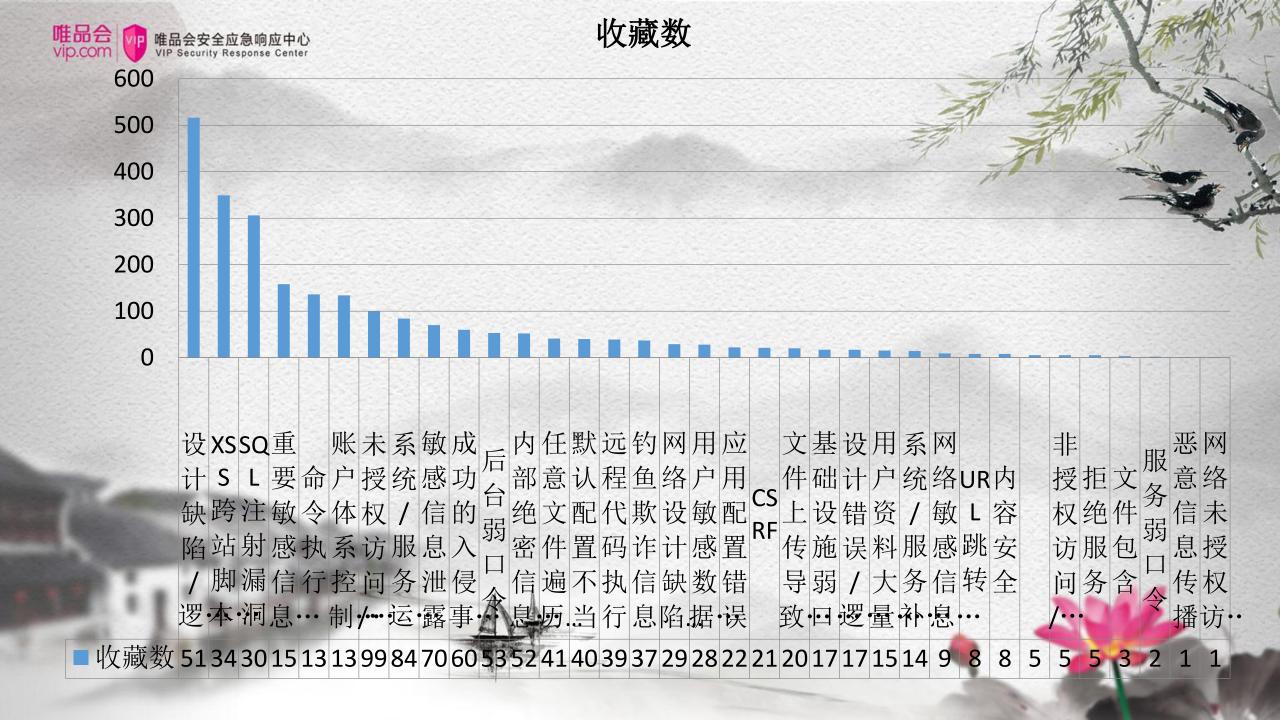






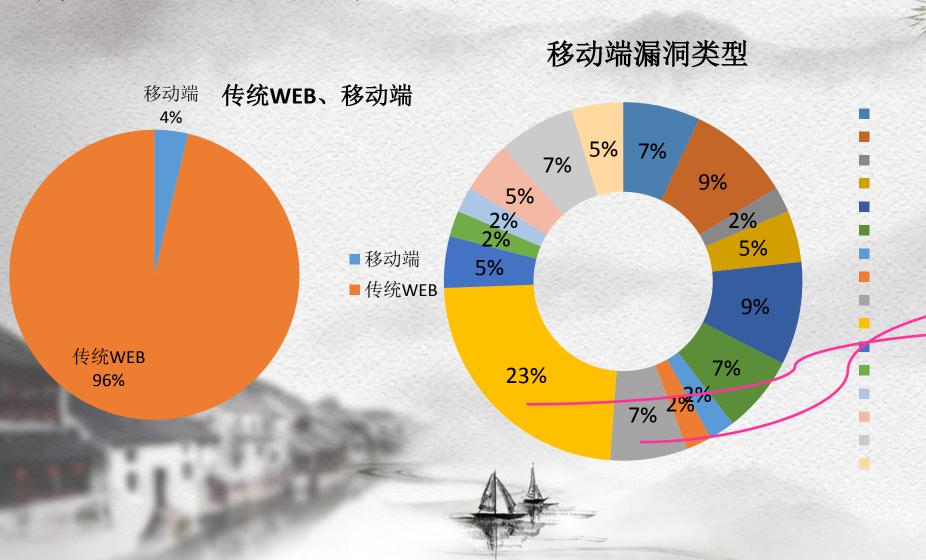


漏洞类型	关注数
	27
CSRF	101
SQL注射漏洞	2018
URL跳转	65
XSS 跨站脚本	2037
攻击	2037
成功的入侵事	222
件	222
钓鱼欺诈信息	406
恶意信息传播	59
非授权访问/	24
认证绕过	24
服务弱口令	25
后台弱口令	410
基础设施弱口	79
令	7.5
拒绝服务	35
敏感信息泄露	639
命令执行	1066
默认配置不当	149
内部绝密信息	381
泄漏	301
内容安全	119





传统WEB---移动端的兴起



SQL注射漏洞 XSS 跨站脚本攻击 成功的入侵事件 非授权访问/认证绕过 拒绝服务 敏感信息泄露 命令执行 默认配置不当 设计错误/逻辑缺陷 设计缺陷/逻辑错误 未授权访问/权限绕过 应用配置错误 用户敏感数据泄漏 远程代码执行 账户体系控制不严 重要敏感信息泄露



电商安全现状

业务安全漏洞分析

如何应对业务安全漏洞



0x04用户 输入合规 性

0x05密码 找回漏洞 0x06验证 码突破

0x07业务

授权安全

0x03业务 数据篡改

0x02业务 一致性安 全

0x01身份 认证安全

业务漏 洞挖掘

0x08业务 流程乱序

> 0x09业务 接口调用

> > 0x10时效 绕过测试





0X01身份认证

暴力破解

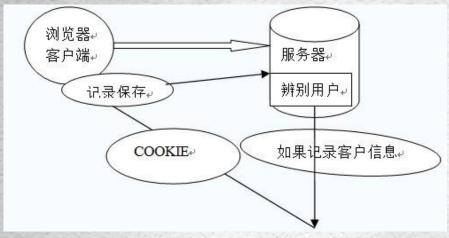
- *无验证码限制,或验证码可多次使用,或有验证码但仅作当前页面验证,接口无视
- *使用已知用户对密码进行暴力破解或者用一个通用密码对用户进行暴力破解



验证码:



Cookie



简要描述:

益云广告平台任意帐号登录

详细说明:

只需要添加cookie

yibouid=数字 即可登录任意用户帐号!

漏洞证明:

通过遍历 找到一个官方管理的ID 291

Session



一些网站对于用户是否成功登录不是看用户名与密码是否与数据库里面的匹配,而是看cookies是否为空或session是否为true。这样的问题的假设就是开发者认为用户能够登录,那么cookies就不会为空或session就不会为false。但是逻辑缺陷很明显,那么只要能知道用户ID,然后构造一个cookies或让session值为true就可以绕过这样的认证了。





0X02业务一致性安全







0X02业务一致性安全

手机号篡改

订单号篡改

用户id篡改

Cookie: language=zh CN; PHPSESSID=c24b6cb1b5792a92c552794865eb4ce3

sk 5D=150

商品编号篡改

其他业务篡改

www.woovun.org

抓包修改手机号码参数为 尝试,例如在办理查询页 自己的号码然后抓包,修 码参数为其他人号码,登 查询其他人的业务



www.gzl.com.cn/Users/Or	rder/Groups.aspx?OrderId=1056	
会 设为首页	夏 经营许可证 新版介绍	
www.gzl.com.cn/	然后修改审计员密码,抓包,将referer处的auditor和post的数据里面的auditor一律修改为admin,也就是管理员号,2处修改完后的数据包如下图:	灵师
1	Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts	
4	Intercept History Options	
	Request to https://202.108.90.133.443 Forward Drop Intercept is on Action Comment this item	
	Raw Params Headers Hex POST /user/update HTTP/1.1	
,	Accept: text/html, application/xhtml+xml, */* Referer: https://202.108.90.133/user/edit/account/admin Accept-Language: zh-CN	
	User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip, deflate	
•	Host: 202.108.90.133 Content-Length: 275 Connection: Keep-Alive	
	Cache-Control: no-cache	

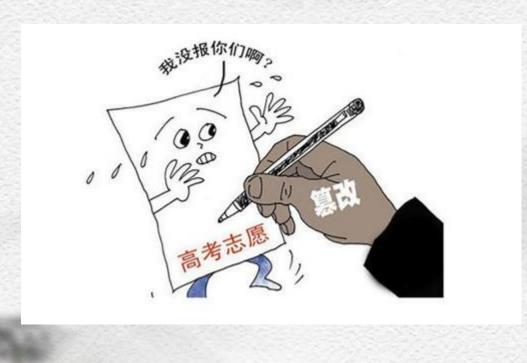
user*5Baccount*5D=admin&user*5Bname*5D=Admin&user*5Bpassword*5D=4rfv#EDC2vsx!QAZ&user*5Bpassword.confirm*5D=Arfv#EDC

2 wsx 10A2&user & 5Bmail & 5D = admin@example.com&user & 5Broles & 5D = ADMINISTRATORS & user & 5BallowLoginIp & 5D

jQuery110107779618303757161_1430405784487({"content":{"rows":[]},"message"<mark>:"操作成功",</mark>"state":1})



0X03业务数据篡改







0X03业务数据篡改

金额篡改

源代码

数量篡改

漏洞根 商品信息: 数量 总价 商品编号 ■缺陷编-16款哈弗H9背负式尊贵型_极地白外观_灰黑内 103257 ¥ 5800.00 ¥ 5800.00 漏洞标题 运费: ¥0.00: 总价: ¥5800.00 ■相关厂i 支付方式: ◎ 线上支付 ■漏洞作: 结算信息: ■提交时 ■ POST b 应付金额: ¥5800.00 参数 购车人信息: 参数 购车人: 请填写真实姓名 * 该姓名需要与最终购车发票上一致 baidaJso 手机号: 请填写正确的手机号 * 用于销售商与您联系,请确保准确 本次应付(整车订金): ¥5000.00 余款总金额: ¥800.00 (线上支付) (线下支付)

notify*2Fsync*2F20 bankInput=1&interf &mac=1cd([]Obd332c0

> 服务器仅在页面通过js 脚本限制,未在服务器 端校验用户提交的数量

▶ 提交订单 Www.wooyun.org

《 返回购物车修改



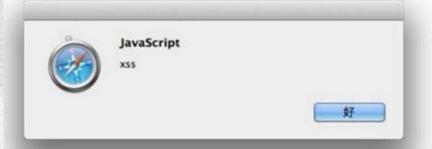
0X04用户输入合规性





跨站XSS

注入



其他交互功能导致的应用漏洞

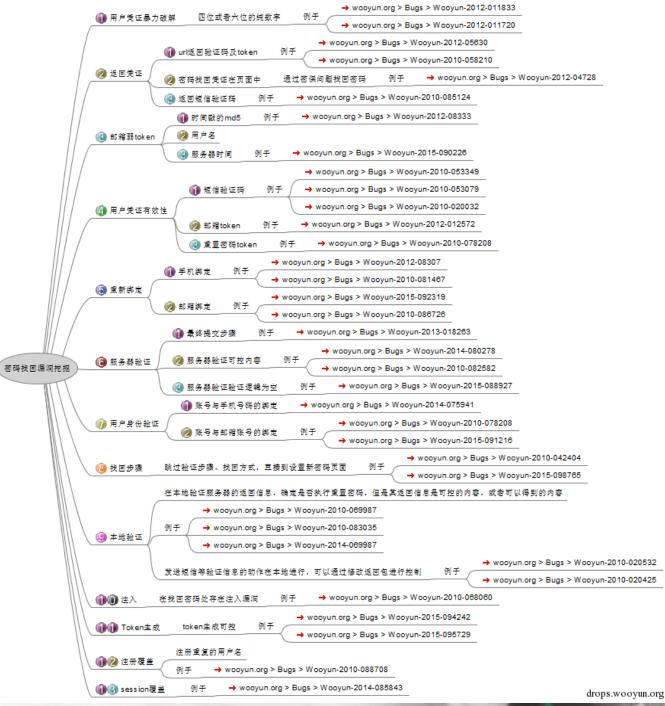




0X05密码找回漏洞

- i.首先尝试正常密码找回流程,选择不同 找回方式,记录所有数据包
- ii. 分析数据包, 找到敏感部分
- iii. 分析后台找回机制所采用的验证手段
- iv. 修改数据包验证推测









0x06 验证码突破

暴力破解

使用burp对 特定的验证 码进行暴力 破解

客户端回显

当客户端有需要和服务器进行交互,发送验证码时,即可使用firefox按F12调出firebug就可看到客户端与服务器进行交互的详细信息

重复提交、忽略次数

抓取携带验证码的数据 包不断重复提交,例 如:在投诉建议处输入 要投诉内容信息,及 验证码参数,此时抓包 重复提交数据包,查看 历史投诉中是否存 复提交的参数信息





0x07业务授权安全

未授权访问



未授权勿入

用户在没有通过认证授权的情况 下能够直接访问需要通过认证才 能访问到的页面或文本信息。可 以尝试在登录某网站前台或后台 之后,将相关的页面链接复制于 其他浏览器或其他电脑上进行访 问,看是否能访问成功





水平越权

垂直越权

开发人员在对数据进行 增、删、改、查询时对客 户端请求的数据过分相信 而遗漏了权限的判定





漏洞概要

缺陷编号: WooYun-2015-108184

漏洞标题: 淘美网逻辑漏洞美女QQ、手机号等信息免费任意看(1分钱都不给)

www.3need.com/index.php?controller=ucenter&action=online_recharge

相关厂商: 淘美网

漏洞作者: 提莫

提交时间: 2015-04-15 19:11

公开时间: 2015-05-30 19:12

漏洞类型: 设计缺陷/逻辑错误

危害等级: 高

自评Rank: 20

漏洞状态: 未联系到厂商或者厂商积极忽略

请填写冲值金额

wooyun

123

请选择冲值方式

◎支付宝



网银支付:











http://www.3need.com/index.php?controller=site&ac =payok&out_trade_no=充值订单号

com 国家真实美女资料库

明星图片集锦 人体艺术欣赏 两性生活话题 淘美专题资讯



充值成功!



墨茕Ⅴ□

昵称: 墨茕



查看资料

(每次花费0.1元)

昵称: 念念, 年年

编号: 75

年龄: 25岁

地点:湖北省

(每次花费0.1元) 查看资料

给她送花 (每次花费0.1元)

给她写信 (每次花费0.1元)

(每次花费1.0元) 查看联系方式

1.联系方式

电话: 1858 06257



158 = 1048

念念, 年年 🗸 🚨

QQ:

邮箱: y.sl 19@hotmail.com







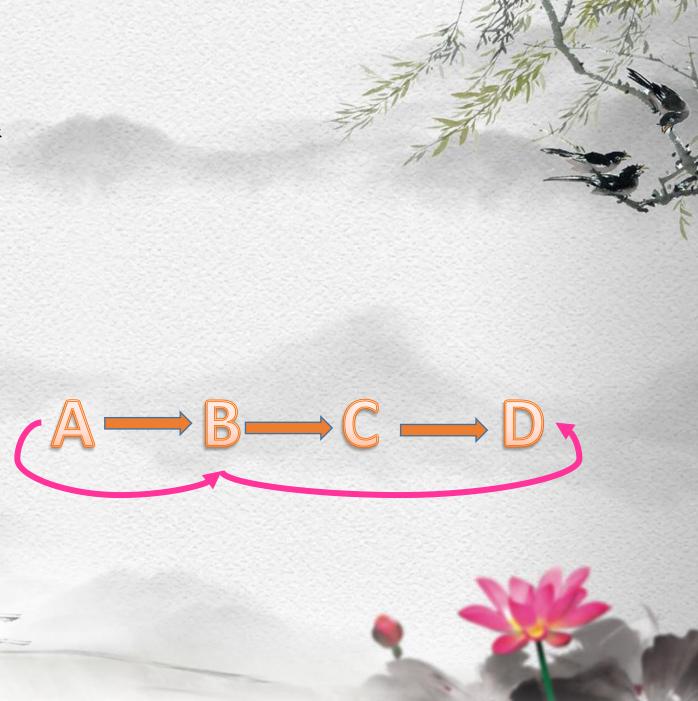


0x08业务流程乱序

a) 部分网站逻辑可能是先A过程后B过程然后 C过程最后D过程

b) 用户控制着他们给应用程序发送的每一个请求,因此能够按照任何顺序进行访问。于是,用户就从B直接进入了D过程,就绕过了C。如果C是支付过程,那么用户就绕过了支付过程而买到了一件商品。如果C是验证过程,就会绕过验证直接进入网站程序了。

c) 案例:





0x09业务接口调用安全



恶意注册/评论

短信轰炸

其他



drops.wooyun.org

内容编辑

</value></param><param><key>sendData/insrotxtk/key><value>您正在进行更改手机银行手机号码操作,验证码为: XXXXXXxx



0x10 时效绕过测试

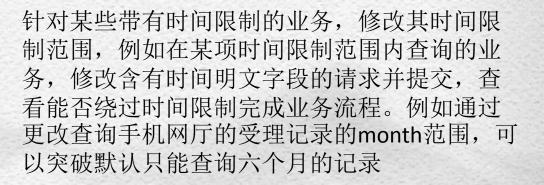
时间刷新缺陷

12306网站的买票业务是每隔5s,票会刷新一次。但是这个时间确实在本地设置的间隔。于是,在控制台就可以将这个时间的关联变量重新设置成1s或者更小,这样刷新的时间就会大幅度缩短(主要更改autoSearchTime本地参数)。

案例:

WooYun: 12306自动刷票时间可更改漏洞

时间范围测试



初探电商

电商安全现状

业务安全漏洞分析

如何应对业务安全漏洞





C 保密性 (Confidentiality) —— 确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体。

完整性(Integrity)——确保信息在存储、使用、传输过程中不会被非授权篡改,防止授权用户或实体不恰当地修改信息,保持信息内部和外部的一致性。

可用性 (Availability) —— 确保授权用户或实体对信息及资源的正常使用不会被异常拒绝,允许其可靠而及时地访问信息及资源。







用户输入合规性

可用性

验证码突破 业务授权安全

保密性

身份认证安全 业务接口调用安全

时效绕过测试 业务一致性安全 密码找回漏洞

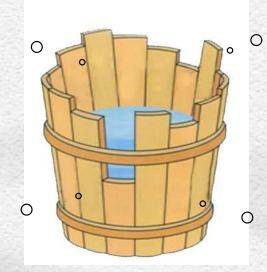
完整性

业务数据篡改

业务流程乱序

















Mary的爸爸有5个女儿:

第1个女儿 Nana,

第2个女儿 Nene,

第3个女儿 Nini,

第4个女儿 Nono,

第5个女儿?????











不忽略任何可能出现风险或者歧义的细节

保障企业以及消费者安全最大化

建设一个更加安全、高效的电商环境



感谢您的聆听!



