



看雪 **2017** 安全开发者峰会

Kanxue 2017 Security Developer Summit

2000-2017



浅析WEB安全编程

汤青松@中国婚博会

常见漏洞有哪些？

代码注入

CSRF

0元支付

短信轰炸

密码找回

本地限制

验证码爆破

SQL注入

XSS跨站

文件上传

文件包含

命令执行



目录大纲

一、SQL注入

二、XSS跨站

三、请求伪造

四、越权漏洞

五、支付漏洞



SQL注入

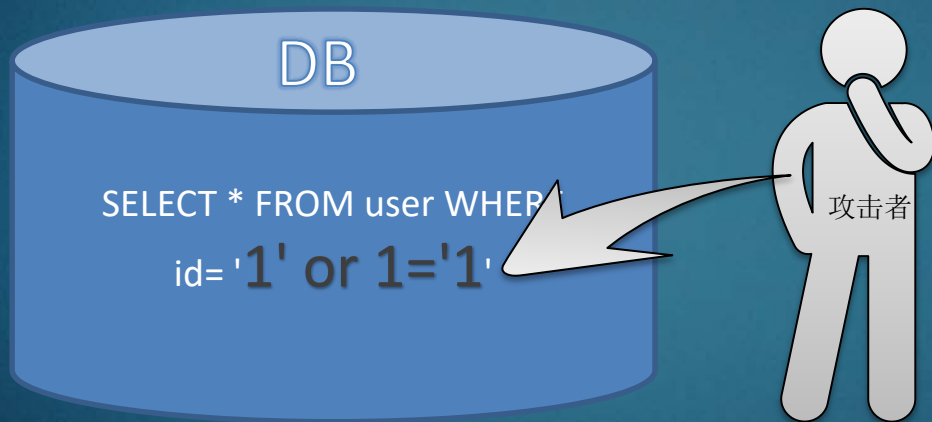


SQL注入

- 漏洞成因
- 攻击方式
- 防御方法



基本原理



1. 使用用户的参数拼接SQL语句
2. 参数改变了原SQL语句的结构



攻击方式

回显注入

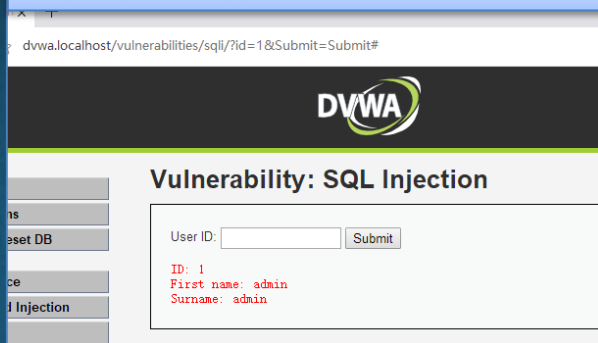
报错注入

盲注

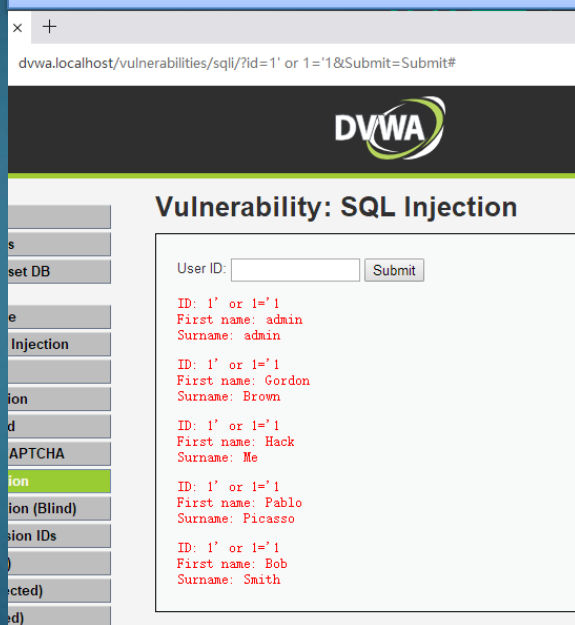


回显注入

正常请求返回的数据



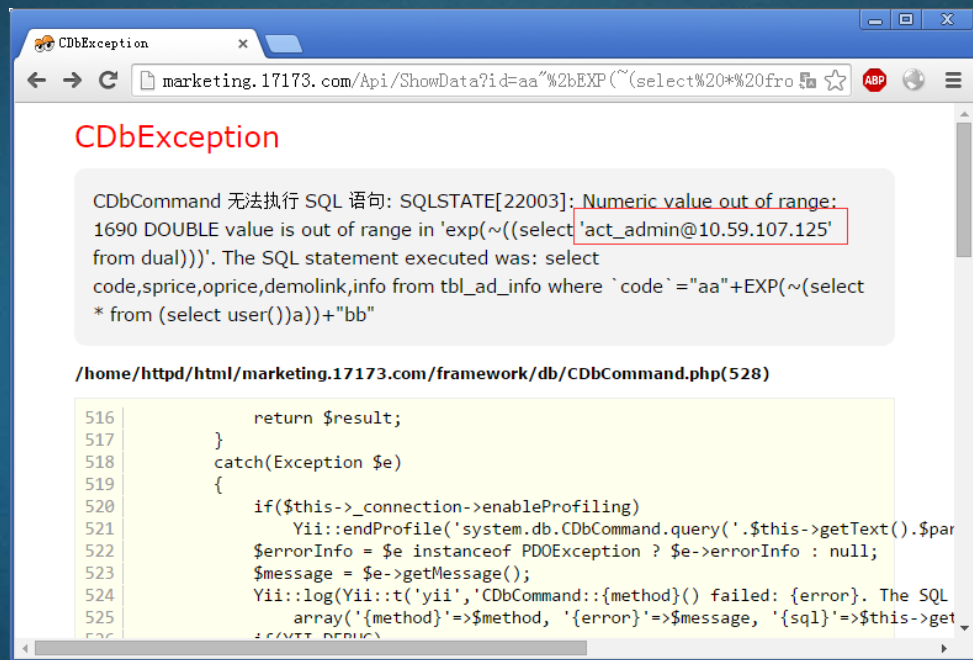
URL中加入一些SQL语句后的返回结果



利用注入漏洞可以改变页面返回数据，则称之为回显注入



报错注入



在URL加入了一些错误的SQL语句，被执行后返回了异常信息，这些异常信息当中包含了敏感信息，我们可以通过屏蔽数据库连接错误来防范此问题



盲注

布尔盲注

通过条件是否成立来判断

`substr`截取第一个字符判断是否大于
'a'，成立则页面返回数据

时间盲注

通过返回时间的长短判断
获取第一个字符的ascii码，判断是
否大于115，不成立延时5秒返回

`http://127.0.0.1/sqli-labs/Less-1/?id=1`
URL

//正常

`' and (select substr(email_id,1,1) from emails where id=3) > 'a'`
//布尔

`if(ascii(substr(database(),1,1))>115,0,sleep(5))%23`
//时间



检测方法

sqlmap.py -u "http://www.xxxx.com/index.php?id=1"

```
命令提示符
C:\Users\Administrator>sqlmap.py -u "http://dwva.localhost/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie "PHPSESSID=m04bo0m3gqs12997hrcbus4dv1; security=low"

(1.1.8.2#dev)
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 23:55:32

[23:55:33] [INFO] resuming back-end DBMS 'mysql'
[23:55:33] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment) (NOT)
  Payload: id=1' OR NOT 7951=7951#&Submit=Submit

  Type: error-based
  Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: id=1' AND ROW(7950,4864)>(SELECT COUNT(*),CONCAT(0x7170706271,(SELECT (ELT(7950=7950,1))),0x716b766b71,FLOOR(RAND(0)*2))x FROM (SELECT 5152 UNION SELECT 9654 UNION SELECT 9205 UNION SELECT 9140)a GROUP BY x)-- eyzc&Submit=Submit

  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: id=1' AND SLEEP(5)-- YNqr&Submit=Submit

  Type: UNION query
  Title: MySQL UNION query (NULL) - 2 columns
  Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7170706271,0x7a7a5341764e437667444a6446464559614263634d4b4b706b51586c6d466779496a6e70534f7972,0x716b766b71)#&Submit=Submit
---
[23:55:33] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.23, PHP 5.6.25
back-end DBMS: MySQL >= 4.1
[23:55:33] [INFO] fetched data logged to text files under 'C:\Users\Administrator\.sqlmap\output\dwva.localhost'
```



如何防范?

1. 拦截带有SQL语法的参数的传入

```
//整型参数过滤处理
$storeId = intval($_GET['store_id']);
//字符串参数过滤处理
$statusArr = ['on','off','del'];
$status = in_array($_GET['status'],$statusArr) ? $_GET['status'] : '';
```

2. 通过预编译处理拼接参数的SQL语句

```
//不可预测参数处理
$stmt = $pdo->prepare("SELECT * FROM user WHERE name = ?");
$stmt->bindValue(1, "daxia");
$stmt->execute();
```

3. 定期分析数据库执行日志, 是否有异常SQL执行



XSS跨站



漏洞成因

- 漏洞成因
- 攻击场景
- 防御方法



产生原因?

`http://www.daxia.xxx/search?keyword=test</div><script>alert(123)</script>`

`<html>`

`<head>`

`<title>搜索结果页</title>`

`</head>`

`<body>`

`.....`

`<div>搜索(test</div><script>alert(123)</script>)结果如下</div>`

`.....`

`</body>`

`</html>`



漏洞成因

1. 参数输入未经过安全过滤
2. 恶意脚本到被输出到网页
3. 用户的浏览器执行恶意脚本



漏洞分类

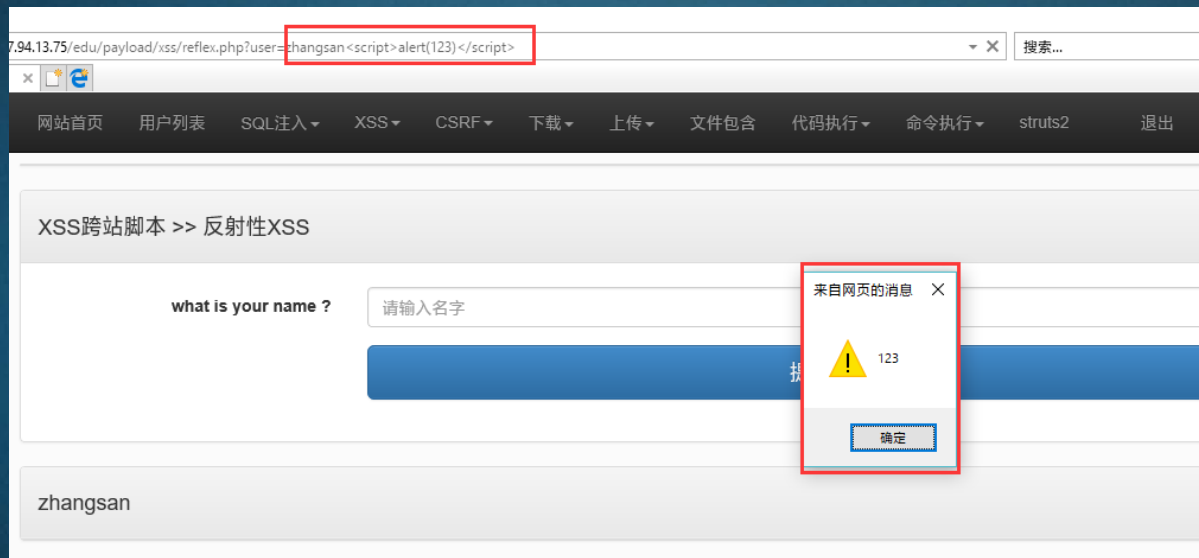
反射型

存储型

dom型



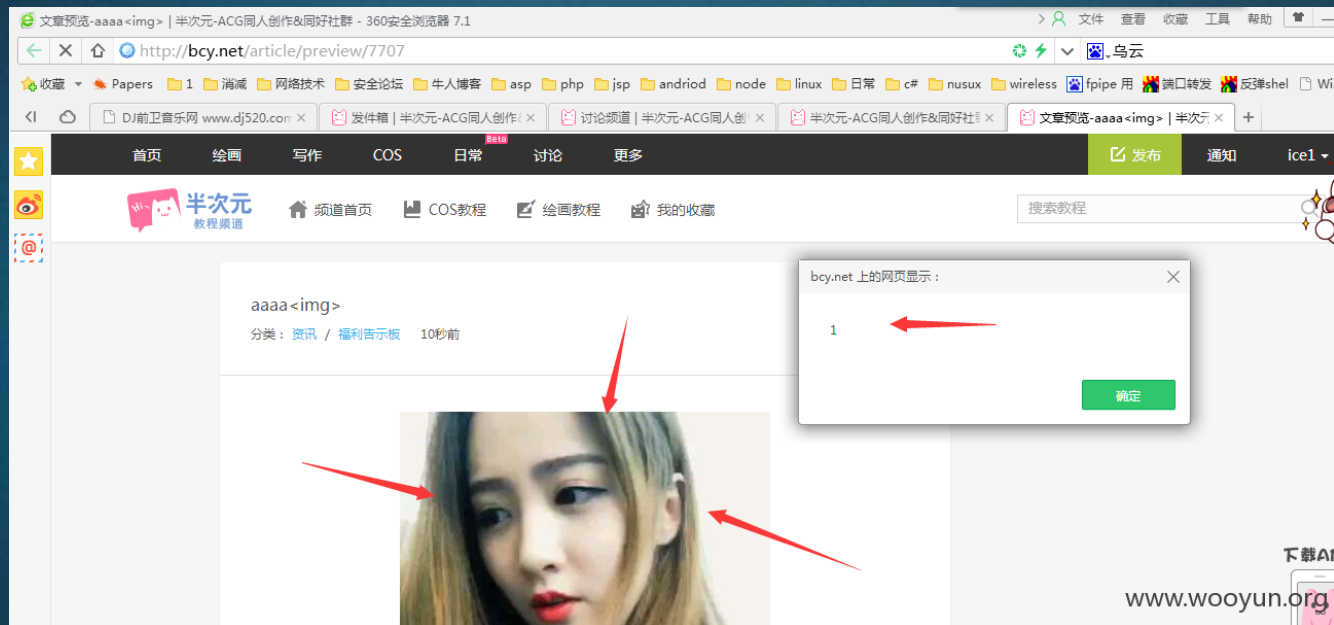
反射型



URL中的alert代码被放到
页面中且被执行
弹框中已经获取到cookie
信息c



存储型

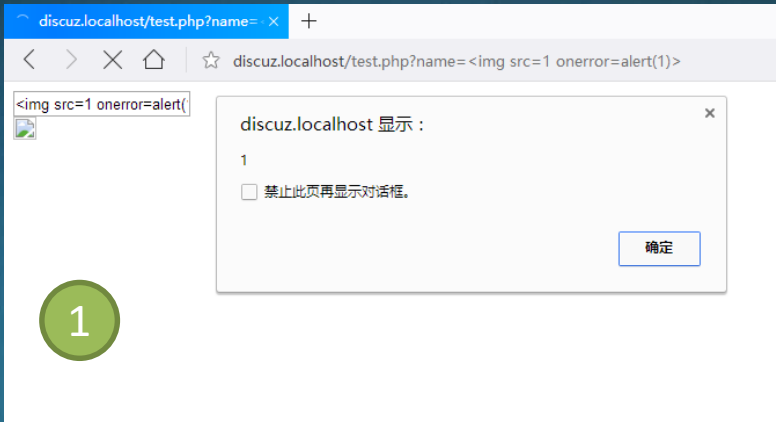


在自己的个人资料
填入JavaScript代码

其他人正常访问页面，代码被执行



DOM型



参数name虽然经过编码后放入到模板中

但是经过dom操作后,参数再次被转为实体字符

```
<?php
error_reporting(0);
$name = htmlspecialchars($_GET["name"]);
?>
<input id="username" type="text" value="<?php echo $name;?>" />
<div id="content"></div>

<script type="text/javascript">
// 获取输入的名称, 并且输出在content内。导致了一个dom-xss。
var username = document.getElementById("username");
var content = document.getElementById("content");
content.innerHTML = username.value;
</script>
```

2



如何防范?

1. 标签黑白名单过滤

```
//过滤HTML标签  
$desc = removeXss($_POST['desc']);
```

2. 代码实体转义

```
//把HTML实体标签转为符号，ENT_QUOTES指单引号也需要转义  
$desc = htmlspecialchars($_GET['desc'], ENT_QUOTES)
```

3. httponly 防止cookie被盗取

```
//设置HttpOnly  
setcookie("user", "daxia", NULL, NULL, NULL, NULL, TRUE);
```



越权漏洞



产生原因？

1. 业务系统存在**用户**权限验证
2. 对**用户**的权限验证不严谨
3. 用户能操作不属于自己权限的操作



漏洞分类

平行越权

垂直越权



平行越权

个人中心



1. [REDACTED]

普通会员

安全退出

交易管理

我的订单

我的购物车

个人信息管理

个人资料

修改密码

收货地址

第三方绑定管理

收货信息

订单号：20[REDACTED] 下单时间：2015/6/16 14:29:40

订单状态：取消 会员用户名：4579[REDACTED]

收货人：谭[REDACTED] 发票抬头：

手机：18c[REDACTED] 电话：08[REDACTED]

地址：四川省,攀枝花市[REDACTED]

配送方式：同城快递 快递费用：¥ 25.00

票品应付总金额：¥ 1305.00 票品实付总金额：¥ 1305.00

备注：

订单详情

票务信息	价格	数量	小计
 <div>TFBOYS FANS' TIME 2015/8/8 16:00 首都体育馆</div>	¥ 1280.00	1	¥ 1280.00

票品总计：¥ 1280.00
+ 运费：¥ 25.00

返回

商城系统中一般会有订单详情

在订单详情URL中，不断的切换订单ID，可以获取到他人订单信息。

可见后端查询数据的条件是并没有加上当前用户的UID。



平行越权防御方法

```
//普通用户查询订单，必须有UID  
$orderId = intval($_GET['orderId']);  
//UID 必须从服务器取，而不是用户所传入  
$uid = $_SESSION['uid'];  
$sql = "SELECT * FROM order WHERE uid=$uid AND order_id = $orderId";
```

越权不仅限于查询数据的时候
在修改数据的时候同样适用



垂直越权

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

新闻管理 车商通

fuja 上次登陆时间: 2015-08-21 浏览会员 退出

新闻管理 >

51 全部新闻

47 优惠促销

0 新车到店

4 企业动态及保养

发布时间: 全部 新闻标题: 确定 新闻发布

新闻标题	新闻类别	浏览量	发布时间	操作
这款SUV满足你对浪漫七夕的所有想象	优惠促销	2301	2015-08-18 09:18	已置顶 修改 删除
七夕带女朋友出去约会开SUV更配哟	优惠促销	65	2015-08-21 09:33	置顶 修改 删除
与道奇酷威一起打造完美七夕之旅	优惠促销	91	2015-08-20 09:13	置顶 修改 删除
传奇车型进口克莱斯勒300C音响的奥义	优惠促销	104	2015-08-19 09:09	置顶 修改 删除
陪你看流星雨Jeep大切诺基浪漫不缺席	优惠促销	91	2015-08-19 09:01	置顶 修改 删除
听说“小长假”与7座SUV更配哦	优惠促销	845	2015-08-16 08:46	置顶 修改 删除
大切西南行 开启非凡极致之旅	企业动态	1391	2015-08-11 08:55	置顶 修改 删除

www.wooyun.org

普通用户进入
了管理后台



屏蔽自增长主键

```
//尽量不要暴露连续的订单号给用户;  
$orderId = 100;  
//如果底层改造麻烦, 我们可以通过订单ID对称加密的方法  
$orderId = encode($orderId);  
echo $orderId;  
  
//接收参数做对称解密处理  
$orderId = decode($orderId);
```

不显示自增长订单号不仅仅在于防范被黑客攻击
有的时候还可以防止友商知道一天订单量



越权防范建议

1. 前台和后台的查询尽量不用同一个查询接口
2. 尽量不要暴露出连续ID如订单号
3. 越权不仅限于展示，修改数据也会出现



CSRF跨站请求伪造



产生原因？

1. 服务端错把“浏览器发起的请求”当“用户发起的请求”
2. 已登录的浏览器，打开恶意网址后，被执行了相应操作



POST型CSRF

```
<html>
<body>
  <form action="http://i.emao.com/homecp/user/dosetting" method="POST">
    <input type="hidden" name="nickname" value="eeeeeeeq" />
    <input type="hidden" name="sex" value="1" />
    <input type="hidden" name="year" value="" />
    <input type="hidden" name="month" value="" />
    <input type="hidden" name="day" value="" />
    <input type="hidden" name="provinceid" value="" />
    <input type="hidden" name="cityid" value="" />
    <input type="hidden" name="areaid" value="" />
    <input type="hidden" name="major" value="" />

    <input type="submit" value="Submit request" />
  </form>
</body>
</html>
```

后端没有限定数据的来源，导致用户在不知情的情况下修改了用户信息

中心首页 资料设置

消息与互动 ▲

- 系统消息
- 猫友动态
- 评论我的
- 我评论的
- @我的

交易中心 ▲

- 我的关注
- 提醒设置
- 我的订单
- 我的分期订单

我的钱包 ▲

- 我的猫豆
- 我的卡券

用户名 4321

不可更改

昵称* eeeeeeeq

2-32个中/英文、数字_与减号

性别* ☒ 男 ☐ 女

出生日期 请选择 年 请选择 月 请选择 日

所在地 请选择 请选择 请选择

职业

确定 取消

www.wooyun.org



检测方法?

1. 去掉token参数尝试能否正常请求
2. 去掉referer是否可以提交成功
3. 是否能用GET提交替代POST提交



编码方法

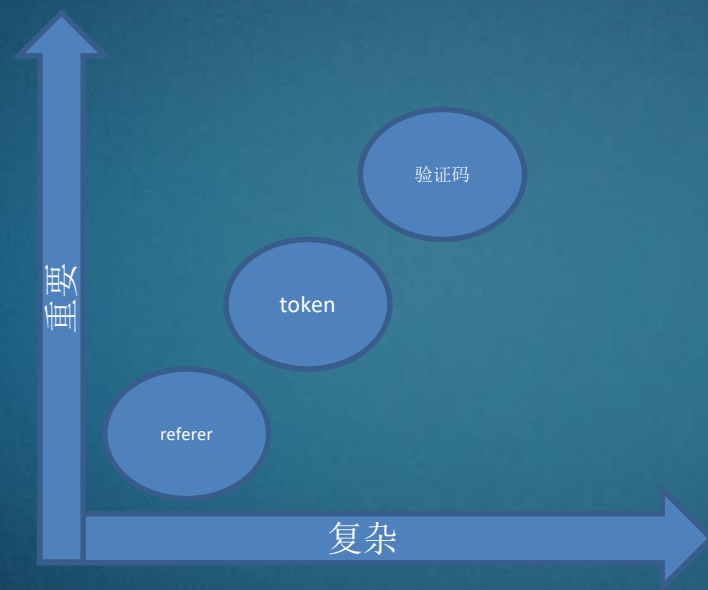
```
//验证Referer
if ($_SERVICE['HTTP_REFERER'] != $host) {
    return false;
}
//验证token
if ($_POST['token'] != $token) {
    return false;
}
//图片验证码
if ($_POST['verify_code'] != $verify_code) {
    return false;
}
```

REFERER 信息不符合
TOKEN 验证不通过
图片验证码验证失败

则不接受请求



防范等级



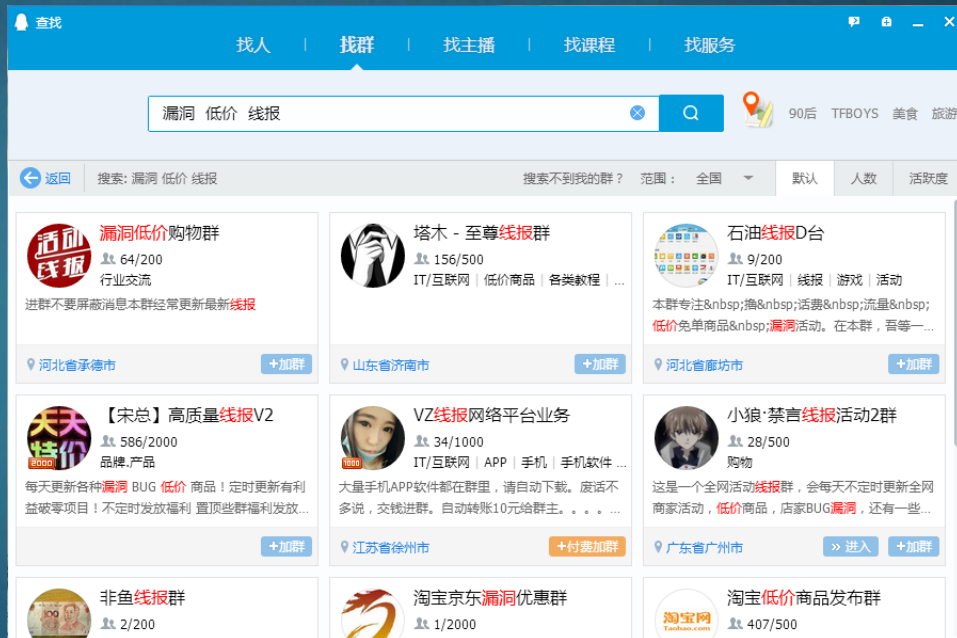
业务类型越重要的位置
使用相对复杂的验证机制



支付漏洞



QQ群黑产线报群



产生原因？

1. 开发者在数据包中传递支付的金额
2. 后端并没有对金额做校验或者签名
3. 导致攻击者可以随意篡改金额提交



修改支付金额

人气推荐 >>
套餐 >>
工作日特惠午餐 >>
轻松下午茶 >>
披萨 >>
饭食 >>
港式米线 >>
意面 >>
诱人小吃 >>
鲜蔬 >>

应付总价/Total Amount: ¥94.0元

☐ 货到付款/Cash On Delivery

☒ 网上支付/Online Payment-请关闭屏蔽浏览器弹出窗口的插件

送餐/外带时间: 2012 年 03 月 23 日 19 时 13 分 整
Delivery/Take Away Time

友情提示: 根据当前时间, 以上为预估的最快送餐/外带时间, 或是您选择的送餐/外带时间, 送餐/外带时间.
Reminder

☒ 中国工商银行 ☒ 招商银行 ☒ 中国建设银行
☒ 中国农业银行 ☒ 中国银行 ☒ 交通银行
☒ 杭州银行 ☒ 兴业银行 ☒ 中国民生银行
☒ 广东发展银行 ☒ 深圳发展银行 ☒ 浦发银行

```
input type="hidden" name="aflag" id="aflag" value="2">
iv class="menucontent">
<input type="hidden" name="donation" id="donation" value="0">
<form name="alipaysubmit" id="alipaysubmit" method="post" action="/phsios/OrderingAction/alipay.jsp" target="_bl
  <input type="hidden" name="iorderid" value="07434797">
  <input type="hidden" name="storecode" value="Psh728">
  <input type="hidden" name="seller_email" value="ECN_PH_FIN_Alipay.China@yum.com">
  <input type="hidden" name="total_fee" id="alipay_fee" value="0.01">
</form>
```

www.wooyun.org

支付宝 Lab | 收银台

您好, 欢迎使用支付宝付款! 支付遇到问题?

您正在使用即时到账交易: 付款后资金直接进入对方账户

KFCIPsh72007434797 详单

收款方: 上海必胜客有限公司

0.01元

订单创建时间: 2012-03-23 18:15:27 (交易将在1小时后关闭, 请及时付款!)

www.wooyun.org

后端在确认订单信息的时候, 完全依靠前端传过来的信息, 导致金额可以被用户自己所修改



看雪 2017 安全开发者峰会
Kanxue 2017 Security Developer Summit

修改数量

1. 我的购物车

2. 填写核对订单信息

3. 成功提交订单

商品名称	单价	数量	操作
 威刚 (ADATA) C906 U盘 (典雅黑) (4GB)	¥ 26.00	<input type="text" value="-1"/>	删除 收藏
 威刚 (ADATA) C008 U盘 (黑红) (4GB)	¥ 27.00	<input type="text" value="1"/>	删除 收藏

[继续购物](#) | [清空购物车](#)

商品总金额: ¥ 1.00 [立即结算](#)

收银台信息

商品总数: 0
应收金额: ¥ 1.00
活动返现: ¥ 0.00
商品总金额:
 RMB
[立即结算 >>](#)

帮助中心
为什么我的商品无法加入购物车?

www.wboyun.org

商品数量可以为负数，导致最终的支付金额减少



数据包重放问题

充值-帐户明细 - docin.com豆丁网 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.docin.com/app/my/fin/transactionHistory_cn#

充值-帐户明细 - docin.com豆丁网

docin 豆丁

在一亿文档库里搜索文档

文档 搜索 帮助 我要上传

首页 文档分类 书城 杂志 会议 社区 移动应用 我的豆丁 我的书架

首页 | 我的任务 | 我的关注 | 消息 | 充值/兑换 | 基本设置

账单明细 奖励明细 充值 兑换

充值余额: 3.000 豆元 文档收益余额: 0.000 豆元 历史总收入: 3.000 豆元

时间	项目	收入	支出	余额统计
2013-07-07	存款	+1.000		3.000
2013-07-07	存款	+1.000		2.000
2013-07-07	存款	+1.000		1.000

* 查询历史明细, 请使用右侧搜索 (仅支持连续6个月区间查询)。

查询特定明细

- ☒ 全部
- ☐ 收入
- ☐ 支出

开始日期

结束日期

www.w00yun.org

在充值过程中，把数据包多次提交，发现多了一笔订单，并且增加了余额



如何防范？

1. 限制超量购买限量商品
2. 限制低价、免费购买付费商品
3. 限制免费商品获得金钱、积分等利益



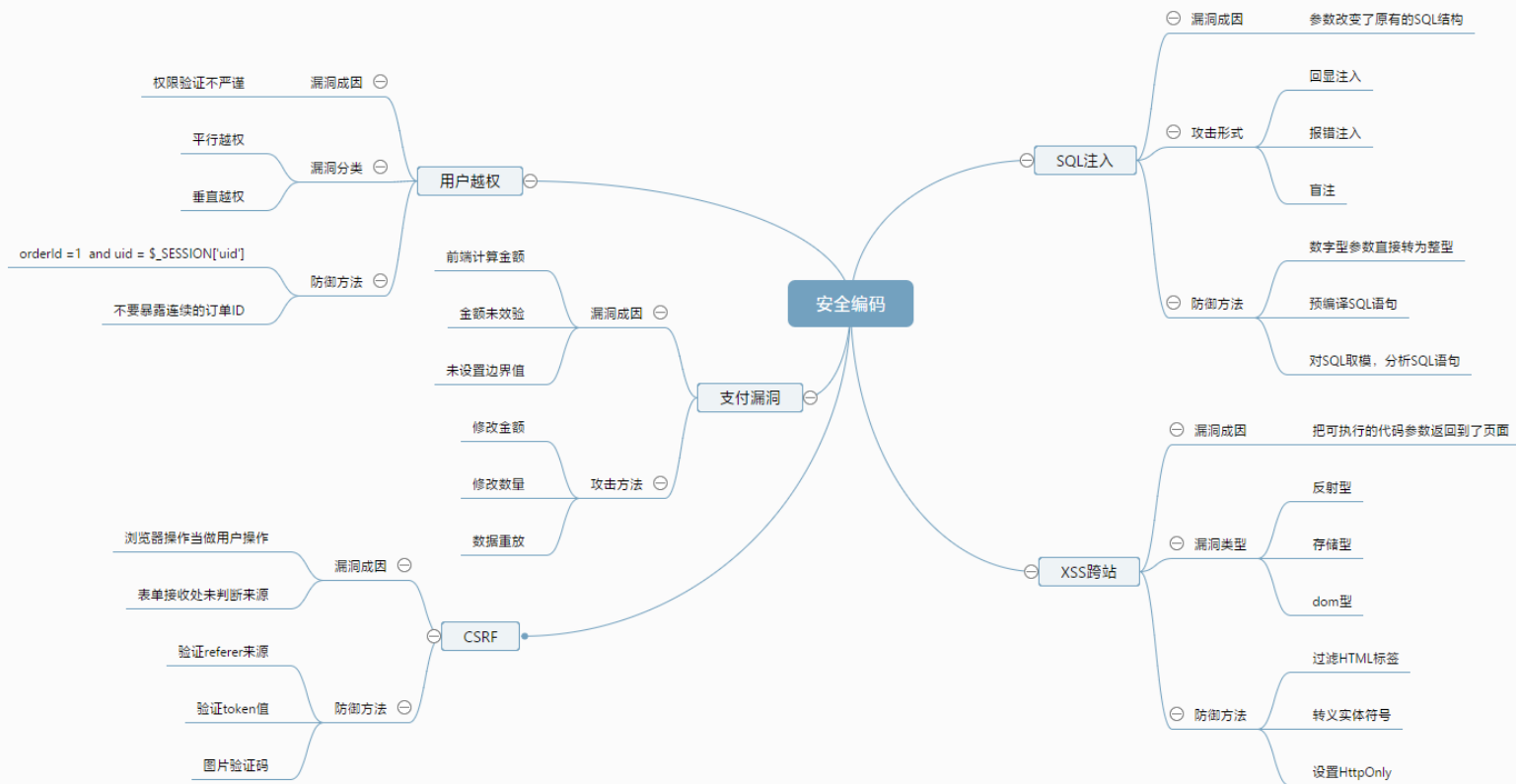
如何防范?

```
//验证参数的有效性
if ($num > $maxNum || $num < $minNum) {
    return false;
}
//由后端计算金额
$totalMoney = $price * $num;
//判断支付金额是否异常
if ($totalMoney <= 0) {
    return false;
}
//生成订单签名信息
$signin = createSign($totalMoney, $price, $otherParam);
```

参数合法验证
后端计算金额
金额是否异常
对订单签名



回顾总结





WeChat: songboy8888

Email:soupqingsong@foxmail.com

