

汽车之家存在支付逻辑漏洞

危险等级：高

来到该网站注册一个账号来购买视频URL下发现购买视频金额可以任意修改

漏洞详情

<https://club.autohome.com.cn/bbs/thread/fd07d8353154bdf/85528070-1.html>

来到该URL下发现可以购买视频打开burpsuite抓包

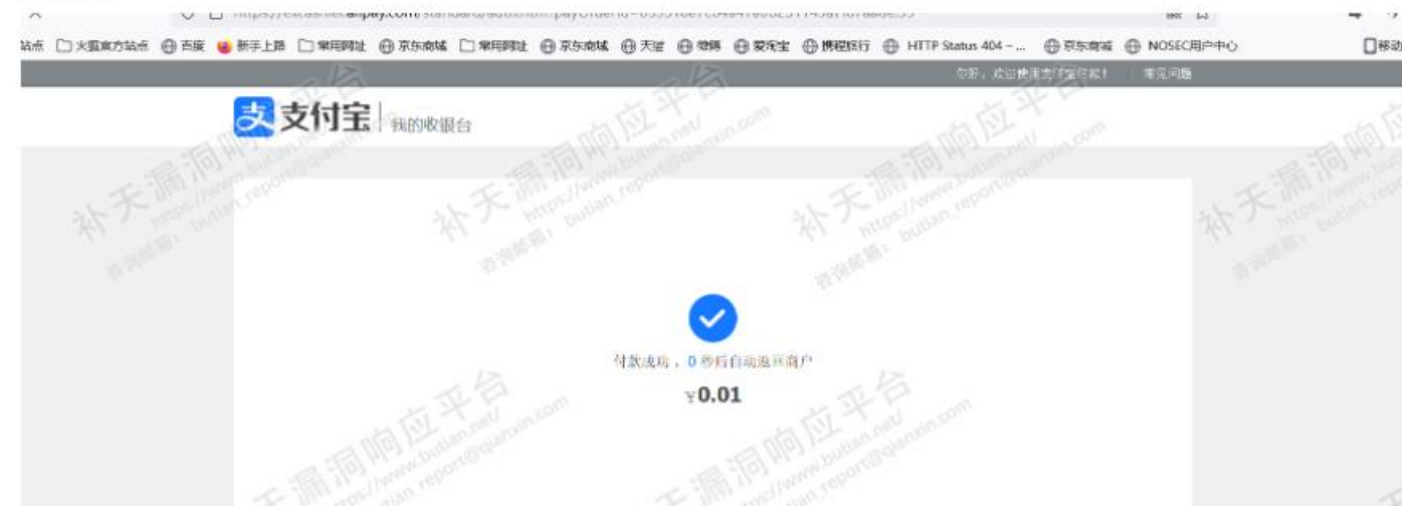


发现参数可控且参数price 将参数改为0.01放包

发现金额为0.01元可以购买



支付成功



发现该视频可以播放」

[51 网站](#)
[火狐官方网站](#)
[百度](#)
[新手上路](#)
[常用网址](#)
[京东商城](#)
[常用网址](#)
[京东商城](#)
[天猫](#)
[微博](#)
[爱淘宝](#)
[携程旅行](#)
[HTTP Status 404 - ...](#)
[京东商城](#)
[N](#)



我就是Young

0 2 精华标准 只看楼主



在该SRC对高危漏洞定义发现该漏洞满足此要求

應同定級標準：

其他藥物等項包括：

- 1、严重的可直接获取系统权限漏洞，包括但不限于远程命令执行、远程代码执行、文件上传获取高权限Webshell、SQL注入获取系统权限等。
- 2、严重的漏洞设计缺陷和流程缺陷，包括但不限于涉及支付、金额、核心机密敏感数据的漏洞设计缺陷和业务流程缺陷，批处理程序包含重置、严重敏感数据暴露问题等。
- 3、严重的敏感信息泄露，包括但不限于可以获取重要敏感数据的SQL注入漏洞、可直接获取大量内网敏感信息的SSRF、涉及重要业务接口的越权越权(如涉及身份证、银行卡、手机号、真实姓名等敏感数据)。
- 4、其他经研判判定，可严重危害系统安全或数据安全的情况。

补天平台

地址: butian_report@foxmail.com

諮詢郵箱: butian_report@foxmail.com

在该SRC对高危漏洞定义发现该漏洞满足此要求

漏洞定级标准:

高危漏洞等级包括:

- 1、严重的可直接获取系统权限的漏洞。包括但不限于远程命令执行、远程代码执行、文件上传获取高权限Webshell、SQL注入获取系统权限等。
- 2、严重的逻辑设计缺陷和流程缺陷。包括但不限于涉及支付、金额、核心机密敏感数据的逻辑设计缺陷和业务流程缺陷。批量任意账号密码重置、严重数据校验逻辑漏洞等。
- 3、严重的软件信息泄露。包括但不限于可以获取重要敏感数据的SQL注入漏洞、可直接获取大量内网敏感信息的SSRF、涉及重要业务接口的批量越权(如涉及身份证、银行卡、手机号、真实姓名等敏感数据)。
- 4、其他经审核判定,可严重危害系统安全或数据安全的情况。

补天平台
https://www.butian.net/
咨询邮箱: butian_report@qianxin.com

包含支付逻辑漏洞所以该漏洞等级为: 高

修复方案

严格校验参数并在后端验证

厂商回复