01 物品描述处存在存储型XSS+绕WAF

漏洞名称：物品描述处存在存储型 XSS
漏洞类别：存储型XSS + Bypass WAF
危害等级：中危
漏洞赏金：/
漏洞触发点：修改物品的描述详情处
漏洞细节简述：添加 Content-Encoding 字段绕过 WAF
参考来源：https://twitter.com/Jayesh25_/status/1719072435939459532
记录时间：2023.11.01

如何发现 XSS？

- 在修改物品描述处，输入框可控，但有 WAF

如何绕过 WAF?

- 通过在请求头中添加“Content-Encoding: any_random_text”