

0x01 前言

如有技术交流或渗透测试/代码审计/SRC漏洞挖掘/红队方向综合培训 或 红蓝对抗评估/安全产品研发/安全服务需求的朋友

欢迎联系QQ/VX 547006660

<https://github.com/J0o1ey/BountyHunterInChina>

重生之我是赏金猎人系列，欢迎大家点个star

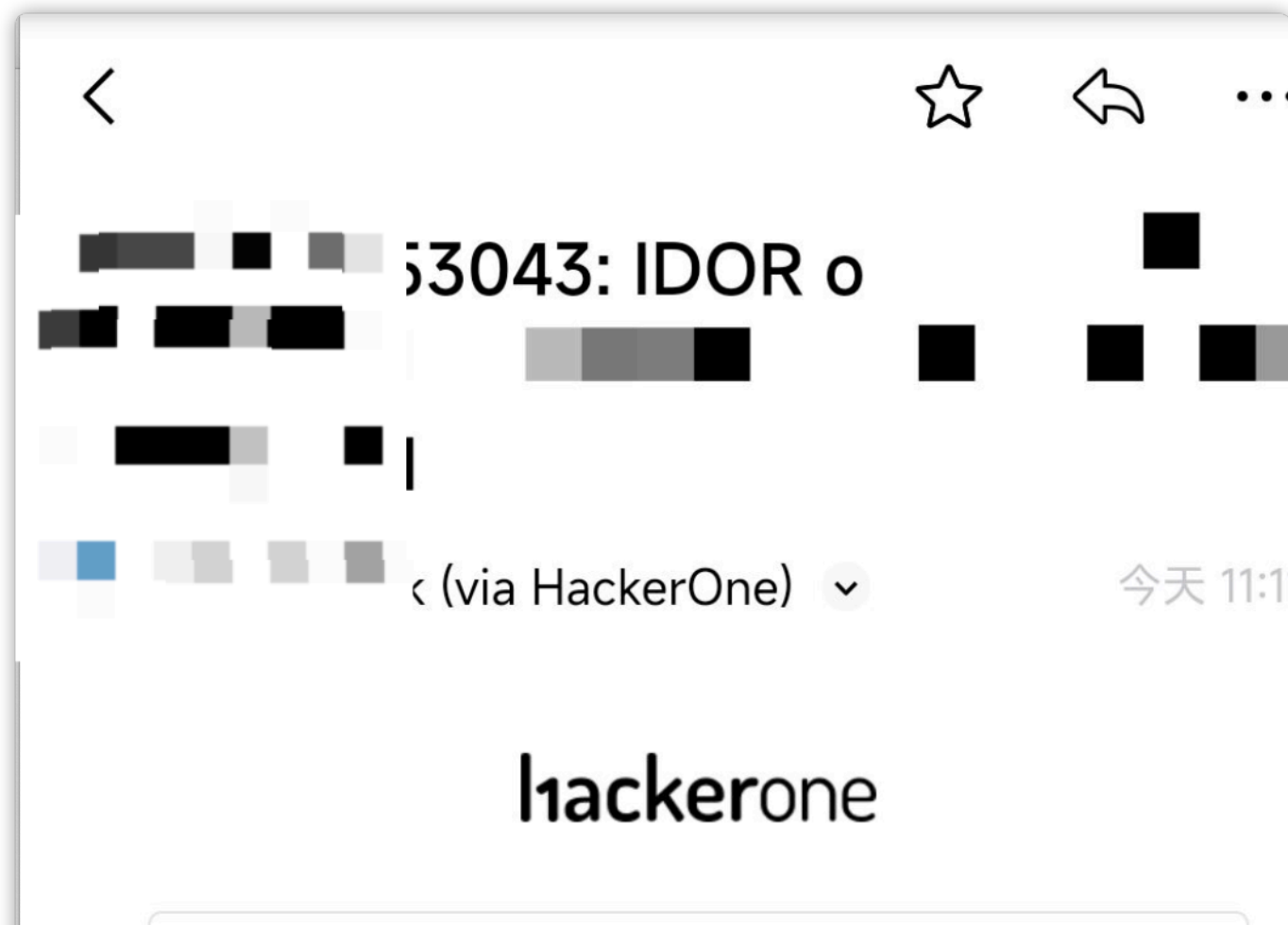
0x02 缘起


2022年一年，遭受疫情重创，自己的业务收入非常惨淡~

迫不得已2023年过完年后想点赚钱的路子补补窟窿，于是将目光对准了hackerone

众所周知，hackerone的**美金奖励**一直是让人垂涎欲滴的，本人也参与到了赏金猎人的大军里，但是深刻感受到了**hackerone**项目的挖掘难度之高远超国内，美金的确不是那么好赚的

不过还是用一个有趣的trick拿到了4000美金的奖励，特来和大家分享一下



 rewarded you with a bounty of **\$4000**
for **IDOR** on



Beyond the bounty amount, do not disclose any weakness information without the express permission of the bounty program operator.

@j0o1ey, thanks for the report! After our in



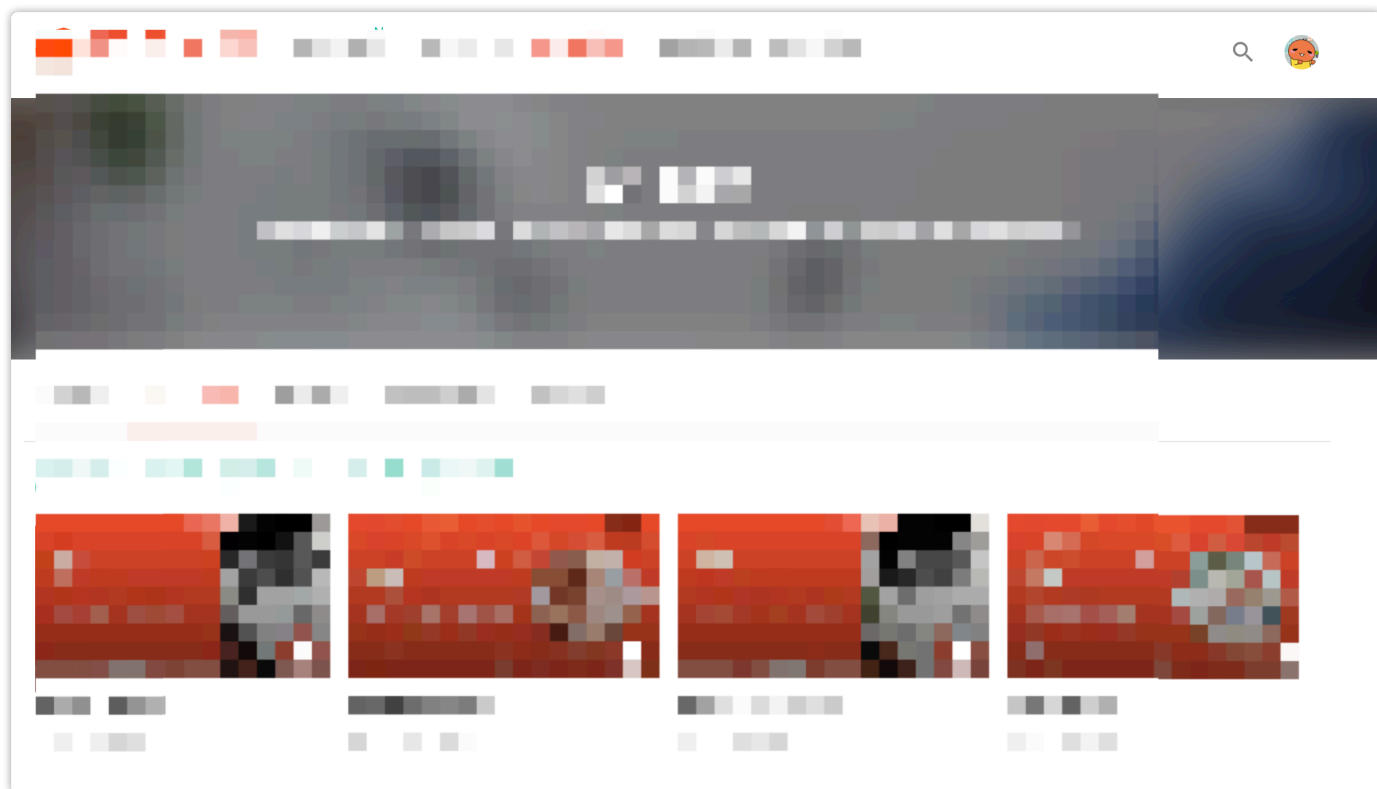
0x03 目标搜寻与IDOR碰壁

针对目标的recon，我选择直接简单粗暴进行google dork其域名

并迅速确定我们可以注册的业务

```
site:xxxx.cn register
```

随后便发现了一个我们可以注册登录的站点



该站点的主要形式是“论坛”，经过简单的指纹识别recon，发现并没有使用那几大论坛CMS系统，是开发自研的论坛系统

测试了一些应用层程序技术漏洞无果后，我便将注意力放在了IDOR漏洞测试上

希望能通过IDOR出货~

最终在测试到“删除帖子”和“编辑帖子”两个功能点时，出现了有趣的请求

1926为我自己的帖子ID

```
POST /api/forum-posts/1926 HTTP/2
Host: xxx.com
Cookie: Xxx
Content-Length: 12
Cache-Control: max-age=0
Sec-Ch-Ua: "Not_A Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"
Accept: application/json
Content-Type: application/json; charset=utf-8
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "macOS"
Origin: https://xxx.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://xxx.com
Accept-Encoding: gzip, deflate
```

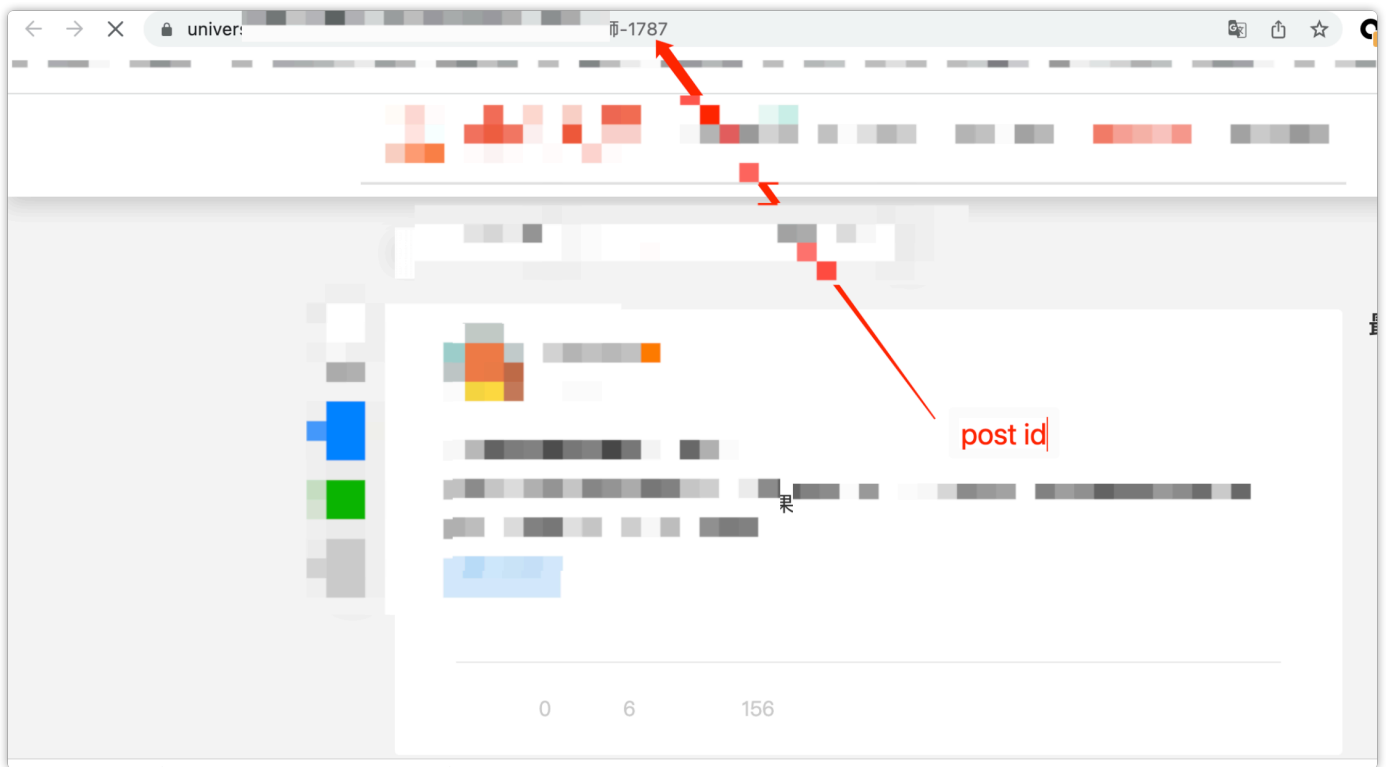
Accept-Language: zh-CN,zh;q=0.9,ja;q=0.8

{"status":2}

The screenshot shows a web browser's developer tools interface. The 'Request' tab on the left is selected, displaying a large, pixelated, and mostly redacted image. The 'Response' tab on the right is also selected, showing the following HTTP response details:

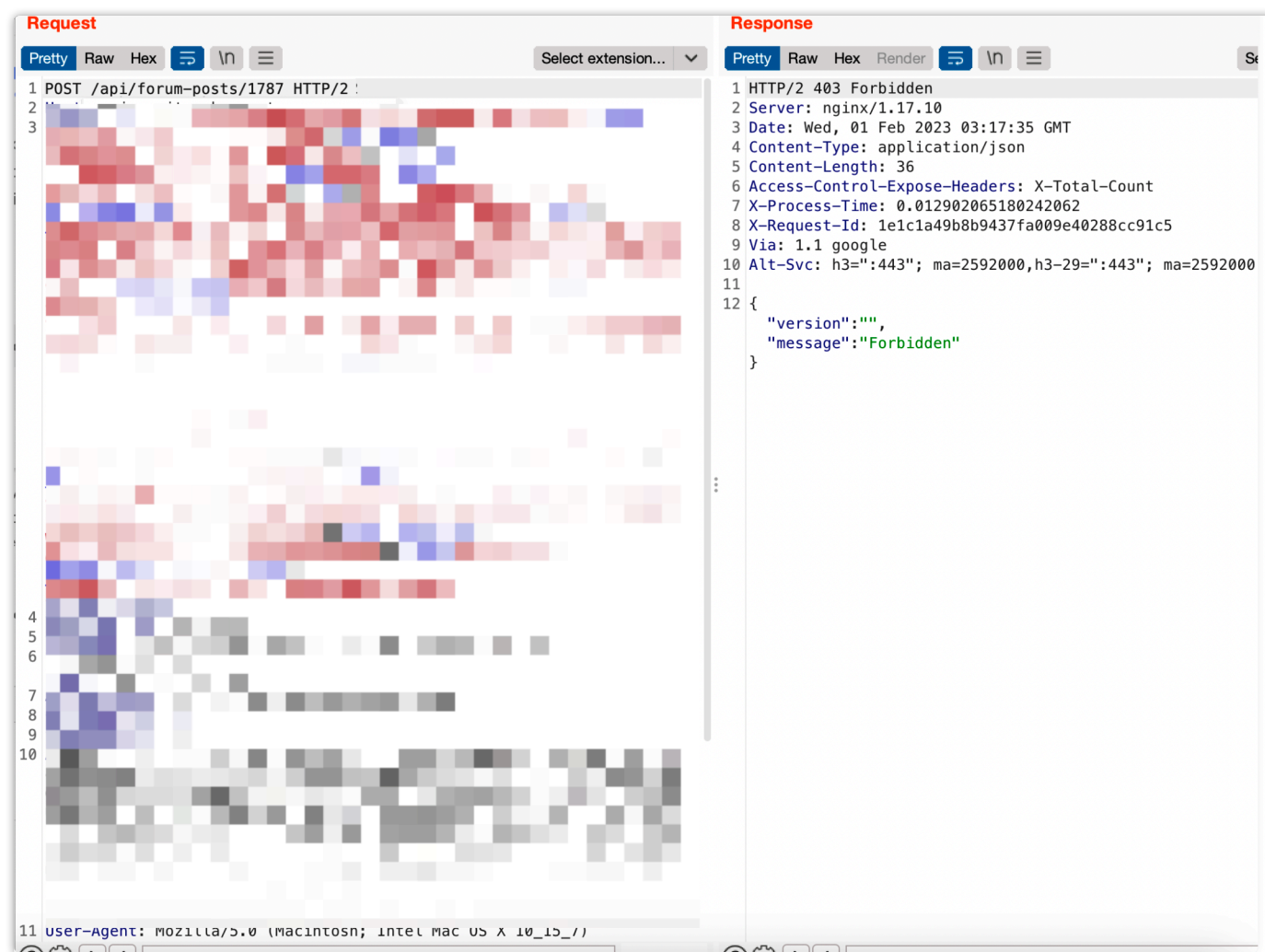
```
1 HTTP/2 204 No Content
2 Server: nginx/1.17.10
3 Date: Tue, 31 Jan 2023 03:49:49 GMT
4 Access-Control-Expose-Headers: X-Total-Count
5 X-Process-Time: 0.029397984966635704
6 X-Request-Id: c970213c7d3c4f509f2fc7d41e9ec5fb
7 Via: 1.1 google
8 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
9
10
```

发现成功删除了我自己的帖子，那么最简单的IDOR测试思路来了，找个别人的帖子，换一下ID



```
POST /api/forum-posts/1787 HTTP/2
Host: xxx.com
Cookie: Xxx
Content-Length: 12
Cache-Control: max-age=0
Sec-Ch-Ua: "Not_A Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"
Accept: application/json
Content-Type: application/json; charset=utf-8
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/109.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "macOS"
Origin: https://xxx.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://xxx.com
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,ja;q=0.8

{"status":2}
```



结果直接一波Forbidden寄掉了。。。让人陷入了沉思

翻了翻http history，发现目标站点有一些OPTIONS请求方式的请求，并且提示该站点支持DELETE,PUT,PATCH等等请求方式

众所周知，目标的接口风格是Restful接口，而Restful接口往往支持多种请求方式(GET,POST,DELETE,PUT,PATCH等等)

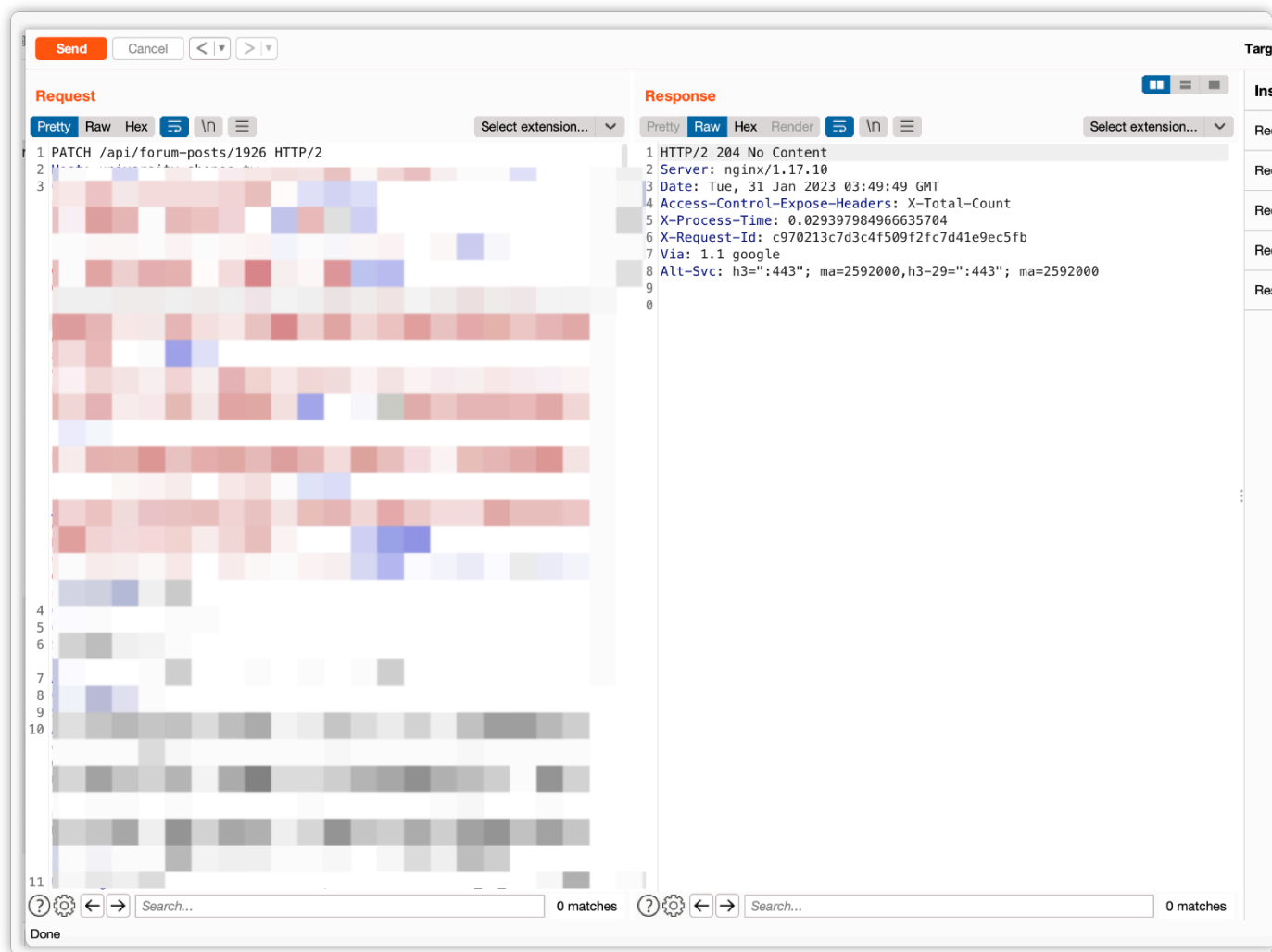
我们能否通过修改请求方式来绕过IDOR限制呢？

说干就干

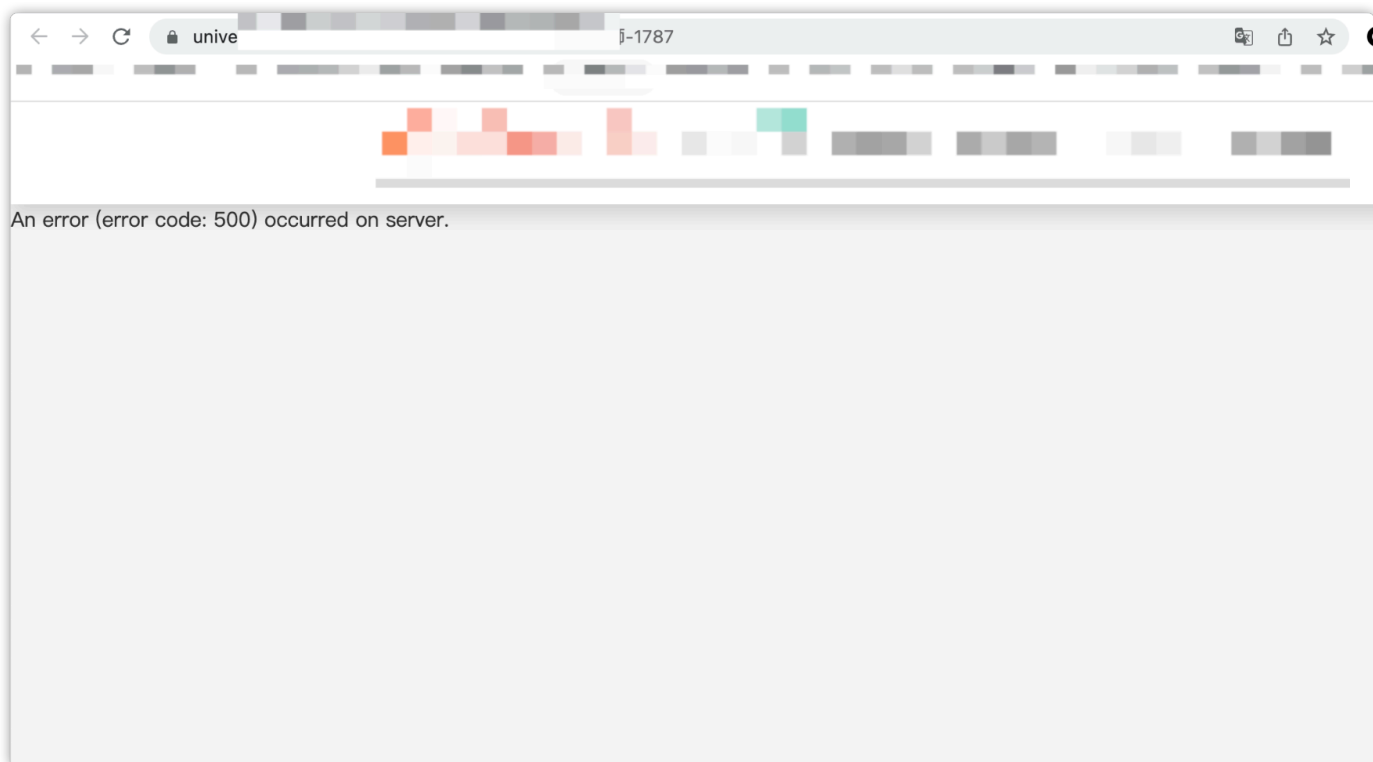
0x04 突破IDOR限制

尝试对请求方式进行FUZZ

最终发现PATCH和DELETE请求方式均可删除目标帖子，而PATCH在编辑帖子功能中，甚至可以直接覆盖帖子的内容！




删除目标帖子后，目标帖子直接抛出500状态码~删除成功



让人兴奋的ending，我在hackerone报告了这个IDOR问题，并且获得了high评级的Bugbounty

Partic



State

Triaged (Open)

Severity

Medium (7 ~ 8.9)

Weakness

Insecure Direct Object Reference (IDOR)

Bounty

\$4000

Time spent

2h

Visibility

Private

0x05 技术点总结

- 1.针对各类API接口，可尝试多种请求方式FUZZ，发掘隐藏的idor漏洞点
- 2.OPTIONS请求在某些情景下可以探测目标服务器、api支持的请求方法

漏洞始于细心和灵活的思路