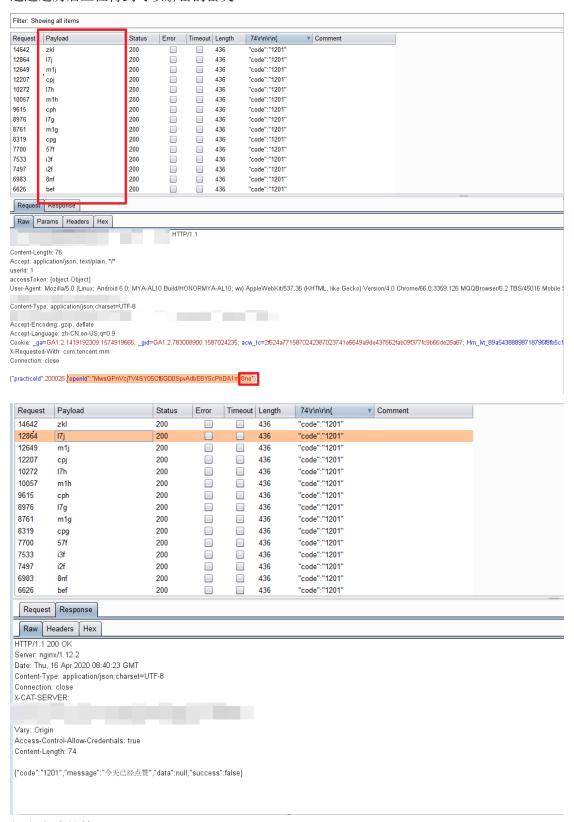
"openId":"MwsGPnVcjTV4SY05Cf6GD0SpvAdbE8Y5cPbDA1mr8ne"

通过遍历后三位得到可以解密的密文



Request	Payload	Status	Error	Timeout	Length	74\r\n\r ▼
1854	rpb	200			436	"code":"1201"
1650	3jb	200			436	"code":"1201"
861	6xa	200			436	"code":"1201"
586	jqa	200			436	"code":"1201"
558	rpa	200			436	"code":"1201"
354	3ja	200			436	"code":"1201"
0		200			436	"code":"1201"
14774	nol	200			433	
14773	mol	200			433	
14772	lol	200			433	
14771	kol	200			433	
14770	jol	200			433	
14769	iol	200			433	
14768	hol	200			433	
14767	gol	200			433	
Request Response						
Raw Headers Hex						

HTTP/1.1 200 OK Server: nginx/1.12.2

Date: Thu, 16 Apr 2020 08:40:59 GMT Content-Type: application/json;charset=UTF-8

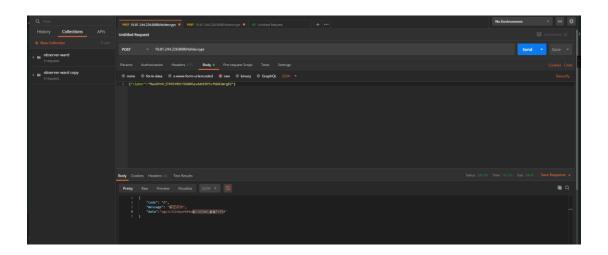
Connection: close X-CAT-SERVER:

Vary: Origin

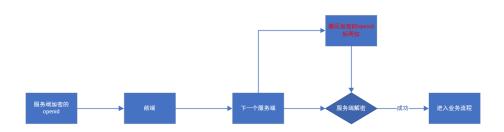
Access-Control-Allow-Credentials: true

Content-Length: 71

{"code":"1201","message":"openId不合法","data":null,"success":false}



业务流程



问题出现在遍历 openid 之后,通过损坏密文字节来改变明文字节就可以正常业务流程,导致可以刷赞。AES 算法暂时都存在这个问题。解决办法是在增加一层业务校验

相关漏洞分析参考

http://drops.xmd5.com/static/drops/tips-7828.html https://xz.aliyun.com/t/4552