



Privilege Escalation



Mahmoud M. Awali

 **@0xAwali**



My Methodology

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


-  Tweet
-  Tweet


BUG BOUNTY TIP

UUID IDOR Trick


Need to find the UUID for a specific user?
Try registering the target username or e-mail!
The response will often include their UUID.

```
{"statusCode": "409",  
  "error": "This user already exists.",  
  "ref": "f2837aea-2d51-11ea-978f-2e728ce88125"}
```

 @securinti

 @IntiDC

www.intigriti.com





attacker

My Methodology

There Is **Option Based On UUID** , **ID** OR **Email** , Try To Replace Your UUID , ID OR Email To Victim UUID , ID OR Email To Ge IDOR



Slides

```
POST /idor 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
```

```
uuid=*****
```



attacker

My Methodology

Try To **Change The UUID To null** , **Insert Zeros** as Value OR Try To Inject an Array e.g. **UUID=[]** To Expose Sensitive Information



Tweet

```
POST /misconfiguration 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
```

UUID=**00000000-0000-0000-0000-000000000000**



attacker

My Methodology

There Is **Option Based On Your Privilege** , Try To Replace Your Privilege To High Level Privilege



Blog

```
POST /privilege-escalation 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
```

Role=**admin**



attacker

My Methodology

Try To **Change The Role To null** OR **Inject an Empty Array e.g. Role=[]** To Expose Sensitive Information



Tweet

```
POST /privilege-escalation/misconfiguration 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
```

Role=**[]**



attacker

My Methodology

Try To Use **Parameter Pollution** Techniques **With UUID** OR **Role Parameters**



Tweet

BUG BOUNTY TIP

Authorization bypass

Add multiple ID's to HTTP requests.
This sometimes bypasses authorization
checks for the 2nd ID!

`?id=me`

`200 OK`

`my data`

`?id=victim`

`401 UNAUTHORIZED`

`no data`

`?id=me&id=victim`

`200 OK`

`my & victim data`



@pxmme1337

www.intigriti.com



attacker

My Methodology

Try To Use **Separators e.g. | , %20 OR , With UUID Parameter** To Ge IDOR



Mine

```
POST /idor 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
```

UUID=**victim-UUID,me-UUID**



attacker

My Methodology

Try To Use **Separators e.g. | , %20 OR , With Role Parameter** To Get Privilege Escalation



Mine

```
POST /privilege-escalation 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
```

Role=**admin,user**



attacker

My Methodology

Try To Change **Content Type Header To application/json** AND Insert Value Of UUID As Array e.g **{"UUID":["victim-UUID","me-UUID"]}** To Get IDOR



Mine

```
POST /idor 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

{"UUID":["victim-UUID","me-UUID"]}
```



attacker

My Methodology

Try To Change **Content Type Header To application/json AND Insert Value Of Role As Array e.g {"Role":["admin","user"]}** To Get Privilege Escalation



Mine

```
POST /privilege-escalation 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
```

```
{"Role":["admin","user"]}
```



attacker

My Methodology

Try To **Change Method To POST , GET , PUT OR DELETE etc** With **UUID** Parameter



Mine

```
GET /idor?uuid=Victim-UUID HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```



attacker

My Methodology

Try To **Change Method To POST , GET , PUT OR DELETE etc** With Role Parameter



Mine

```
GET /privilege-escalation?Role=admin HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```



attacker

My Methodology

Enter **Victim UUID** Then Try To **Manipulate The Response To Change The Response To Response Of The Correct UUID Code** , Maybe Something Will Happen



Mine

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: https://www.company.com
Access-Control-Allow-Credentials: true
Content-Type: application/json; charset=utf-8
Content-Length: length

{
  "msg" : "Right To Do Next Action"
}
```



attacker

My Methodology

Try To **Manipulate The Response By Changing false To true etc** To Get Privilege Escalation



Tweet

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: https://www.company.com
Access-Control-Allow-Credentials: true
Content-Type: application/json; charset=utf-8
Content-Length: length

{
  "admin" : "true"
}
```



attacker

My Methodology

Try To Send The **Additional properties In The Request** As Parameters Or Using This Burp Suite Extension **JSONandHTTPP**

•  Tweet

•  Blog

BUG BOUNTY TIP

Send back responses!

See object properties in the response but not in the request?
Add them to the request! You may be able to gain control over these properties!

Request:

```
{"id": "7"}  
{"id": "7", "admin": true}
```

Response:

```
{"id": "7", "admin": false}  
{"id": "7", "admin": true}
```

 YassineAboukir





attacker

My Methodology

Create Two Accounts Then Try To **Replace ID To Another ID While Doing Action e.g. Get , Add , Edit , Remove** On One Of Them



Video

Steps to produce :-

- 1 - **Create Two** Account , One On **Firefox** and The Second On **Chrome**
- 2 - Try To **Get UUID Of Both**
- 3 - Do **Replace And Match In Burp Suite** OR Use **Autorize And AutoRepeater**
- 4 - **Do Any Action** On One Of Them



attacker

My Methodology

Create Two Accounts One To High-level Privilege , Second To Low-level Privilege Then **Replace Cookie Of High-level Privilege To Low-level Privilege While Doing Action** On One Of Them



Video

Steps to produce :-

- 1 - **Create Two** Account , One On **Firefox With High-level** and The Second On **Chrome With Low-level Privilege**
- 2 - Try To **Get Cookie Of Both**
- 3 - Do **Replace And Match Cookie Of High-level And Low-level In Burp Suite** OR Use **Autorize**
- 4 - **Do Any Action** On One Of Them



attacker

My Methodology

Create Two Accounts One To High-level Privilege , Second To Low-level Privilege Then **Replace Authorization Of High-level Privilege To Low-level Privilege While Doing Action On One Of Them**



Video

Steps to produce :-

- 1 - **Create Two** Account , One On **Firefox With High-level** and The Second On **Chrome With Low-level Privilege**
- 2 - Try To **Get Authorization Of Both**
- 3 - Do **Replace And Match Authorization Of High-level And Low-level In Burp Suite** OR Use **Autorize**
- 4 - **Do Any Action** On One Of Them



attacker

My Methodology

Create **Account** Then **Add Your UUID OR ID To All Sensitive Endpoints**
As Parameter To Get IDOR

-  Writeup
-  Video

Steps to produce :-

- 1 - Create **Account**
- 2 - Find All **Sensitive Endpoints On Your Account**
e.g. `http://company.com/privilege-escalation`
- 3 - **Add uuid As Parameter** To This endpoint e.g
`http://company.com/privilege-escalation?uuid=*****`



attacker

My Methodology

Create **Account** Then **Add isAdmin=True** OR **admin=True** etc To All Sensitive Endpoints To Override Your Privilege

-  Tweet
-  Blog

Steps to produce :-

- 1 - Create **Account**
- 2 - Find All **Sensitive Endpoints On Your** Account
e.g. <http://company.com/privilege-escalation>
- 3 - **Add admin=True** To This endpoint e.g
<http://company.com/privilege-escalation?admin=True>



attacker

My Methodology

Create **Two Accounts Admin AND User** , From Admin Account Find All Sensitive Endpoints Then From User **Add .json** To All Endpoints



Tweet

Steps to produce :-

- 1 - Create **Two Accounts Admin And User**
- 2 - Find All **Sensitive Endpoints From Admin** Account
e.g. `http://company.com/privilege-escalation`
- 3 - From **User Account Add .json** To This Endpoint e.g
`http://company.com/privilege-escalation.json`

Thank You

Mahmoud M. Awali

 **@0xAwali**