BAC

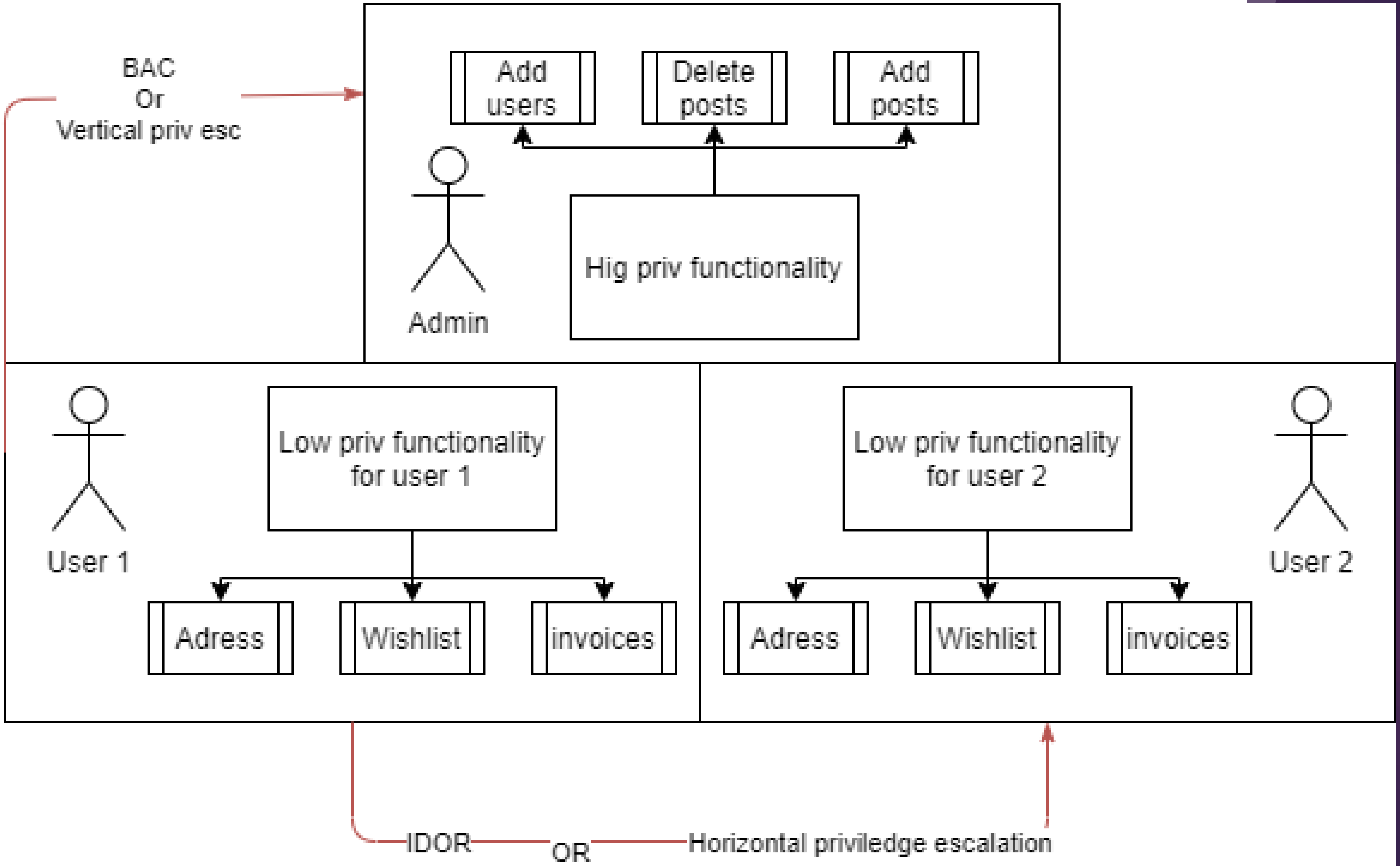
BY UNCLE RAT

Agenda

- What is BAC
- Attack Strategy
  - Manually
  - Semi-automated strategy

What is BAC?

What is BAC (Broken Access Control)



What is BAC (Broken Access Control)

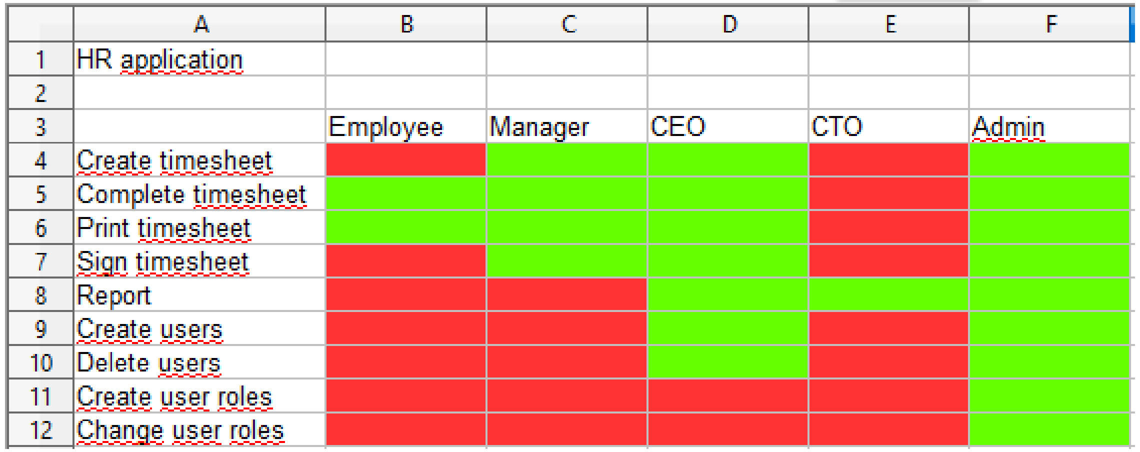
- Privilege escalation
  - Vertical
  - Horizontal
- Examples:
  - We have an admin and a normal user. We can test the admin settings with the low priv user
  - We have a normal user and a prospect user. The prospect user can not execute all the functions because he only has a trial account
  - We have two users of the same authorization level: See IDOR

Attack strategy

Attack Strategy – General tips

- Make sure we have the right target
  - Need users with different access levels for vertical priv esc
  - Need multiple accounts for IDOR (See IDOR chapter)
    - No static websites
- Create a mindmap of the target
  - Note down functionalities
  - Note down priviledge levels
  - Indicate if priviledge level can execute functionality

Attack Strategy – General tips



	A	B	C	D	E	F
1	HR application					
2						
3		Employee	Manager	CEO	CTO	Admin
4	Create timesheet	🟥	🟩	🟩	🟥	🟩
5	Complete timesheet	🟩	🟩	🟩	🟥	🟩
6	Print timesheet	🟩	🟩	🟩	🟥	🟩
7	Sign timesheet	🟥	🟩	🟩	🟥	🟩
8	Report	🟥	🟥	🟩	🟩	🟩
9	Create users	🟥	🟥	🟩	🟥	🟩
10	Delete users	🟥	🟥	🟩	🟥	🟩
11	Create user roles	🟥	🟥	🟥	🟥	🟩
12	Change user roles	🟥	🟥	🟥	🟥	🟩

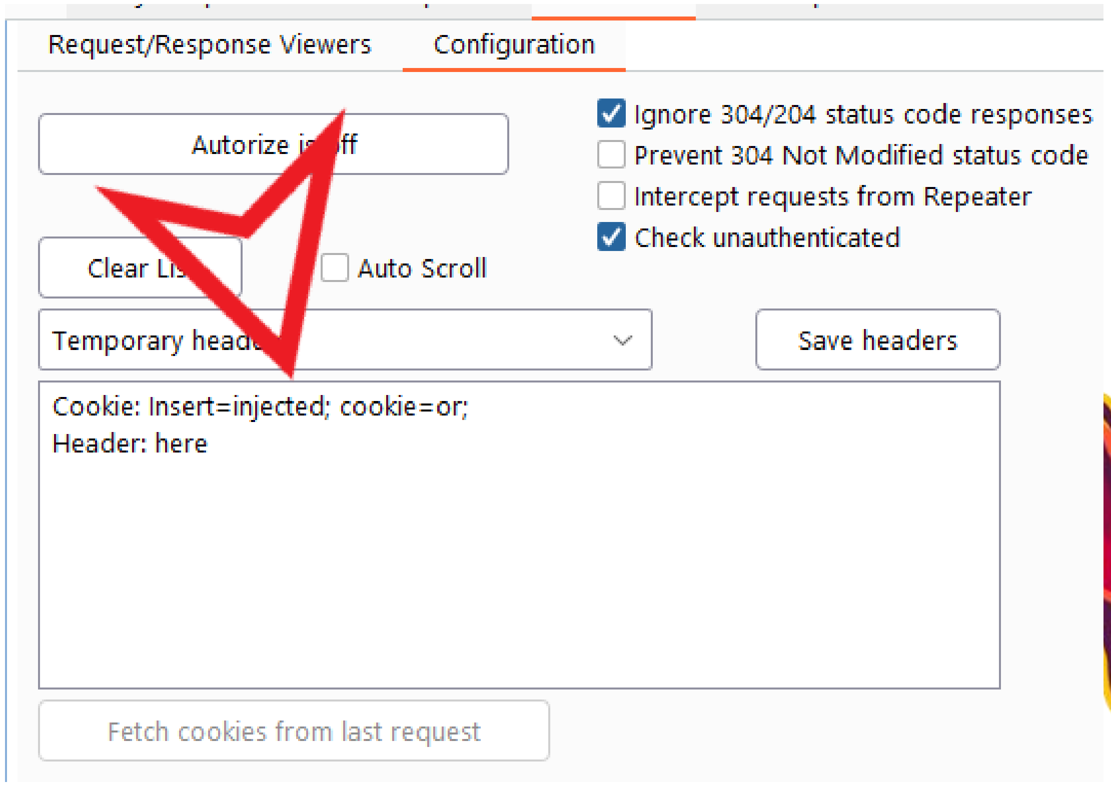
- Test BAC for all different priviledge levels
- The CTO might have different BAC issues than an employee

Attack Strategy – Manual

- Sometimes if user can not execute function, front end button is just hidden
  - Javascript function might still work
  - We can execute javascript function via the developer console
- We can just log in as admin and copy & paste URL of functions we should not execute as low priv user
- We can execute request as admin and capture in burp, then send to repeater and paste in low priv user authorization header

Attack Strategy – Semi-automated

- We can use authorise – free burp extension
  - Log in as low priv user
  - Copy their cookie
  - Paste it in authorise
  - Log in as admin user
  - Activate Authorise
  - See tools chapter for guide

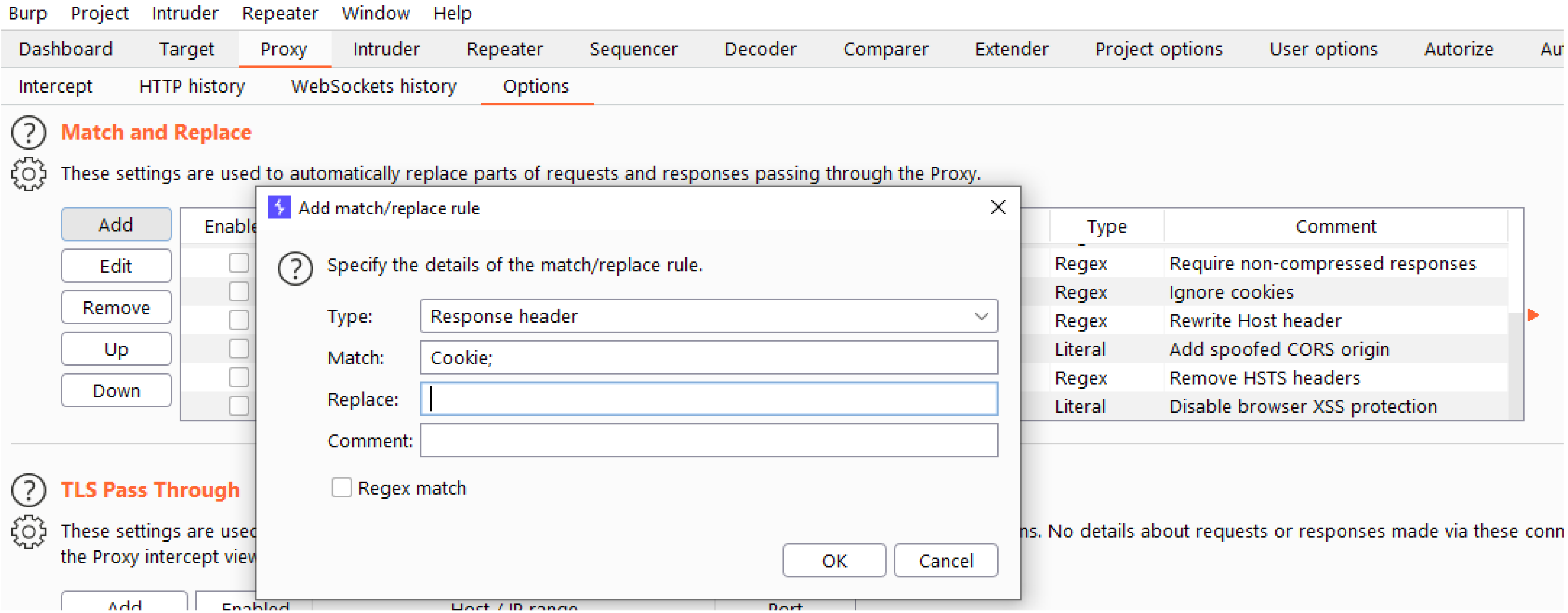


☑ Ignore 304/204 status code responses
□ Prevent 304 Not Modified status code
□ Intercept requests from Repeater
☑ Check unauthenticated
□ Auto Scroll

```
Cookie: Insert=injected; cookie=or;
Header: here
```

Attack Strategy – Semi-automated

- Auto repeater
- Match and replace


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Autorize Au
Intercept HTTP history WebSockets history Options
Add
Edit
Remove
Up
Down
OK
Cancel
Add
Enabled
Host / IP range
Port

Match and Replace

These settings are used to automatically replace parts of requests and responses passing through the Proxy.

Enable	Type	Comment
□	Regex	Require non-compressed responses
□	Regex	Ignore cookies
□	Regex	Rewrite Host header
□	Literal	Add spoofed CORS origin
□	Regex	Remove HSTS headers
□	Literal	Disable browser XSS protection

Add match/replace rule

Specify the details of the match/replace rule.

Type: Response header

Match: Cookie;

Replace:

Comment:

□ Regex match

TLS Pass Through

These settings are used ... ns. No details about requests or responses made via these conn

the Proxy intercept view