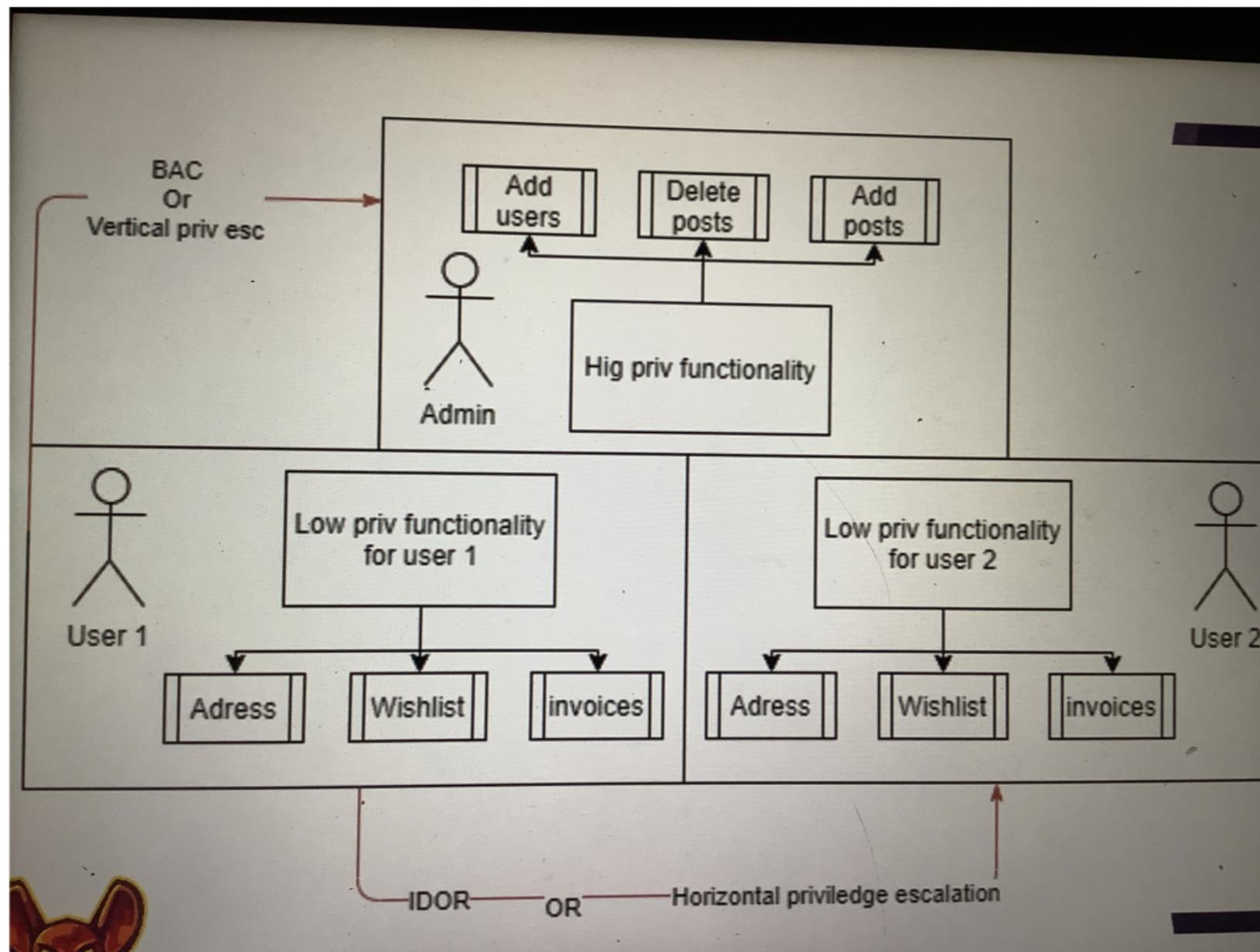


XSS rat broken access control

Requires access to different priv-levels ↗



↗ this is mainly focused on Vertical

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 privilege levels
 - ▶ Indicate if privilege level can execute functionality

* make sure there are privilege levels!!

* if application is qualified for BAC record priv levels

in min may

tips

Attack Strategy – General tips

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

	A	B	C	D	E	F
1	HR application					
2						
3		Employee	Manager	CEO	CTO	
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					



Y
test all levels!

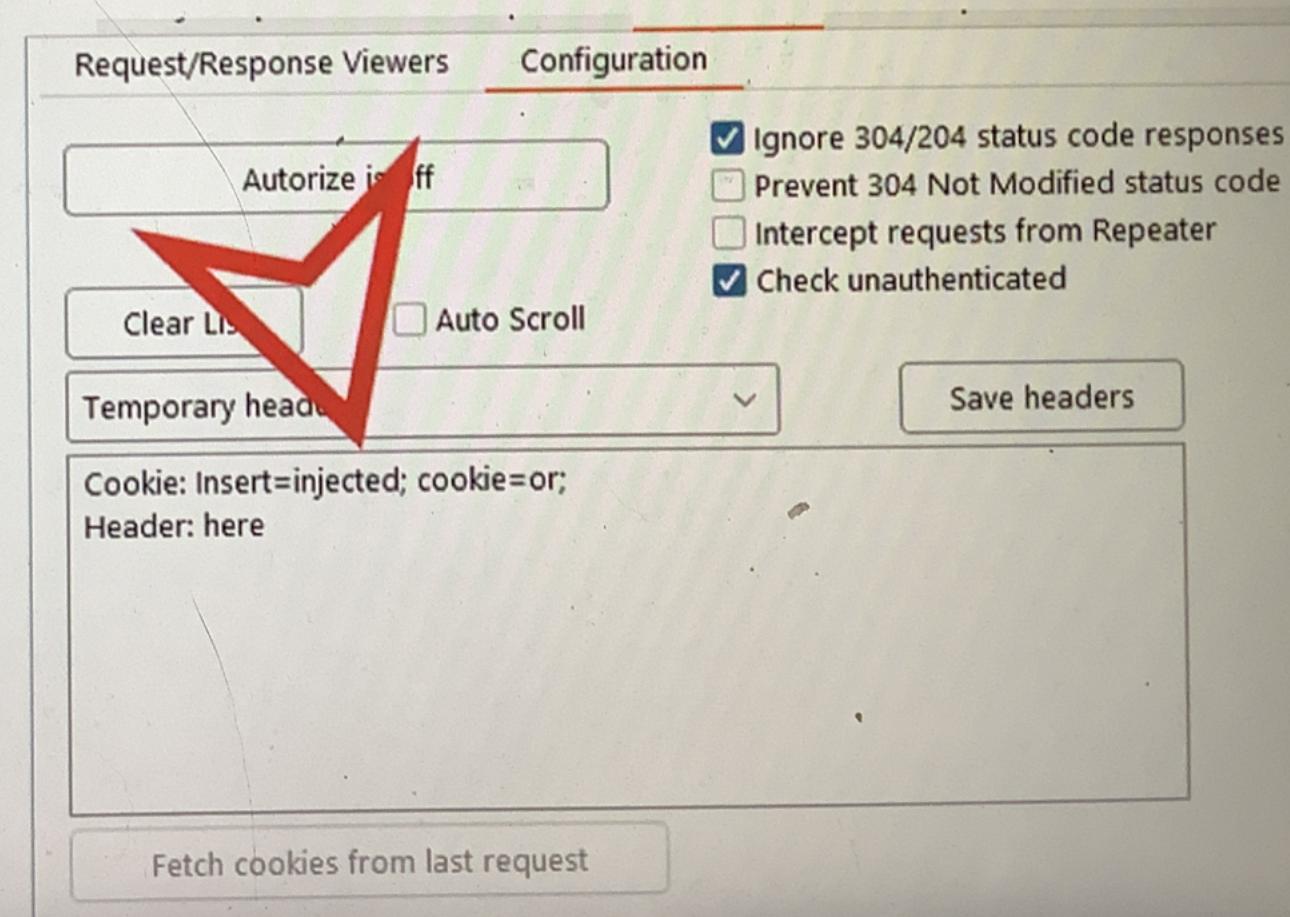
Attack Strategy – Manual

- ▶ 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



Attack Strategy – Semi-automated

- ▶ Auto repeater
- ▶ Match and replace

The screenshot shows the Burp Suite proxy tab interface. The 'Proxy' tab is selected, and the 'Match and Replace' option under the 'Options' menu is highlighted with a red oval. A large red oval also highlights the 'Match and Replace' section in the main pane. The 'Add match/replace rule' dialog is open, showing a configuration for a 'Response header' type rule. The 'Match' field contains 'Cookie:' and the 'Replace' field contains 'Ko'. A list of available rules is visible on the right.

Match and Replace

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

Add match/replace rule

Type: Response header

Match: Cookie:

Replace: Ko

Comment:

Regex match

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

↳ as we browse burp will auto - update the headers
will show more false positives but still good

Really make sure to take good notes, and
really map out functionality and different privileges.