



BAC

BY UNCLE RAT

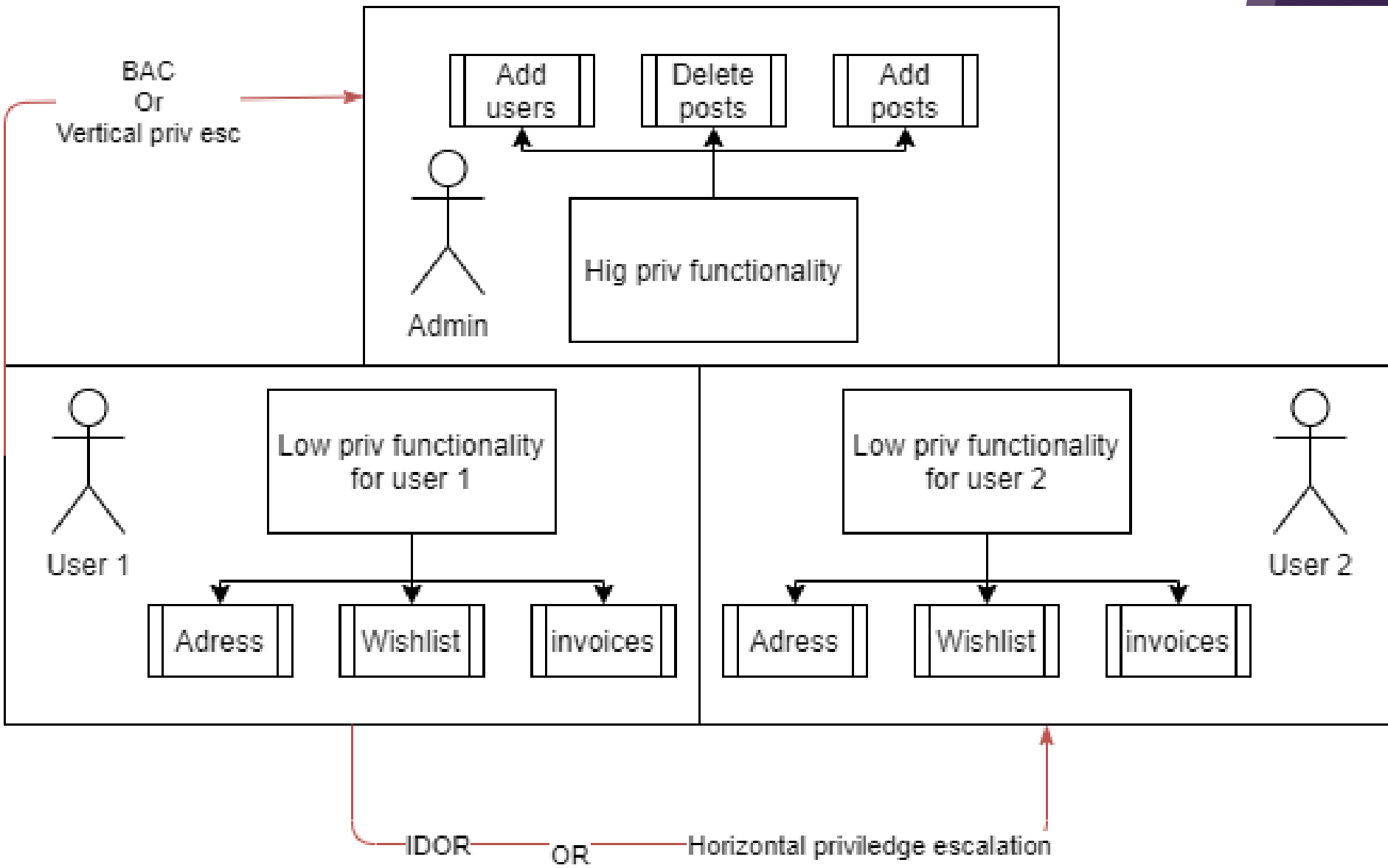
Agenda

- ▶ 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 privilege levels
 - ▶ Indicate if privilege level can execute functionality



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	<u>HR application</u>					
2						
3		Employee	Manager	CEO	CTO	Admin
4	<u>Create timesheet</u>	Red	Green	Green	Red	Green
5	<u>Complete timesheet</u>	Green			Red	
6	<u>Print timesheet</u>	Green			Red	
7	<u>Sign timesheet</u>	Red	Green		Red	
8	Report	Red	Red	Green	Green	
9	<u>Create users</u>	Red	Red	Green	Red	
10	<u>Delete users</u>	Red	Red	Green	Red	
11	<u>Create user roles</u>	Red	Red	Red	Red	Green
12	<u>Change user roles</u>	Red	Red	Red	Red	Green



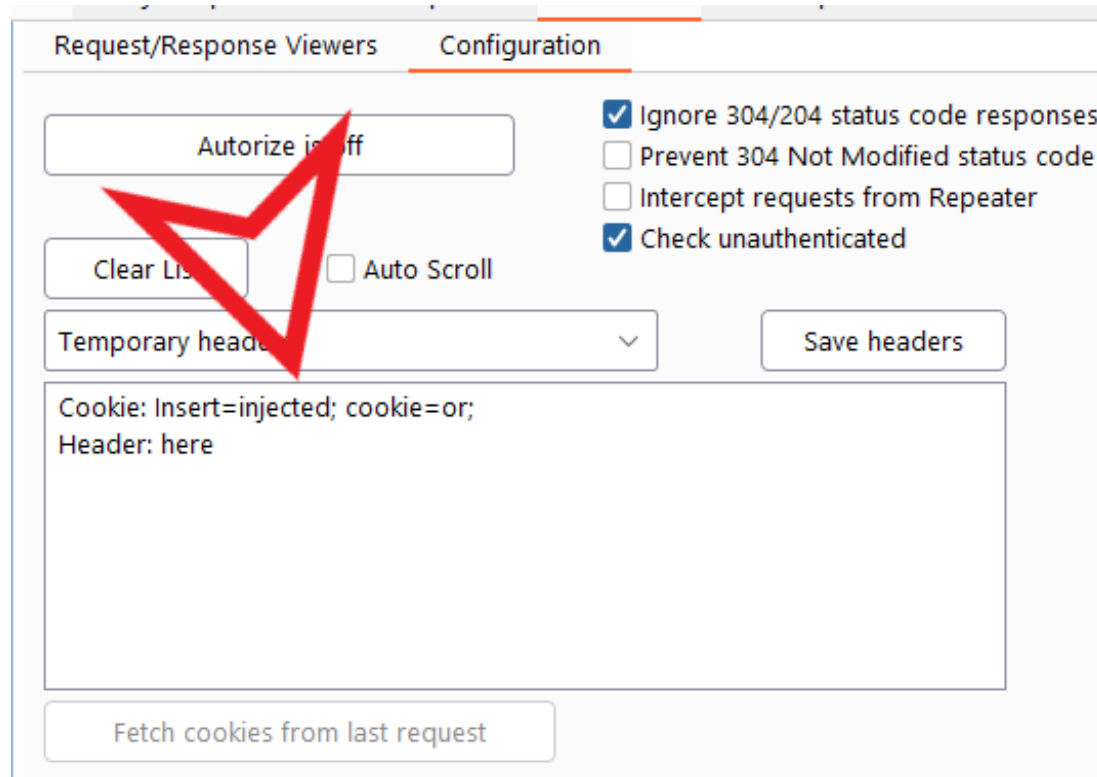
Attack Strategy – Manual

- ▶ 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



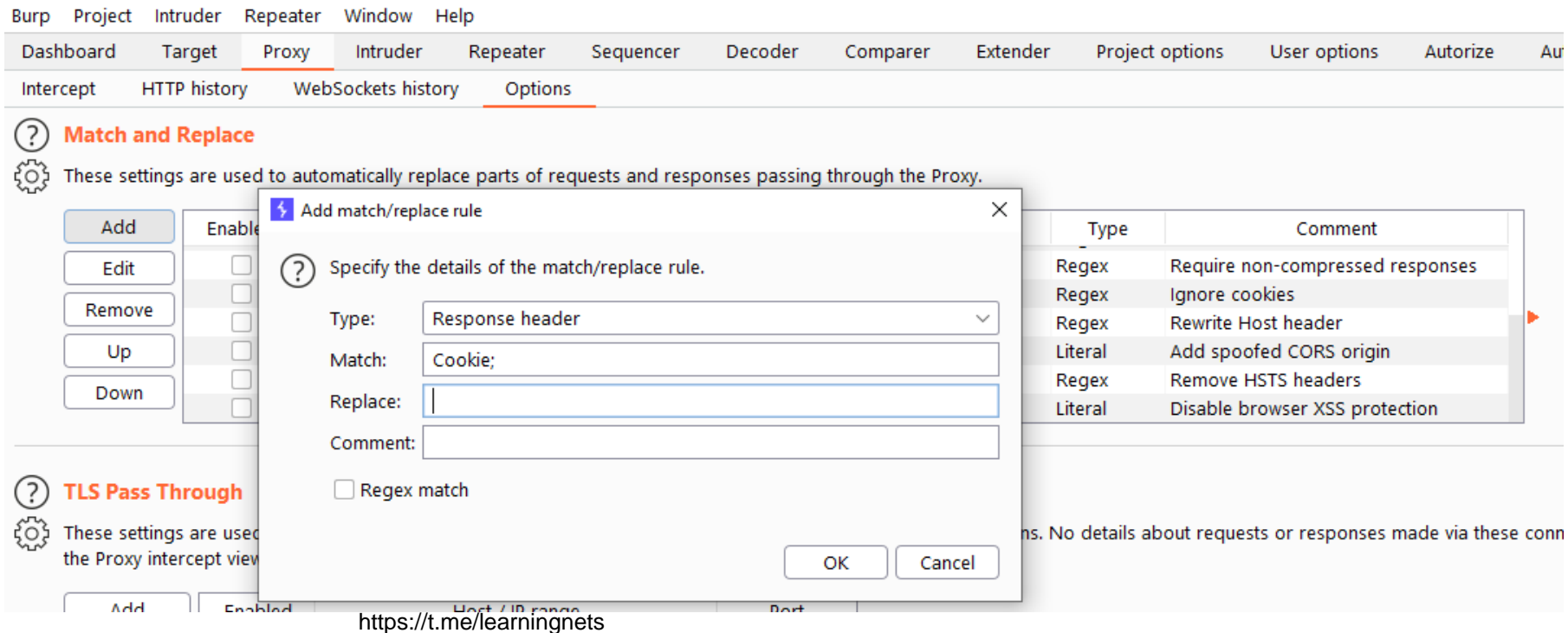
Attack Strategy – Semi-automated

- ▶ 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 interface with the Proxy tab selected. The 'Options' sub-tab is active, displaying the 'Match and Replace' settings. A dialog box titled 'Add match/replace rule' is open, allowing the user to specify details for a new rule. The 'Type' is set to 'Response header', the 'Match' is 'Cookie;', and the 'Replace' field is empty. The 'Comment' field is also empty. The 'Regex match' checkbox is unchecked. In the background, a table lists existing rules:

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

At the bottom of the screenshot, a URL is visible: <https://t.me/learningnets>.

