CAPTURE THE FLAG CHEATSHEET

1 WHERE TO BEGIN

- Read the challenge title & instructions well, as there may be some clues hidden....
- Same for the responses sent back by the server via browser or Burp

2 WHAT TOOLS TO USE

- Browser console
- Client API documentation: apidocs.rnd.mendix.com/9/client/
- Burp Suite or similar
- Ciphx Mendix Developer Tools (CDT)

3 WHAT TO LOOK FOR

- Exposed constants
- Too permissive entity access
- Accessible nano-/microflows that you may not access via UI
- Vulnerable REST endpoints
- Leaked data through exposed documents
- Clues in anything accessible

4 SOME EXTRA HINTS

- Execute found micro-/nanoflows with altered parameters (or none)
- Tamper with data sent when client executes microflow on server
- Retrieve data from entities with more access and adjust if possible
- Intercept data from server with burp and tamper with the data sent to the server

5 WHAT NOT TO DO!

- Rely on the UI as is. The UI will make it seem everything is secure.
- Brute force infrastructure attacks won't work! This will also cause unneeded pressure for the infra, so keep calm and carry on hacking.

STILL STUCK?
Reach out to our coaches!

Blue Green SOLUTIONS

MEET THE BLUE GREEN COACHES

Jay Cadogan

Jappe Kuijlman

Leon De Kuiper

Xavier Veul

Tom Brand

Lucas van Oosten

Eric Weijers

Nina Morsa

Mitchel Mol

Blue Green SOLUTIONS