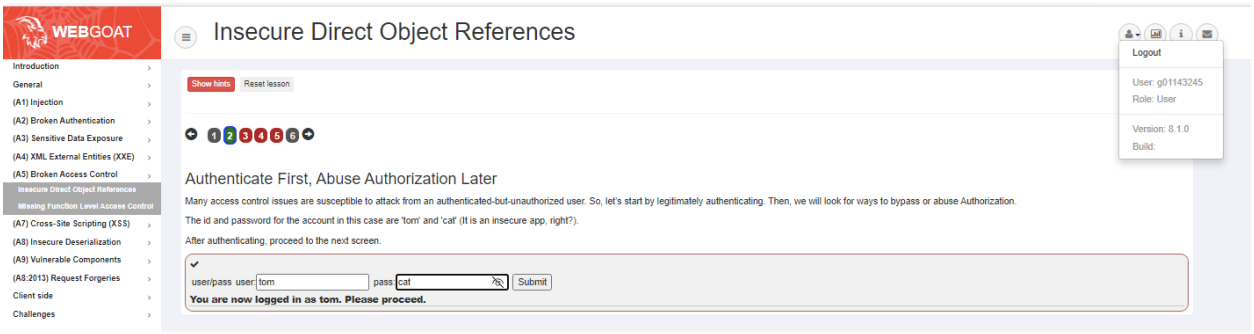
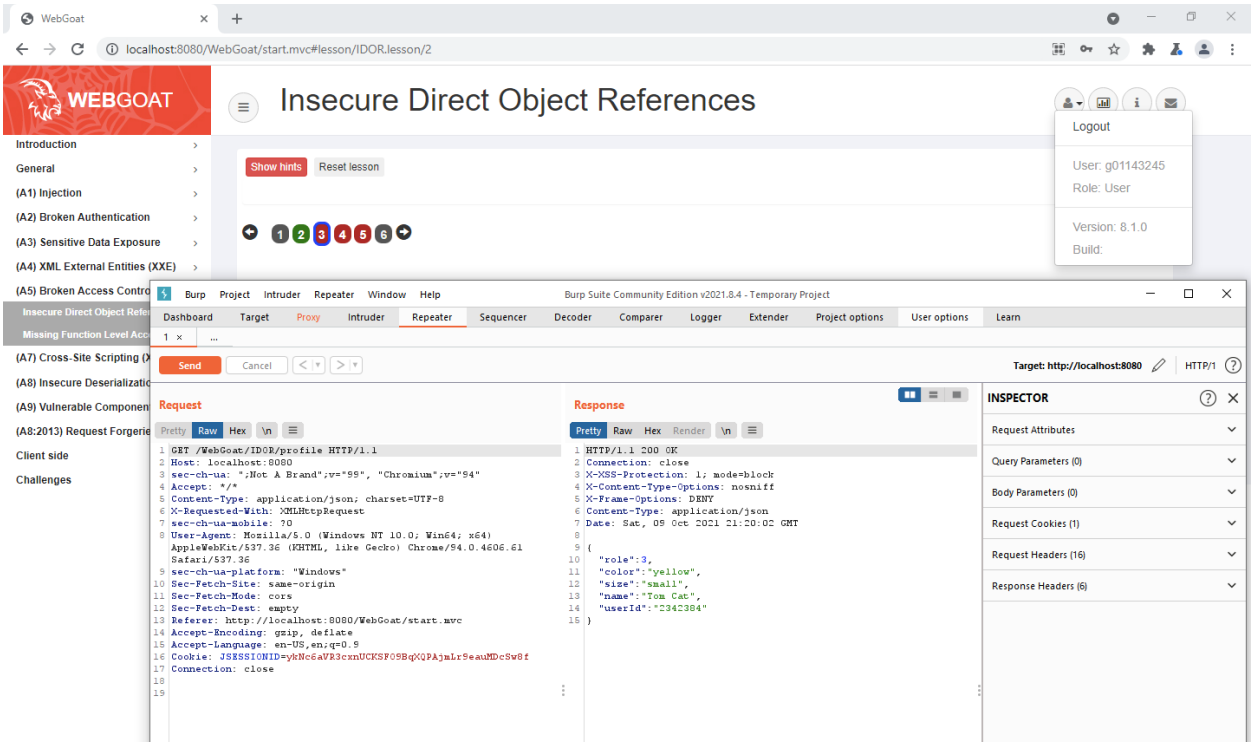
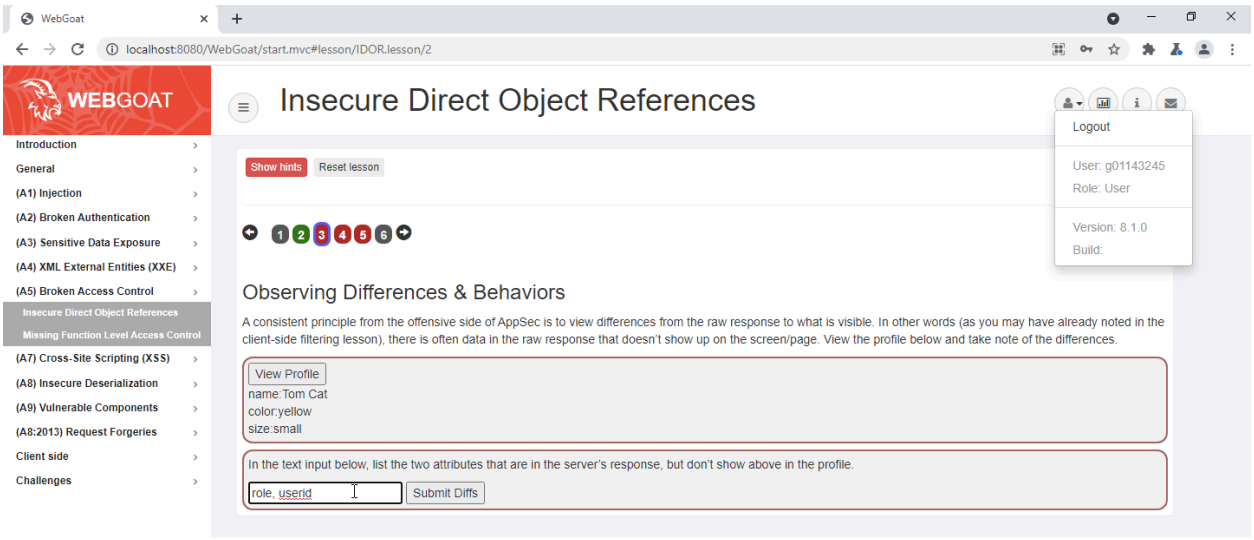
Roozah Khan

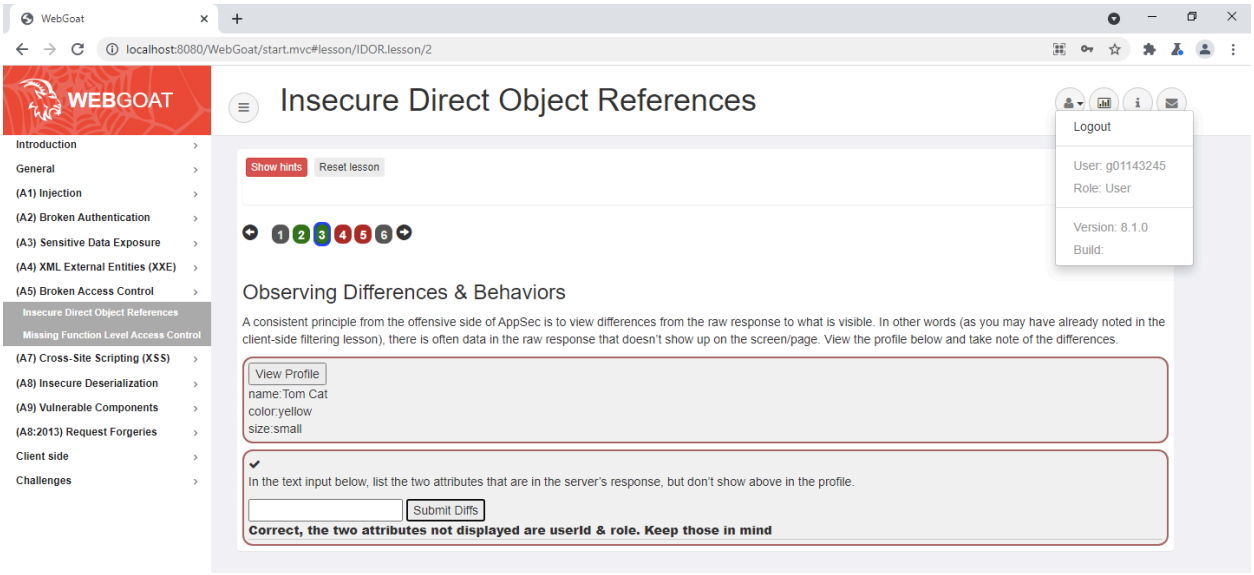
a.





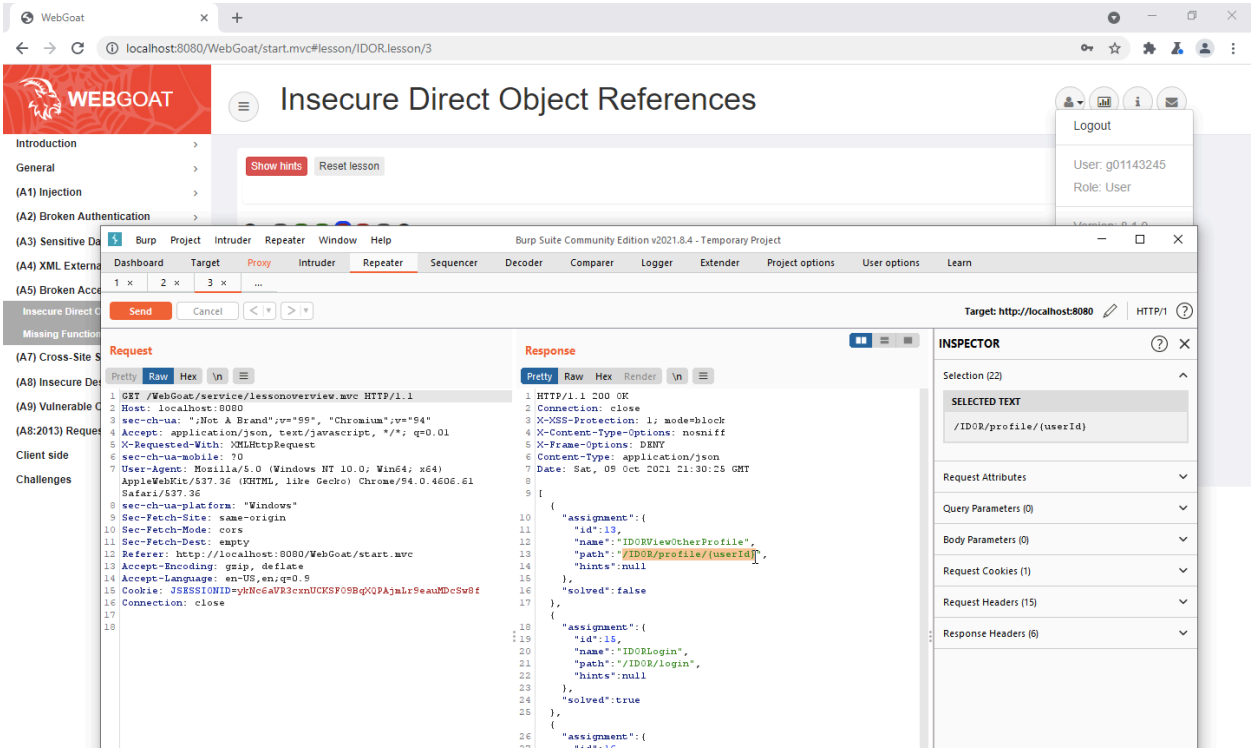
Roozah Khan

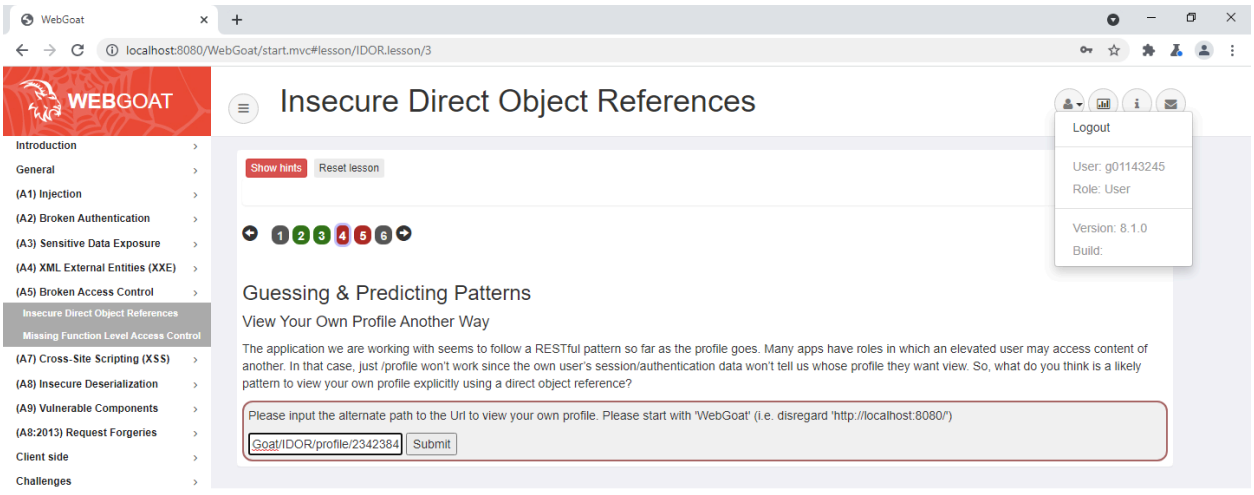

WebGoat
localhost:8080/WebGoat/start.mvc#lesson/IDOR.lesson/2
WEBGOAT
Insecure Direct Object References
Introduction
General
(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
Insecure Direct Object References
Missing Function Level Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A8:2013) Request Forgeries
Client side
Challenges
Show hints
Reset lesson
Logout
User: g01143245
Role: User
Version: 8.1.0
Build:
Observing Differences & Behaviors
A consistent principle from the offensive side of AppSec is to view differences from the raw response to what is visible. In other words (as you may have already noted in the client-side filtering lesson), there is often data in the raw response that doesn't show up on the screen/page. View the profile below and take note of the differences.
View Profile
name:Tom Cat
color:yellow
size:small
In the text input below, list the two attributes that are in the server's response, but don't show above in the profile.
role, userid
Submit Diffs


WebGoat
localhost:8080/WebGoat/start.mvc#lesson/IDOR.lesson/2
WEBGOAT
Insecure Direct Object References
Introduction
General
(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
Insecure Direct Object References
Missing Function Level Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A8:2013) Request Forgeries
Client side
Challenges
Show hints
Reset lesson
Logout
User: g01143245
Role: User
Version: 8.1.0
Build:
Observing Differences & Behaviors
A consistent principle from the offensive side of AppSec is to view differences from the raw response to what is visible. In other words (as you may have already noted in the client-side filtering lesson), there is often data in the raw response that doesn't show up on the screen/page. View the profile below and take note of the differences.
View Profile
name:Tom Cat
color:yellow
size:small
In the text input below, list the two attributes that are in the server's response, but don't show above in the profile.
Submit Diffs
Correct, the two attributes not displayed are userId & role. Keep those in mind

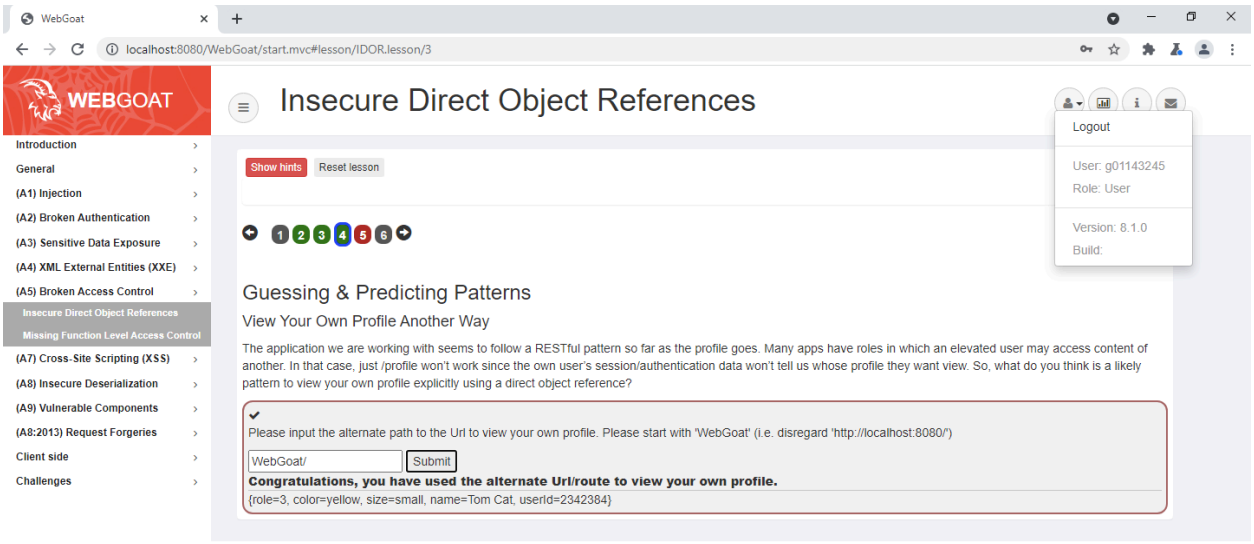
Roozah Khan

b.

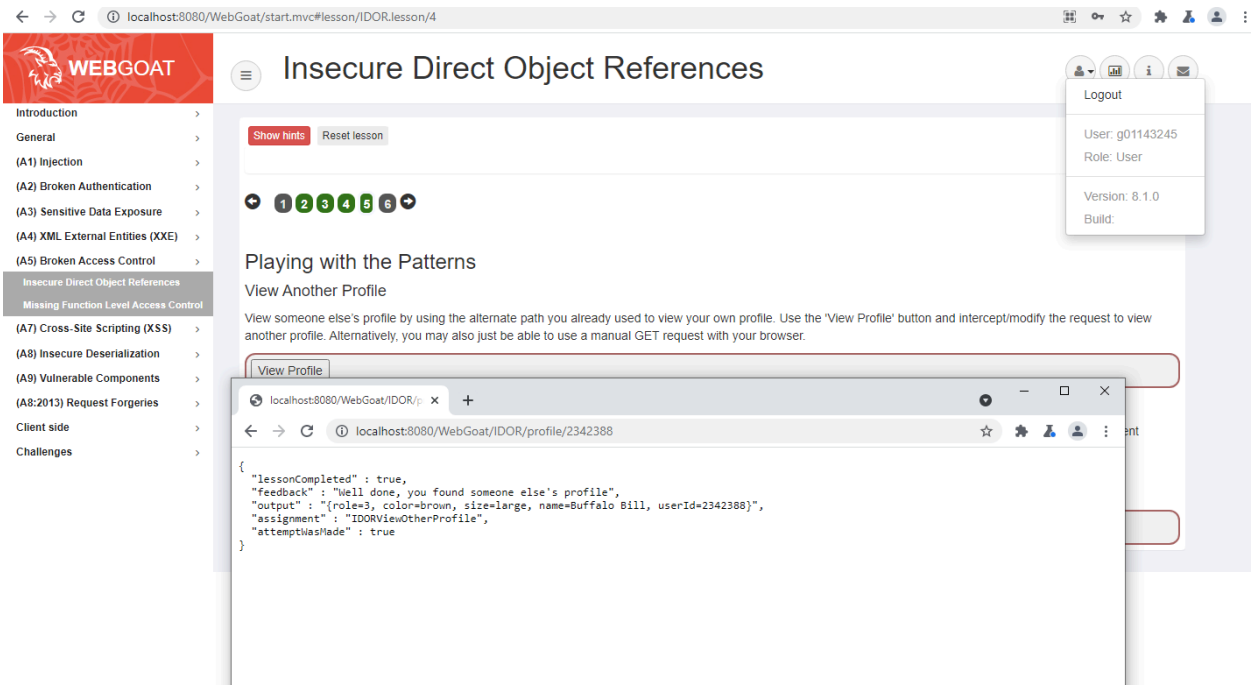




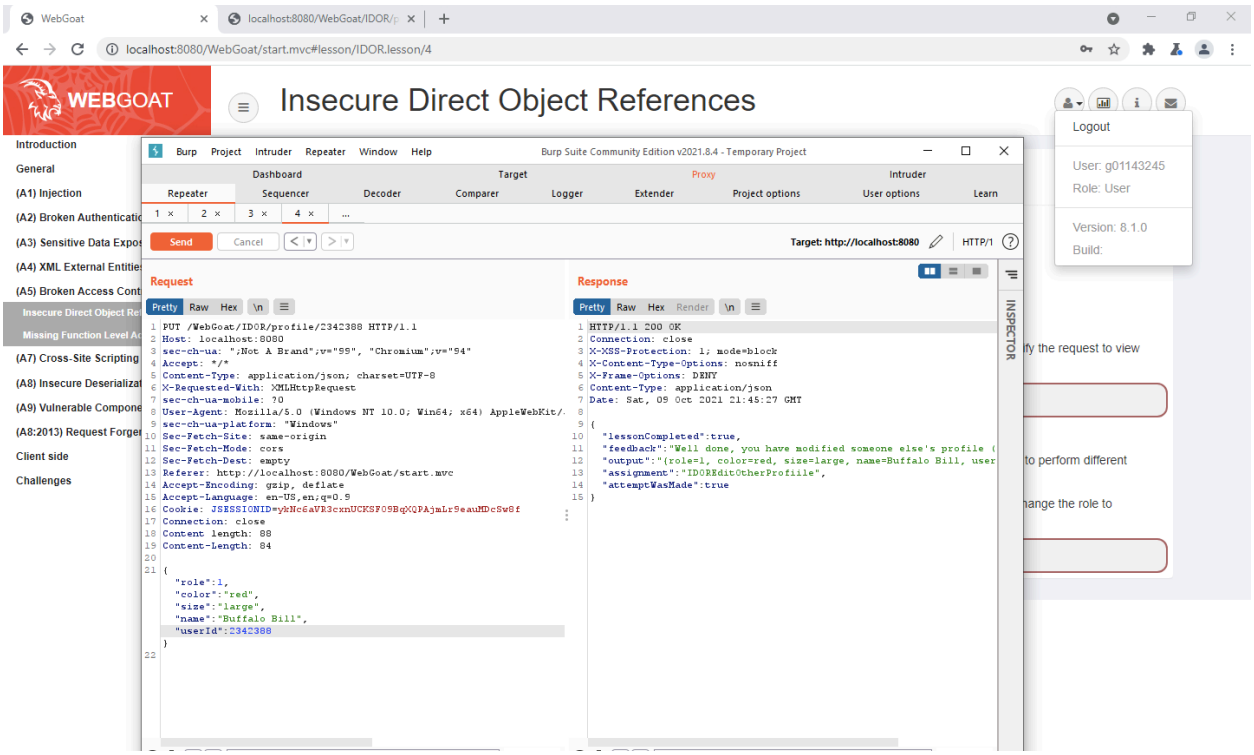
Roozah Khan



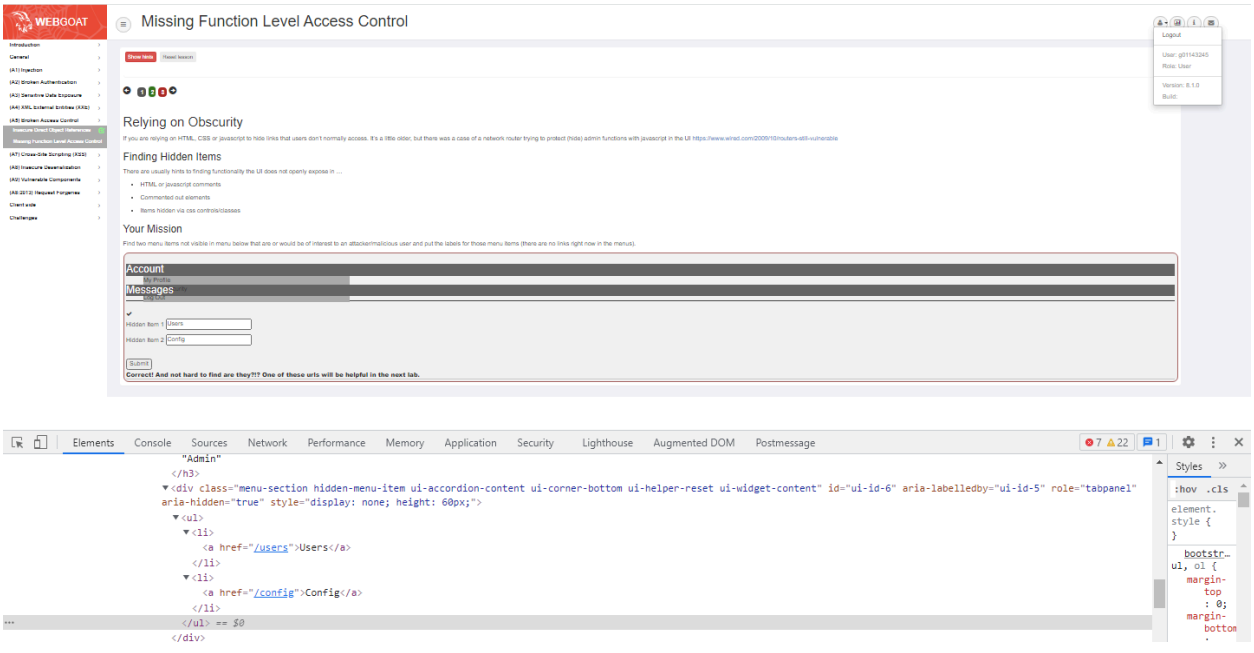
C.



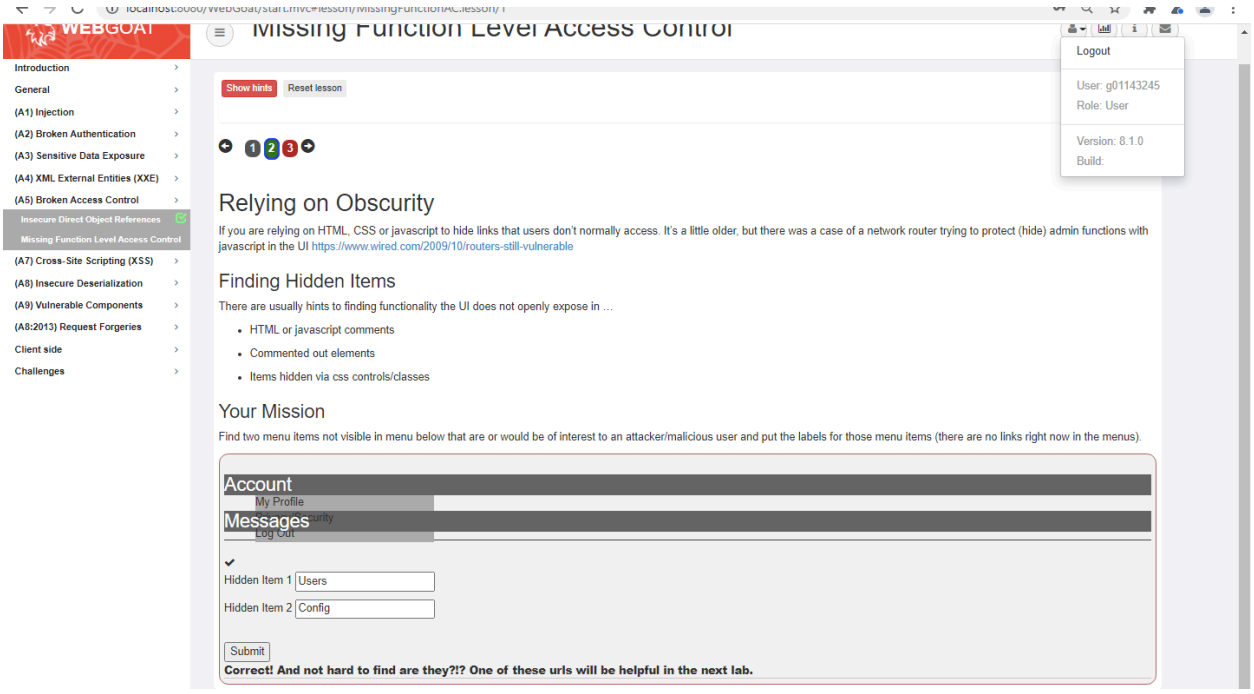
Roozah Khan



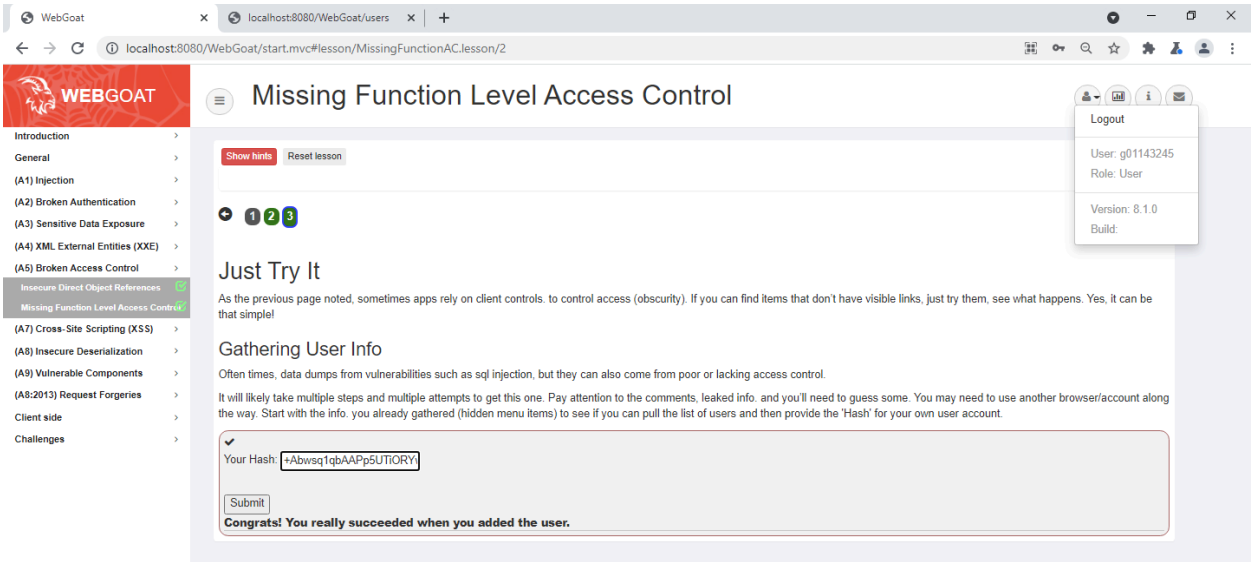
d.



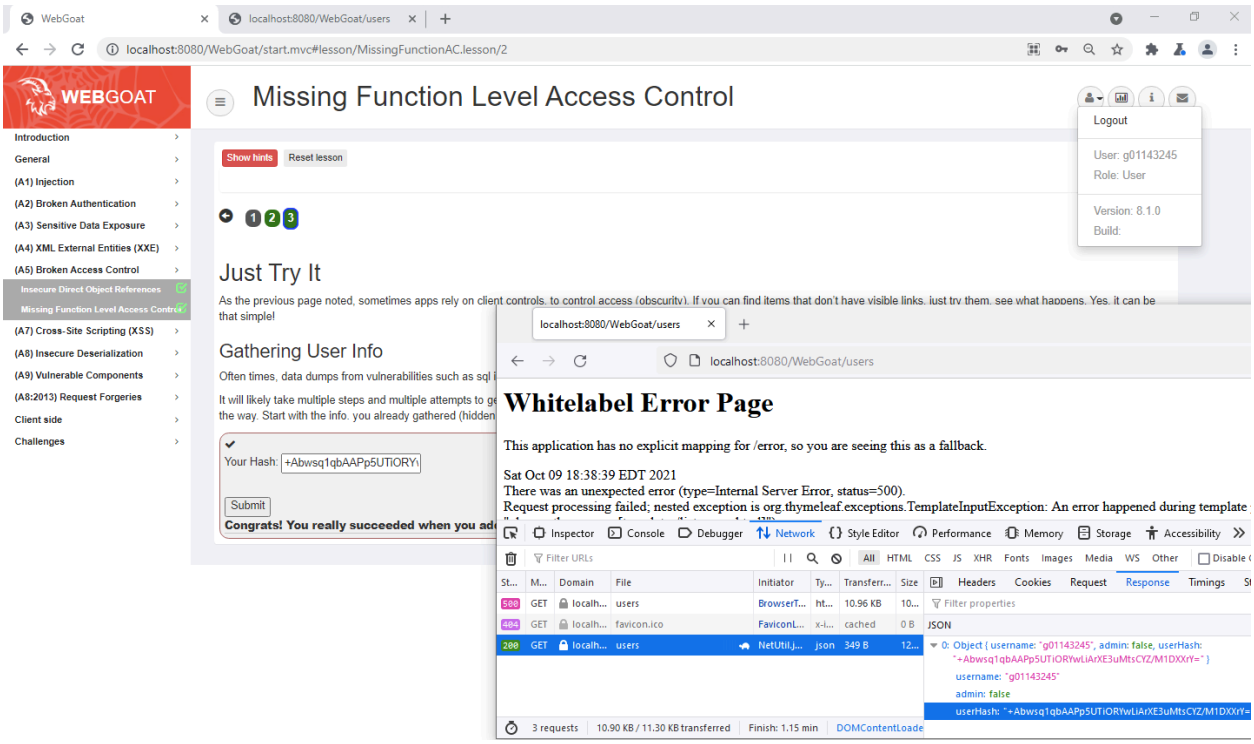
Roozah Khan



e.



Roozah Khan


WebGoat
localhost:8080/WebGoat/users
localhost:8080/WebGoat/start.mvc#lesson/MissingFunctionAC.lesson/2
WEBGOAT
Missing Function Level Access Control
Introduction
General
(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
Insecure Direct Object References
Missing Function Level Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A8:2013) Request Forgeries
Client side
Challenges
Show hints
Reset lesson
Logout
User: g01143245
Role: User
Version: 8.1.0
Build:
Just Try It
As the previous page noted, sometimes apps rely on client controls to control access (obscurity). If you can find items that don't have visible links, just try them, see what happens. Yes, it can be that simple!
Gathering User Info
Your Hash:
Submit
Congrats! You really succeeded when you ad
localhost:8080/WebGoat/users
Whitelabel Error Page
This application has no explicit mapping for /error, so you are seeing this as a fallback.
Sat Oct 09 18:38:39 EDT 2021
There was an unexpected error (type=Internal Server Error, status=500).
Request processing failed; nested exception is org.thymeleaf.exceptions.TemplateInputException: An error happened during template
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Headers
Cookies
Request
Response
Timings
JSON
username: "g01143245"
admin: false
3 requests
10.90 KB / 11.30 KB transferred
Finish: 1.15 min
DOMContentLoade