Title: Broken Access Control — Unauthorized Reaccess to Completed Exam
Reported by: Ali Shaker Alawami, Bakr Abdulaziz Alrayes
Course: Cybersecurity stream
Instructor / Contact: Atharva Bhamburkar
Date discovered: [2025-10-28]
Date reported: [2025-11-02]

Executive summary:

While testing the Academy portal after submitting an exam, it was discovered that navigating directly to the exam's URL allowed the previously submitted exam page to reload. The system appeared to reinitialize the exam interface, presenting the same questions and interface as before submission as long as it was navigated to while the exam is still on going. However, attempts to resubmit did not register a second submission.

This indicates that the portal fails to properly enforce access control or session restrictions on completed exam resources. This constitutes a Broken Access Control vulnerability where exam access states are not properly validated on the backend after submission.

Vulnerability classification / definition:

Name: Broken Access Control — Insecure Direct Object Reference (IDOR) / Missing state validation after exam submission

Definition: Broken Access Control occurs when an application fails to properly enforce access rules on resources or actions. This allows users to access or interact with application components that should be restricted. In this case, the backend does not correctly enforce the "completed" state of an exam, allowing unauthorized reaccess to previously submitted exams by directly visiting the resource URL.

Risk: Allows unauthorized re-access to completed exams, exposing exam content that should be inaccessible after submission. This could enable students to retain exam questions or share them with others, undermining exam integrity and assessment fairness.

Affected URLs / resources

This is not a comprehensive list as its possible with almost all lecture slides pages a student has access to.

- https:/[redacted]/course/24/objective-test

Other test URLs follow the same structure where [TEST_ID] is replaced with the test ID for that specific assessment.

https://[redacted]/course/[TEST_ID]/objective-test

Affected systems / components

- **Frontend exam interface:** Exam viewing and submission logic
- **Backend exam endpoint:** Resource handler that fails to validate completion state before rendering exam content.
- **Access control layer:** Missing server-side checks to restrict access to completed exam resources.

How issue was observed:

1- After we completed and submitted an exam through the Academy portal we refreshed the to see what would happen. We noticed that the exam relaunched as if it was a new attempt.

2- We then copied the assessment URL and closed the tab, then we pasted it in a new tab to go to the exam manually. We observed that it launched the exam again.

3- Attempting to submit again resulted in an error — confirming the system recognizes completion but does not restrict viewing access.

How to reproduce the issue:

1- Log in to the Academy portal.

2- Start and complete any available exam.

3- After submission, copy or note the exam's direct URL (e.g., https://[redacted]/course/[TEST_ID]/objective-test).

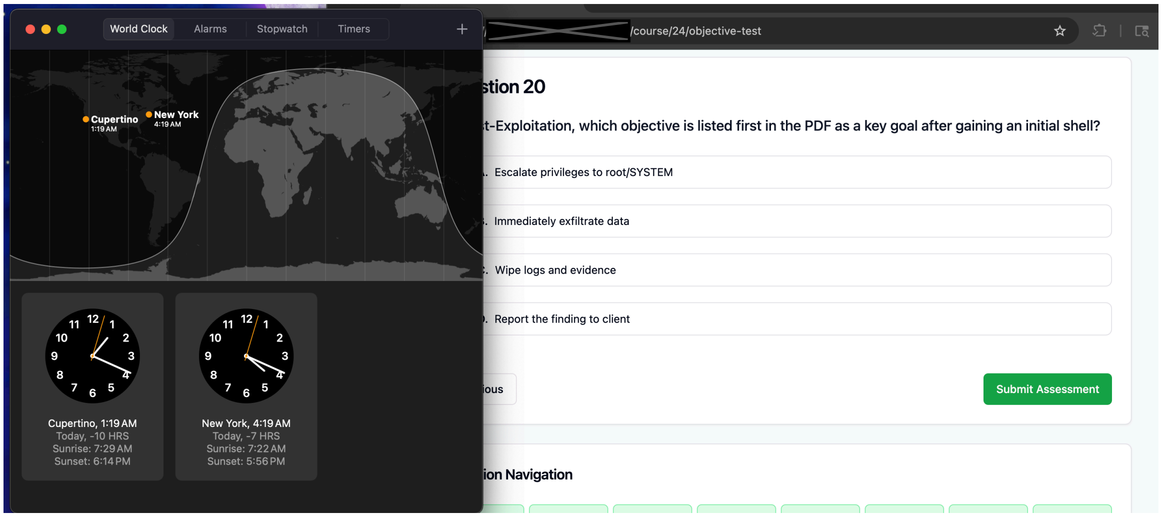
4- Paste the same URL into the browser address bar and load it again.

5- Observe that the exam interface reappears, allowing full access to questions despite completion.

6- Attempting to resubmit does not process, confirming limited backend validation.

Evidence:

1- Take the exam and copy the URL. Note the time.



Cupertino, 1:19 AM
Today, -10 HRS
Sunrise: 7:29 AM
Sunset: 6:14 PM

New York, 4:19 AM
Today, -7 HRS
Sunrise: 7:22 AM
Sunset: 5:56 PM

[redacted]/course/24/objective-test

stion 20

t-Exploitation, which objective is listed first in the PDF as a key goal after gaining an initial shell?

. Escalate privileges to root/SYSTEM

. Immediately exfiltrate data

. Wipe logs and evidence

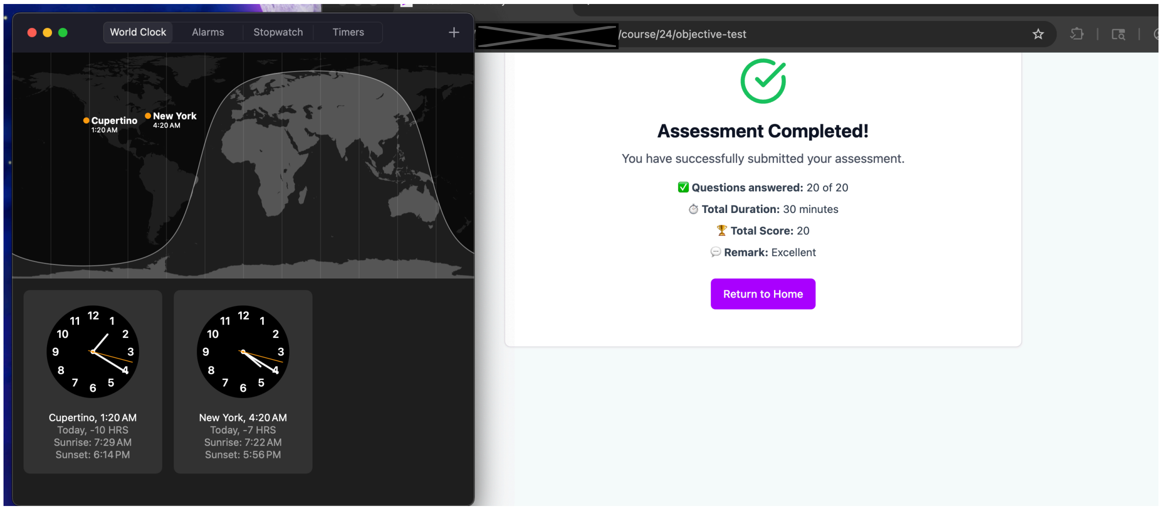
. Report the finding to client

ious

Submit Assessment

ion Navigation

2- Submit the exam. Note that the time is after step 1.



Cupertino, 1:20 AM
Today, -10 HRS
Sunrise: 7:29 AM
Sunset: 6:14 PM

New York, 4:20 AM
Today, -7 HRS
Sunrise: 7:22 AM
Sunset: 5:56 PM

[redacted]/course/24/objective-test

Assessment Completed!

You have successfully submitted your assessment.

✅ **Questions answered:** 20 of 20

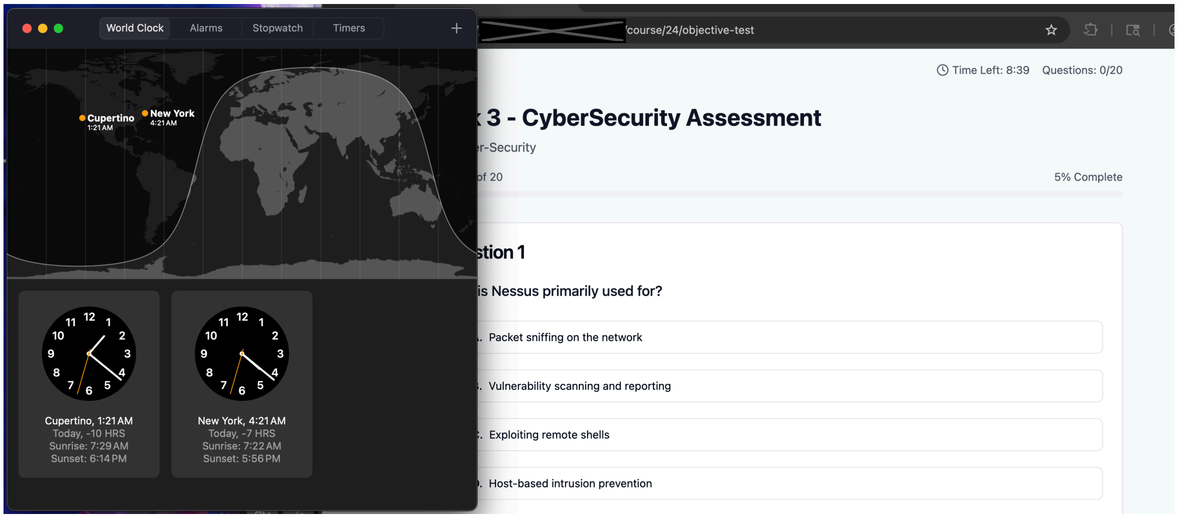
⏱ **Total Duration:** 30 minutes

🏆 **Total Score:** 20

💬 **Remark:** Excellent

Return to Home

3- Refresh the page or paste the URL you copied in step 1. Note the time is after submission.



Cupertino, 1:21 AM
Today, -10 HRS
Sunrise: 7:29 AM
Sunset: 6:14 PM

New York, 4:21 AM
Today, -7 HRS
Sunrise: 7:22 AM
Sunset: 5:56 PM

[redacted]/course/24/objective-test

Time Left: 8:39 Questions: 0/20

k 3 - CyberSecurity Assessment

er-Security

of 20

5% Complete

stion 1

is Nessus primarily used for?

. Packet sniffing on the network

. Vulnerability scanning and reporting

. Exploiting remote shells

. Host-based intrusion prevention

Mitigation and Recommendations:

To mitigate the Broken Access Control vulnerabilities identified we recommend the following:

- Enforce server-side state validation on exam endpoints to ensure that once an exam is submitted, the user cannot re-access it.
- Implement proper session invalidation or redirect users attempting to load completed exams to a summary or results page.
- Use backend checks (not just frontend flags) to restrict rendering of exam content after submission.
- Log and monitor all exam access attempts to detect and prevent post-submission reaccess patterns.