Title: Broken Authentication & Session Management — Cookie Replay and Session Persistence
Reported by: Ali Shaker Alawami, Bakr Abdulaziz Alrayes
Course: Cybersecurity stream
Instructor / Contact: Atharva Bhamburkar
Date discovered: [2025-10-16]
Date reported: [2025-10-27]

Executive summary:

Following the release of the assessment results, each student was assigned a unique results page accessible only through authentication. Initial access control checks correctly prevented unauthorized viewing of other students' results. However, during testing, it was found that replacing the browser's authentication and refresh cookies with those belonging to another student while remaining on the home page—and then clicking on the "Results" button—granted full access to that other student's exam results.

This demonstrates a **session management flaw** that permits user impersonation through **cookie replay**. The issue represents a critical **Broken Authentication and Session Management** vulnerability with potential **confidentiality** and **integrity** impacts on sensitive assessment data.

Further investigation revealed that if the victim logs out and then logs back in, starting a new session, the hijacked session remains active for the attacker. This indicates improper **session termination handling**, allowing concurrent active sessions under the same account and further exacerbating the risk of unauthorized access.

Vulnerability Classification / Definition:

Name: Broken Authentication & Session Management — Cookie Replay & Incomplete Session Invalidation

Definition: Broken authentication occurs when application mechanisms responsible for identity verification, session management, or credential handling are improperly implemented, allowing attackers to assume other users' identities. A cookie replay vulnerability arises when session cookies can be reused or injected into another browser to impersonate the legitimate user. Improper session invalidation occurs when logout actions fail to terminate all active sessions associated with the user, leaving stale sessions exploitable.

Risk: Enables full unauthorized access to another user's account and exam results, compromising confidentiality and integrity of sensitive academic information. Also allows persistent unauthorized sessions to remain active even after logout, violating expected authentication lifecycle controls and privacy requirements.

Affected Systems / Components:

- **Authentication and Session Management Module:** Fails to securely associate session tokens with specific devices, IPs, or user contexts. Accepts replayed cookies from another authenticated session without revalidation, allowing user impersonation.

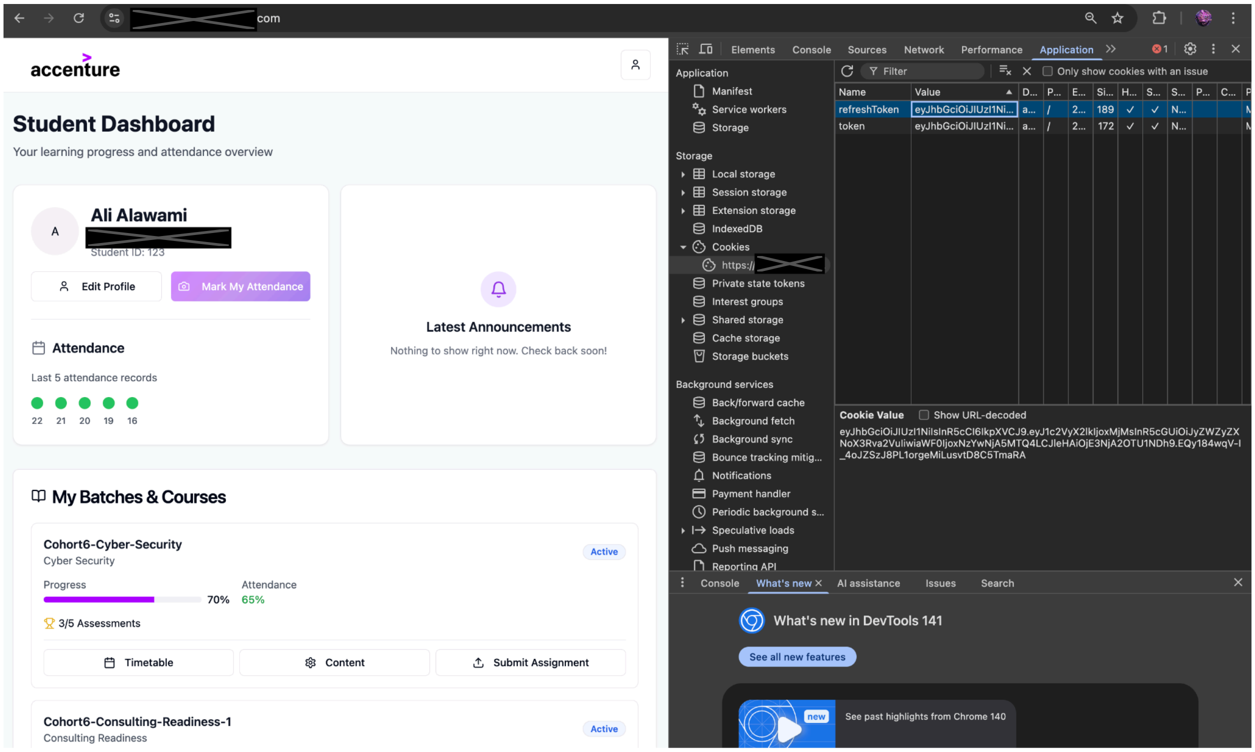
- **Session Invalidation Logic:** Logout functionality does not properly revoke or expire previously issued session tokens, resulting in multiple active sessions for the same user. This allows hijacked sessions to remain valid even after the legitimate user logs out.
- **Backend Token Handling Service (Authentication API):** Responsible for issuing, refreshing, and validating session tokens. Does not verify session uniqueness or enforce token rotation, permitting replayed cookies to remain effective.
- **Frontend Session Storage / Authentication Handling:** Client-side code blindly accepts session cookies without verifying user identity or enforcing session freshness, allowing reuse of stolen or replayed cookies.
- **Assessment Results Endpoint:** The backend endpoint that retrieves and displays student assessment data (/results or /api/results/{student_id}) relies solely on session cookie validity, not on contextual or secondary checks (e.g., token binding or reauthentication).

How issue was observed:

- During post-assessment review, authenticated users were provided with unique result page links accessible only after logging in. Initial attempts to directly access another student's results via URL manipulation were correctly blocked by access control mechanisms.
- Further investigation revealed a session handling weakness. While remaining on the authenticated **home page**, the browser's **authentication** and **refresh cookies** were manually replaced with those belonging to another student account (obtained with consent for testing). Upon refreshing the page and selecting the **"Results"** button, the system successfully loaded the other student's exam results — without reauthentication or error.
- This demonstrated that the backend server was accepting valid session cookies regardless of their origin or device context, indicating a **cookie replay** vulnerability.
- Additional testing confirmed that even after the victim student **logged out** and **logged back in**, initiating a new session, the attacker remained logged in under the same hijacked cookies. This revealed improper **session invalidation** on logout, as multiple concurrent sessions remained active under the same account.

How to reproduce the issue & Evidence:

Step 1: Victim logs in to get a cookie token and a refresh cookie token. To do this you need to press command+options+i on MacOs or Control+shift+i on Windows, then go to the applications tab, then refresh the page.



[redacted].com

accenture

Student Dashboard

Your learning progress and attendance overview

A **Ali Alawami**
[redacted]
Student ID: 123

Edit Profile | Mark My Attendance

Attendance

Last 5 attendance records

●	●	●	●	●
22	21	20	19	16

Latest Announcements

Nothing to show right now. Check back soon!

My Batches & Courses

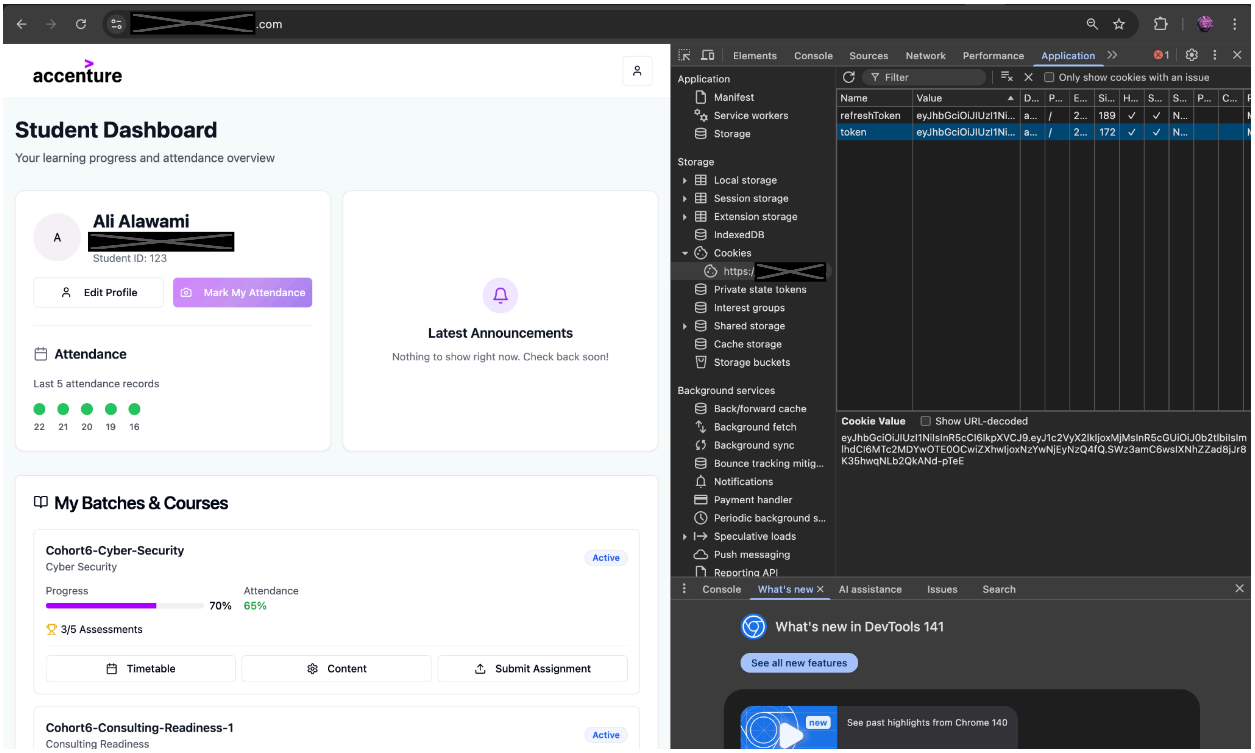
Cohort6-Cyber-Security Active
Cyber Security
Progress 70% Attendance 65%
3/5 Assessments
Timetable | Content | Submit Assignment

Cohort6-Consulting-Readiness-1 Active
Consulting Readiness

Name	Value	D...	P...	E...	Si...	H...	S...	S...	P...	C...	P
refreshToken	eyJhbGciOiJIUzI1Ni...	a...	/	2...	189	✓	✓	N...			M
token	eyJhbGciOiJIUzI1Ni...	a...	/	2...	172	✓	✓	N...			M

Cookie Value □ Show URL-decoded

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxMjMsInR5cGUiOiJyZWZyZX
NoX3Rva2VuIiwiaWF0IjoxNzYwNjA5MTQ4LCJleHAiOjE3NjA2OTU1NDh9.EQy184wqV-I
_4oJZSzJ8PL1orgeMiLusvtD8C5TmaRA
```



[redacted].com

accenture

Student Dashboard

Your learning progress and attendance overview

A **Ali Alawami**
[redacted]
Student ID: 123

Edit Profile | Mark My Attendance

Attendance

Last 5 attendance records

●	●	●	●	●
22	21	20	19	16

Latest Announcements

Nothing to show right now. Check back soon!

My Batches & Courses

Cohort6-Cyber-Security Active
Cyber Security
Progress 70% Attendance 65%
3/5 Assessments
Timetable | Content | Submit Assignment

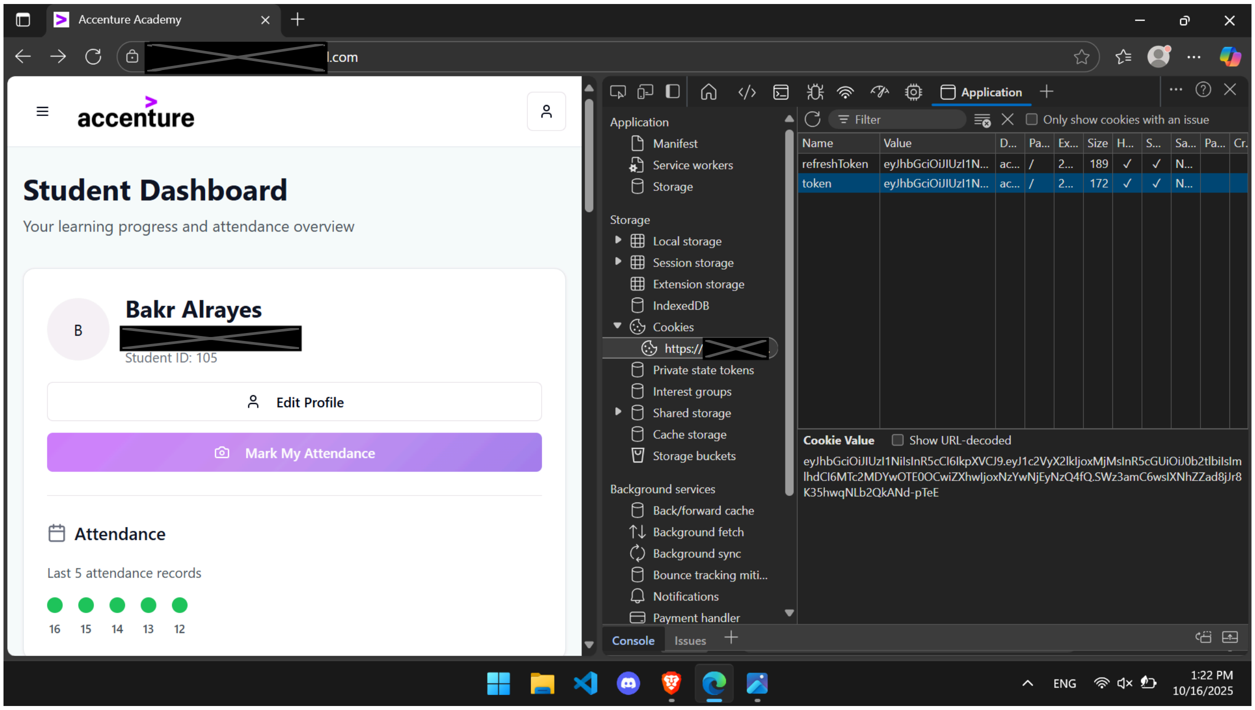
Cohort6-Consulting-Readiness-1 Active
Consulting Readiness

Name	Value	D...	P...	E...	Si...	H...	S...	S...	P...	C...	P
refreshToken	eyJhbGciOiJIUzI1Ni...	a...	/	2...	189	✓	✓	N...			M
token	eyJhbGciOiJIUzI1Ni...	a...	/	2...	172	✓	✓	N...			M

Cookie Value □ Show URL-decoded

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxMjMsInR5cGUiOiJ0b2tlbiIsIm
lhdCI6MTc2MDYwOTE0OCwiZXhwIjoxNzYwNjEyNzQ4fQ.SWz3amC6wsIXNhZZad8jJr8
K35hwqNLb2QkANd-pTeE
```

Step 2: Attacker logs in normally. Then you need to press command+options+i on MacOs or Control+shift+i on Windows, then go to the applications tab, then refresh the page (to get the cookie values of the attacker)



Accenture Academy

[redacted].com

accenture

Student Dashboard

Your learning progress and attendance overview

Bakr Alrayes

[redacted]

Student ID: 105

Edit Profile

Mark My Attendance

Attendance

Last 5 attendance records

16 15 14 13 12

Application

Application: Manifest, Service workers, Storage

Storage: Local storage, Session storage, Extension storage, IndexedDB, Cookies, https://[redacted], Private state tokens, Interest groups, Shared storage, Cache storage, Storage buckets

Background services: Back/forward cache, Background fetch, Background sync, Bounce tracking miti..., Notifications, Payment handler

Filter □ Only show cookies with an issue

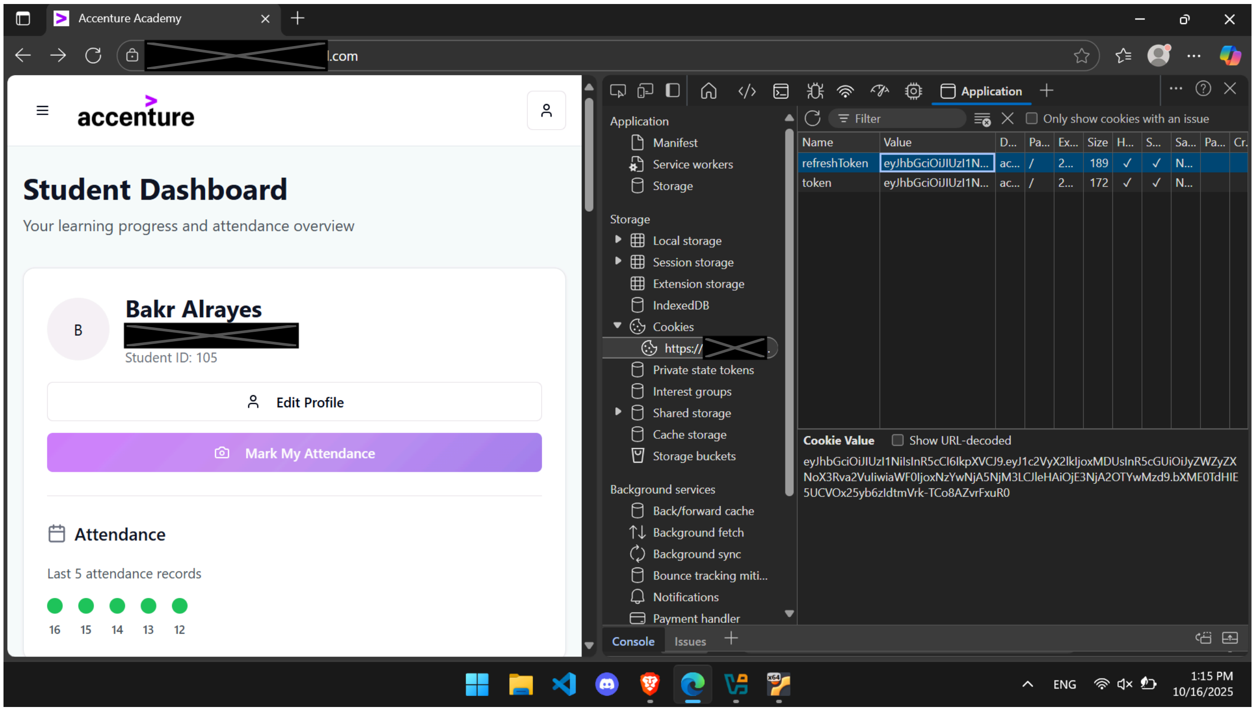
Name	Value	D...	Pa...	Ex...	Size	H...	S...	Sa...	Pa...	Cr.
refreshToken	eyJhbGciOiJIUzI1N...	ac...	/	2...	189	✓	✓	N...		
token	eyJhbGciOiJIUzI1N...	ac...	/	2...	172	✓	✓	N...		

Cookie Value □ Show URL-decoded

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxMjMsInR5cGUiOiJ0b2tlbiIsImlhdCI6MTc2MDYwOTE0OCwiZXhwIjoxNzYwNjEyNzQ4fQ.SWz3amC6wslXNhZZad8jJr8K35hwqNLb2QkANd-pTeE

Console Issues

1:22 PM 10/16/2025



Accenture Academy

[redacted].com

accenture

Student Dashboard

Your learning progress and attendance overview

Bakr Alrayes

[redacted]

Student ID: 105

Edit Profile

Mark My Attendance

Attendance

Last 5 attendance records

16 15 14 13 12

Application

Application: Manifest, Service workers, Storage

Storage: Local storage, Session storage, Extension storage, IndexedDB, Cookies, https://[redacted], Private state tokens, Interest groups, Shared storage, Cache storage, Storage buckets

Background services: Back/forward cache, Background fetch, Background sync, Bounce tracking miti..., Notifications, Payment handler

Filter □ Only show cookies with an issue

Name	Value	D...	Pa...	Ex...	Size	H...	S...	Sa...	Pa...	Cr.
refreshToken	eyJhbGciOiJIUzI1N...	ac...	/	2...	189	✓	✓	N...		
token	eyJhbGciOiJIUzI1N...	ac...	/	2...	172	✓	✓	N...		

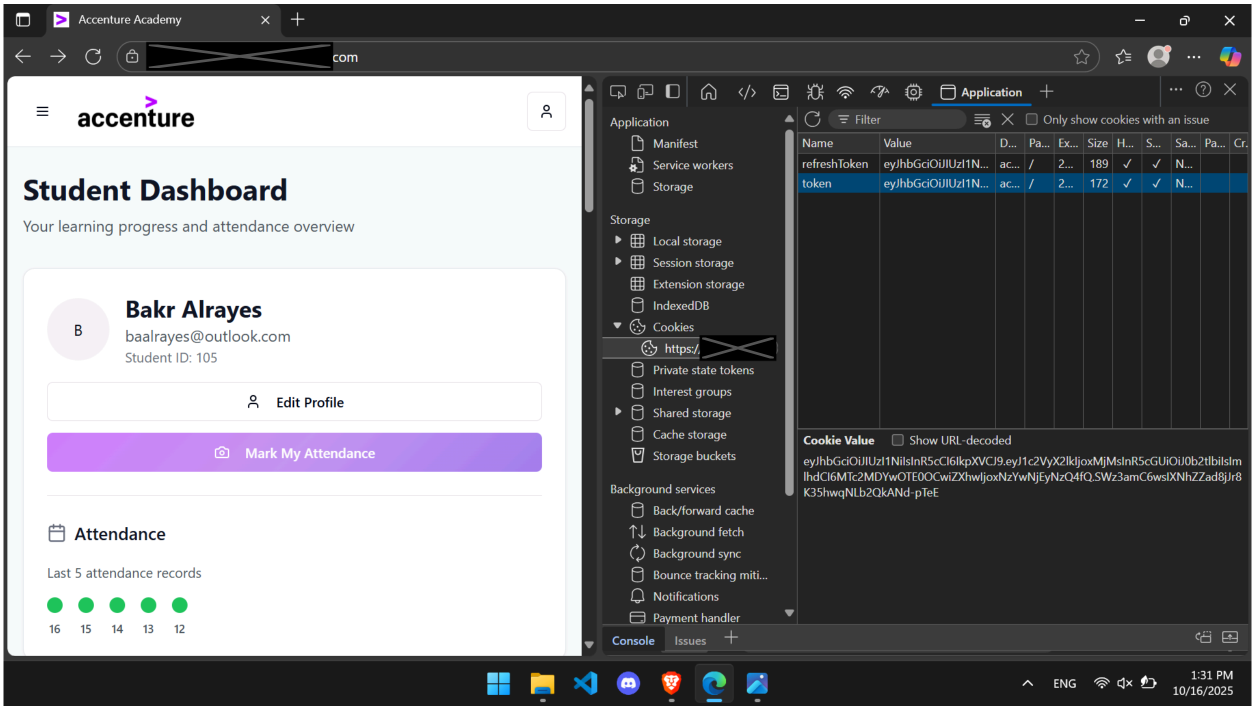
Cookie Value □ Show URL-decoded

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxMDUsInR5cGUiOiJyZWZyZXNoX3Rva2VuIiwiaWF0IjoxNzYwNjA5NjM3LCJleHAiOjE3NjA2OTYwMzd9.bXME0TdHIE5UCVOx25yb6zldtmVrk-TCo8AZvrFxuR0

Console Issues

1:15 PM 10/16/2025

Step 3: Attacker logs in and replaces their cookie and refresh cookie tokens into the victim’s cookie and refresh cookie from step 1. On the application tab from step 2, double click the value field on the refresh token and paste the victim’s refresh token, then double click the value field of the token and paste the victim’s token.



accenture

Student Dashboard

Your learning progress and attendance overview

B

Bakr Alrayes

baalrayes@outlook.com

Student ID: 105

Edit Profile

Mark My Attendance

Attendance

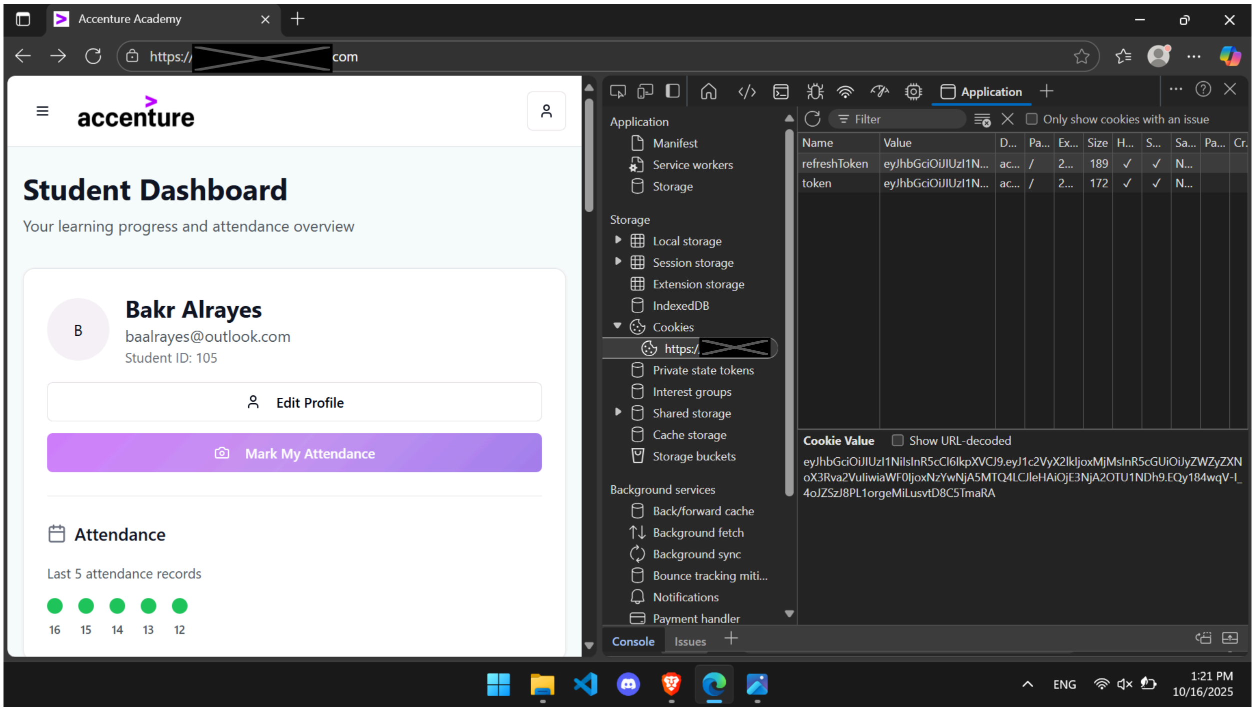
Last 5 attendance records

●	●	●	●	●
16	15	14	13	12

Name	Value	D...	Pa...	Ex...	Size	H...	S...	Sa...	Pa...	Cr.
refreshToken	eyJhbGciOiJIUzI1N...	ac...	/	2...	189	✓	✓	N...		
token	eyJhbGciOiJIUzI1N...	ac...	/	2...	172	✓	✓	N...		

Cookie Value □ Show URL-decoded

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxMjMsInR5cGUiOiJ0b2tlbiIsIm
lhdCI6MTc2MDYwOTE0OCwiZXhwIjoxNzYwNjEyNzQ4fQ.SWz3amC6wsIXNhZZad8jJr8
K35hwqNLb2QkANd-pTeE
```



accenture

Student Dashboard

Your learning progress and attendance overview

B

Bakr Alrayes

baalrayes@outlook.com

Student ID: 105

Edit Profile

Mark My Attendance

Attendance

Last 5 attendance records

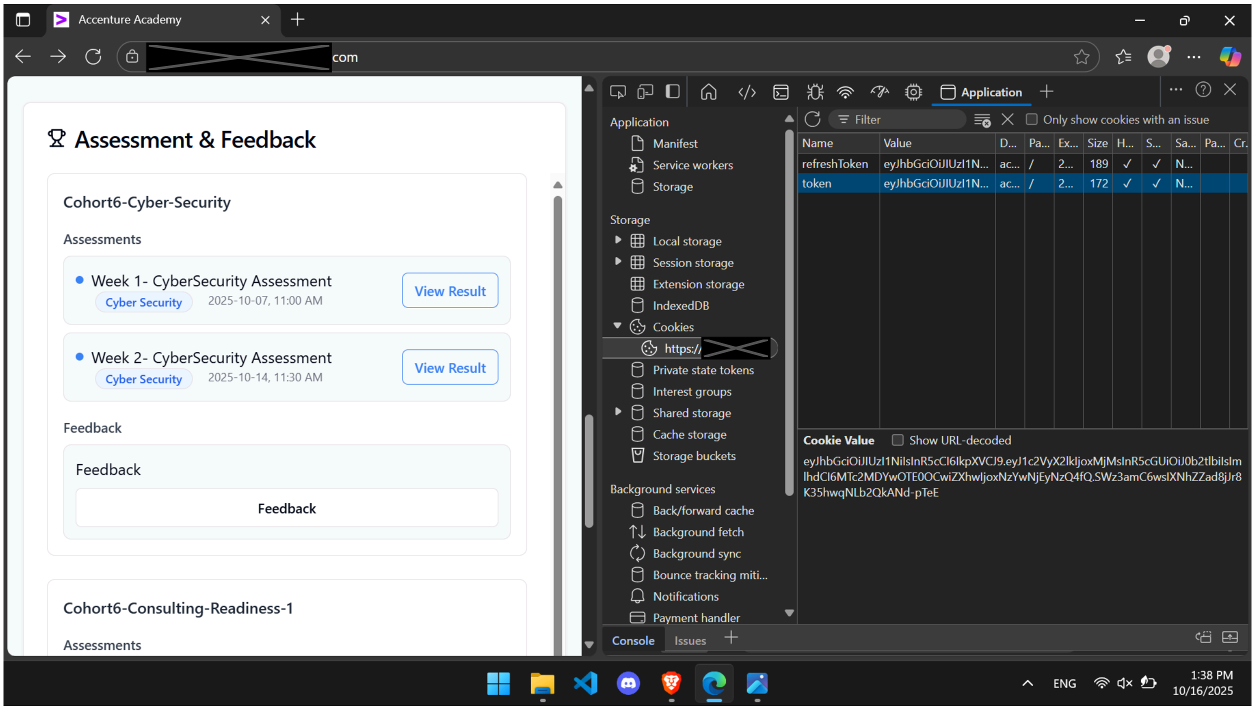
●	●	●	●	●
16	15	14	13	12

Name	Value	D...	Pa...	Ex...	Size	H...	S...	Sa...	Pa...	Cr.
refreshToken	eyJhbGciOiJIUzI1N...	ac...	/	2...	189	✓	✓	N...		
token	eyJhbGciOiJIUzI1N...	ac...	/	2...	172	✓	✓	N...		

Cookie Value □ Show URL-decoded

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxMjMsInR5cGUiOiJyZWZyZXN
oX3Rva2VuIiwiaWF0IjoxNzYwNjA5MTQ4LCJleHAiOjE3NjA2OTU1NDh9.EQy184wqV-I_
4oJZSzJ8PL1orgeMiLusvtD8C5TmaRA
```

Step 4: Click on the view results for the assessment



Assessment & Feedback

Cohort6-Cyber-Security

Assessments

- Week 1- CyberSecurity Assessment
  Cyber Security 2025-10-07, 11:00 AM
  View Result
- Week 2- CyberSecurity Assessment
  Cyber Security 2025-10-14, 11:30 AM
  View Result

Feedback

Feedback

Feedback

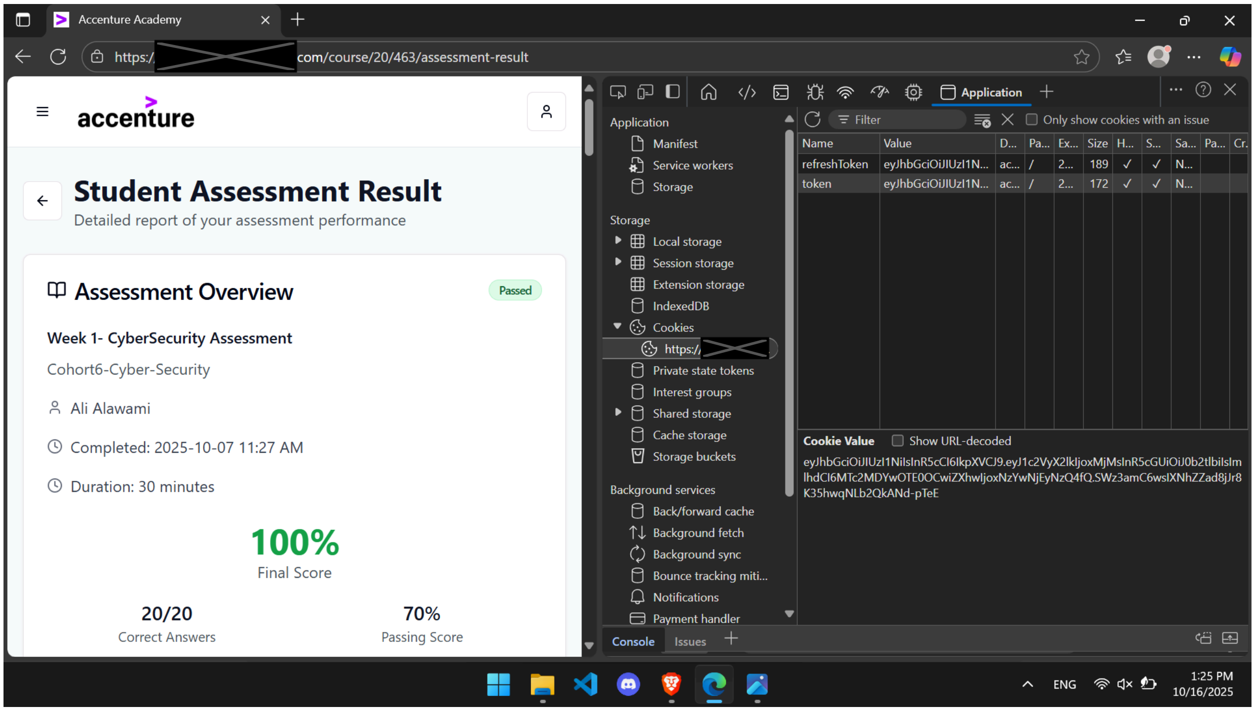
Cohort6-Consulting-Readiness-1

Assessments

Name	Value	D...	Pa...	Ex...	Size	H...	S...	Sa...	Pa...	Cr.
refreshToken	eyJhbGciOiJIUzI1N...	ac...	/	2...	189	✓	✓	N...		
token	eyJhbGciOiJIUzI1N...	ac...	/	2...	172	✓	✓	N...		

Cookie Value □ Show URL-decoded

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxMjMsInR5cGUiOiJ0b2tlbiIsIm
lhdCI6MTc2MDYwOTE0OCwiZXhwIjoxNzYwNjEyNzQ4fQ.SWz3amC6wslXNhZZad8jJr8
K35hwqNLb2QkANd-pTeE
```



accenture

Student Assessment Result

Detailed report of your assessment performance

Assessment Overview

Passed

Week 1- CyberSecurity Assessment

Cohort6-Cyber-Security

Ali Alawami

Completed: 2025-10-07 11:27 AM

Duration: 30 minutes

100%
Final Score

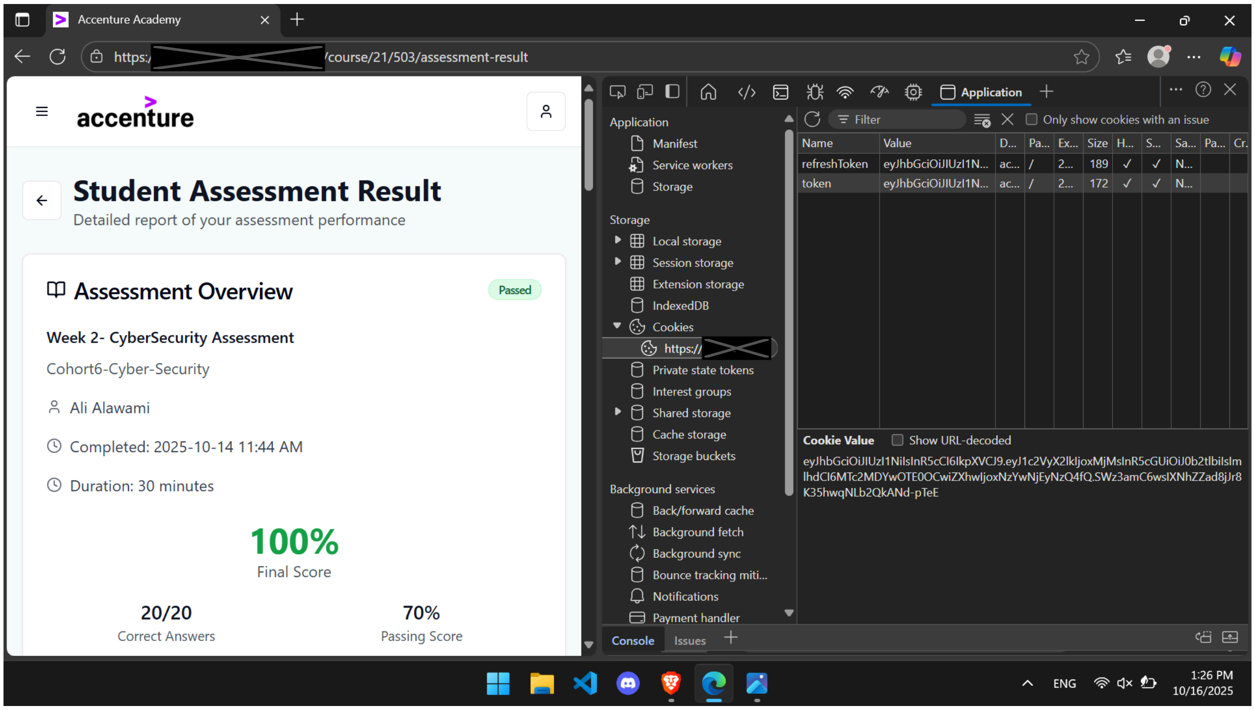
20/20
Correct Answers

70%
Passing Score

Name	Value	D...	Pa...	Ex...	Size	H...	S...	Sa...	Pa...	Cr.
refreshToken	eyJhbGciOiJIUzI1N...	ac...	/	2...	189	✓	✓	N...		
token	eyJhbGciOiJIUzI1N...	ac...	/	2...	172	✓	✓	N...		

Cookie Value □ Show URL-decoded

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxMjMsInR5cGUiOiJ0b2tlbiIsIm
lhdCI6MTc2MDYwOTE0OCwiZXhwIjoxNzYwNjEyNzQ4fQ.SWz3amC6wslXNhZZad8jJr8
K35hwqNLb2QkANd-pTeE
```



Student Assessment Result

Detailed report of your assessment performance

Assessment Overview

Passed

Week 2- CyberSecurity Assessment

Cohort6-Cyber-Security

Ali Alawami

Completed: 2025-10-14 11:44 AM

Duration: 30 minutes

100%
Final Score

20/20
Correct Answers

70%
Passing Score

Name	Value	D...	Pa...	Ex...	Size	H...	S...	Sa...	Pa...	Cr.
refreshToken	eyJhbGciOiJIUzI1N...	ac...	/	2...	189	✓	✓	N...		
token	eyJhbGciOiJIUzI1N...	ac...	/	2...	172	✓	✓	N...		

Cookie Value ☐ Show URL-decoded

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxMjMsInR5cGUiOiJ0b2tlbiIsIm
lhdCI6MTc2MDYwOTE0OCwiZXhwIjoxNzYwNjEyNzQ4fQ.SWz3amC6wslXNhZZad8jJr8
K35hwqNLb2QkANd-pTeE
```

Notice how the name on the results is the victim's name and not the attacker's name.

Step 5: log the victim out and back in and notice how the new cookies issued to the victim and the old cookies the attacker is using are still active at the same time.

Mitigation and Recommendations:

- **Implement Strict Session Binding:** Bind authentication sessions to unique device identifiers, IP addresses, or browser fingerprints to prevent session reuse from different contexts and enforce server-side verification of session cookies against the originating user environment to detect and block replayed tokens.
- **Regenerate Session Tokens on Login:** Issue a new session token upon each successful login and immediately invalidate any existing active sessions associated with that account to prevent concurrent active sessions unless explicitly required and securely managed.
- **Proper Session Invalidation on Logout:** Ensure that the logout process fully invalidates the associated session tokens and refresh tokens in the backend so that any previously hijacked cookies become unusable.
- **Monitor and Log Session Activity:** Implement detailed session activity logs, including IP addresses, login timestamps, and device details and alert administrators upon detection of concurrent sessions or anomalous login patterns.