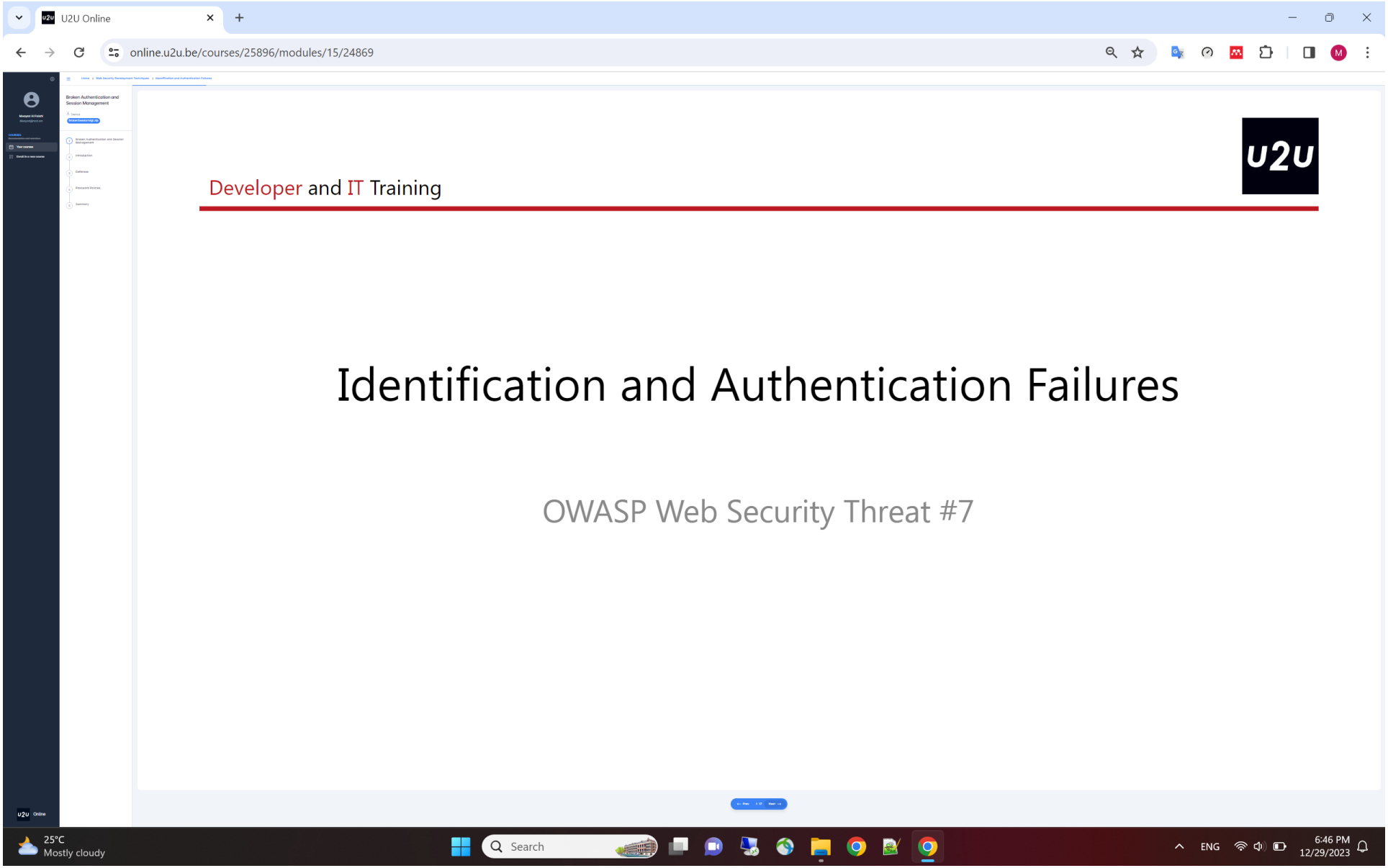
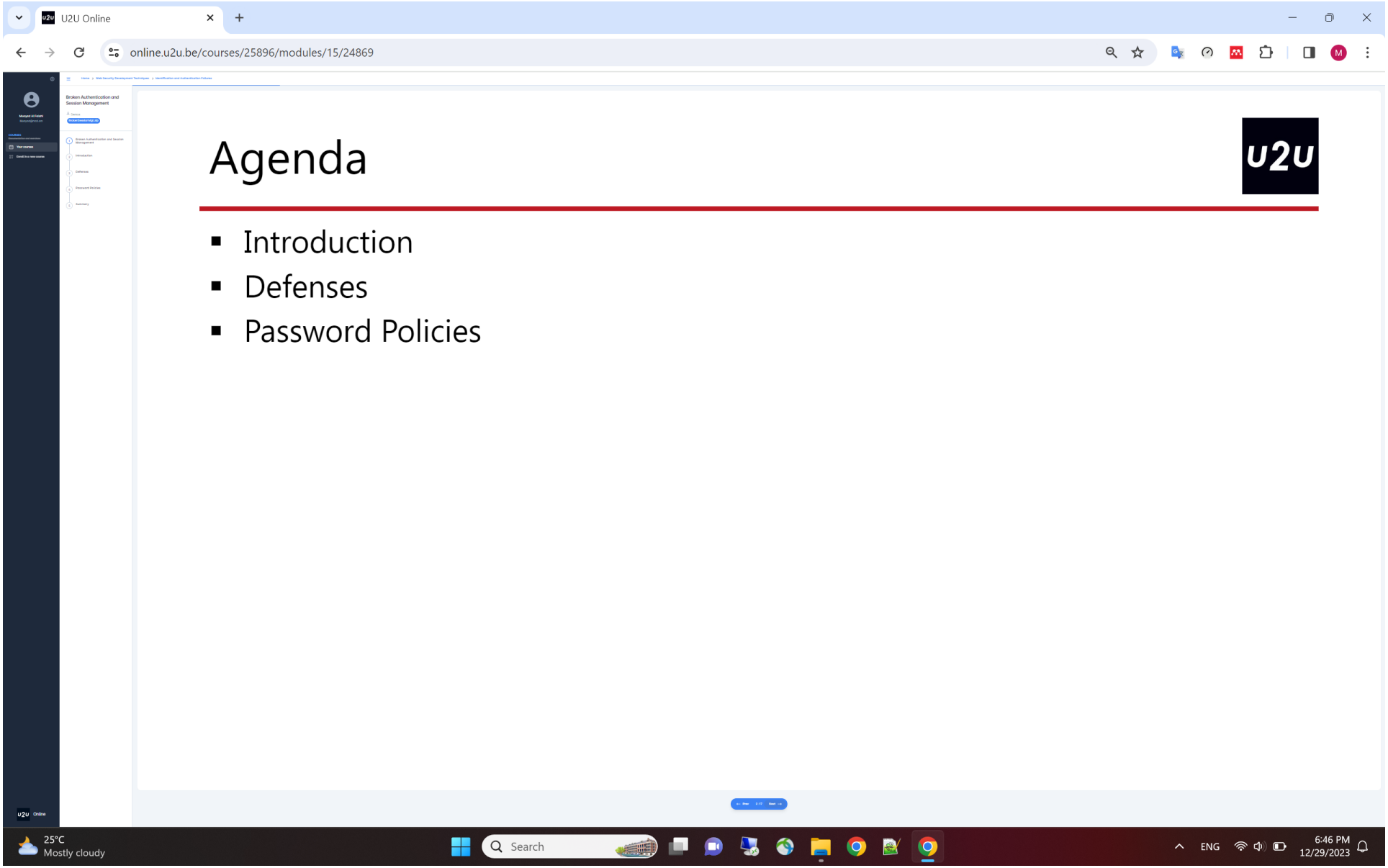
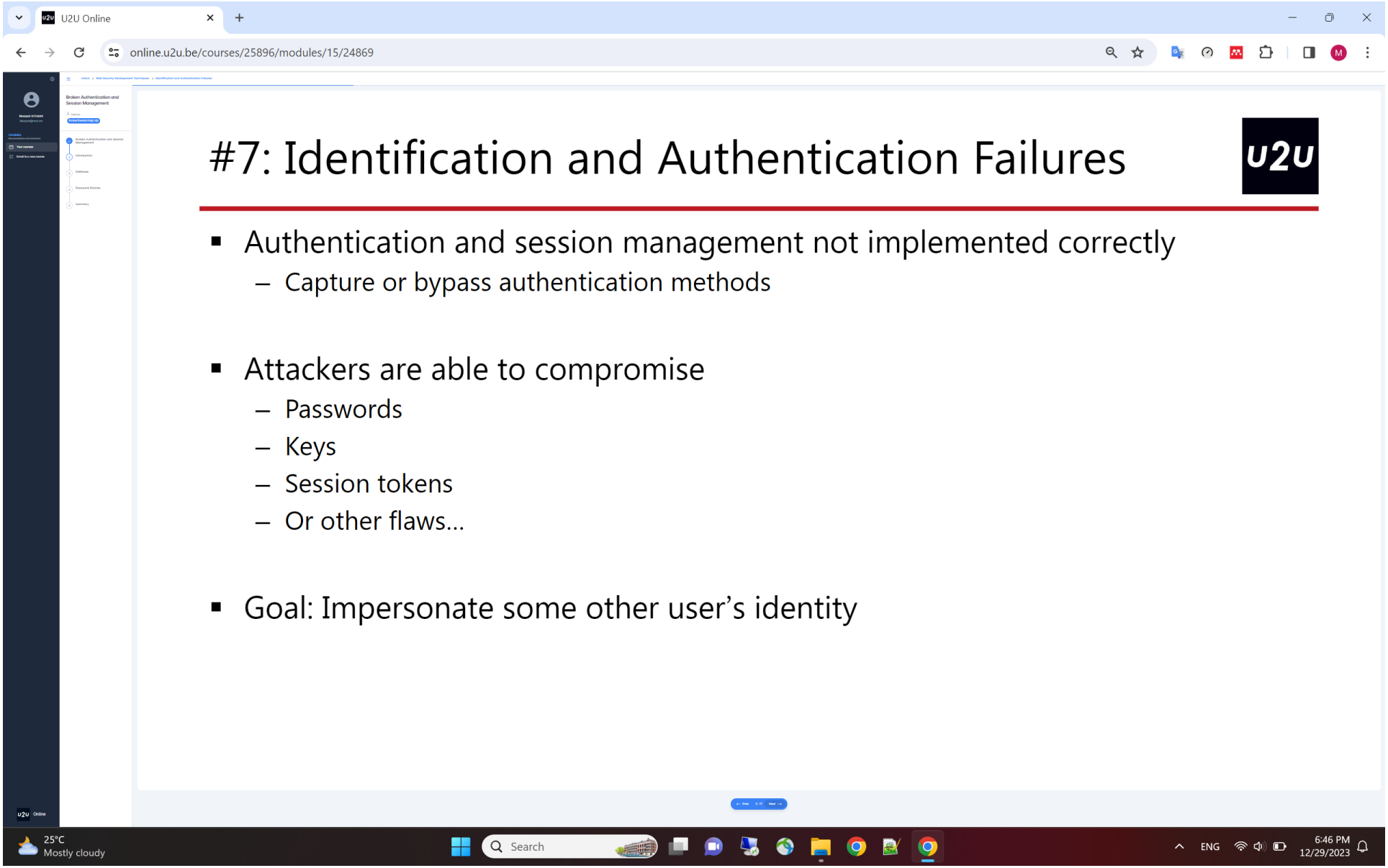
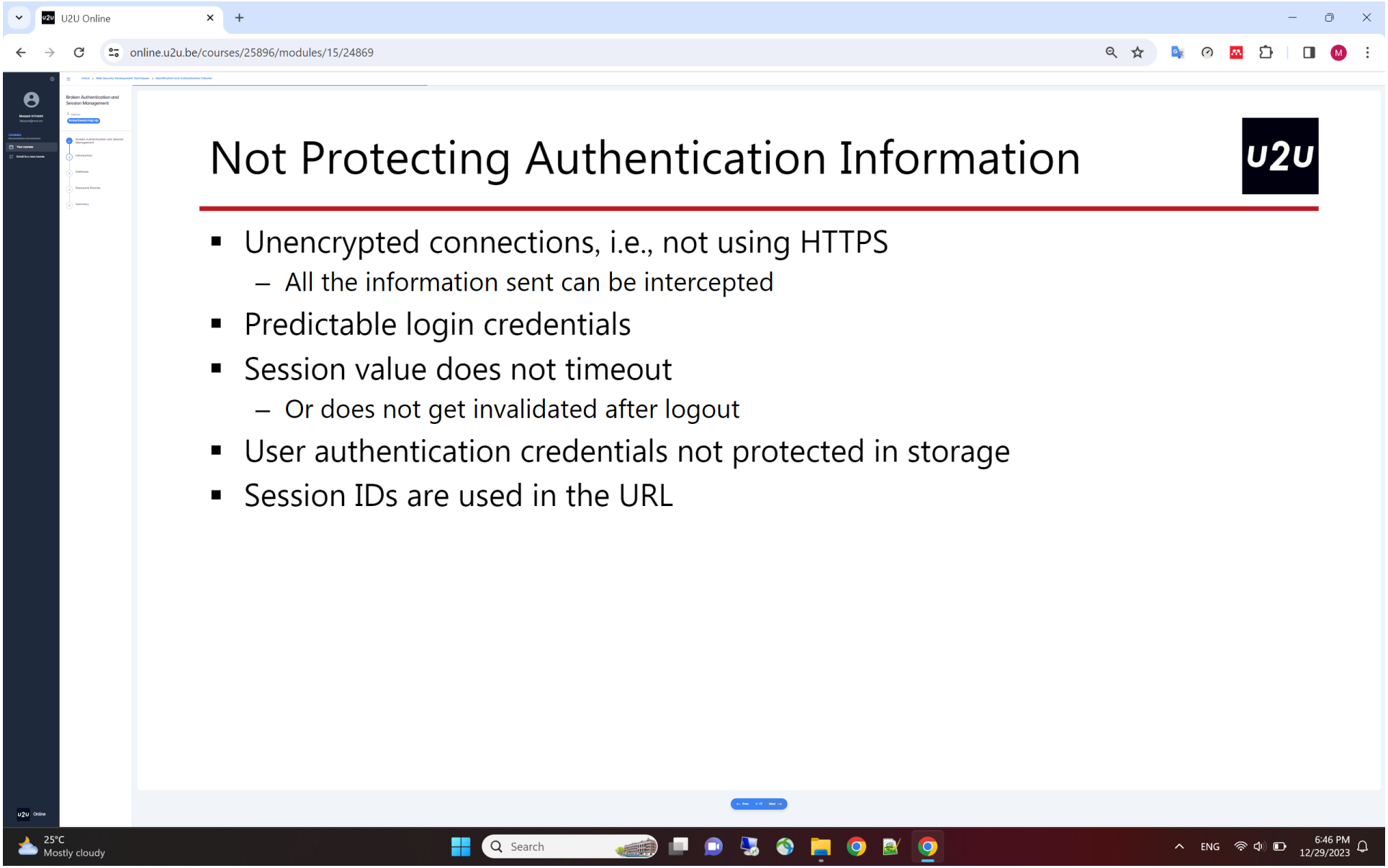
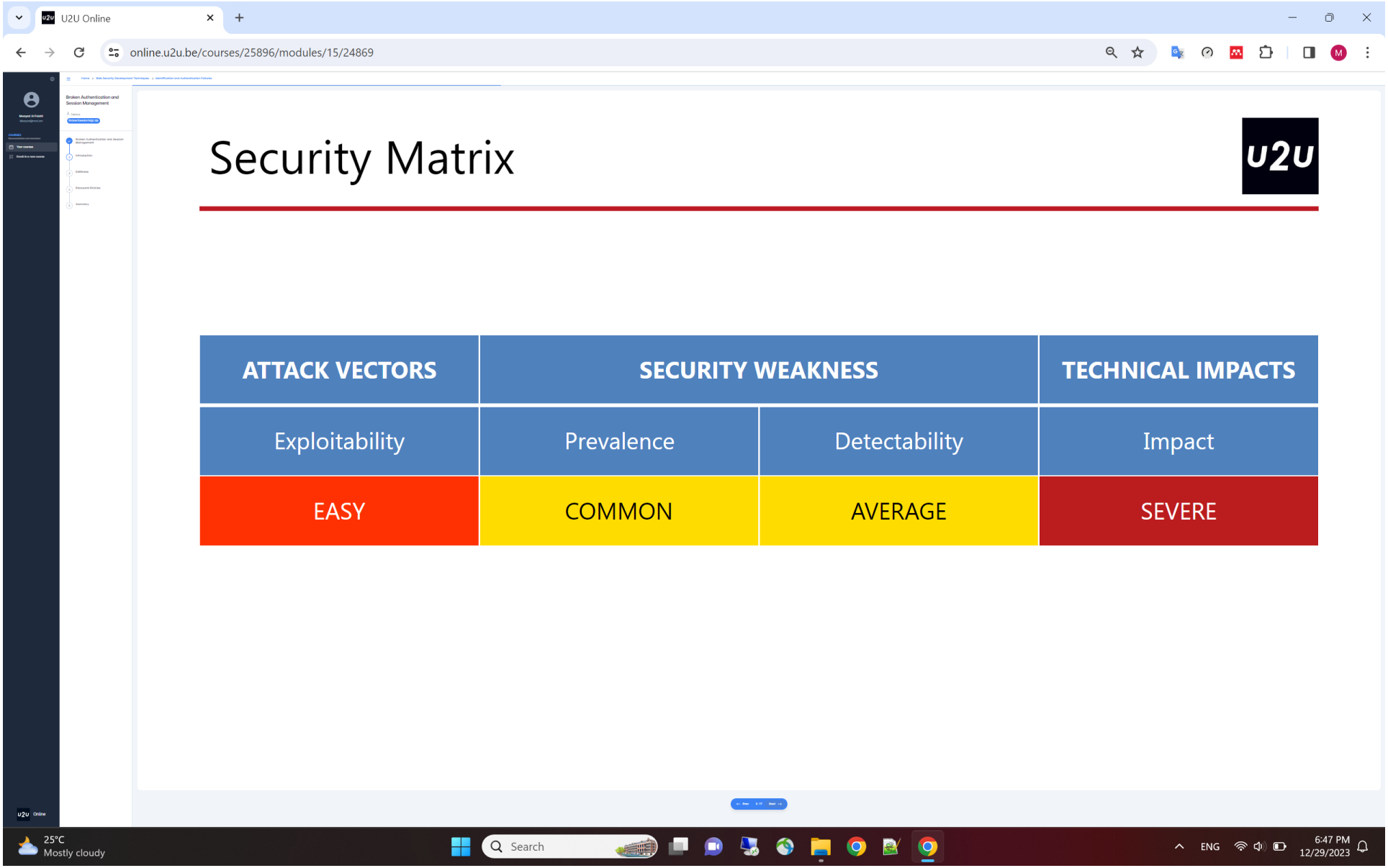
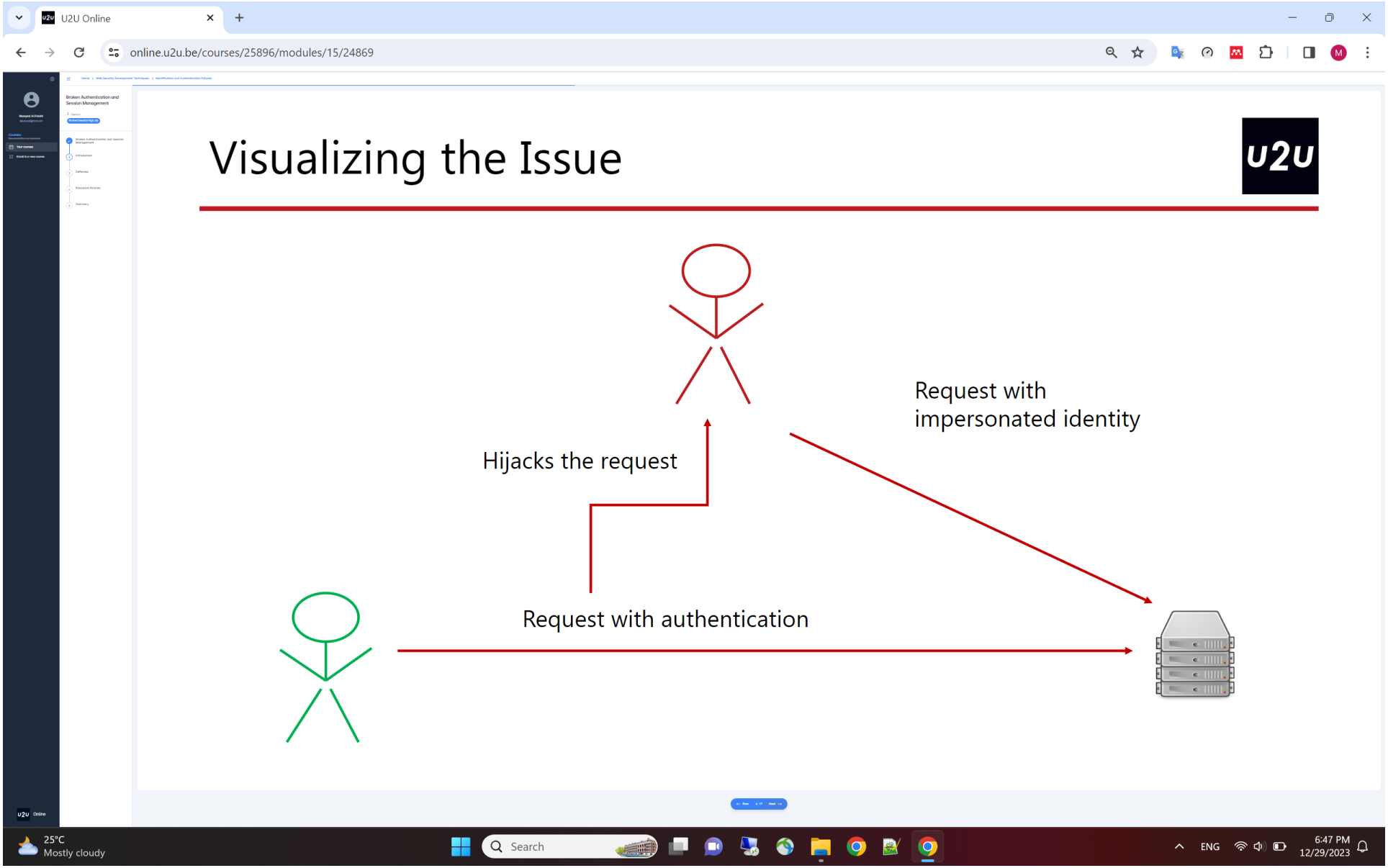

U2U Online
online.u2u.be/courses/25896/modules/15/24869
Developer and IT Training
u2u
Identification and Authentication Failures
OWASP Web Security Threat #7
25°C
Mostly cloudy
Search
ENG
6:46 PM
12/29/2023

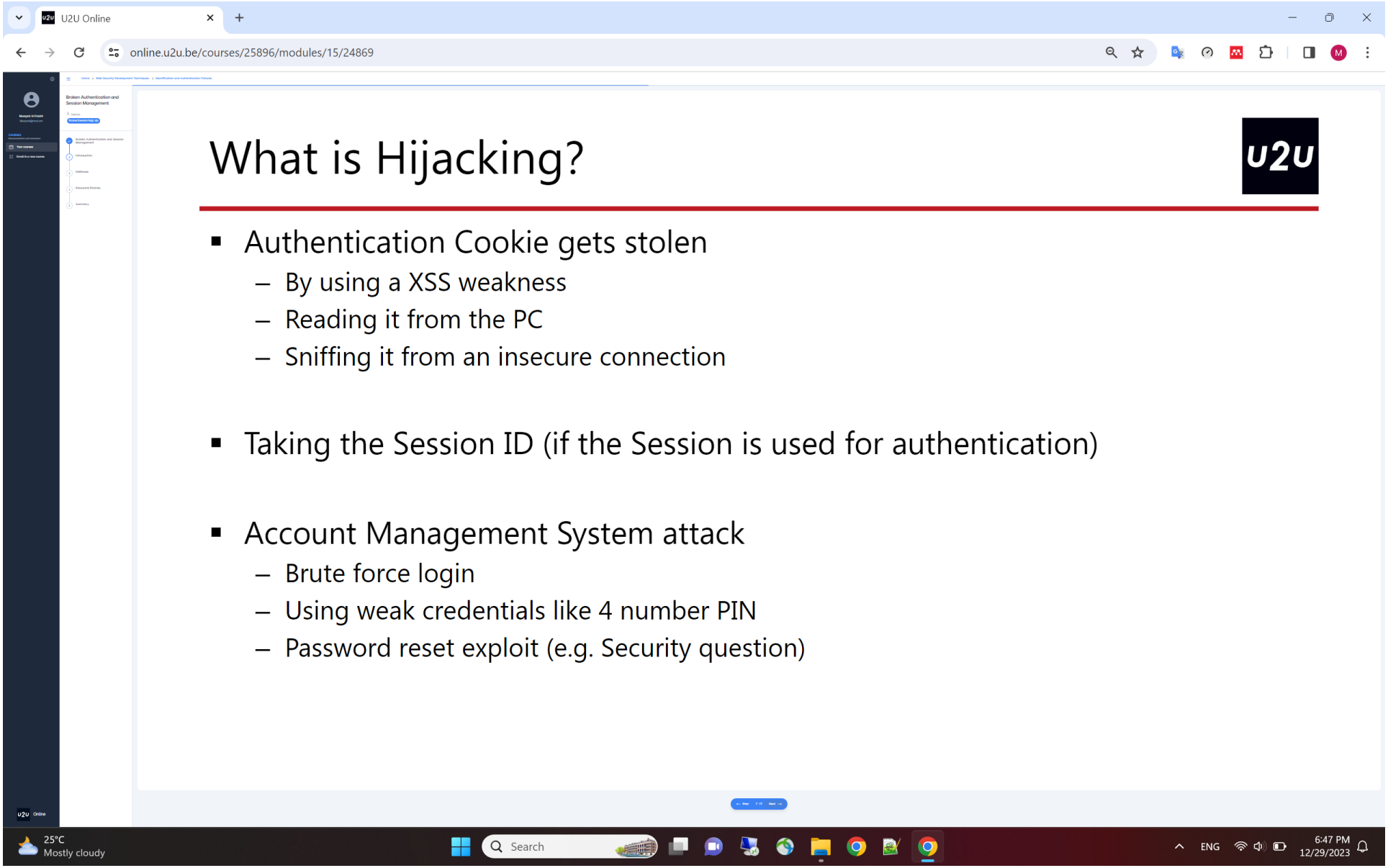

U2U Online
online.u2u.be/courses/25896/modules/15/24869
Agenda
u2u
Introduction
Defenses
Password Policies
25°C
Mostly cloudy
Search
ENG
6:46 PM
12/29/2023

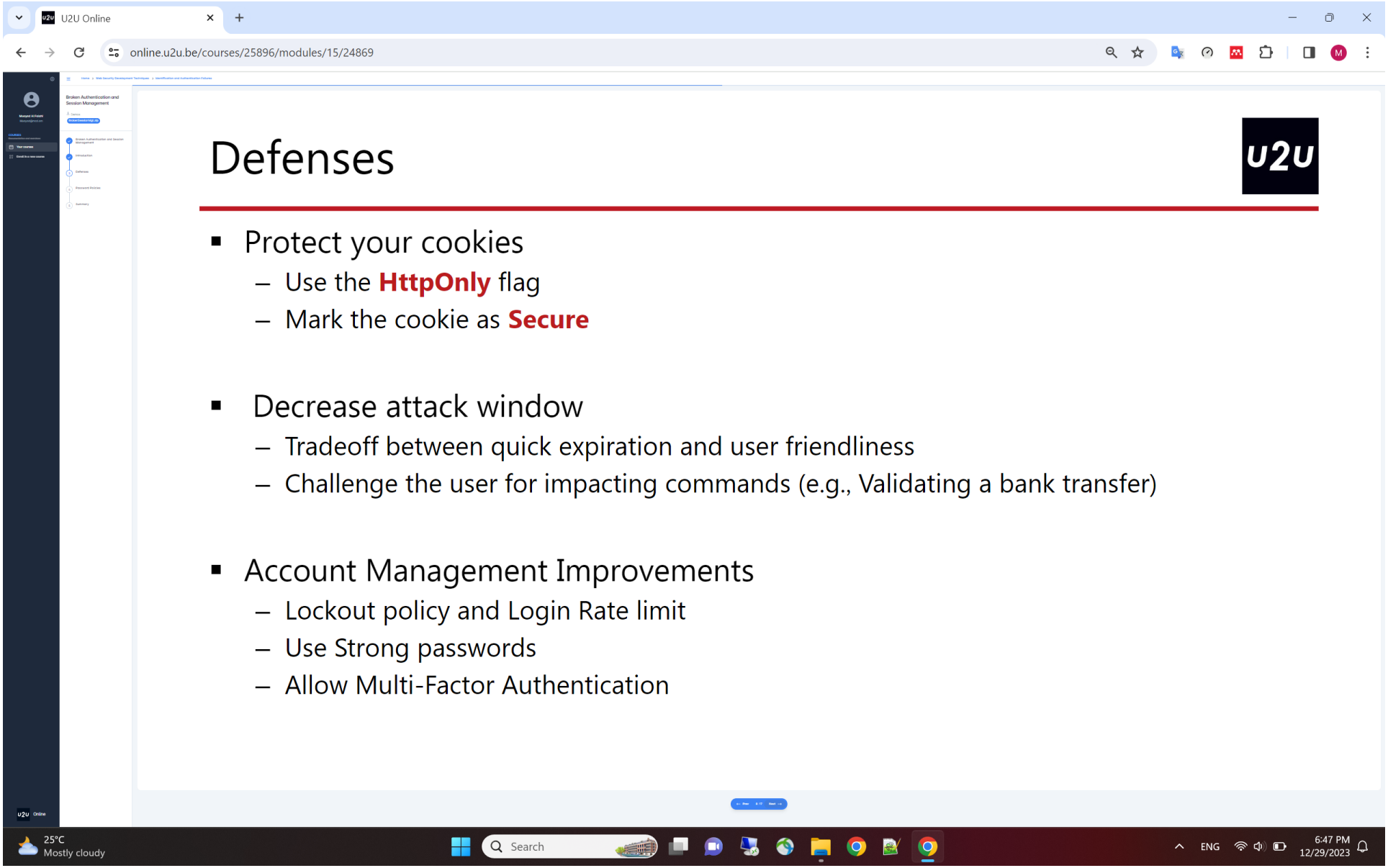

U2U Online
online.u2u.be/courses/25896/modules/15/24869
#7: Identification and Authentication Failures
U2U
Authentication and session management not implemented correctly
Capture or bypass authentication methods
Attackers are able to compromise
Passwords
Keys
Session tokens
Or other flaws…
Goal: Impersonate some other user's identity
25°C
Mostly cloudy
Search
ENG
6:46 PM
12/29/2023

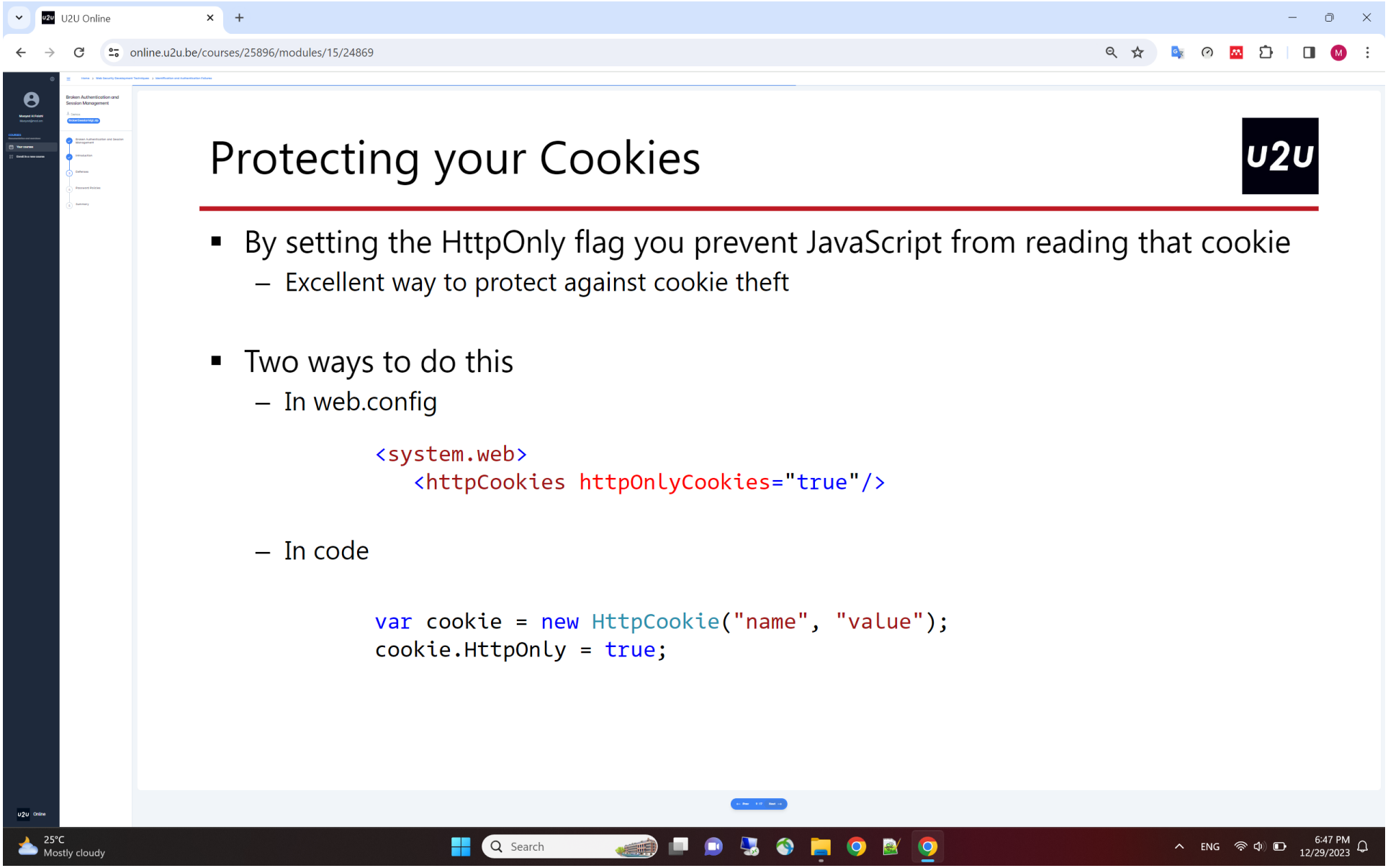

U2U Online
online.u2u.be/courses/25896/modules/15/24869
Not Protecting Authentication Information
U2U
Unencrypted connections, i.e., not using HTTPS
All the information sent can be intercepted
Predictable login credentials
Session value does not timeout
Or does not get invalidated after logout
User authentication credentials not protected in storage
Session IDs are used in the URL
25°C
Mostly cloudy
Search
ENG
6:46 PM
12/29/2023

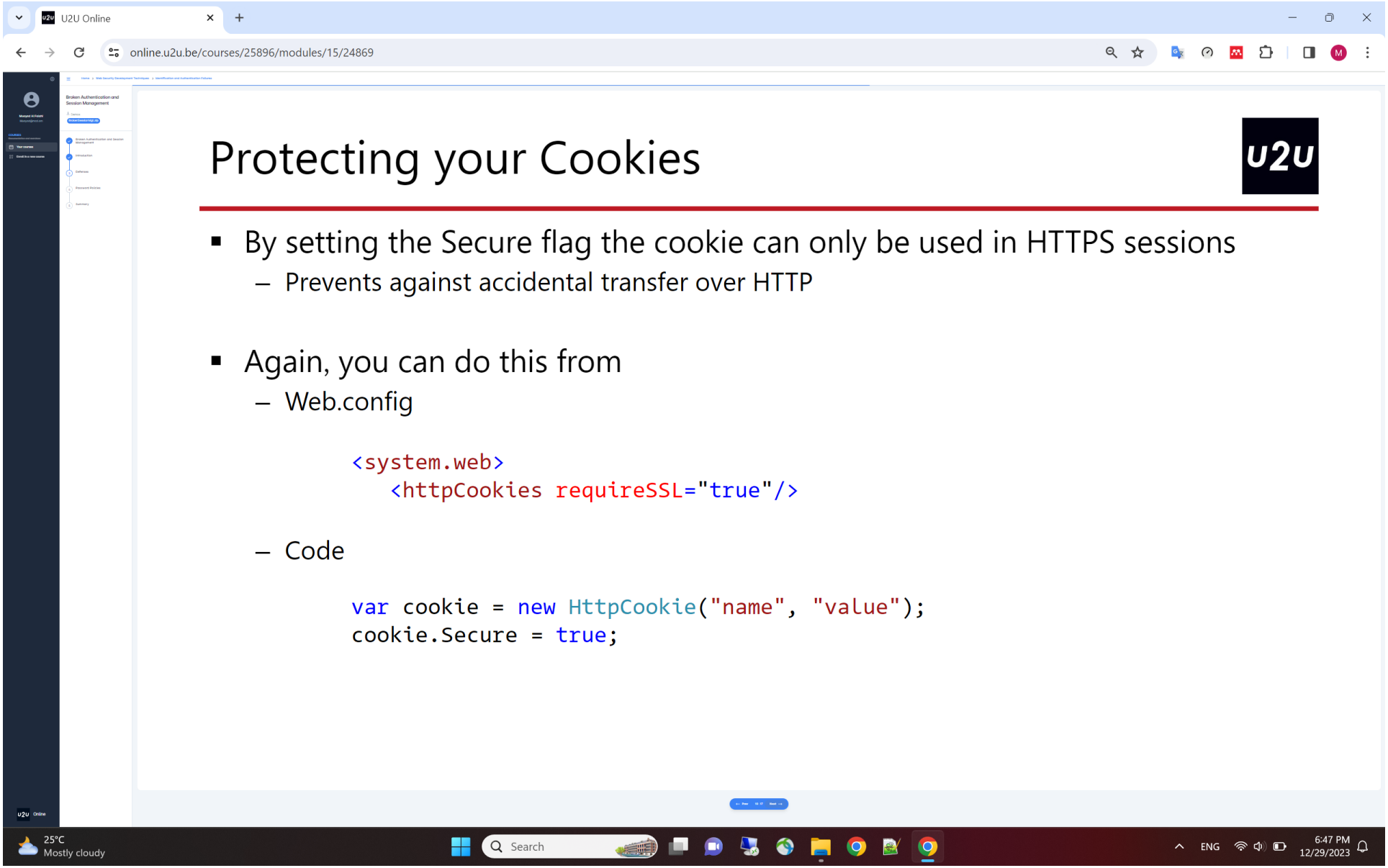

U2U Online
online.u2u.be/courses/25896/modules/15/24869
Security Matrix
u2u
ATTACK VECTORS
SECURITY WEAKNESS
TECHNICAL IMPACTS
Exploitability
Prevalence
Detectability
Impact
EASY
COMMON
AVERAGE
SEVERE
25°C
Mostly cloudy
Search
ENG
6:47 PM
12/29/2023

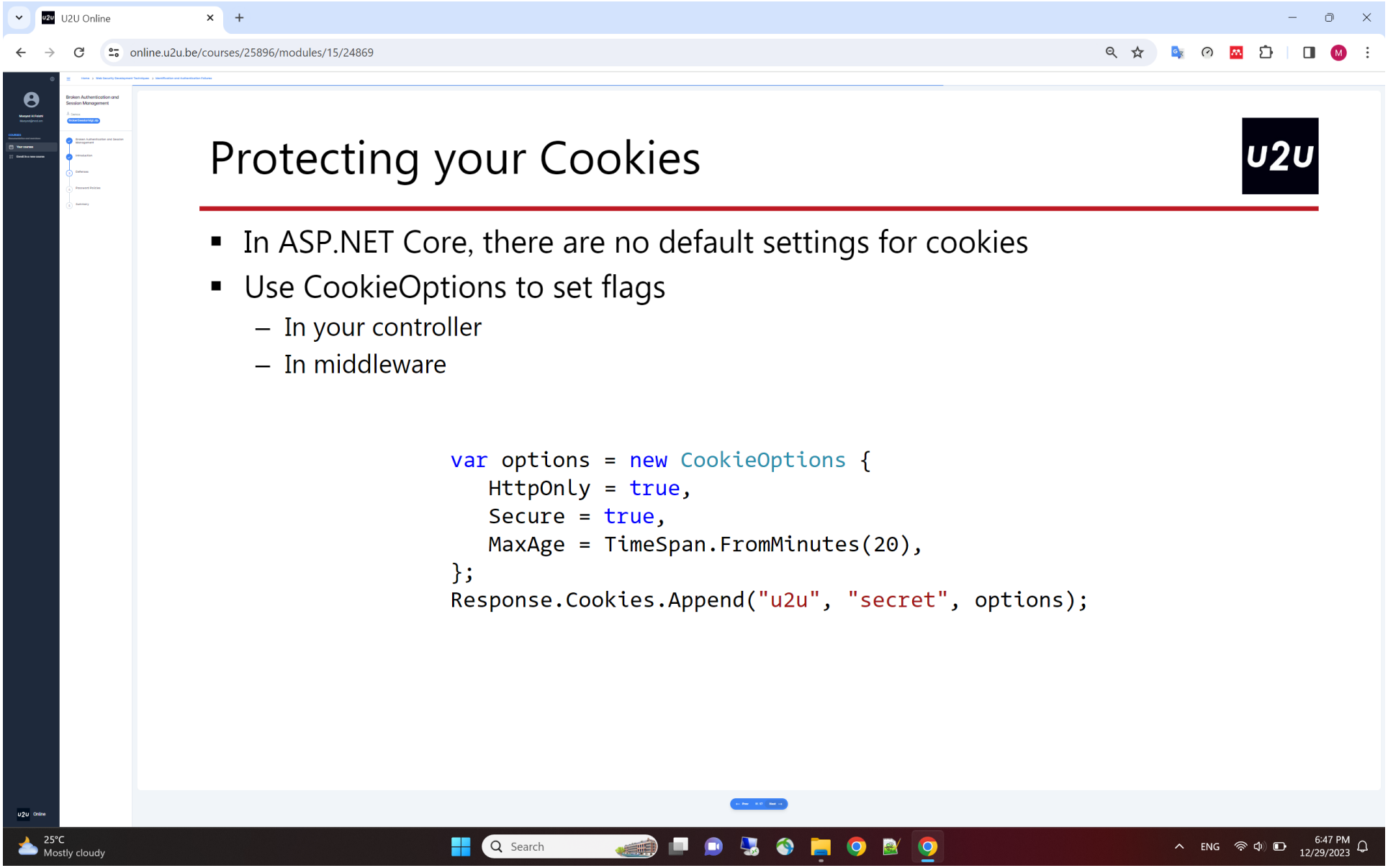

U2U Online
online.u2u.be/courses/25896/modules/15/24869
Visualizing the Issue
u2u
Request with
impersonated identity
Hijacks the request
Request with authentication
25°C
Mostly cloudy
Search
ENG
6:47 PM
12/29/2023

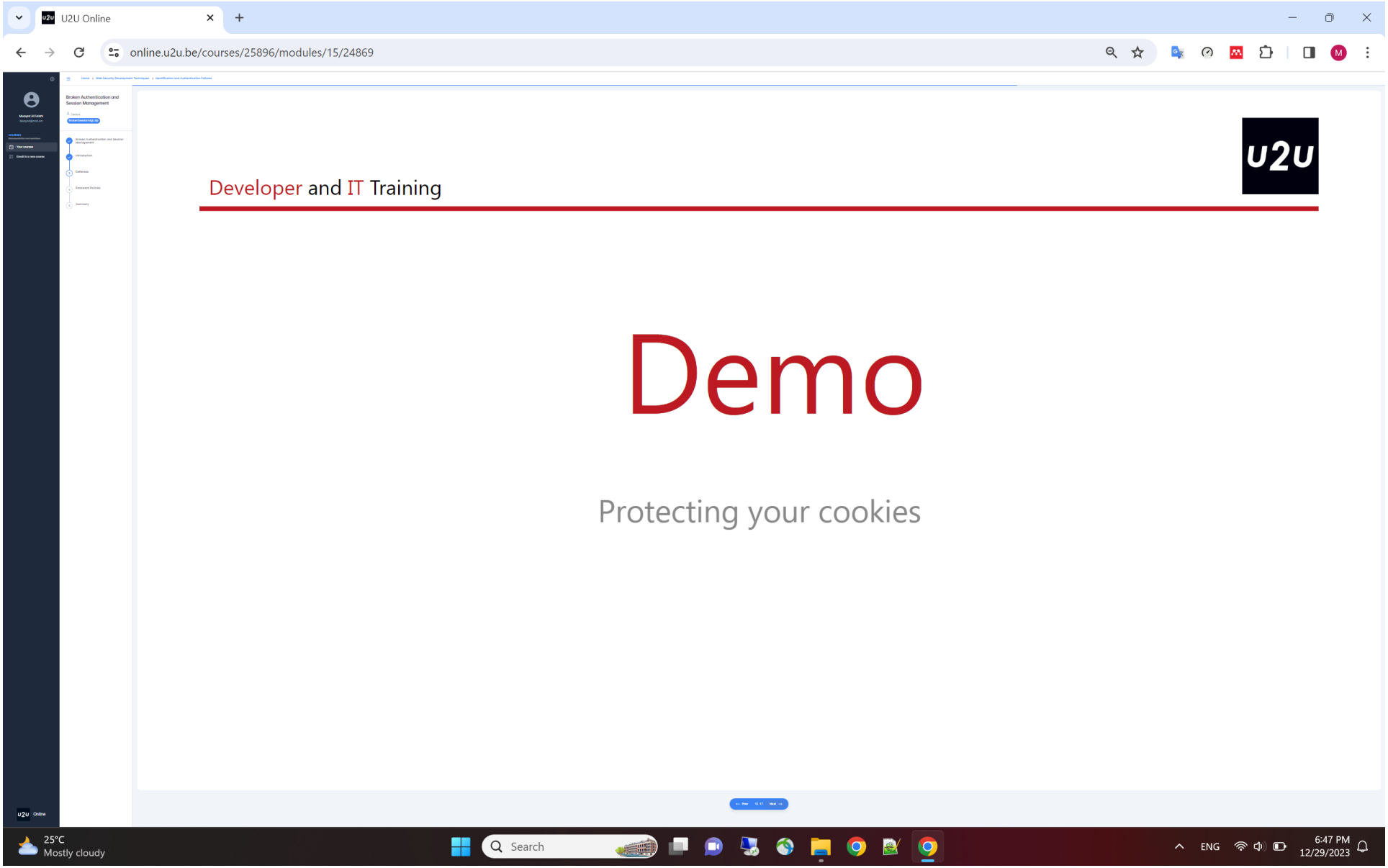

U2U Online
online.u2u.be/courses/25896/modules/15/24869
What is Hijacking?
u2u
Authentication Cookie gets stolen
By using a XSS weakness
Reading it from the PC
Sniffing it from an insecure connection
Taking the Session ID (if the Session is used for authentication)
Account Management System attack
Brute force login
Using weak credentials like 4 number PIN
Password reset exploit (e.g. Security question)
25°C
Mostly cloudy
Search
ENG
6:47 PM
12/29/2023

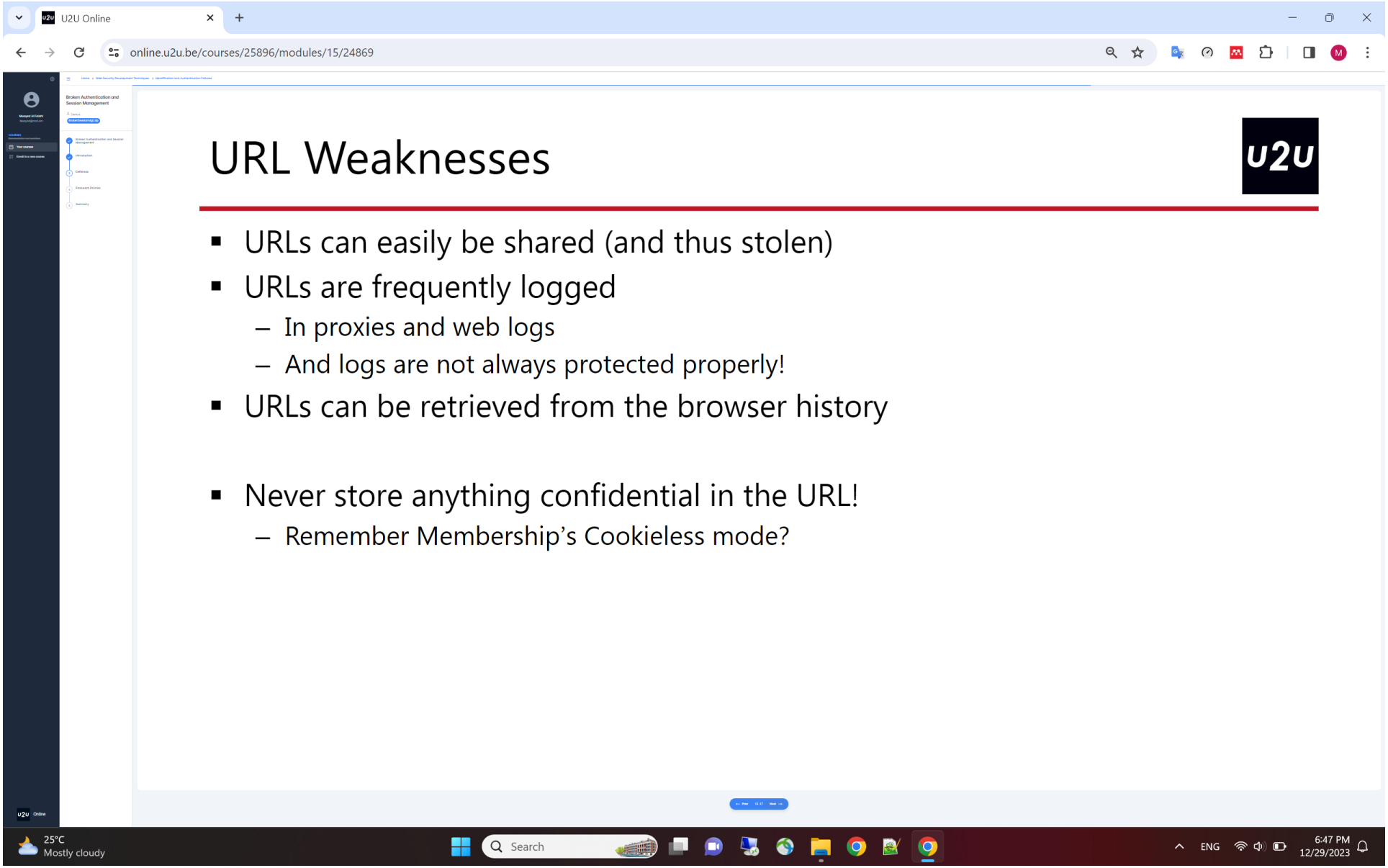

U2U Online
online.u2u.be/courses/25896/modules/15/24869
Broken Authentication and Session Management
Introduction
Defenses
Password Policies
Summary
Defenses
U2U
Protect your cookies
Use the HttpOnly flag
Mark the cookie as Secure
Decrease attack window
Tradeoff between quick expiration and user friendliness
Challenge the user for impacting commands (e.g., Validating a bank transfer)
Account Management Improvements
Lockout policy and Login Rate limit
Use Strong passwords
Allow Multi-Factor Authentication
25°C
Mostly cloudy
Search
ENG
6:47 PM
12/29/2023

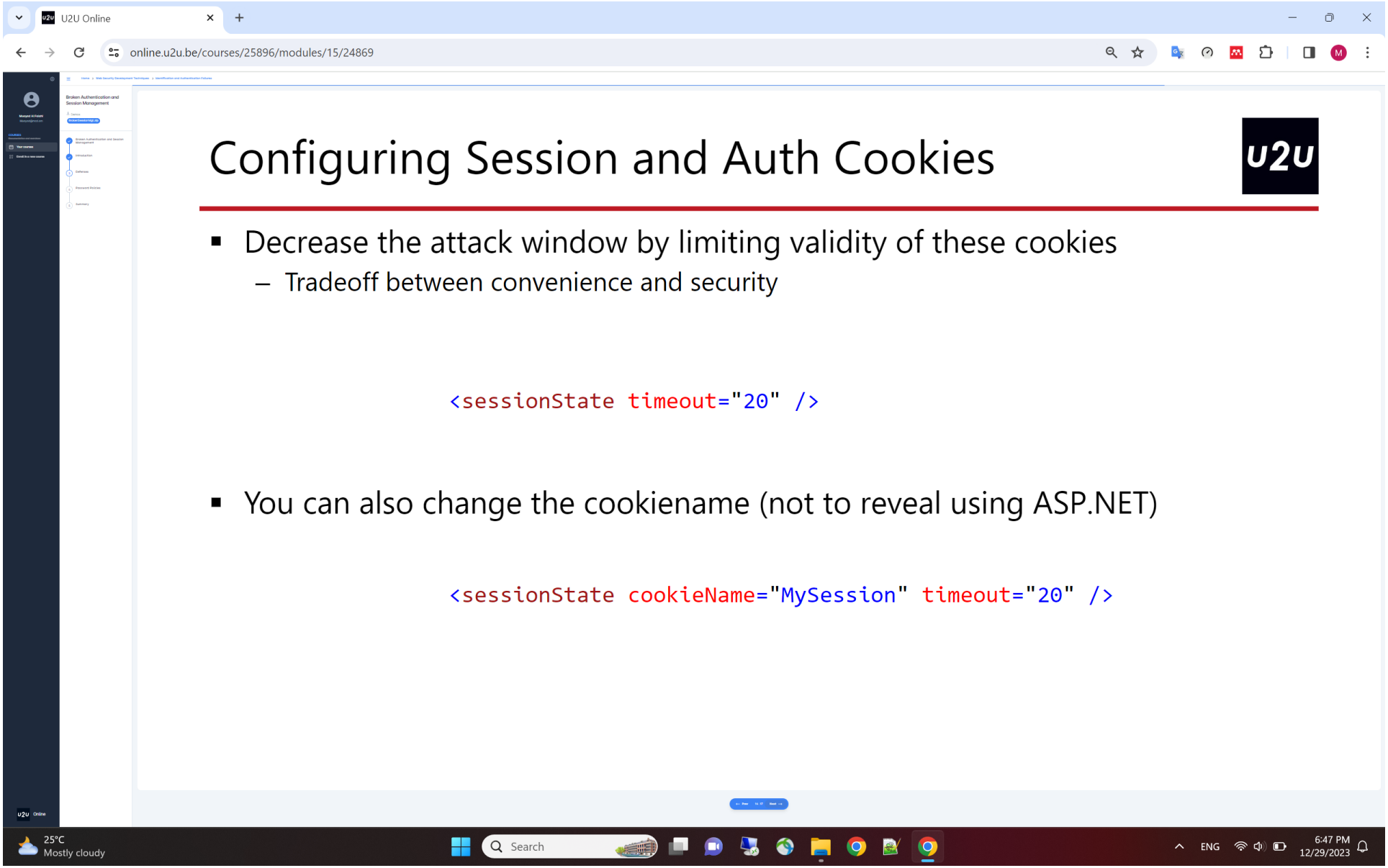

U2U Online
online.u2u.be/courses/25896/modules/15/24869
Protecting your Cookies
U2U
By setting the HttpOnly flag you prevent JavaScript from reading that cookie
Excellent way to protect against cookie theft
Two ways to do this
In web.config
<system.web>
<httpCookies httpOnlyCookies="true"/>
In code
var cookie = new HttpCookie("name", "value");
cookie.HttpOnly = true;
25°C
Mostly cloudy
Search
ENG
6:47 PM
12/29/2023

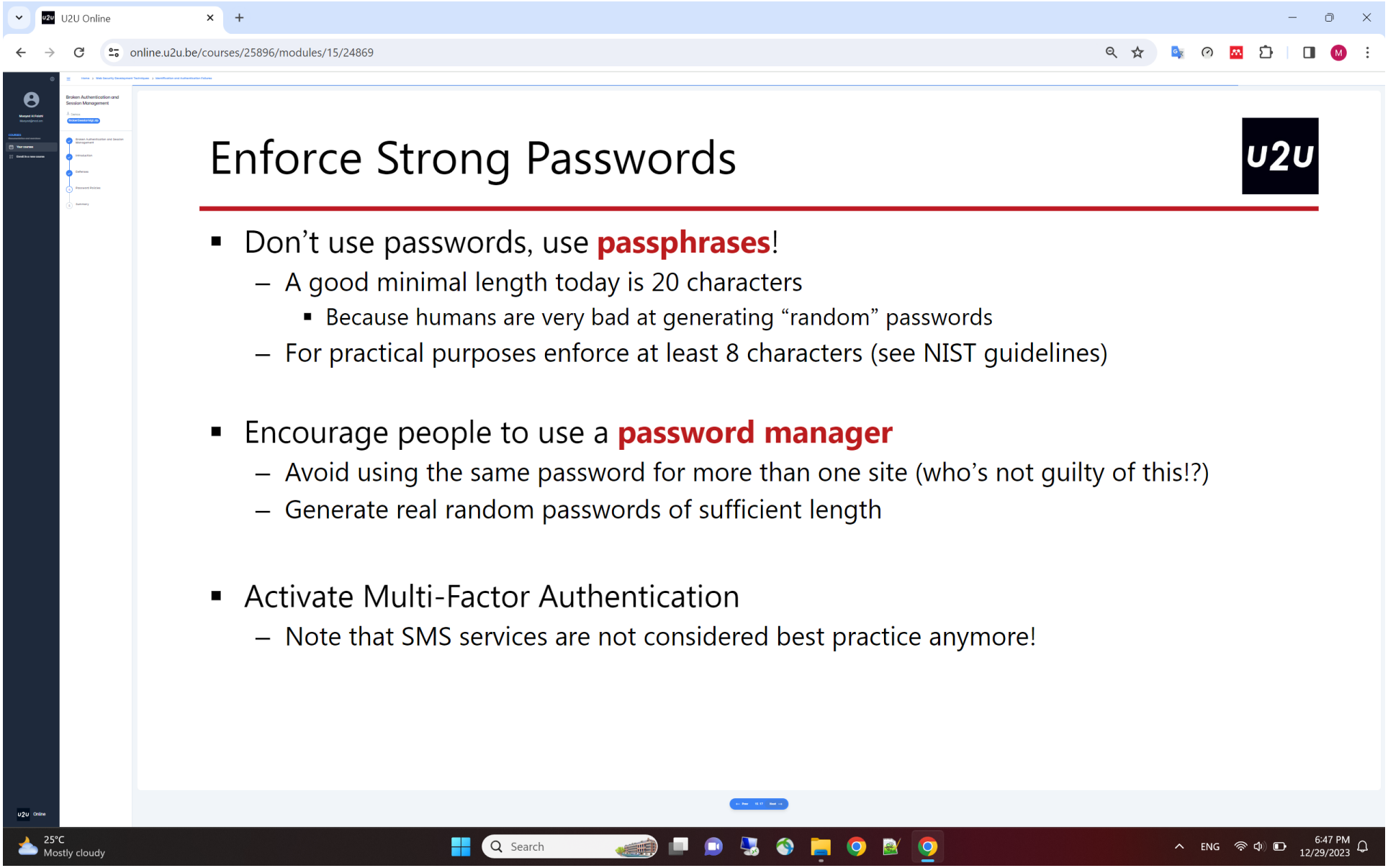

U2U Online
online.u2u.be/courses/25896/modules/15/24869
Protecting your Cookies
U2U
By setting the Secure flag the cookie can only be used in HTTPS sessions
Prevents against accidental transfer over HTTP
Again, you can do this from
Web.config
<system.web>
<httpCookies requireSSL="true"/>
Code
var cookie = new HttpCookie("name", "value");
cookie.Secure = true;
25°C
Mostly cloudy
Search
ENG
6:47 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/15/24869
Protecting your Cookies
u2u
In ASP.NET Core, there are no default settings for cookies
Use CookieOptions to set flags
In your controller
In middleware
var options = new CookieOptions {
HttpOnly = true,
Secure = true,
MaxAge = TimeSpan.FromMinutes(20),
};
Response.Cookies.Append("u2u", "secret", options);
25°C
Mostly cloudy
Search
ENG
6:47 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/15/24869
Developer and IT Training
u2u
Demo
Protecting your cookies
25°C
Mostly cloudy
Search
ENG
6:47 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/15/24869
URL Weaknesses
u2u
URLs can easily be shared (and thus stolen)
URLs are frequently logged
In proxies and web logs
And logs are not always protected properly!
URLs can be retrieved from the browser history
Never store anything confidential in the URL!
Remember Membership's Cookieless mode?
25°C
Mostly cloudy
Search
ENG
6:47 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/15/24869
Configuring Session and Auth Cookies
U2U
Decrease the attack window by limiting validity of these cookies
Tradeoff between convenience and security
<sessionState timeout="20" />
You can also change the cookiename (not to reveal using ASP.NET)
<sessionState cookieName="MySession" timeout="20" />
25°C
Mostly cloudy
Search
ENG
6:47 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/15/24869
Enforce Strong Passwords
u2u
Don't use passwords, use passphrases!
A good minimal length today is 20 characters
Because humans are very bad at generating "random" passwords
For practical purposes enforce at least 8 characters (see NIST guidelines)
Encourage people to use a password manager
Avoid using the same password for more than one site (who's not guilty of this!?)
Generate real random passwords of sufficient length
Activate Multi-Factor Authentication
Note that SMS services are not considered best practice anymore!
25°C
Mostly cloudy
Search
ENG
6:47 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/15/24869

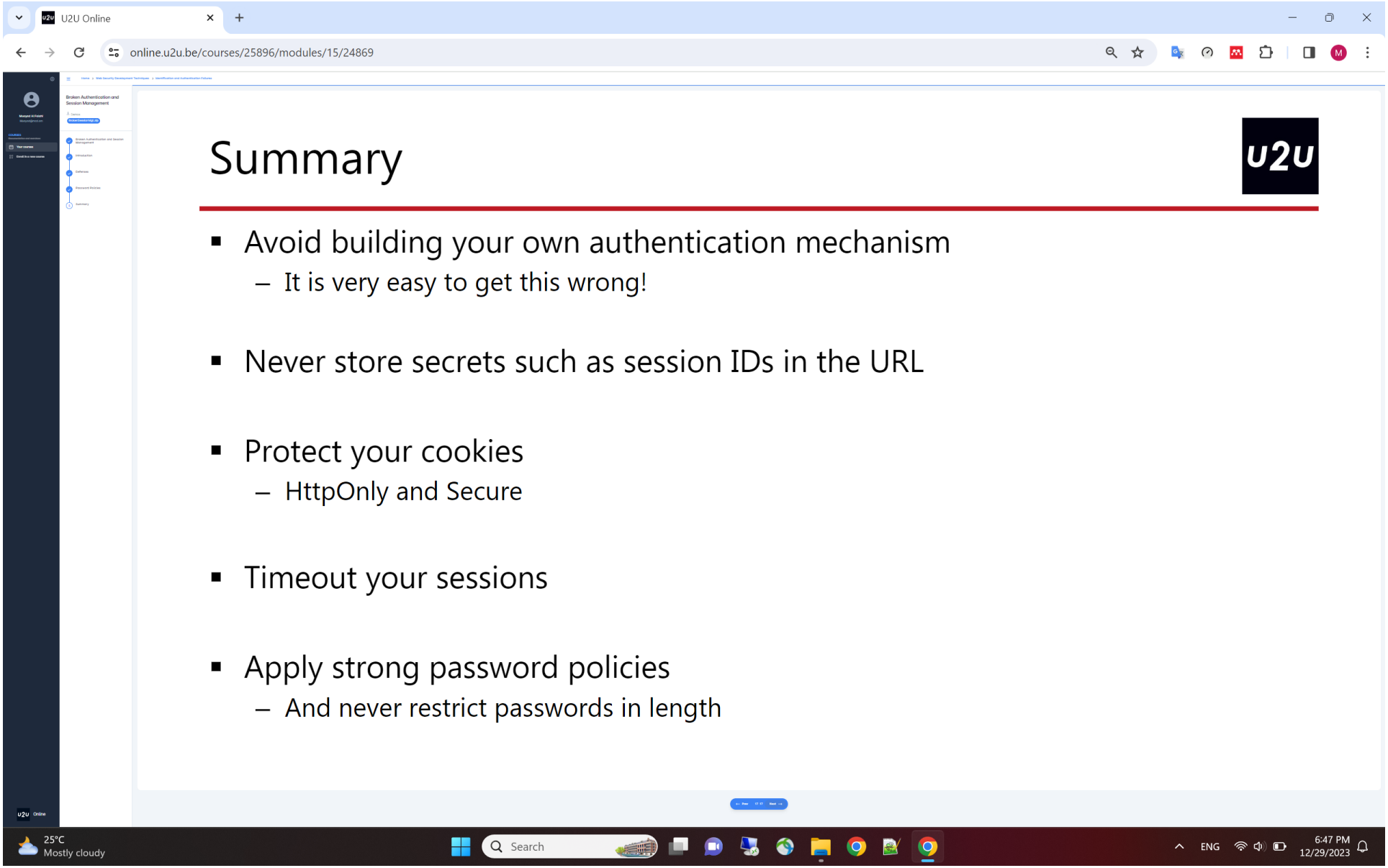
Checking Password Strength

- What makes a password strong?
  - Depends on who is talking (problem is the human factor again)
- Don't
  - Limit the length of a password (longer passwords are always better!)
    - A limit to a password length is a **security smell**!
  - Force people to embed special characters (they will substitute things like 'a' with '@')
  - Allow known words (but how do you check against different languages?!)
    - But do check against things like password, 123456, etc.
    - There are known online repositories for helping with this

25°C Mostly cloudy

Search

ENG 6:47 PM 12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/15/24869
Summary
u2u
Avoid building your own authentication mechanism
It is very easy to get this wrong!
Never store secrets such as session IDs in the URL
Protect your cookies
HttpOnly and Secure
Timeout your sessions
Apply strong password policies
And never restrict passwords in length
25°C
Mostly cloudy
Search
ENG
6:47 PM
12/29/2023