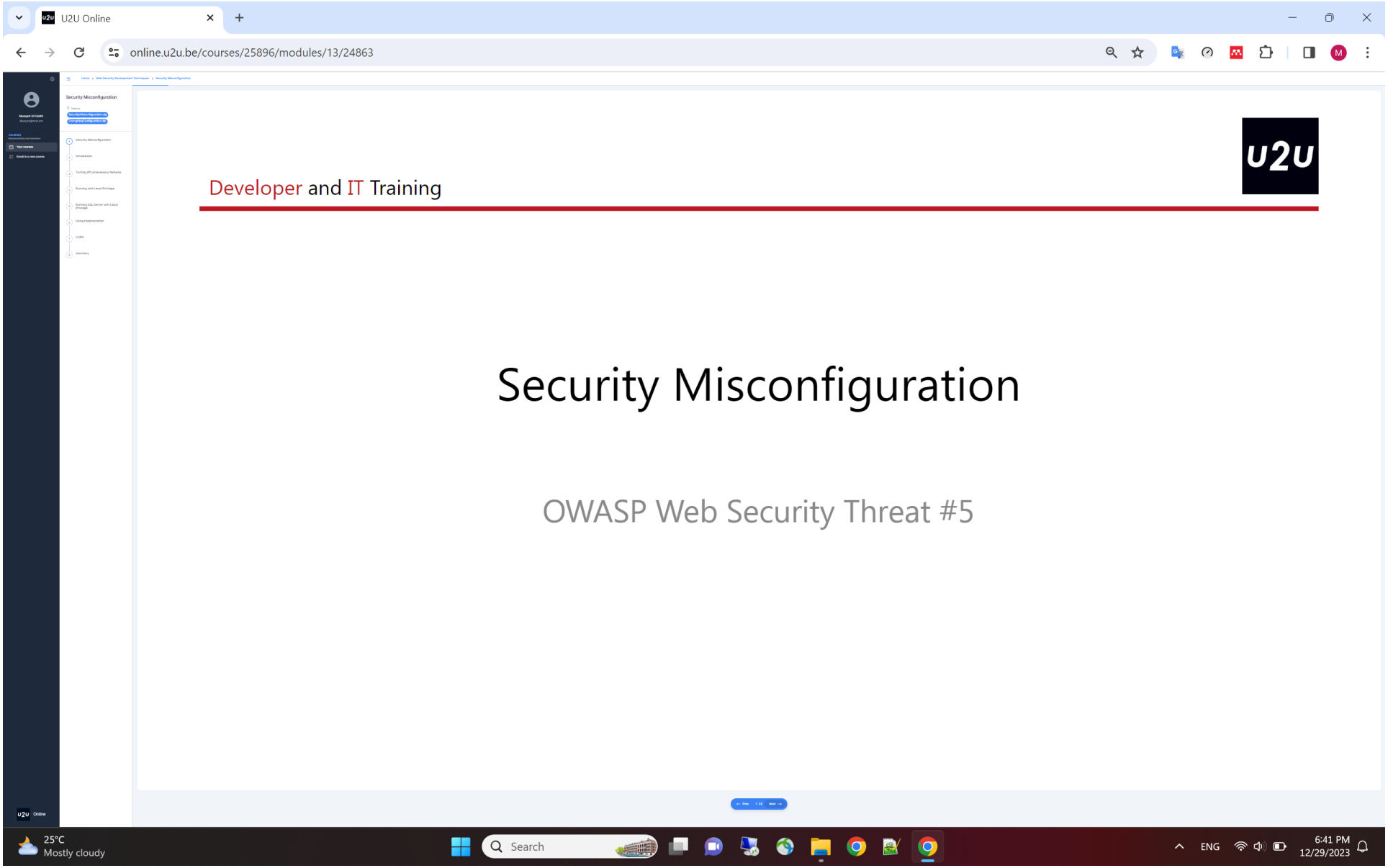
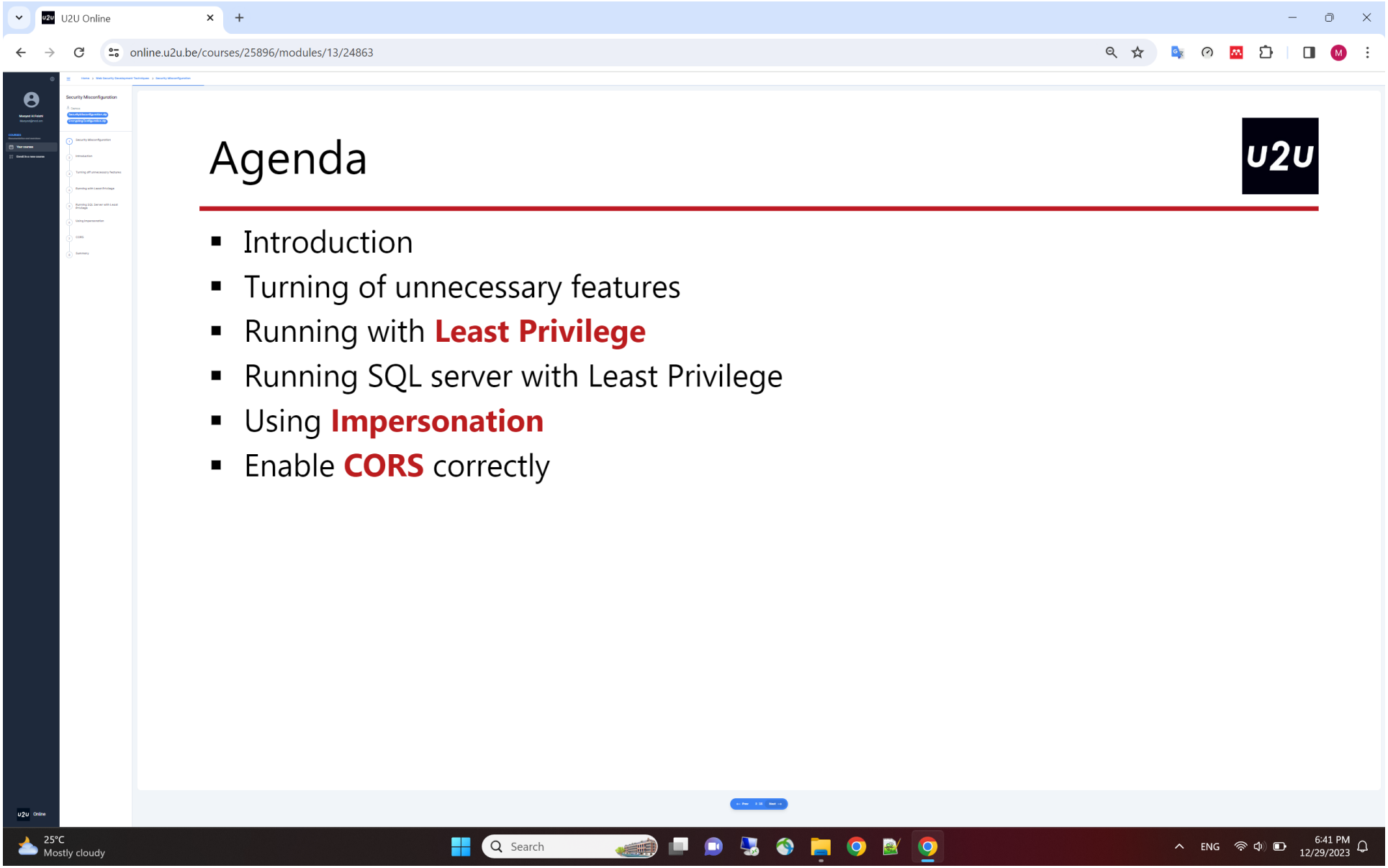
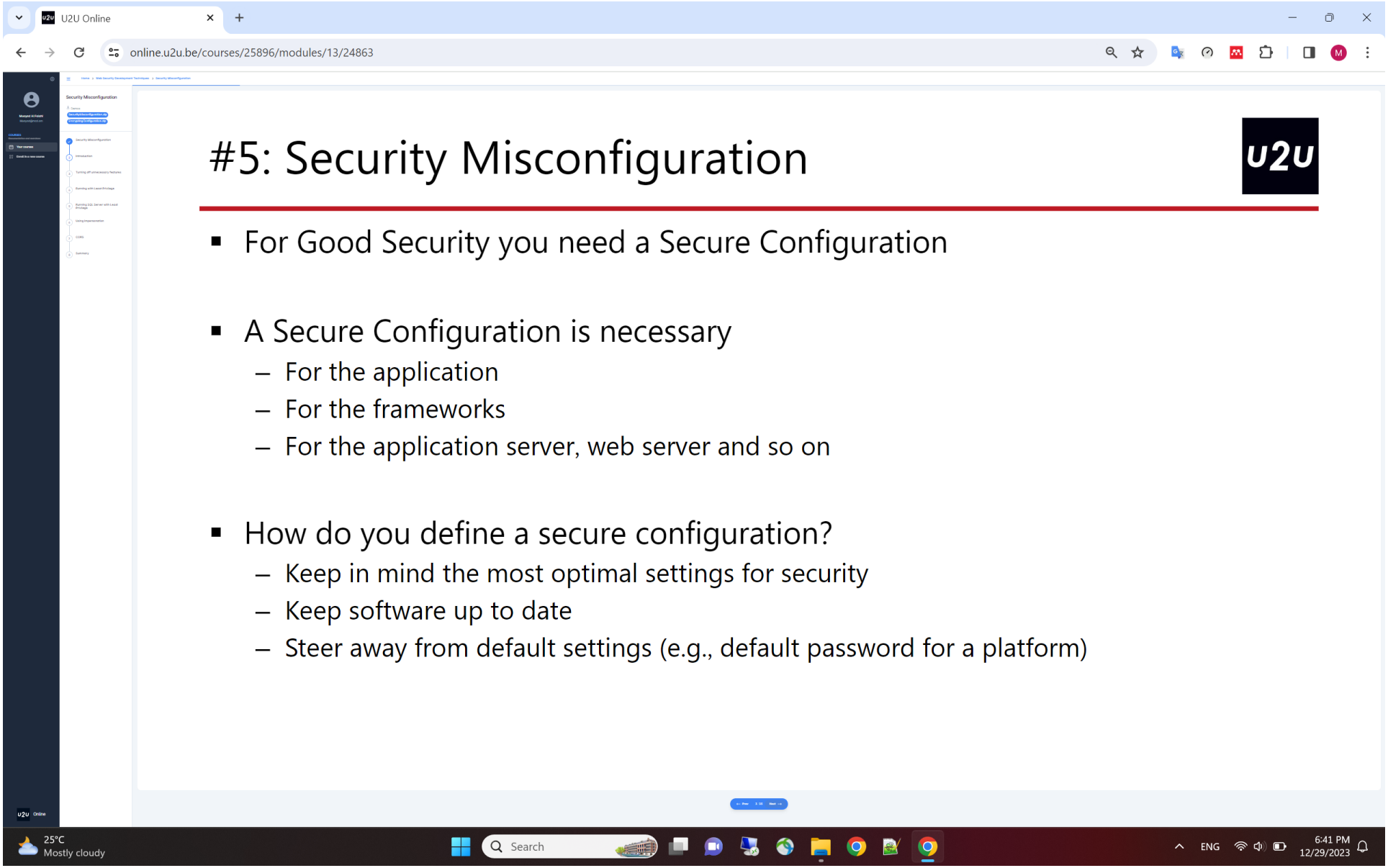
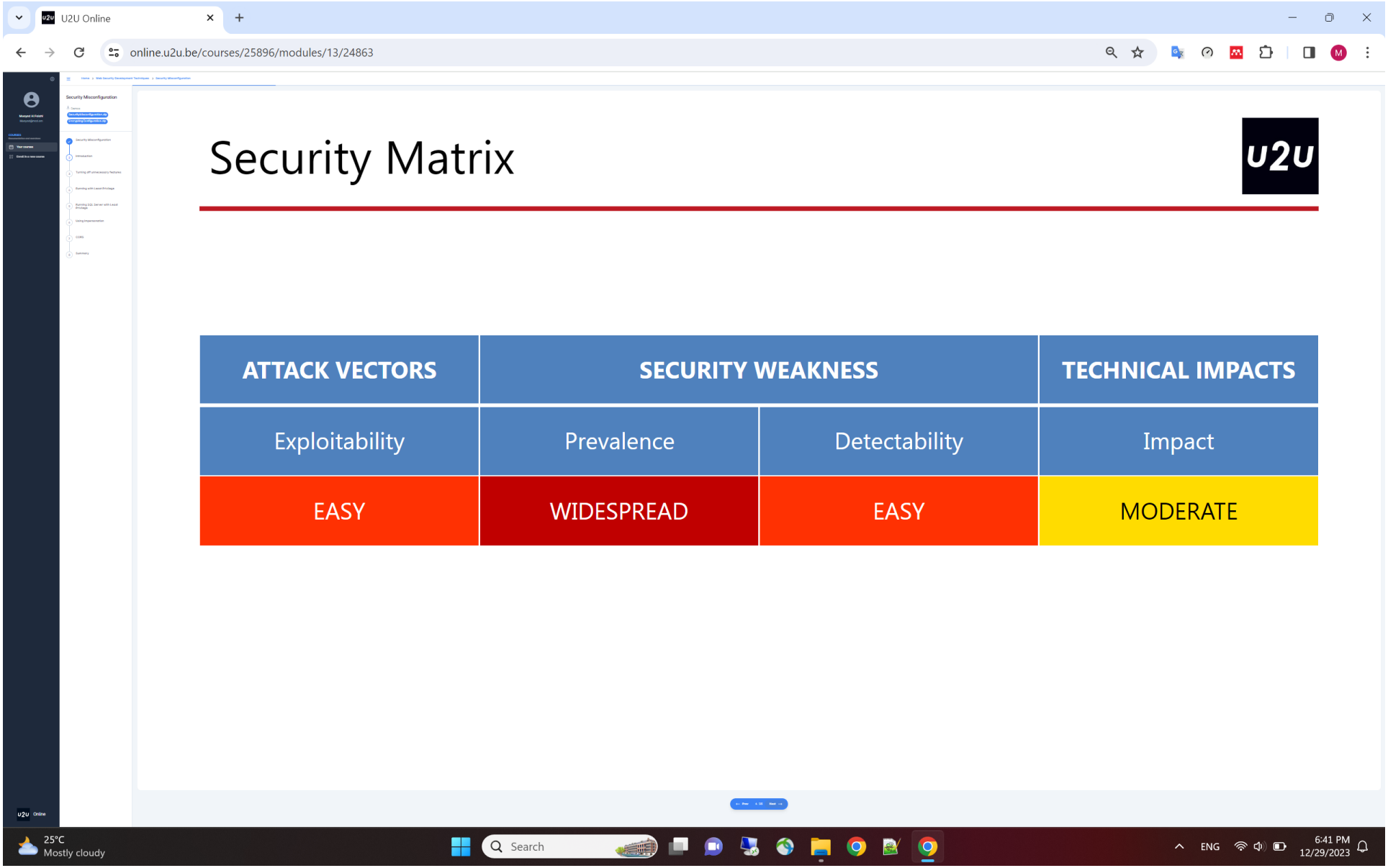

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Developer and IT Training
u2u
Security Misconfiguration
OWASP Web Security Threat #5
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/13/24863
Agenda
u2u
Introduction
Turning of unnecessary features
Running with Least Privilege
Running SQL server with Least Privilege
Using Impersonation
Enable CORS correctly
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

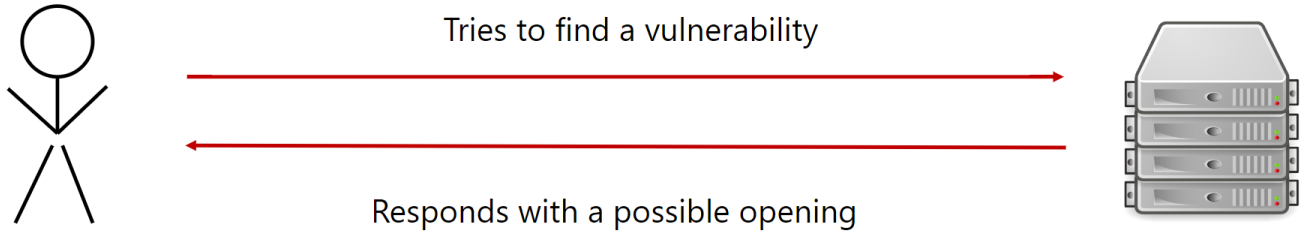

U2U Online
online.u2u.be/courses/25896/modules/13/24863
#5: Security Misconfiguration
U2U
For Good Security you need a Secure Configuration
A Secure Configuration is necessary
For the application
For the frameworks
For the application server, web server and so on
How do you define a secure configuration?
Keep in mind the most optimal settings for security
Keep software up to date
Steer away from default settings (e.g., default password for a platform)
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/13/24863
Security Misconfiguration
Security Matrix
u2u
ATTACK VECTORS
SECURITY WEAKNESS
TECHNICAL IMPACTS
Exploitability
Prevalence
Detectability
Impact
EASY
WIDESPREAD
EASY
MODERATE
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/13/24863

Visualizing an Attack

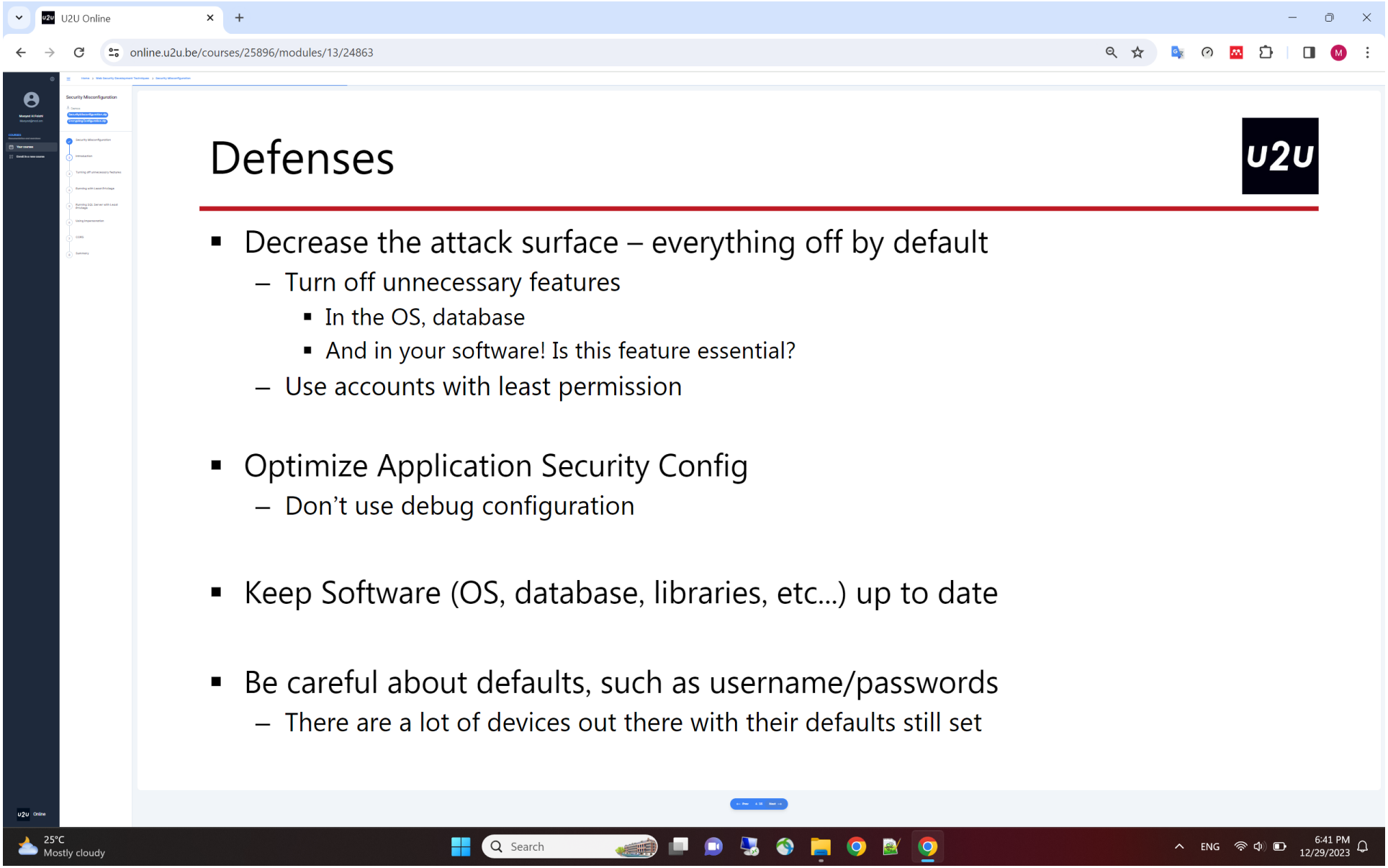


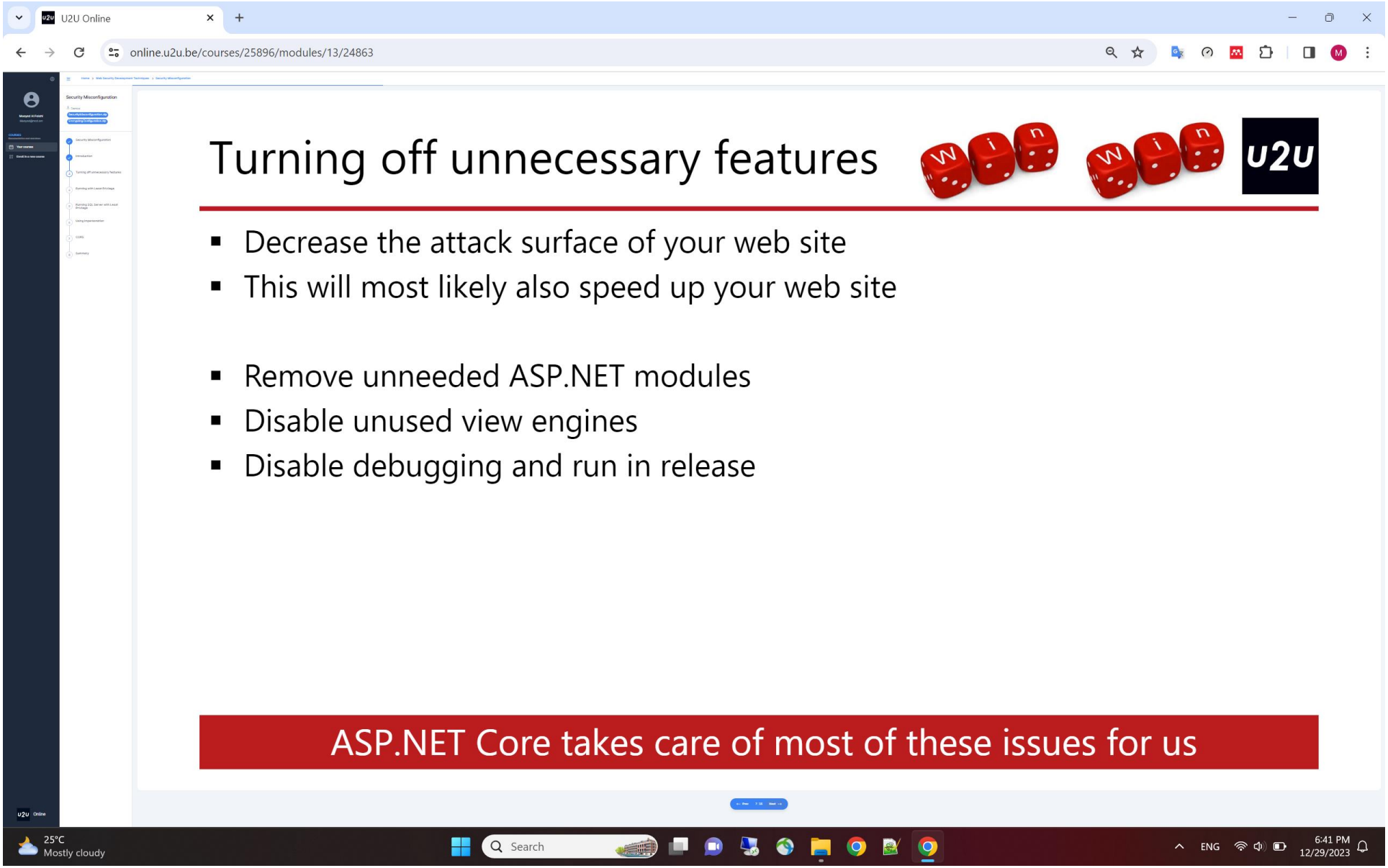
25°C
Mostly cloudy

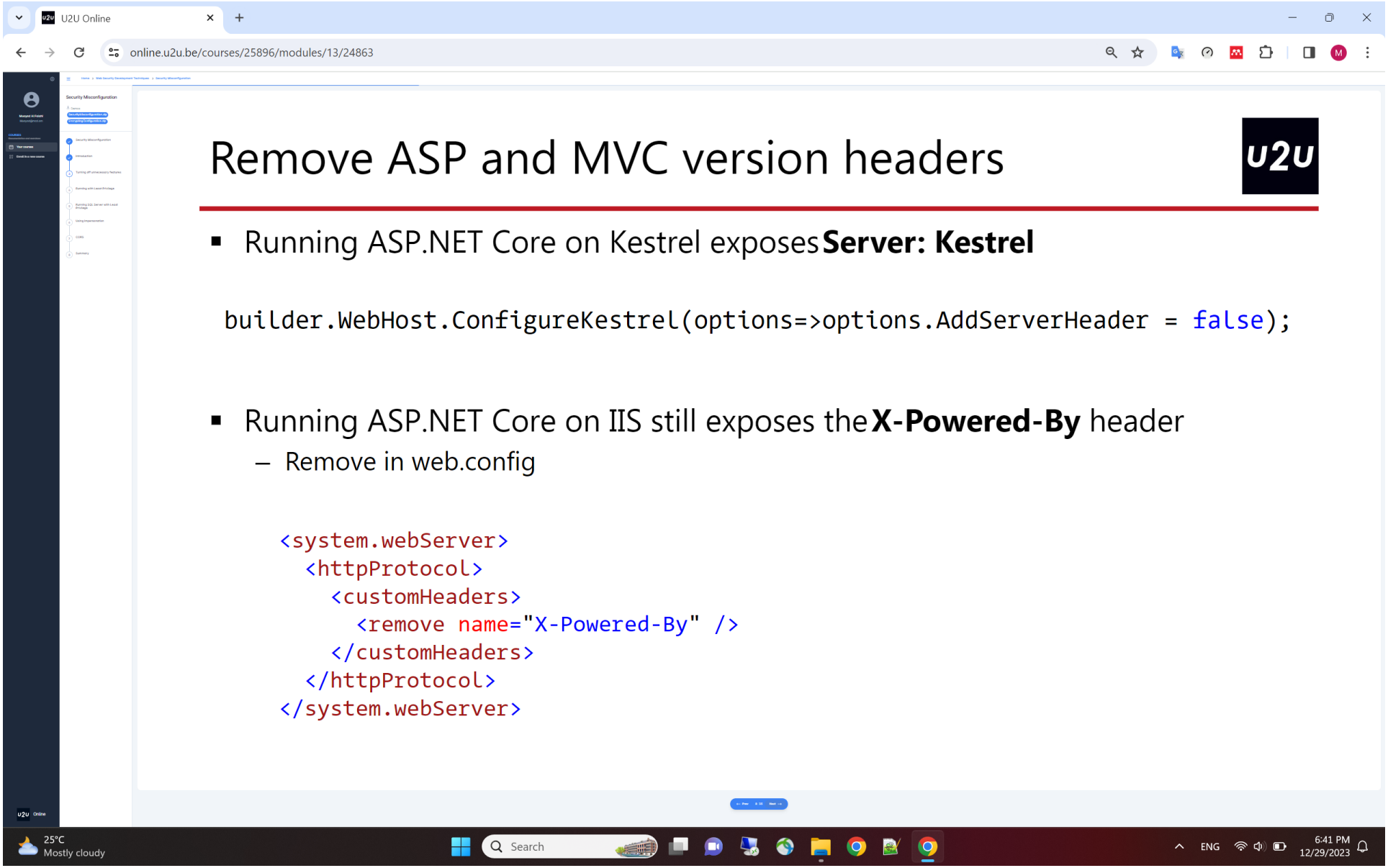
Search

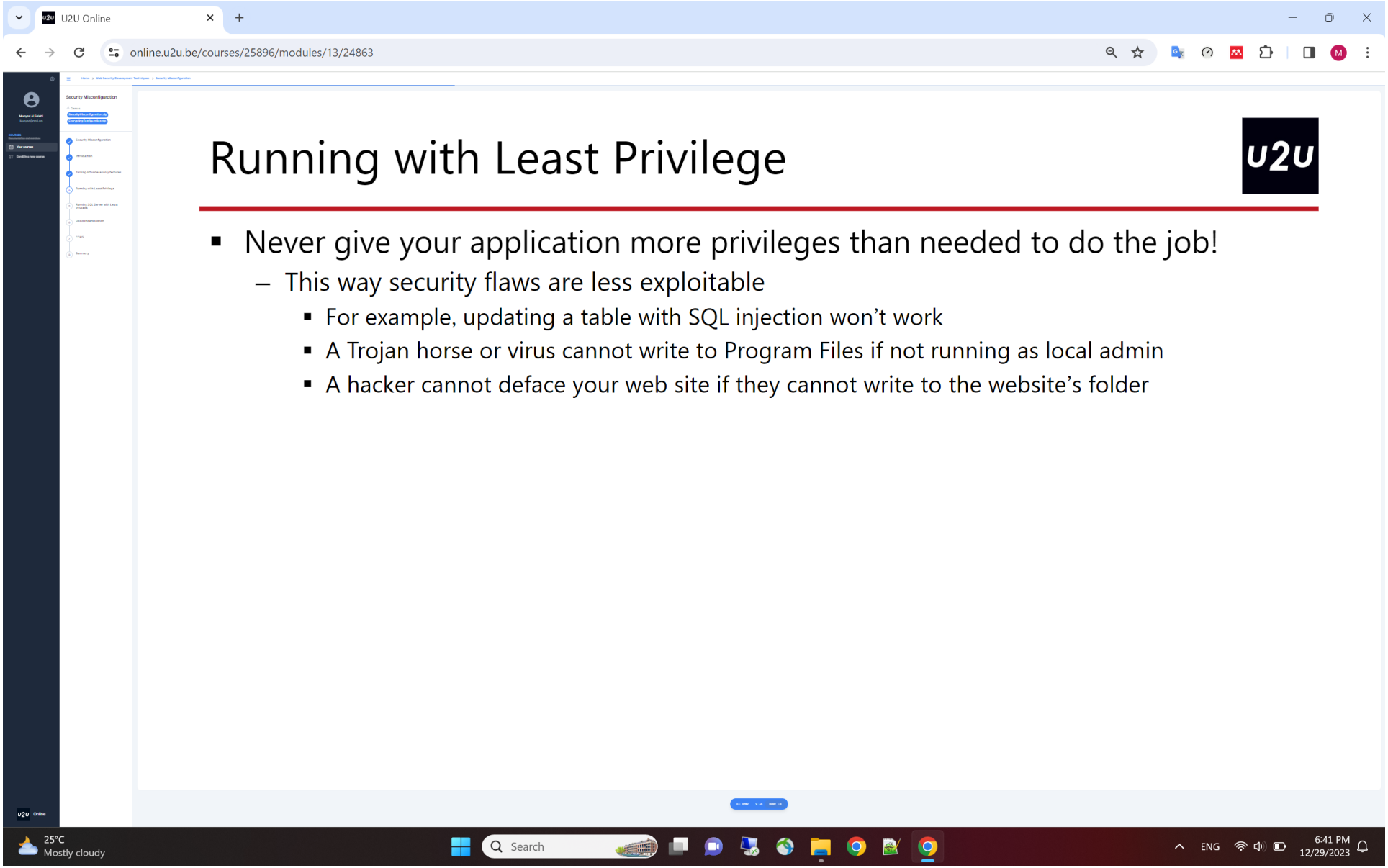
ENG

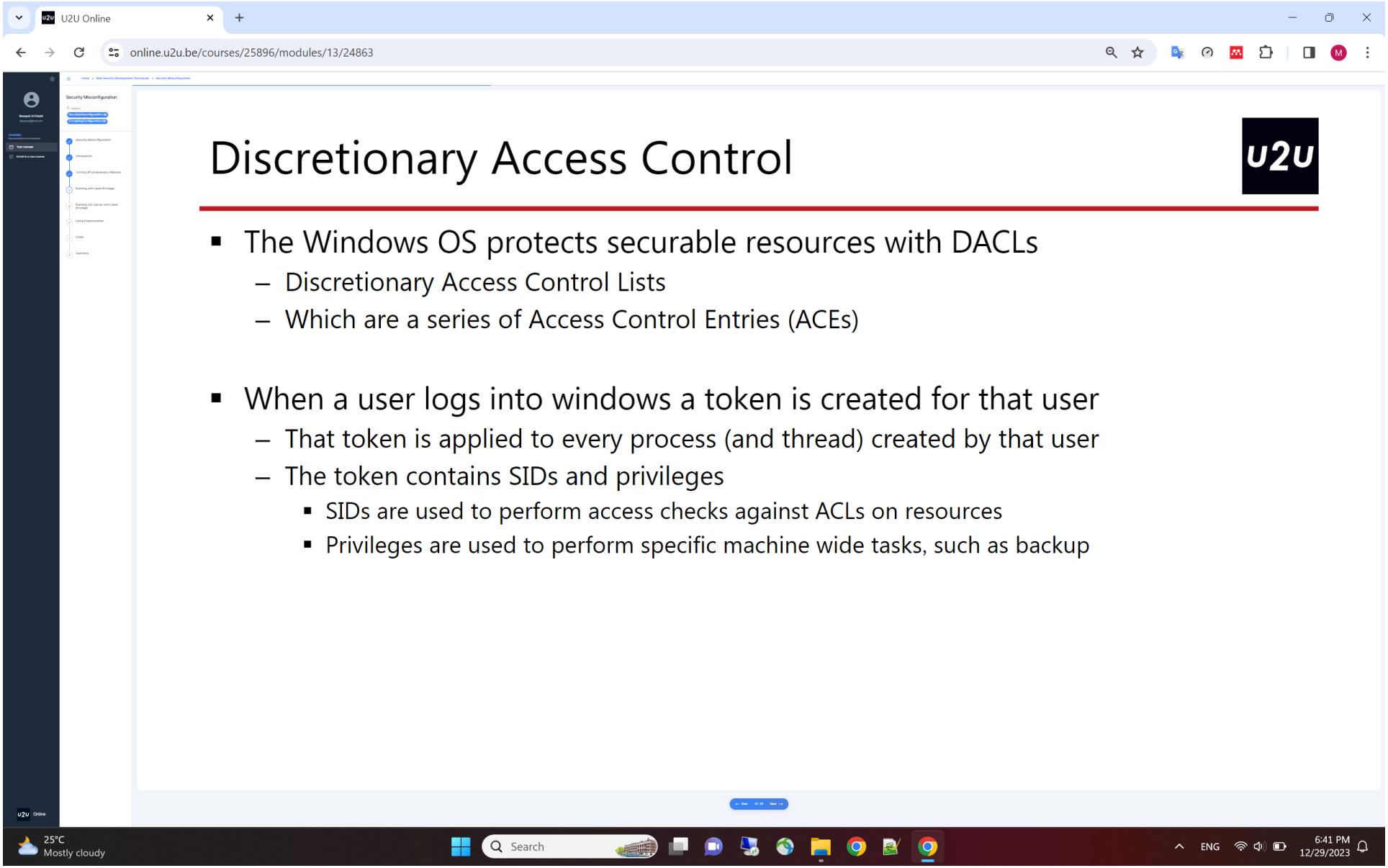
6:41 PM
12/29/2023

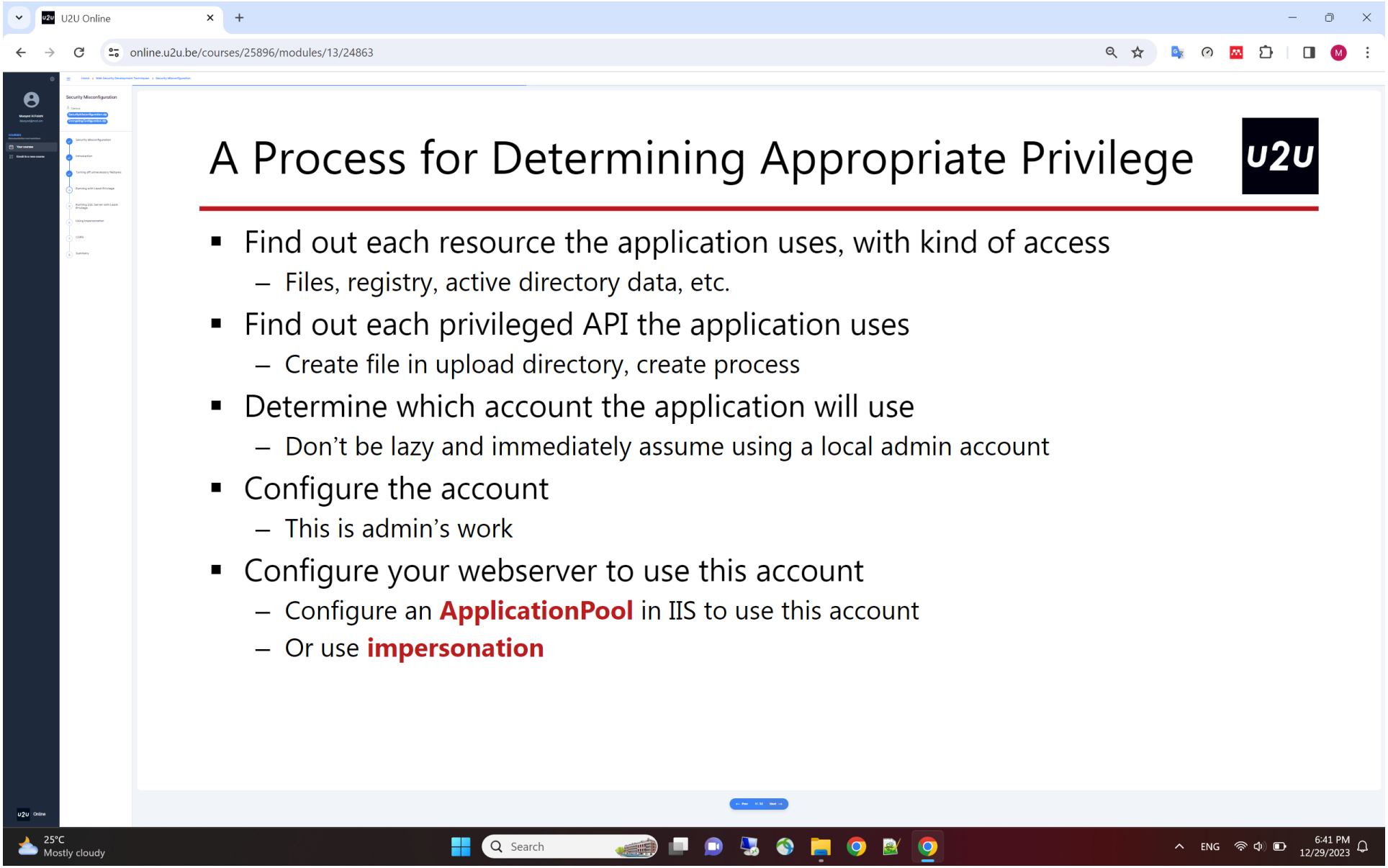

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Defenses
U2U
Decrease the attack surface – everything off by default
Turn off unnecessary features
In the OS, database
And in your software! Is this feature essential?
Use accounts with least permission
Optimize Application Security Config
Don't use debug configuration
Keep Software (OS, database, libraries, etc...) up to date
Be careful about defaults, such as username/passwords
There are a lot of devices out there with their defaults still set
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

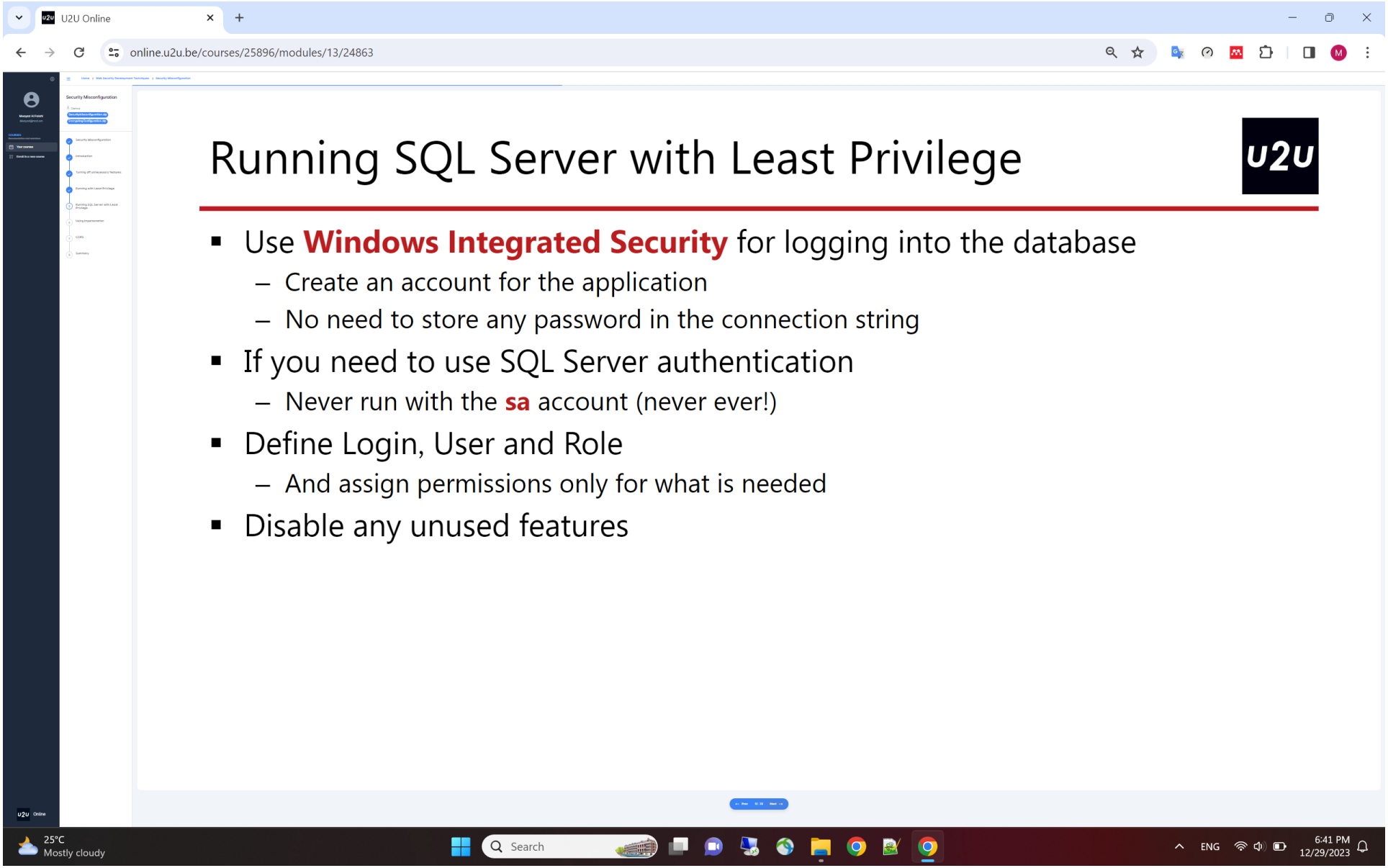

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Turning off unnecessary features
U2U
Decrease the attack surface of your web site
This will most likely also speed up your web site
Remove unneeded ASP.NET modules
Disable unused view engines
Disable debugging and run in release
ASP.NET Core takes care of most of these issues for us
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

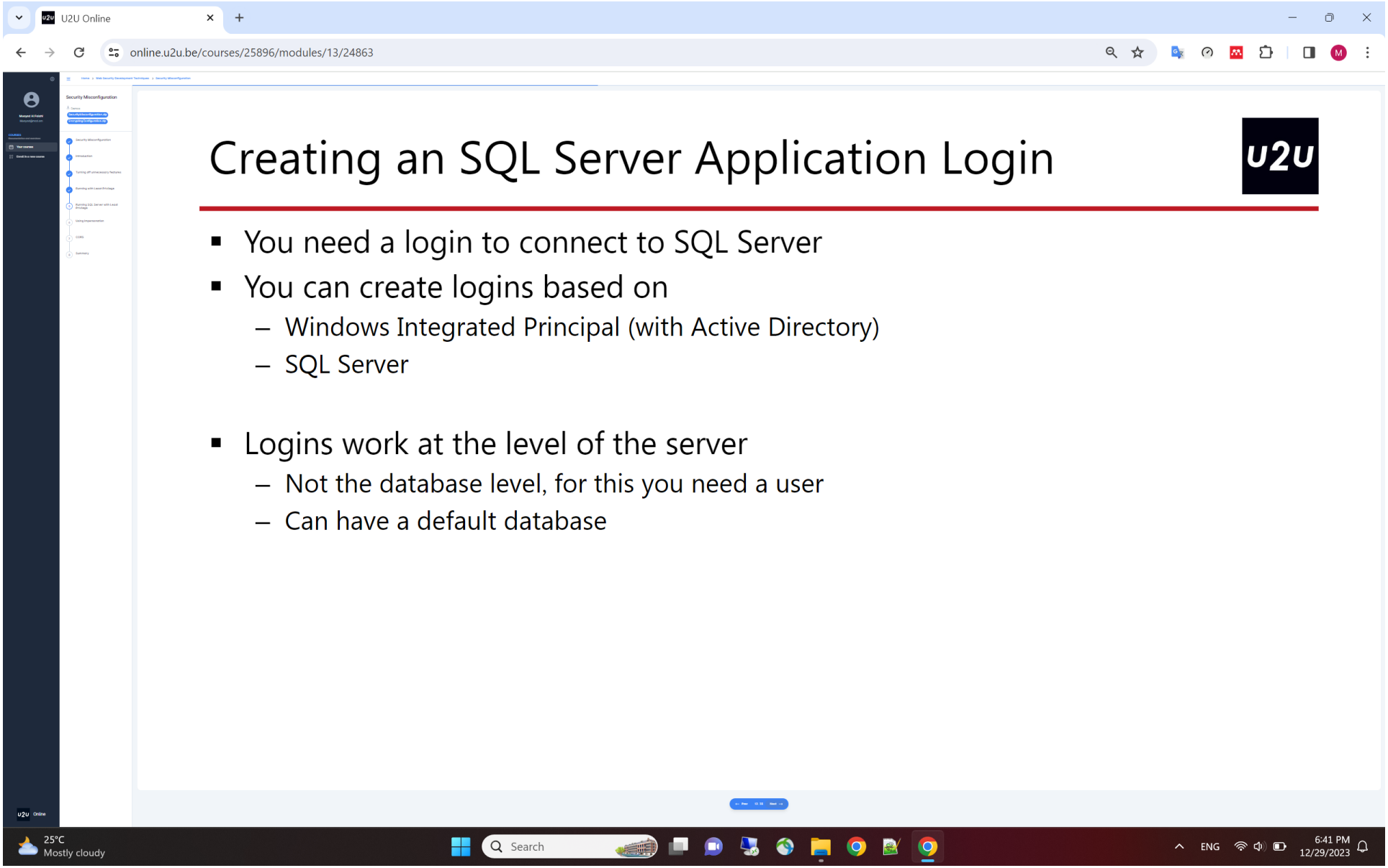

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Remove ASP and MVC version headers
U2U
Running ASP.NET Core on Kestrel exposes Server: Kestrel
builder.WebHost.ConfigureKestrel(options=>options.AddServerHeader = false);
Running ASP.NET Core on IIS still exposes the X-Powered-By header
Remove in web.config
<system.webServer>
<httpProtocol>
<customHeaders>
<remove name="X-Powered-By" />
</customHeaders>
</httpProtocol>
</system.webServer>
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

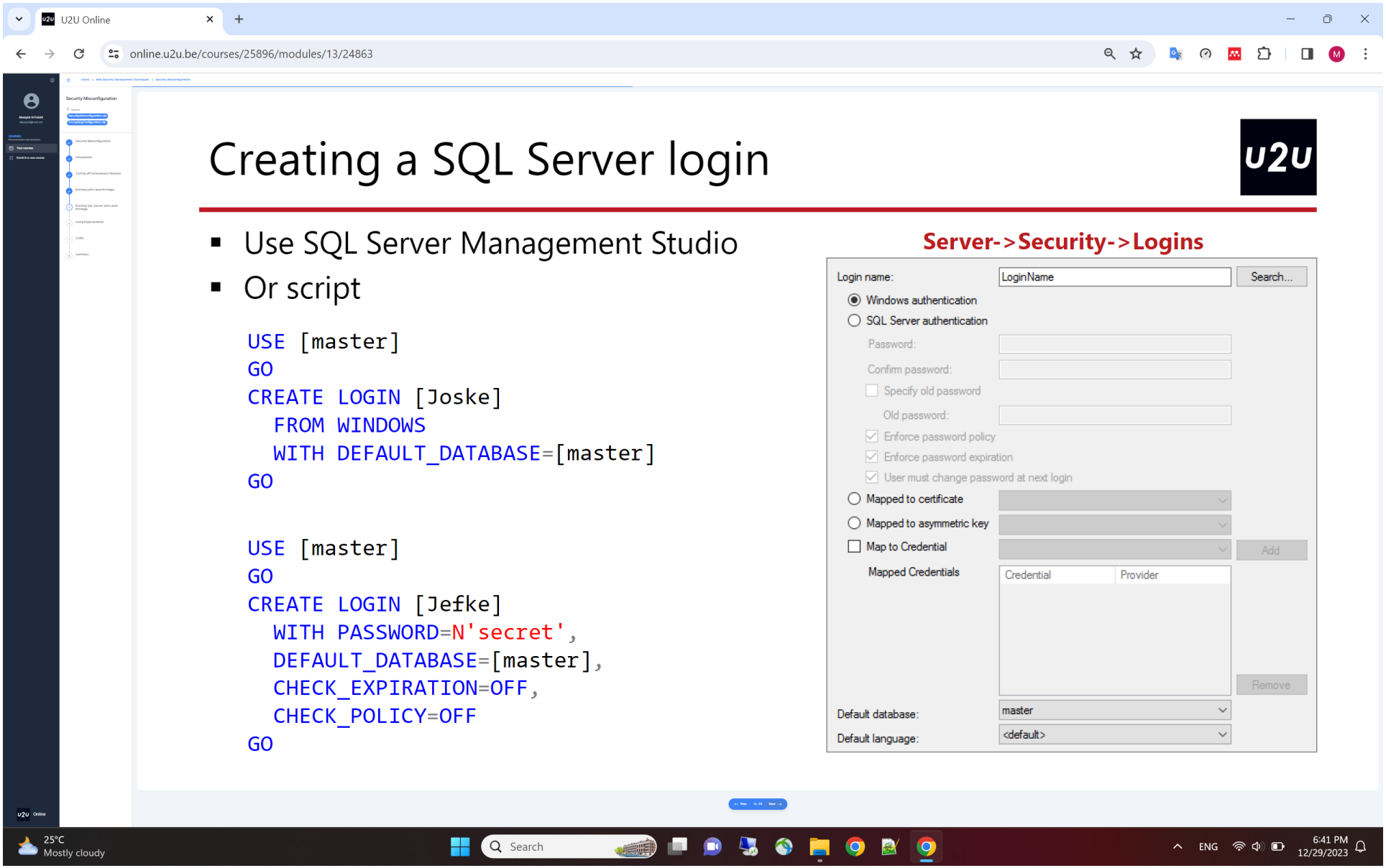

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Running with Least Privilege
U2U
Never give your application more privileges than needed to do the job!
This way security flaws are less exploitable
For example, updating a table with SQL injection won't work
A Trojan horse or virus cannot write to Program Files if not running as local admin
A hacker cannot deface your web site if they cannot write to the website's folder
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

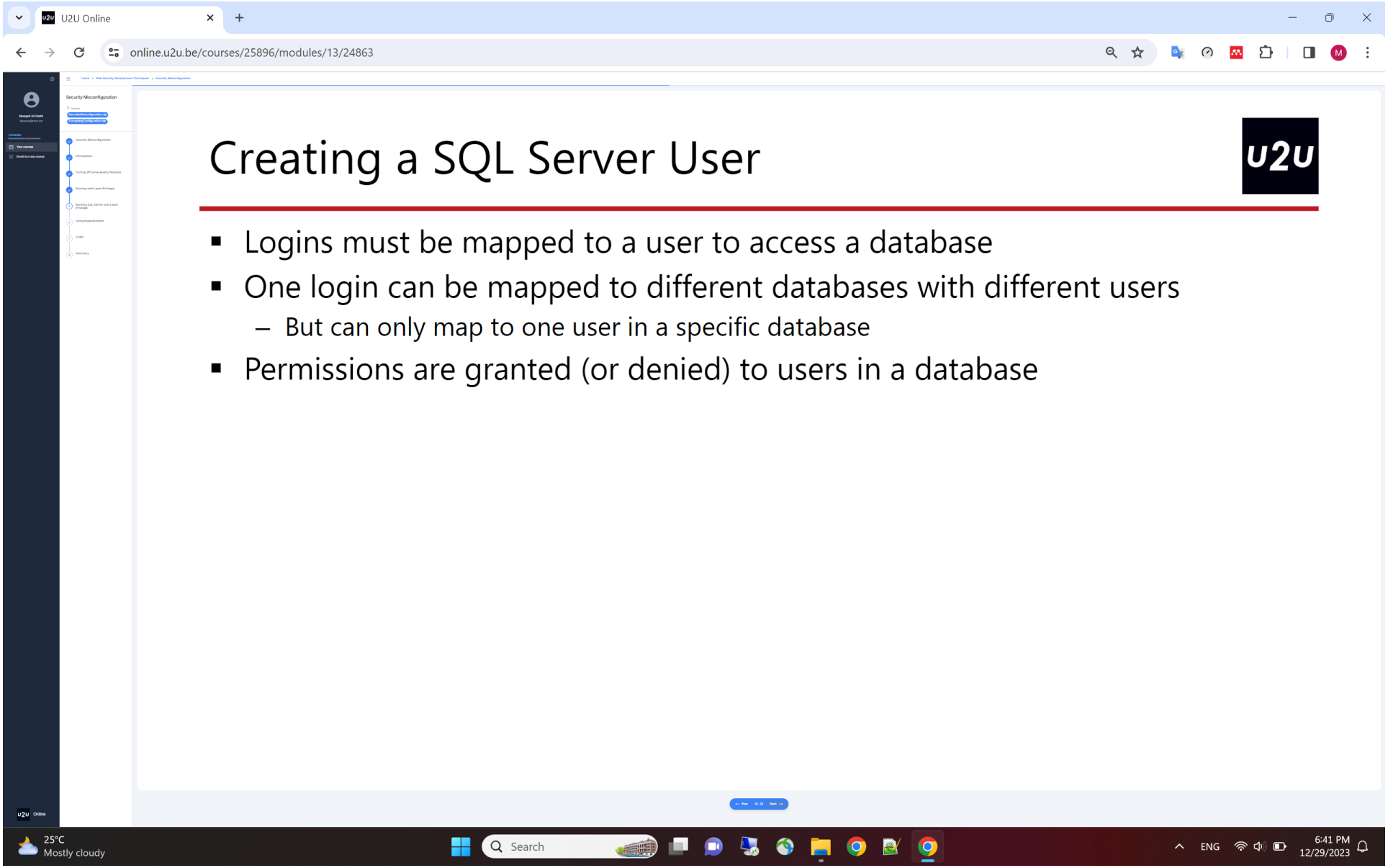

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Discretionary Access Control
u2u
The Windows OS protects securable resources with DACLs
Discretionary Access Control Lists
Which are a series of Access Control Entries (ACEs)
When a user logs into windows a token is created for that user
That token is applied to every process (and thread) created by that user
The token contains SIDs and privileges
SIDs are used to perform access checks against ACLs on resources
Privileges are used to perform specific machine wide tasks, such as backup
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

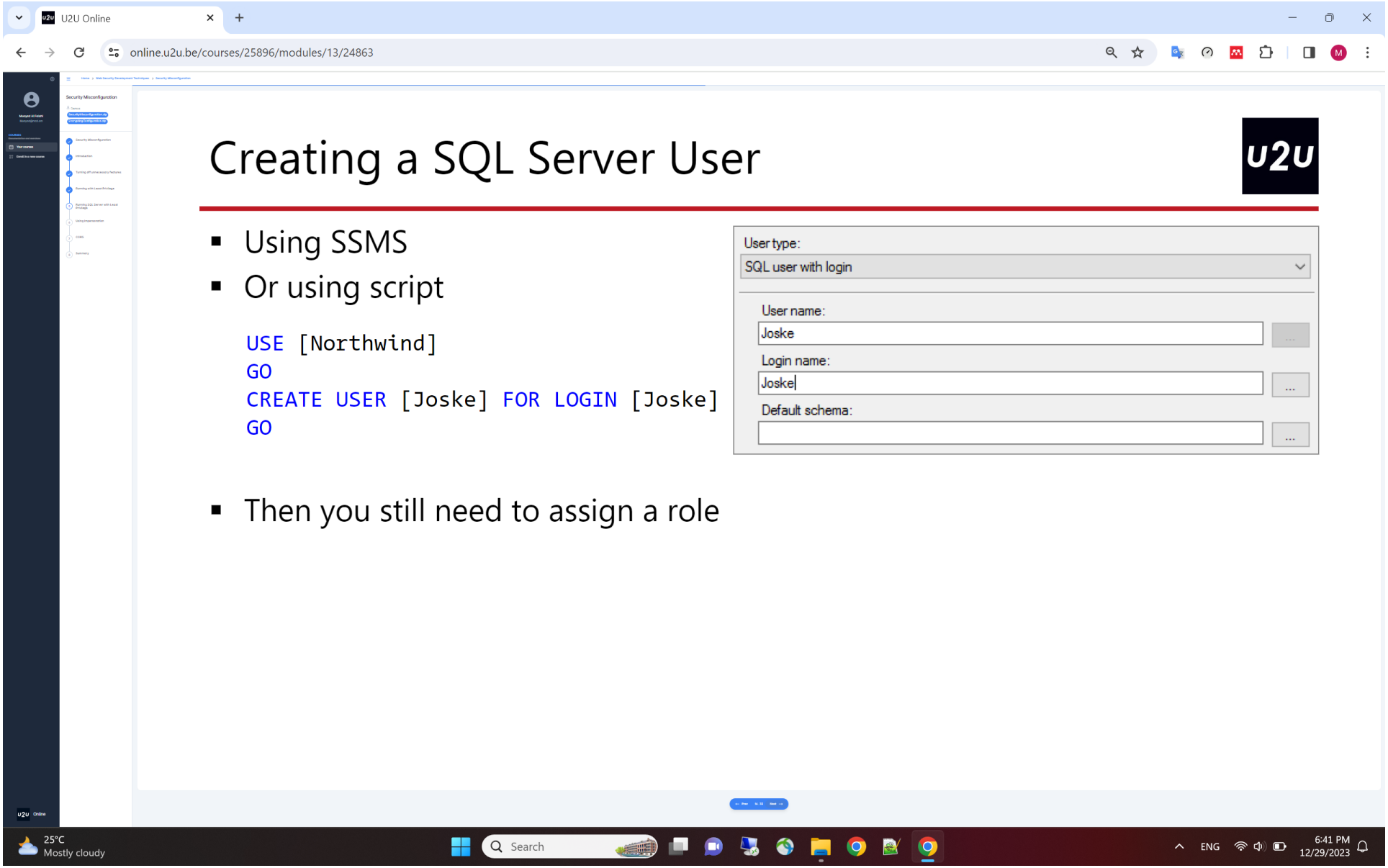

U2U Online
online.u2u.be/courses/25896/modules/13/24863
A Process for Determining Appropriate Privilege
U2U
Find out each resource the application uses, with kind of access
Files, registry, active directory data, etc.
Find out each privileged API the application uses
Create file in upload directory, create process
Determine which account the application will use
Don't be lazy and immediately assume using a local admin account
Configure the account
This is admin's work
Configure your webserver to use this account
Configure an ApplicationPool in IIS to use this account
Or use impersonation
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

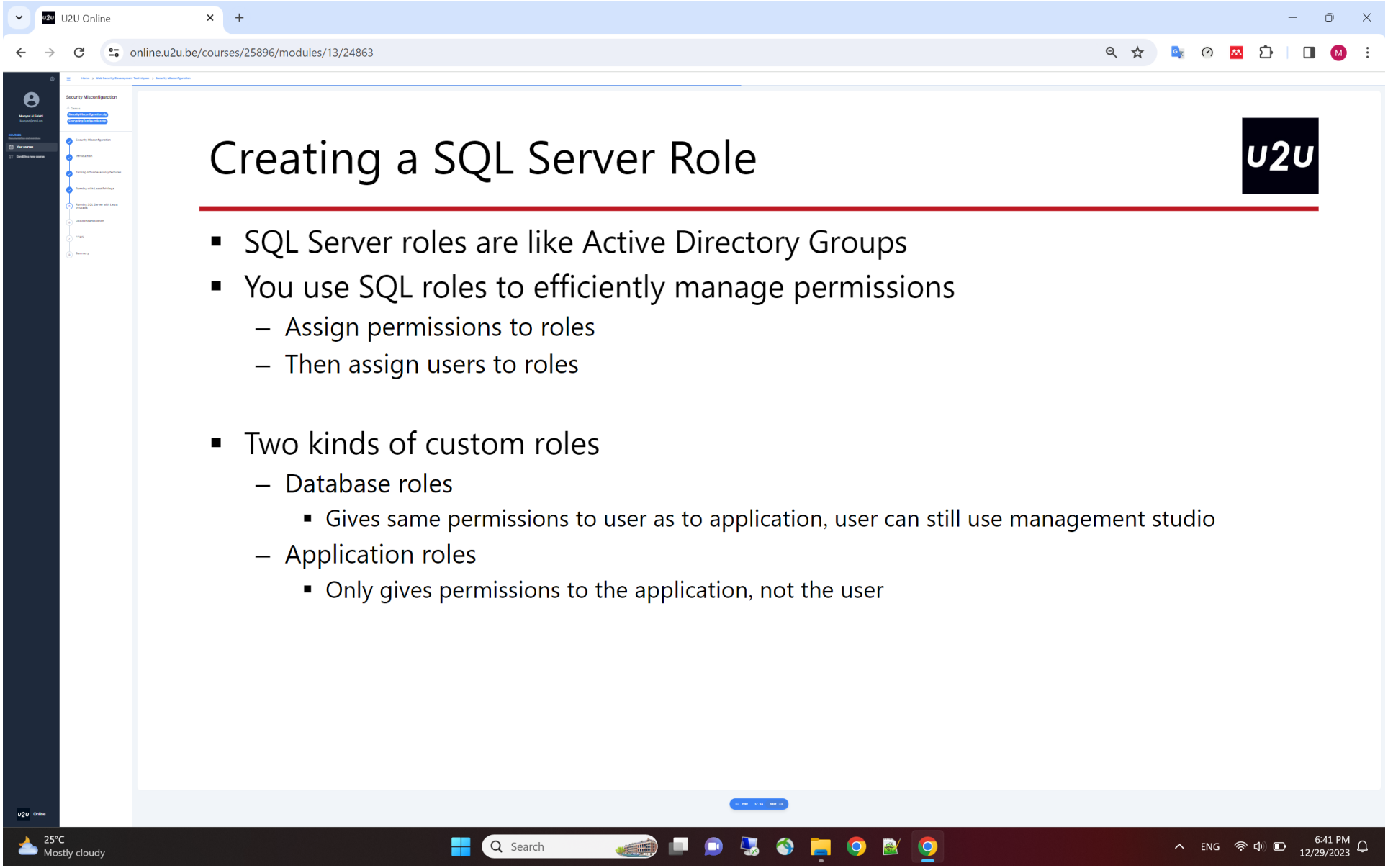

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Running SQL Server with Least Privilege
U2U
Use Windows Integrated Security for logging into the database
Create an account for the application
No need to store any password in the connection string
If you need to use SQL Server authentication
Never run with the sa account (never ever!)
Define Login, User and Role
And assign permissions only for what is needed
Disable any unused features
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/13/24863
Creating an SQL Server Application Login
u2u
You need a login to connect to SQL Server
You can create logins based on
Windows Integrated Principal (with Active Directory)
SQL Server
Logins work at the level of the server
Not the database level, for this you need a user
Can have a default database
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/13/24863
Creating a SQL Server login
U2U
Use SQL Server Management Studio
Or script
USE [master]
GO
CREATE LOGIN [Joske]
FROM WINDOWS
WITH DEFAULT_DATABASE=[master]
GO
USE [master]
GO
CREATE LOGIN [Jefke]
WITH PASSWORD=N'secret',
DEFAULT_DATABASE=[master],
CHECK_EXPIRATION=OFF,
CHECK_POLICY=OFF
GO
Server->Security->Logins
Login name:
LoginName
Search...
Windows authentication
SQL Server authentication
Password:
Confirm password:
Specify old password
Old password:
Enforce password policy
Enforce password expiration
User must change password at next login
Mapped to certificate
Mapped to asymmetric key
Map to Credential
Add
Mapped Credentials
Credential
Provider
Remove
Default database:
master
Default language:
<default>
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/13/24863
Creating a SQL Server User
u2u
Logins must be mapped to a user to access a database
One login can be mapped to different databases with different users
But can only map to one user in a specific database
Permissions are granted (or denied) to users in a database
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

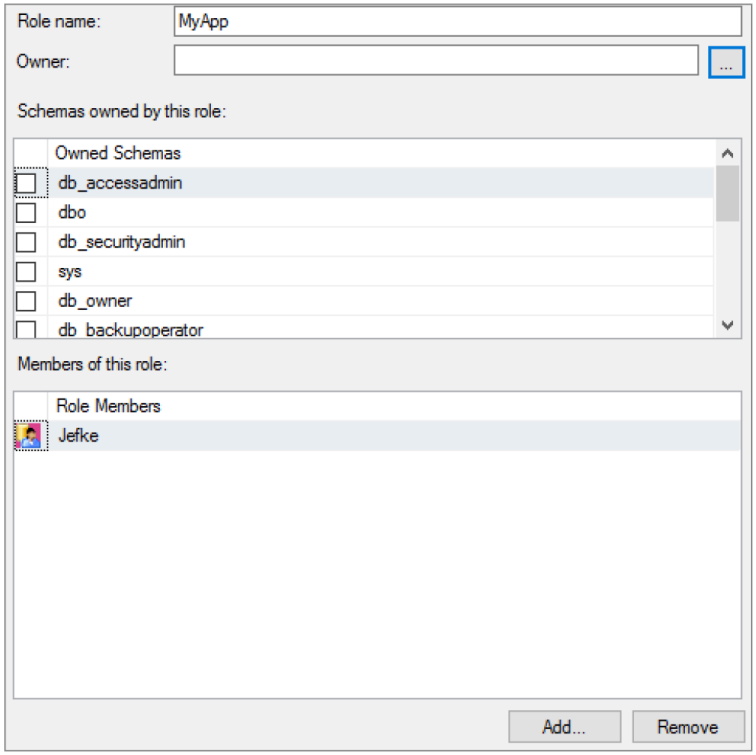

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Creating a SQL Server User
u2u
Using SSMS
Or using script
USE [Northwind]
GO
CREATE USER [Joske] FOR LOGIN [Joske]
GO
Then you still need to assign a role
User type:
SQL user with login
User name:
Joske
Login name:
Joske
Default schema:
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

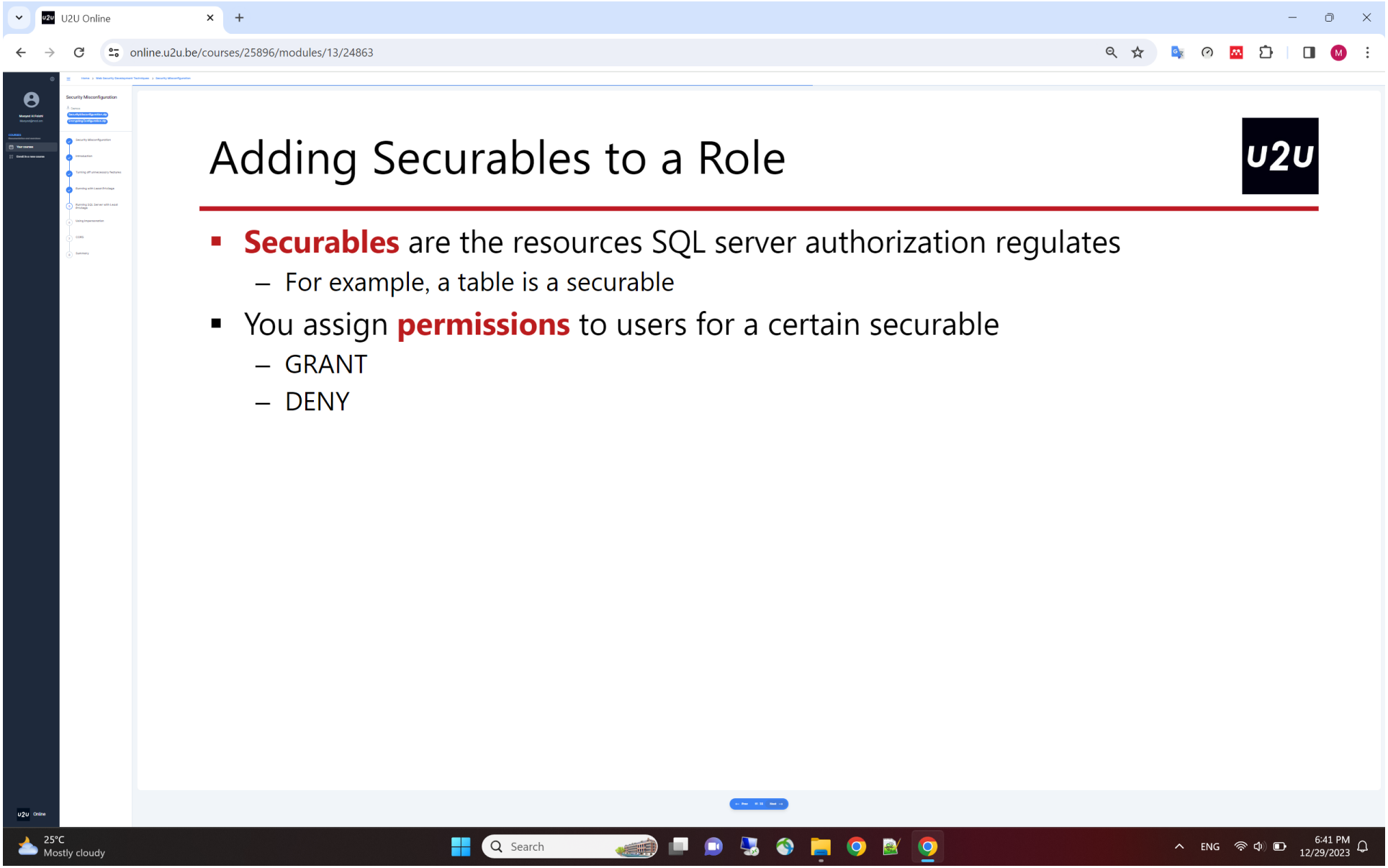

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Creating a SQL Server Role
u2u
SQL Server roles are like Active Directory Groups
You use SQL roles to efficiently manage permissions
Assign permissions to roles
Then assign users to roles
Two kinds of custom roles
Database roles
Gives same permissions to user as to application, user can still use management studio
Application roles
Only gives permissions to the application, not the user
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

Creating a SQL Server Role

- Using SSMS
  - Select role name
  - Add owned schemas
  - Add members
- Or using script

```
USE [Northwind]
GO
CREATE ROLE [MyApp]
GO
USE [Northwind]
GO
ALTER ROLE [MyApp] ADD MEMBER [Jefke]
GO
```

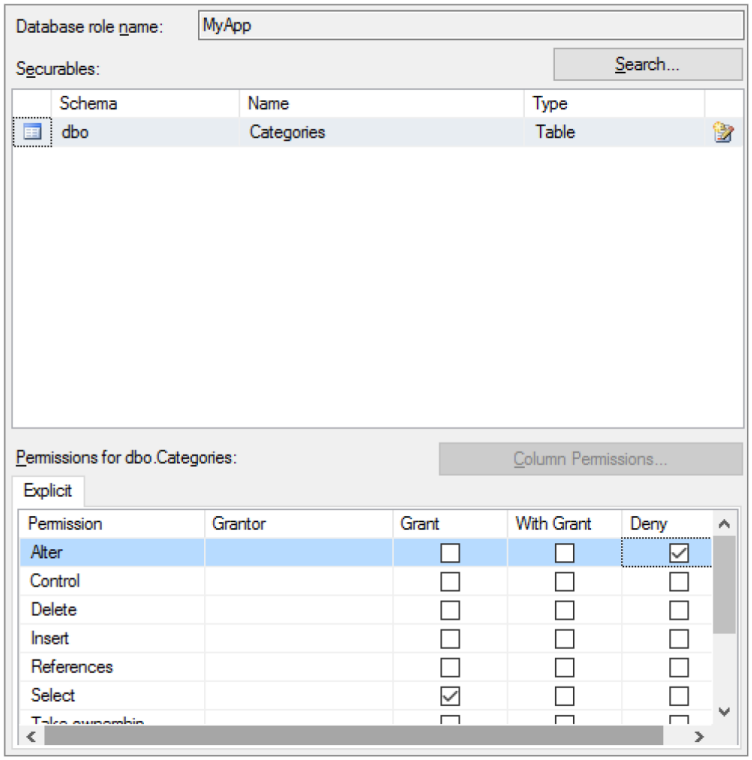


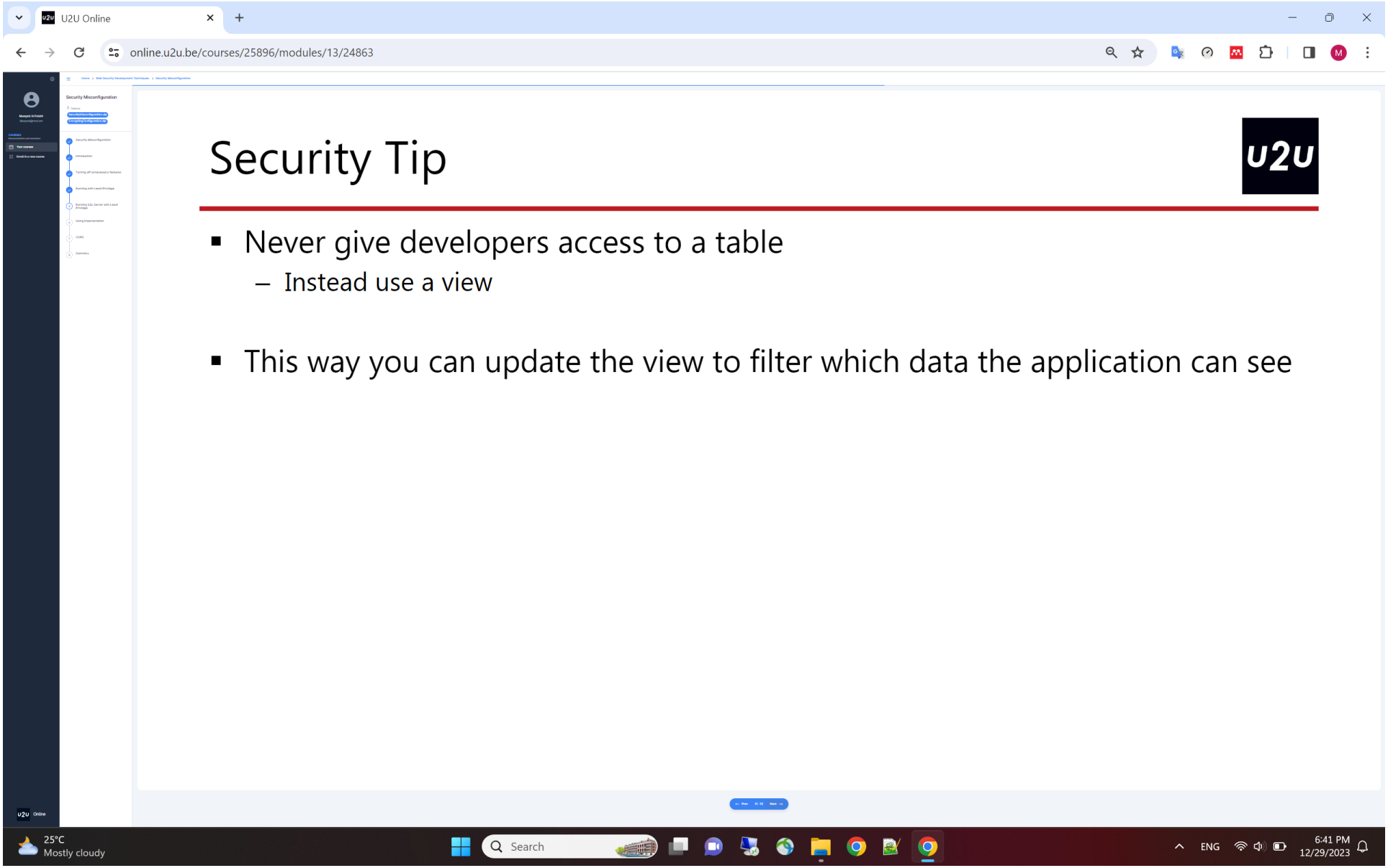

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Adding Securables to a Role
u2u
Securables are the resources SQL server authorization regulates
For example, a table is a securable
You assign permissions to users for a certain securable
GRANT
DENY
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

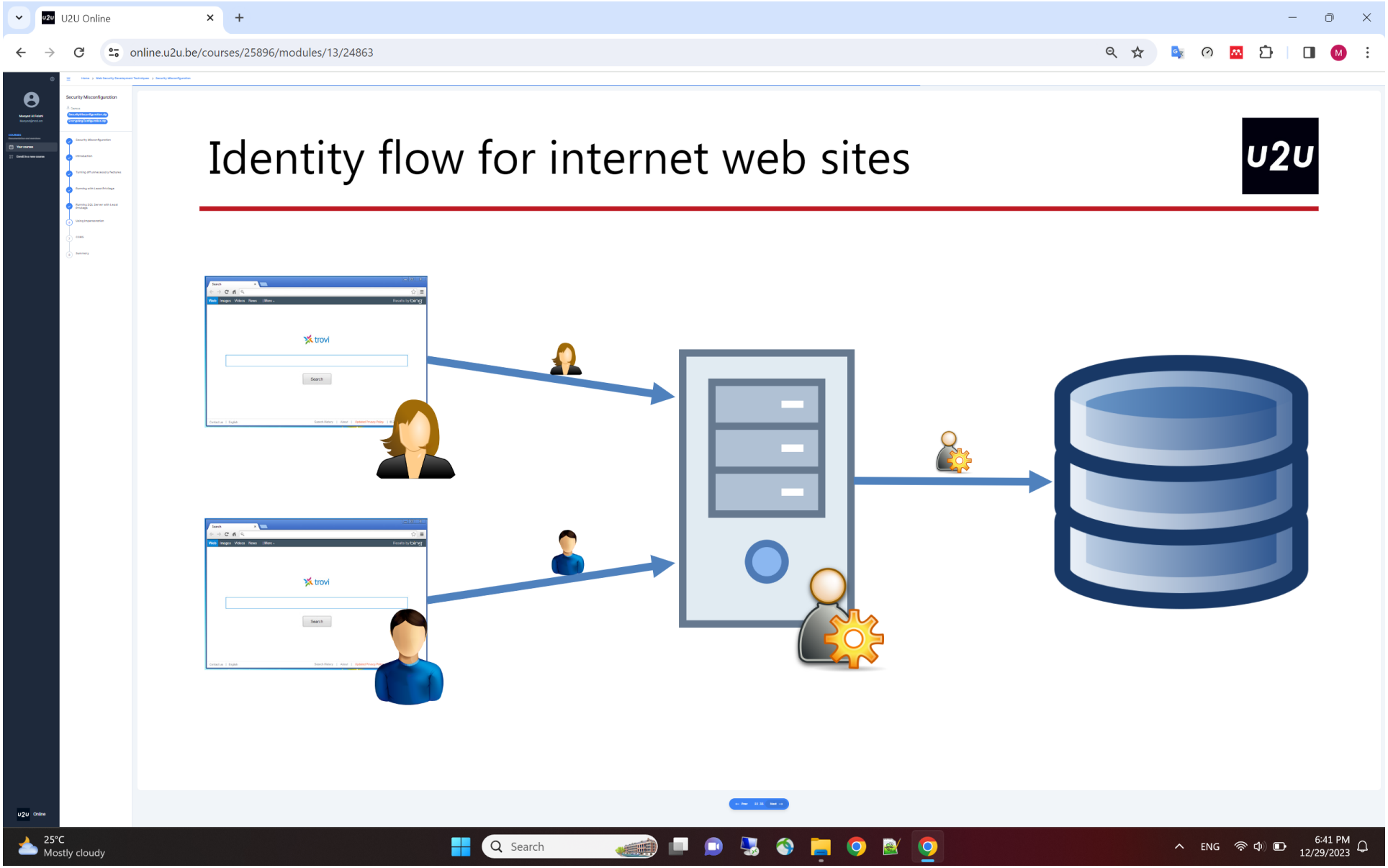
Adding Securables to a Role

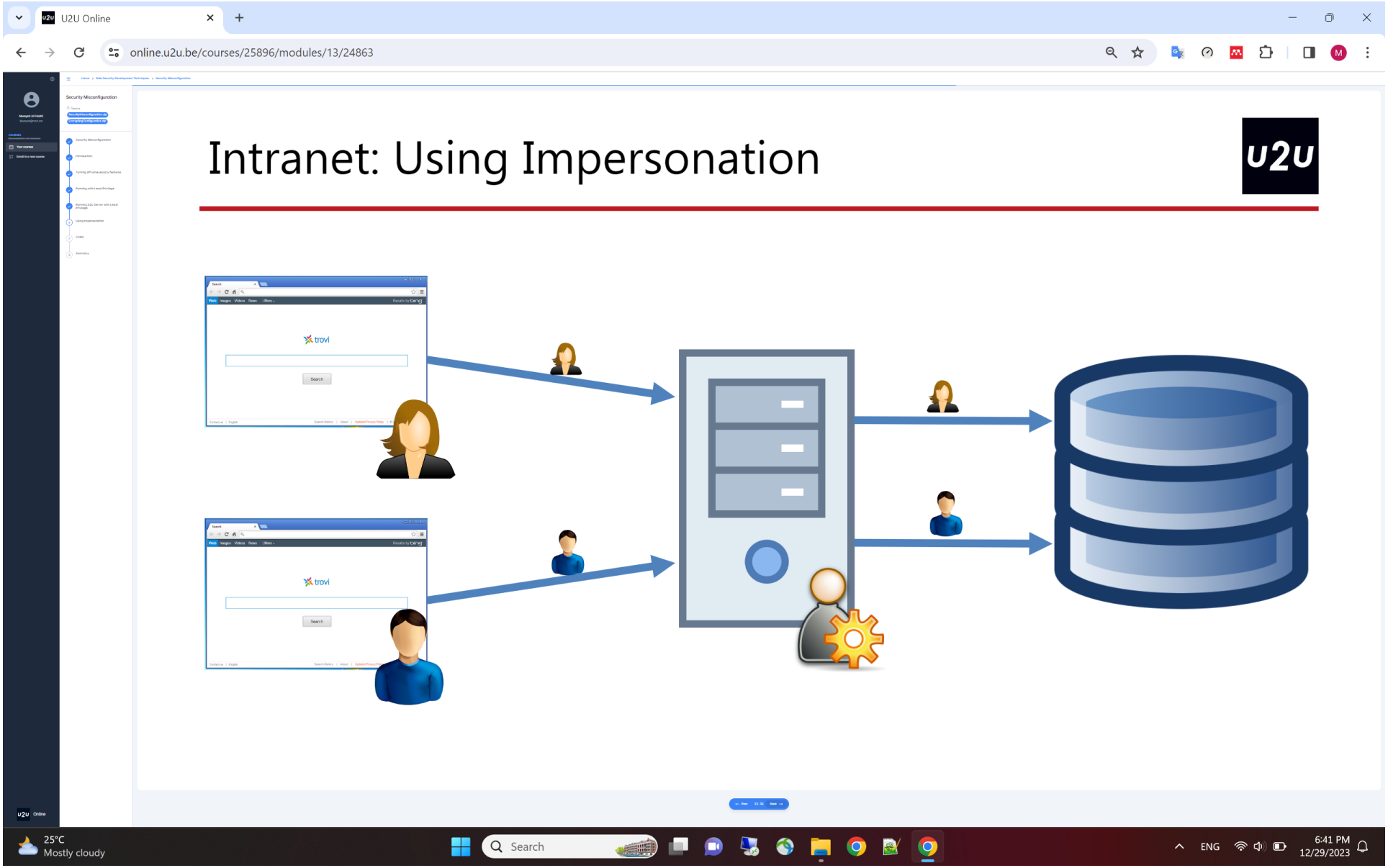
- Using SSMS
  - Select a securable with Search
  - Then configure permissions
- Using script

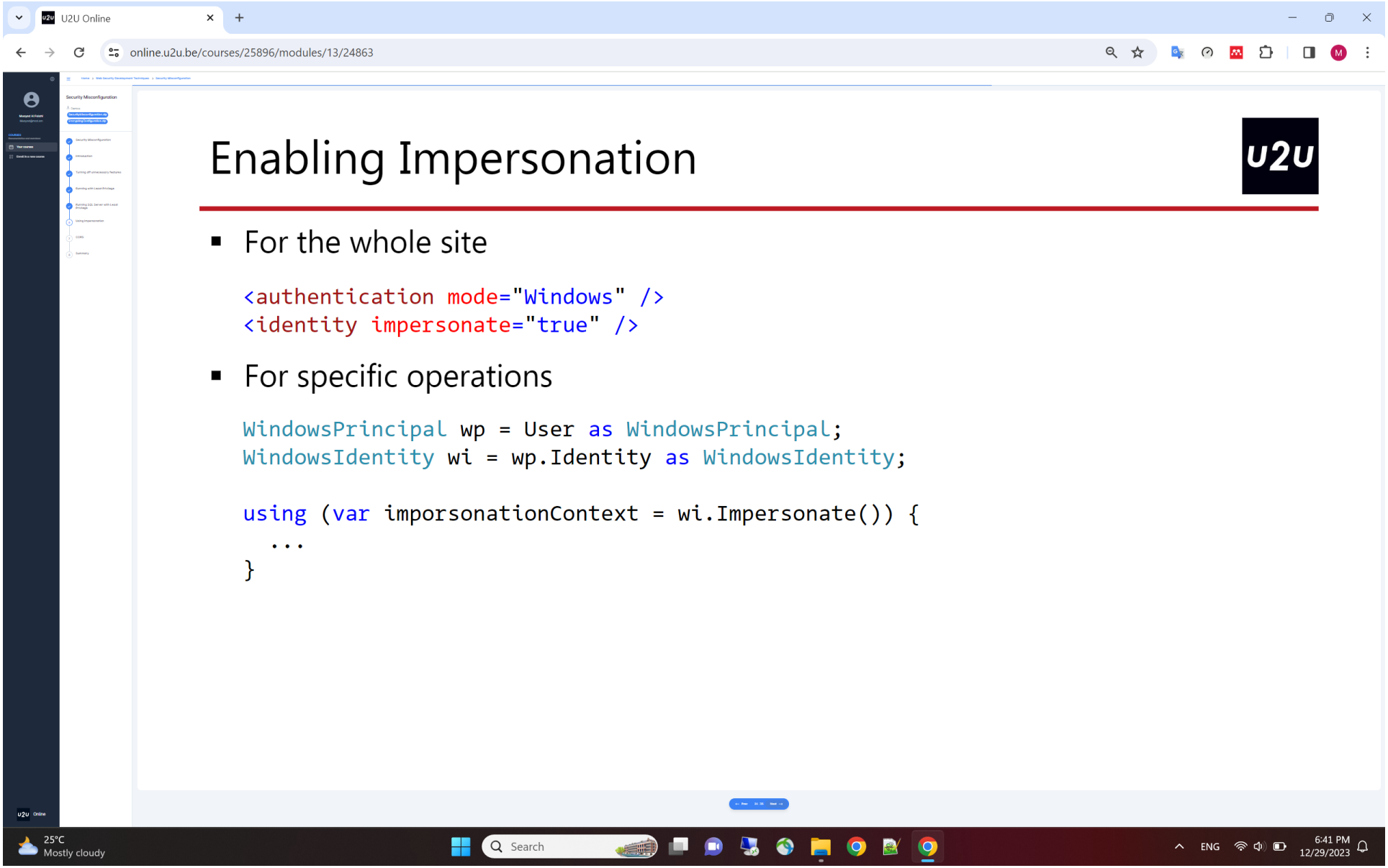
```
use [Northwind]
GO
GRANT SELECT ON [dbo].[Categories]
      TO [MyApp]
GO
use [Northwind]
GO
DENY ALTER ON [dbo].[Categories]
     TO [MyApp]
GO
```

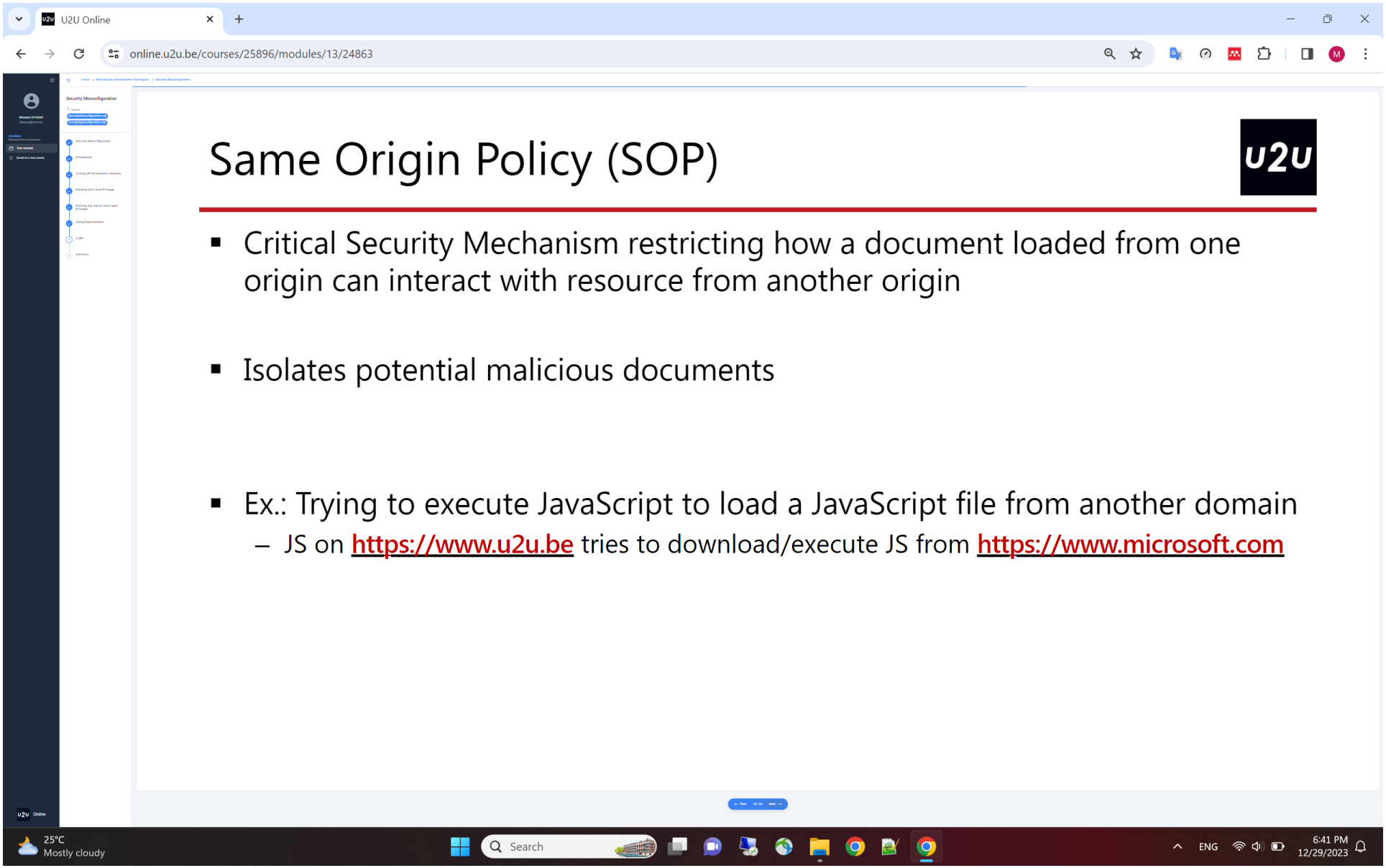


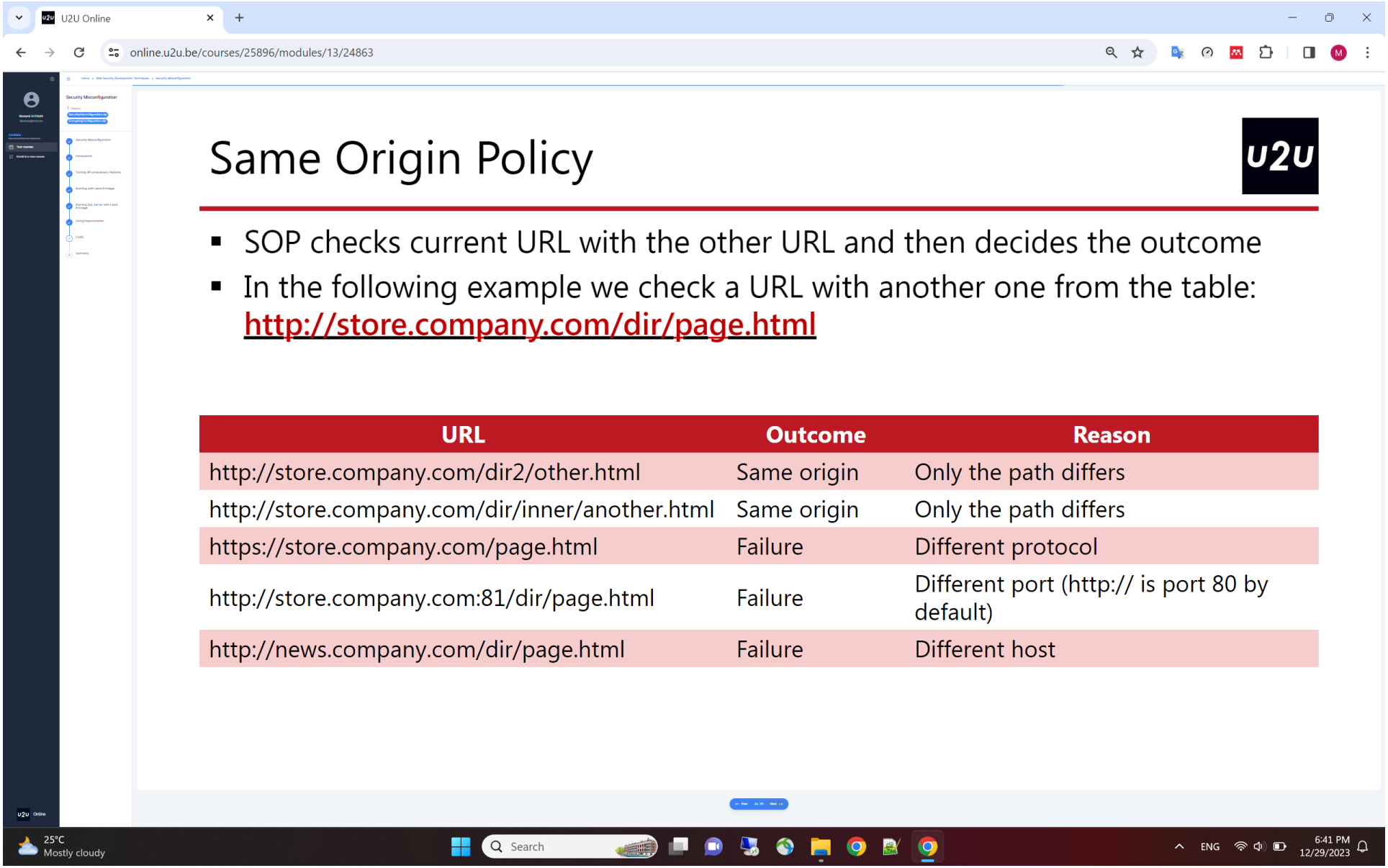

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Security Misconfiguration
Security Tip
u2u
Never give developers access to a table
Instead use a view
This way you can update the view to filter which data the application can see
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

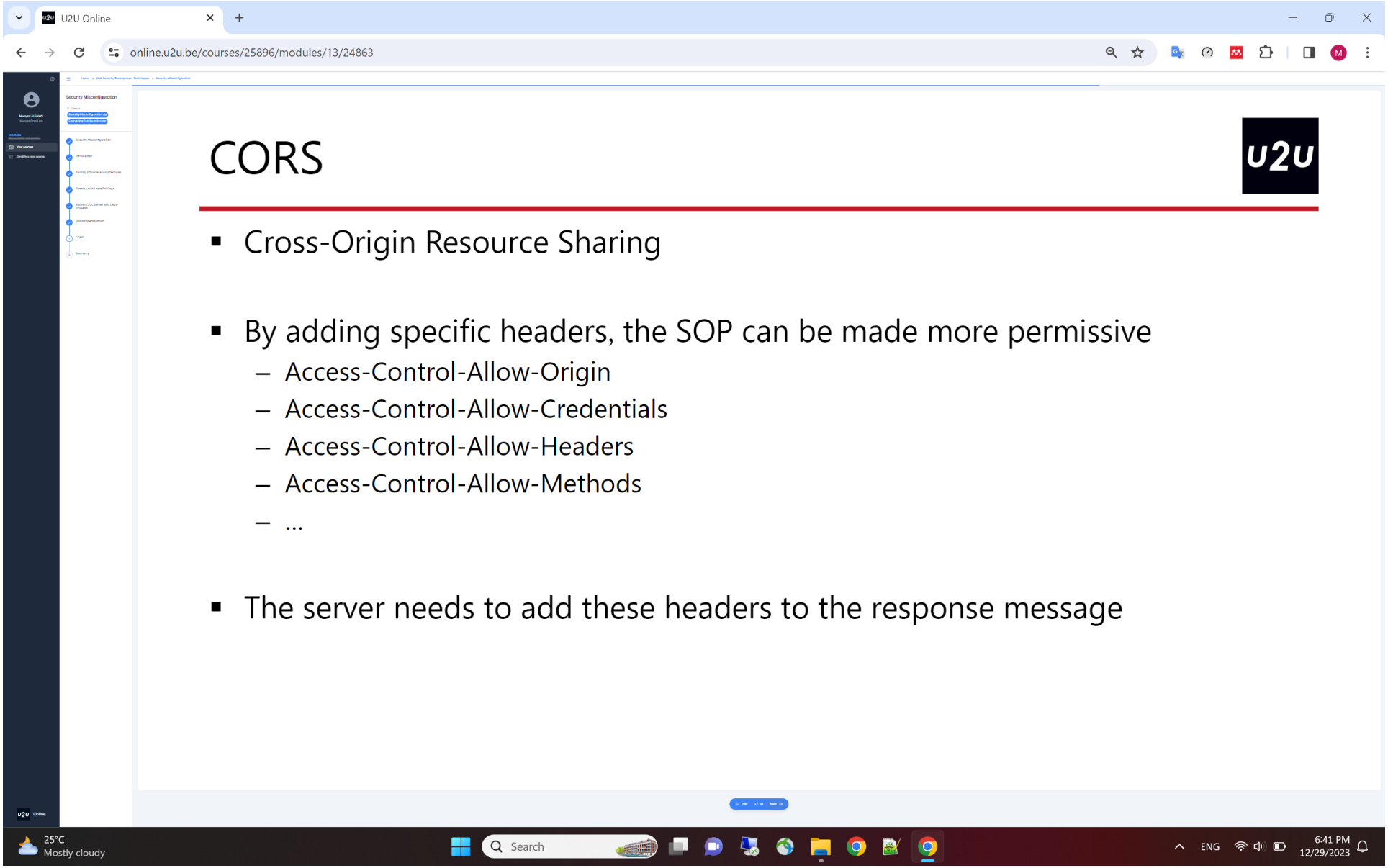

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Identity flow for internet web sites
U2U
trovi
Search
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

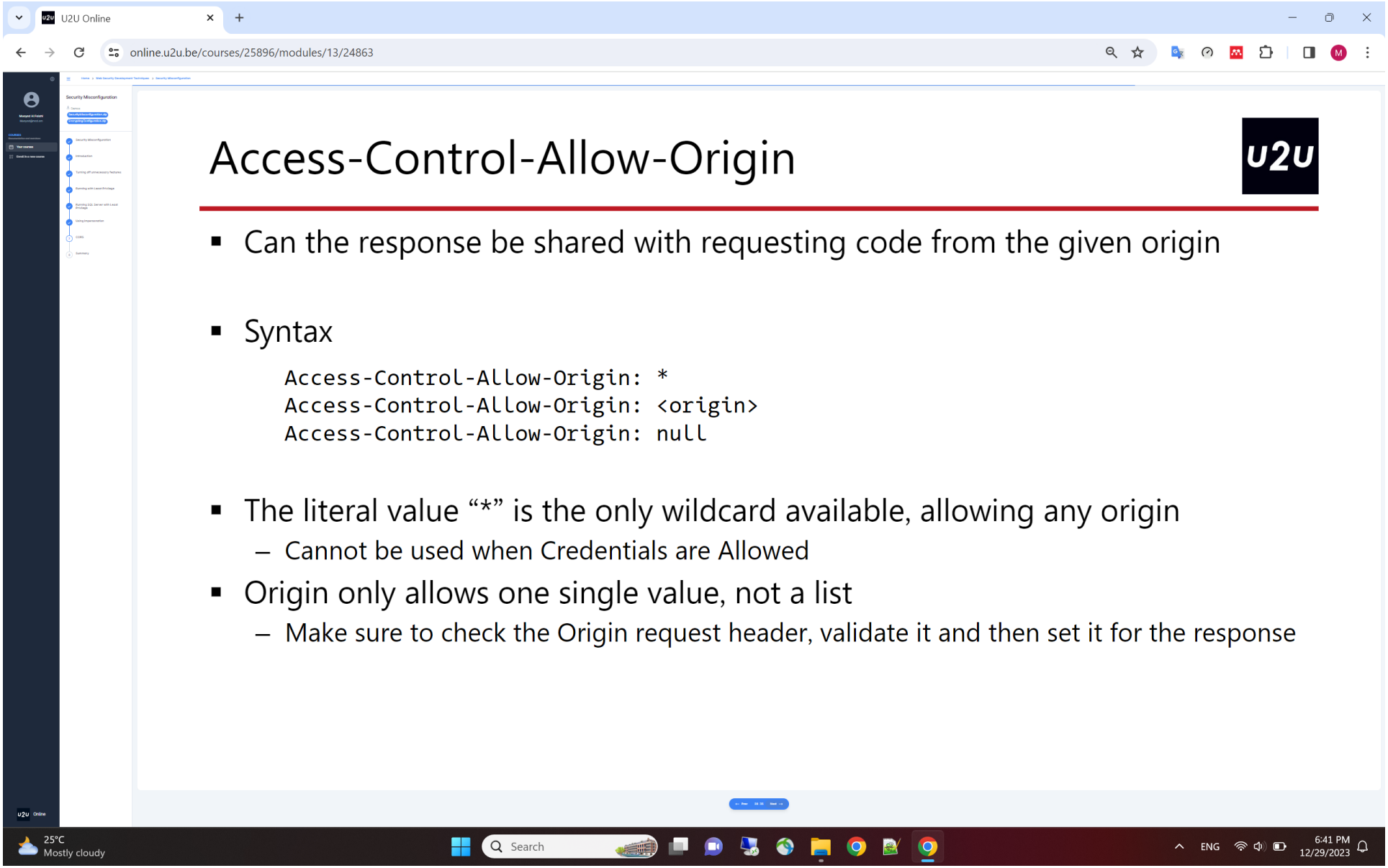

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Intranet: Using Impersonation
U2U
trovi
Search
trovi
Search
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

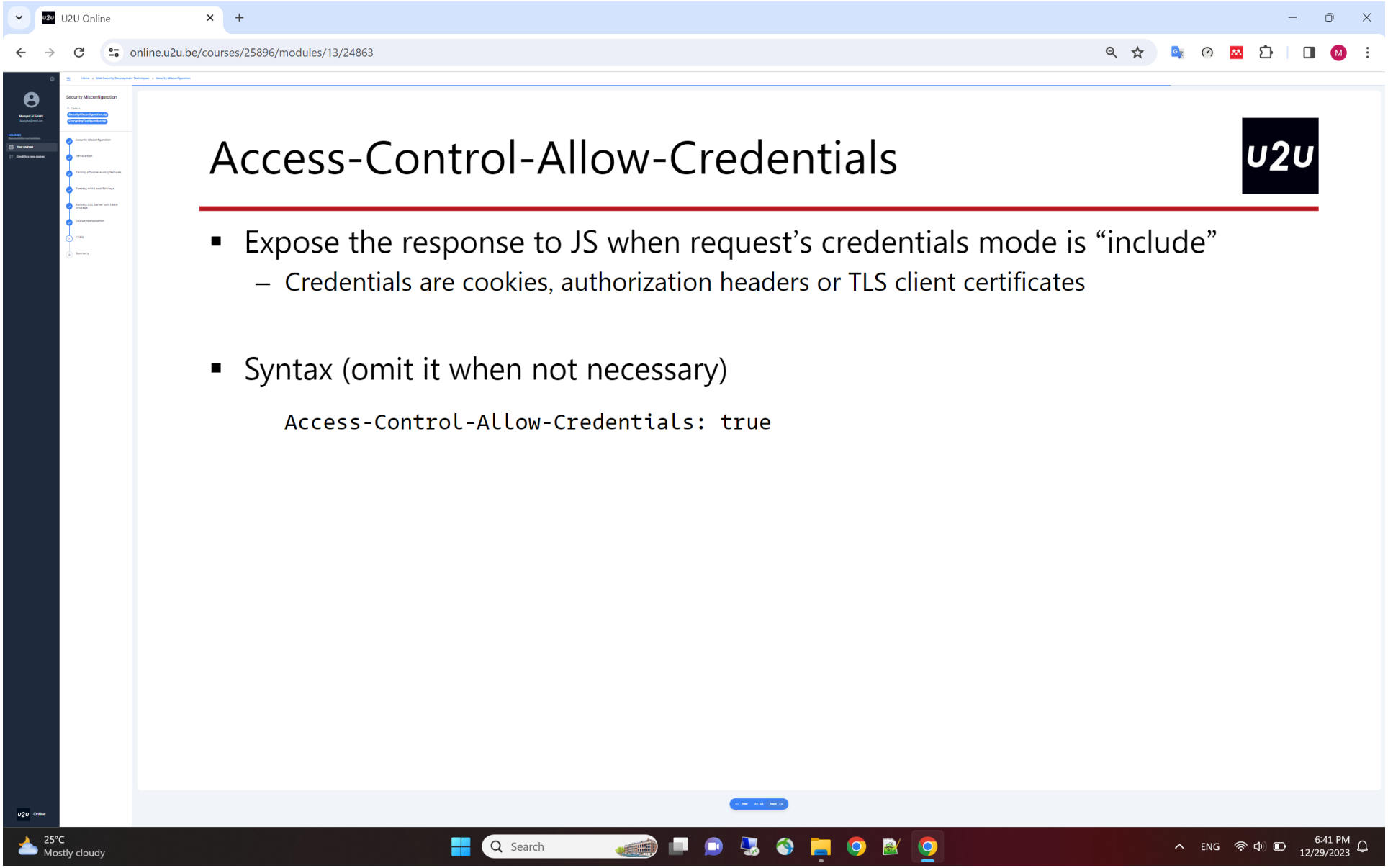

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Enabling Impersonation
U2U
For the whole site
<authentication mode="Windows" />
<identity impersonate="true" />
For specific operations
WindowsPrincipal wp = User as WindowsPrincipal;
WindowsIdentity wi = wp.Identity as WindowsIdentity;
using (var imporsonationContext = wi.Impersonate()) {
...
}
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

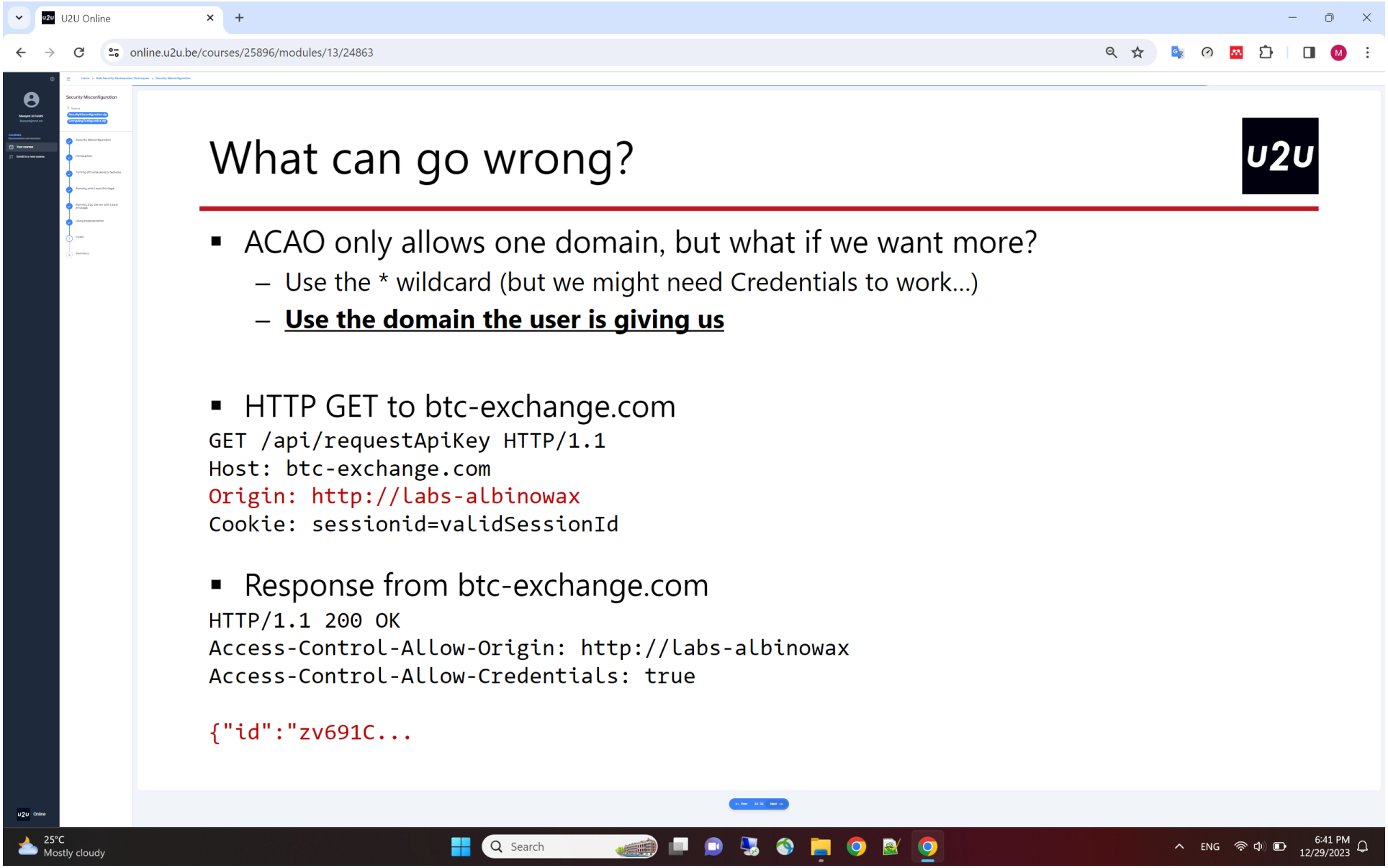

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Same Origin Policy (SOP)
u2u
Critical Security Mechanism restricting how a document loaded from one origin can interact with resource from another origin
Isolates potential malicious documents
Ex.: Trying to execute JavaScript to load a JavaScript file from another domain
JS on https://www.u2u.be tries to download/execute JS from https://www.microsoft.com
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

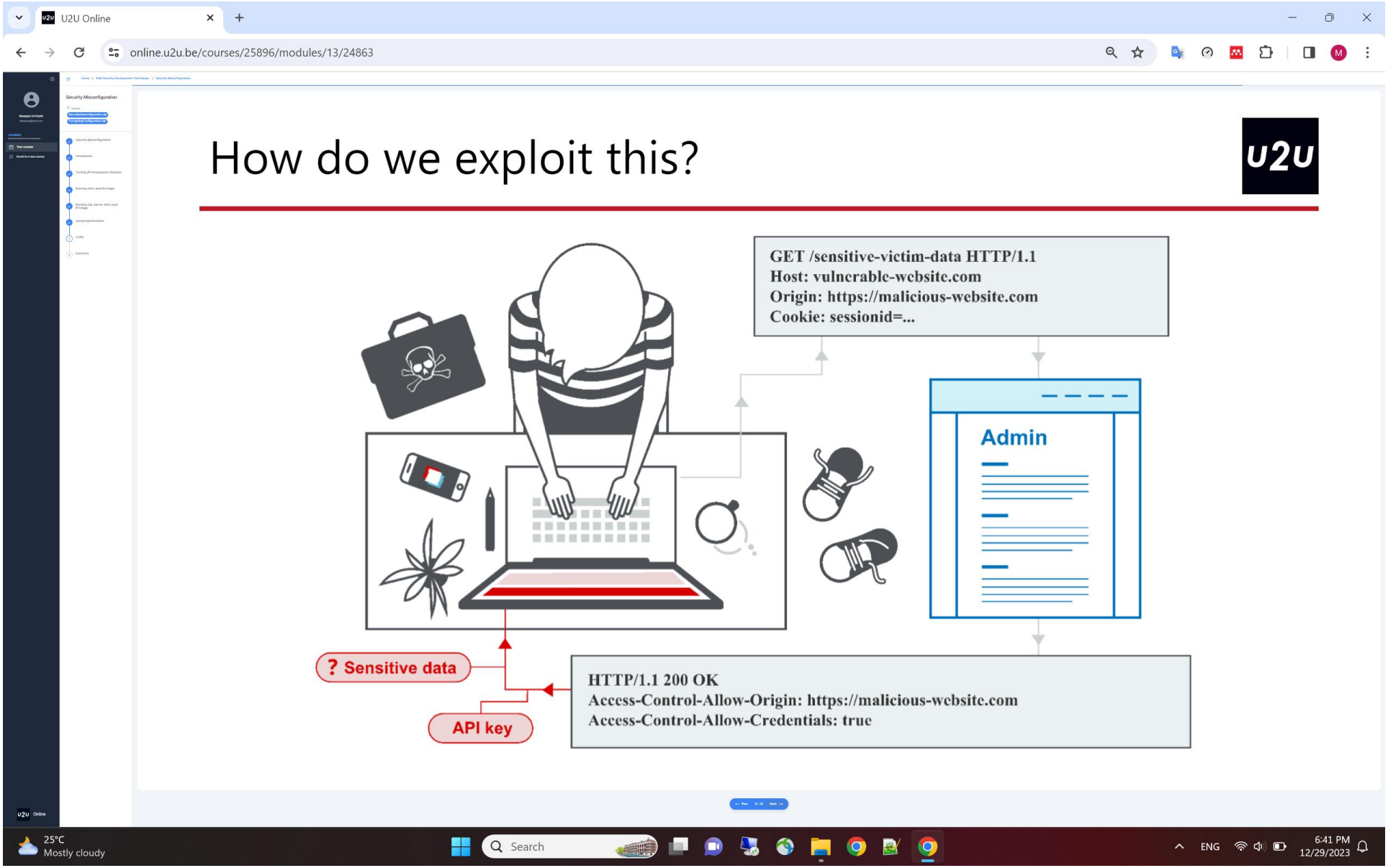

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Same Origin Policy
U2U
SOP checks current URL with the other URL and then decides the outcome
In the following example we check a URL with another one from the table: http://store.company.com/dir/page.html
URL
Outcome
Reason
http://store.company.com/dir2/other.html
Same origin
Only the path differs
http://store.company.com/dir/inner/another.html
Same origin
Only the path differs
https://store.company.com/page.html
Failure
Different protocol
http://store.company.com:81/dir/page.html
Failure
Different port (http:// is port 80 by default)
http://news.company.com/dir/page.html
Failure
Different host
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

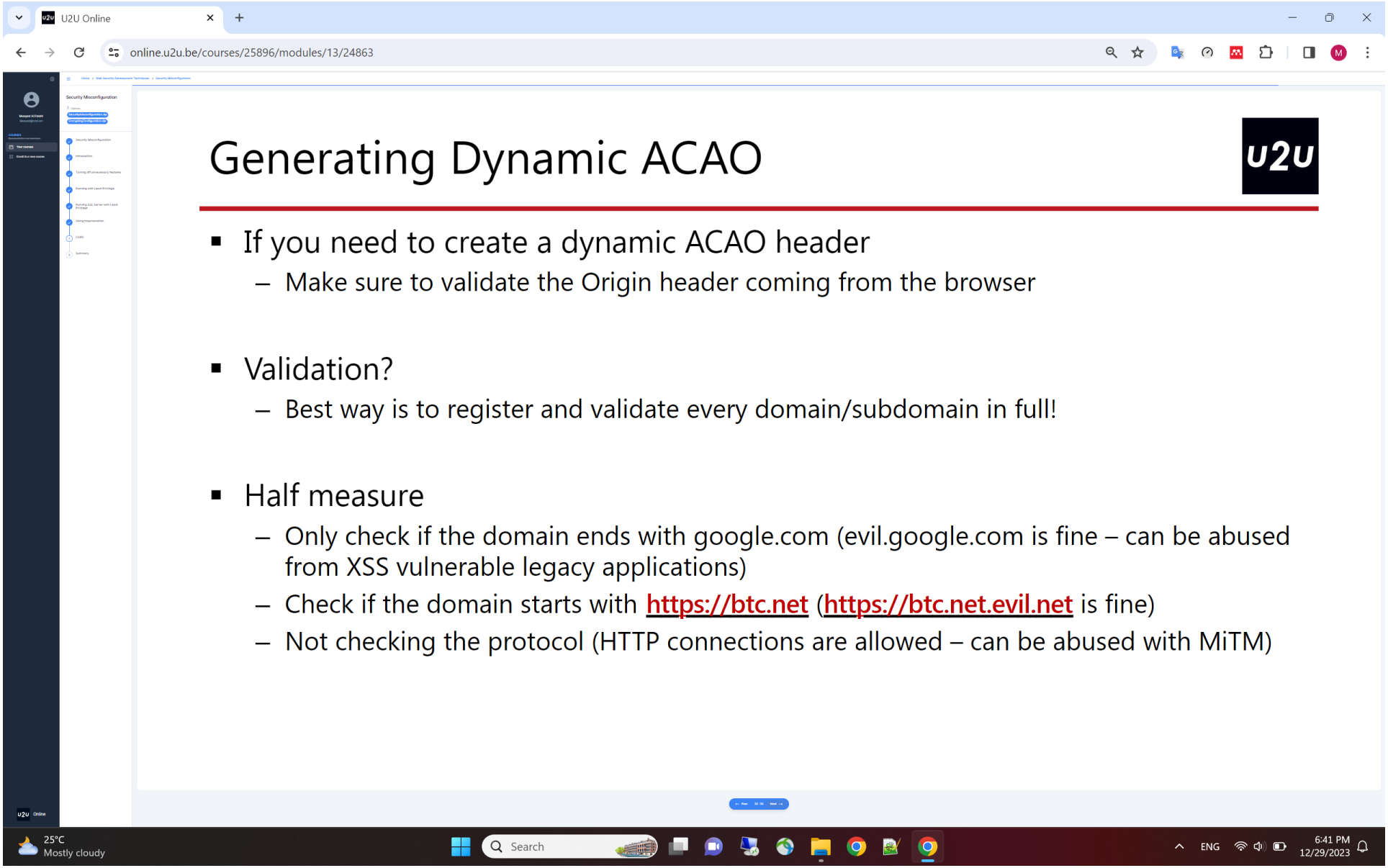

U2U Online
online.u2u.be/courses/25896/modules/13/24863
CORS
u2u
Cross-Origin Resource Sharing
By adding specific headers, the SOP can be made more permissive
Access-Control-Allow-Origin
Access-Control-Allow-Credentials
Access-Control-Allow-Headers
Access-Control-Allow-Methods
...
The server needs to add these headers to the response message
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

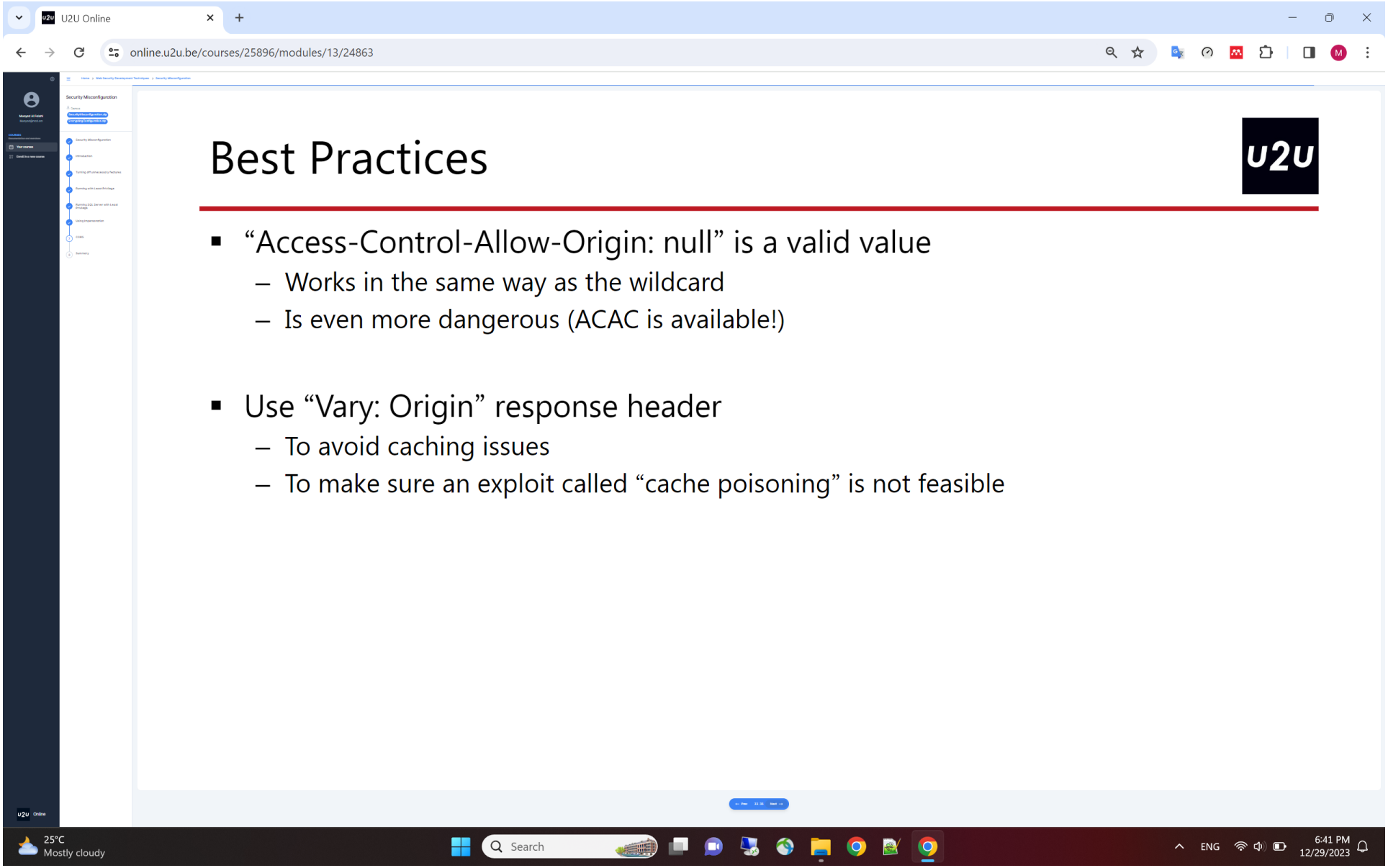

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Access-Control-Allow-Origin
U2U
Can the response be shared with requesting code from the given origin
Syntax
Access-Control-Allow-Origin: *
Access-Control-Allow-Origin: <origin>
Access-Control-Allow-Origin: null
The literal value "*" is the only wildcard available, allowing any origin
Cannot be used when Credentials are Allowed
Origin only allows one single value, not a list
Make sure to check the Origin request header, validate it and then set it for the response
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

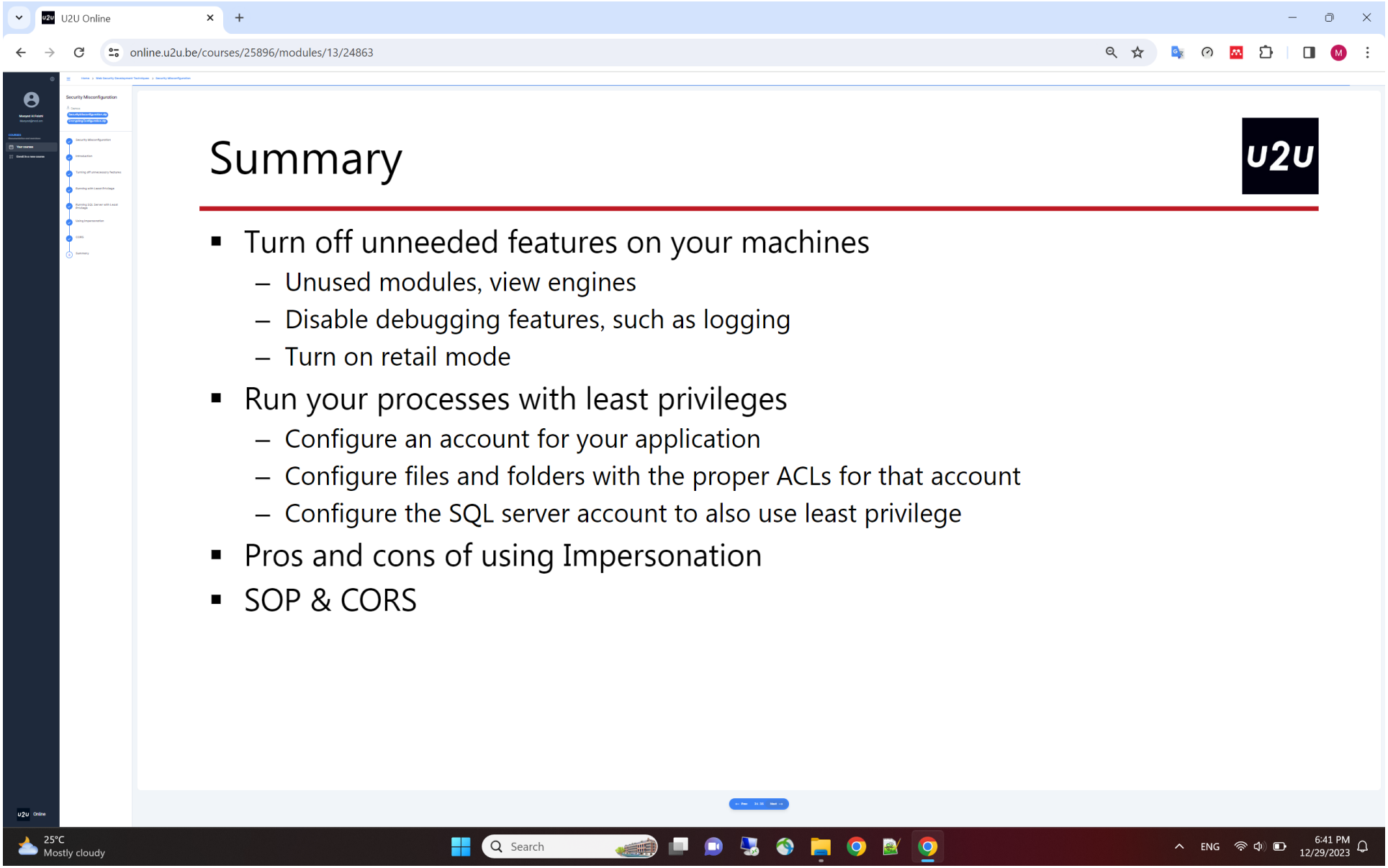

U2U Online
online.u2u.be/courses/25896/modules/13/24863
Access-Control-Allow-Credentials
U2U
Expose the response to JS when request's credentials mode is "include"
Credentials are cookies, authorization headers or TLS client certificates
Syntax (omit it when not necessary)
Access-Control-Allow-Credentials: true
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023

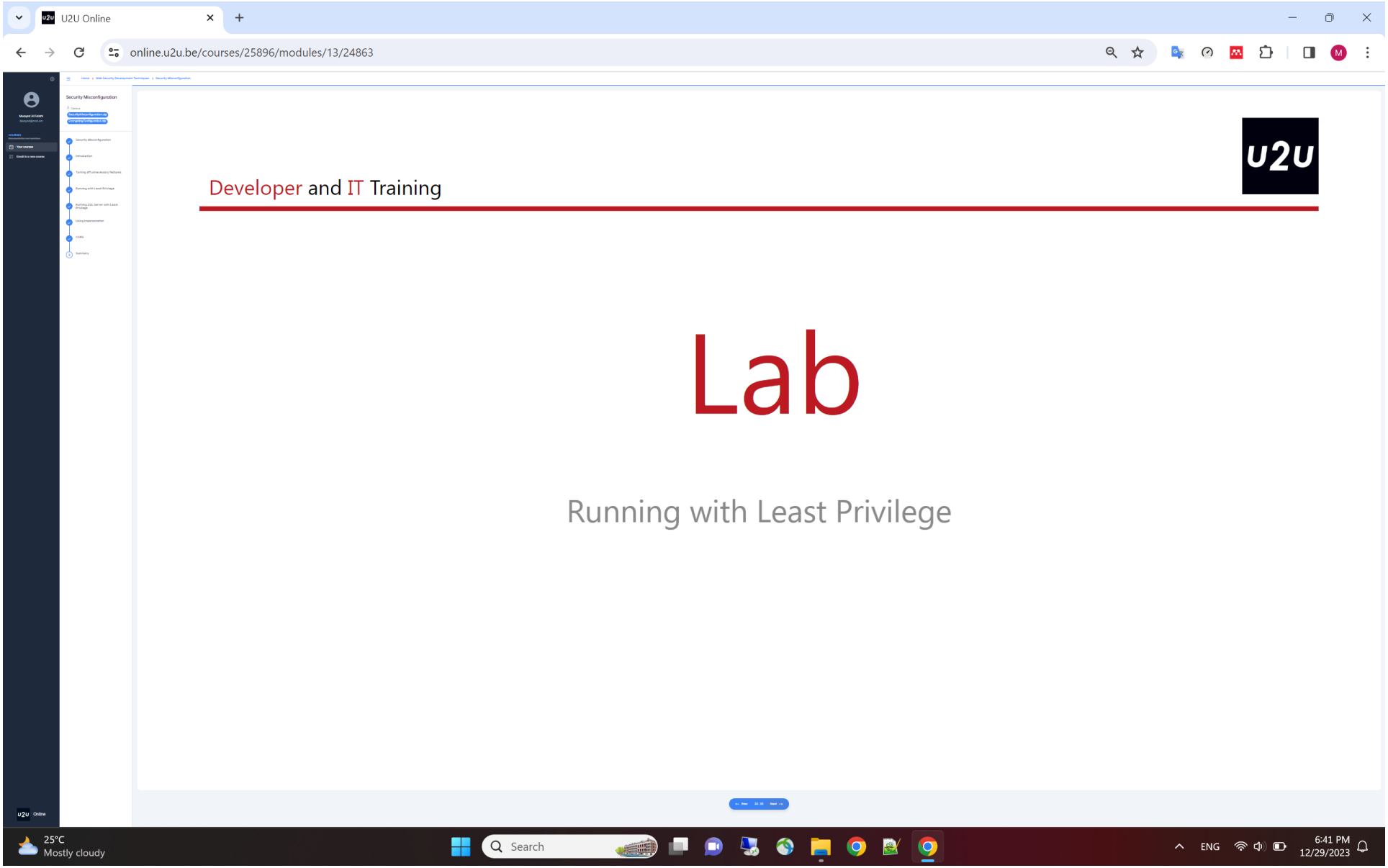

U2U Online
online.u2u.be/courses/25896/modules/13/24863
What can go wrong?
u2u
ACAO only allows one domain, but what if we want more?
Use the * wildcard (but we might need Credentials to work...)
Use the domain the user is giving us
HTTP GET to btc-exchange.com
GET /api/requestApiKey HTTP/1.1
Host: btc-exchange.com
Origin: http://labs-albinowax
Cookie: sessionid=validSessionId
Response from btc-exchange.com
HTTP/1.1 200 OK
Access-Control-Allow-Origin: http://labs-albinowax
Access-Control-Allow-Credentials: true
{"id":"zv691C...
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/13/24863
How do we exploit this?
u2u
GET /sensitive-victim-data HTTP/1.1
Host: vulnerable-website.com
Origin: https://malicious-website.com
Cookie: sessionid=...
Admin
? Sensitive data
API key
HTTP/1.1 200 OK
Access-Control-Allow-Origin: https://malicious-website.com
Access-Control-Allow-Credentials: true
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/13/24863
Generating Dynamic ACAO
u2u
If you need to create a dynamic ACAO header
Make sure to validate the Origin header coming from the browser
Validation?
Best way is to register and validate every domain/subdomain in full!
Half measure
Only check if the domain ends with google.com (evil.google.com is fine – can be abused from XSS vulnerable legacy applications)
Check if the domain starts with https://btc.net (https://btc.net.evil.net is fine)
Not checking the protocol (HTTP connections are allowed – can be abused with MiTM)
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/13/24863
Best Practices
u2u
“Access-Control-Allow-Origin: null” is a valid value
Works in the same way as the wildcard
Is even more dangerous (ACAC is available!)
Use “Vary: Origin” response header
To avoid caching issues
To make sure an exploit called “cache poisoning” is not feasible
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/13/24863
Summary
U2U
Turn off unneeded features on your machines
Unused modules, view engines
Disable debugging features, such as logging
Turn on retail mode
Run your processes with least privileges
Configure an account for your application
Configure files and folders with the proper ACLs for that account
Configure the SQL server account to also use least privilege
Pros and cons of using Impersonation
SOP & CORS
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/13/24863
Developer and IT Training
U2U
Lab
Running with Least Privilege
25°C
Mostly cloudy
Search
ENG
6:41 PM
12/29/2023