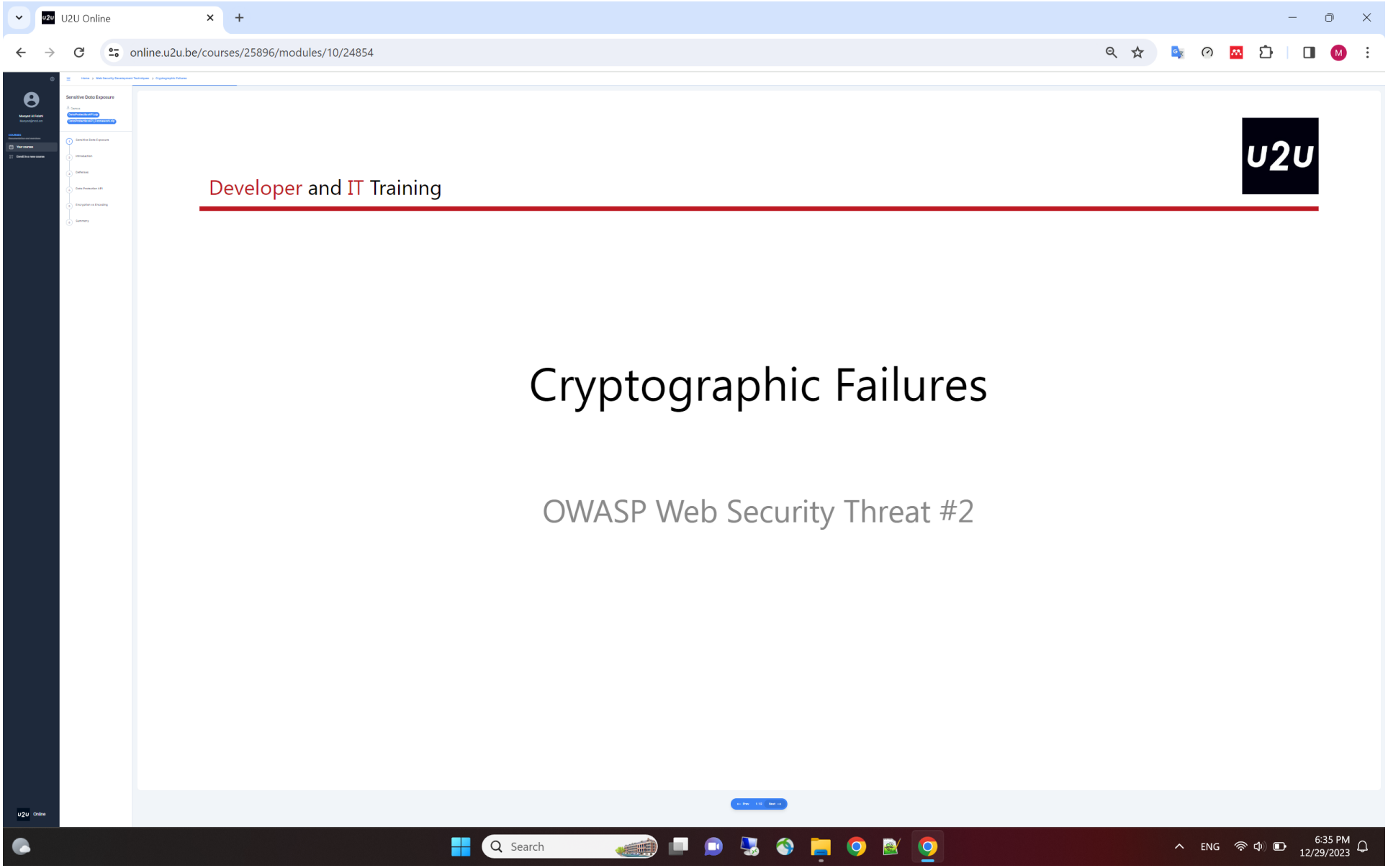
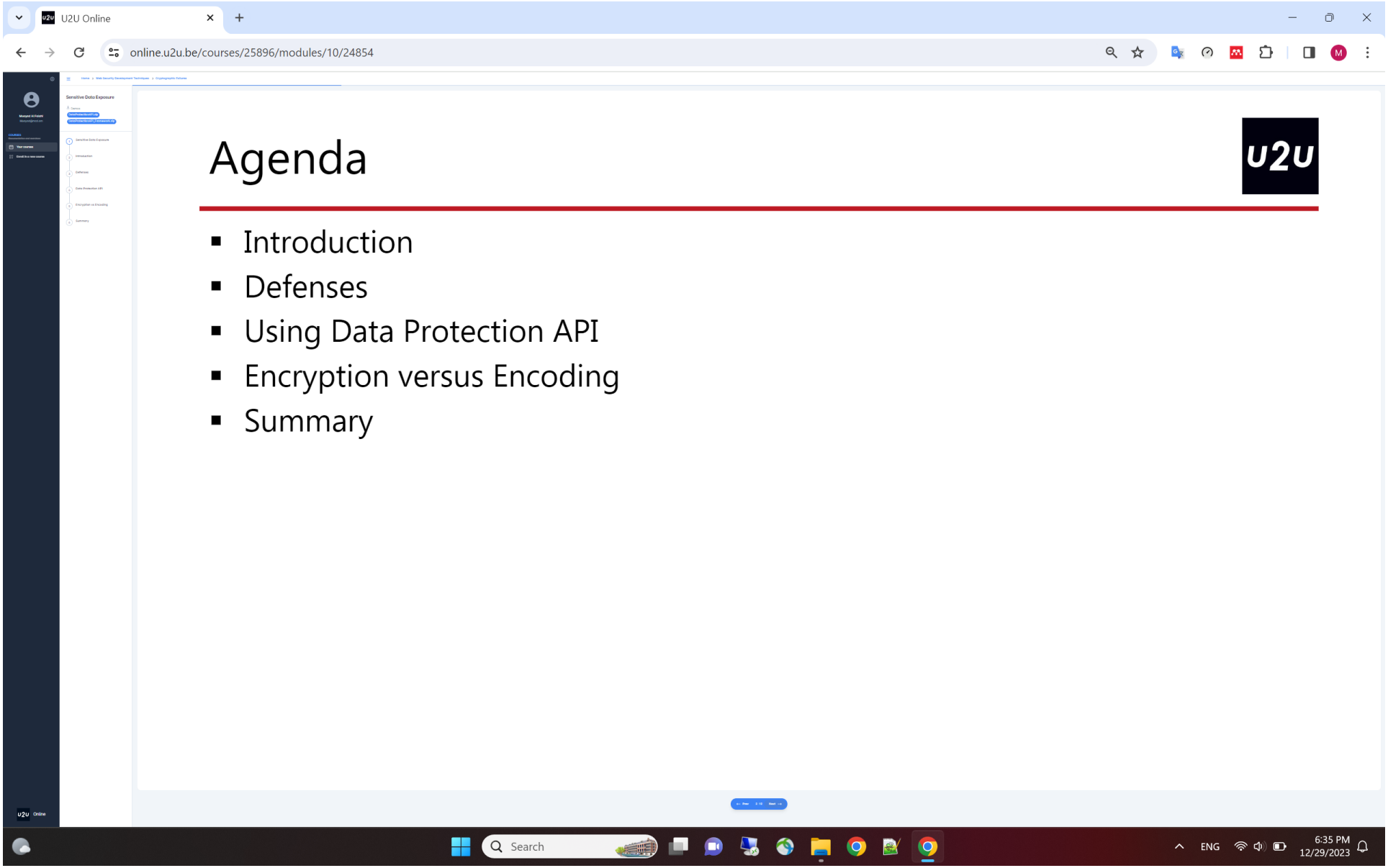
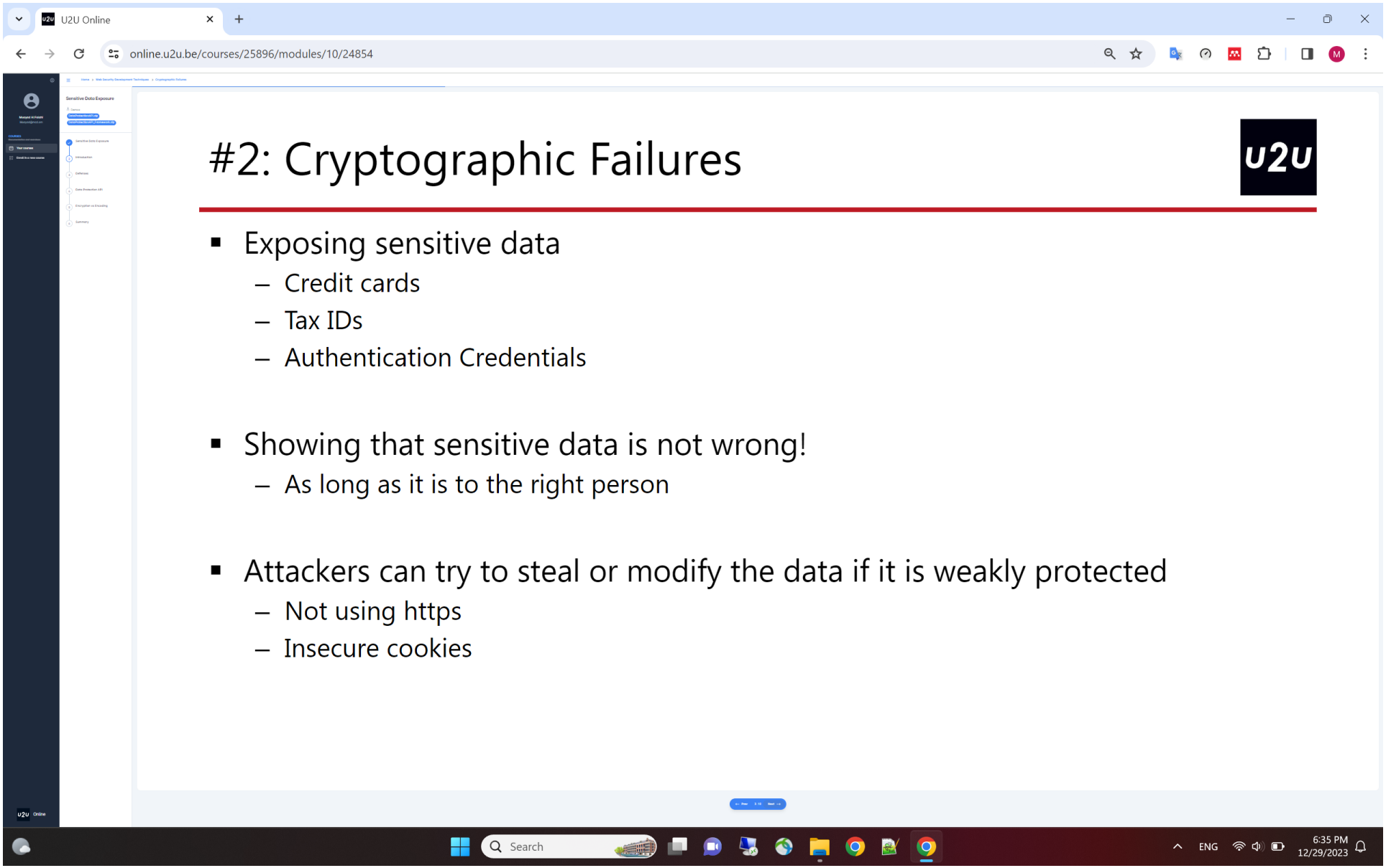
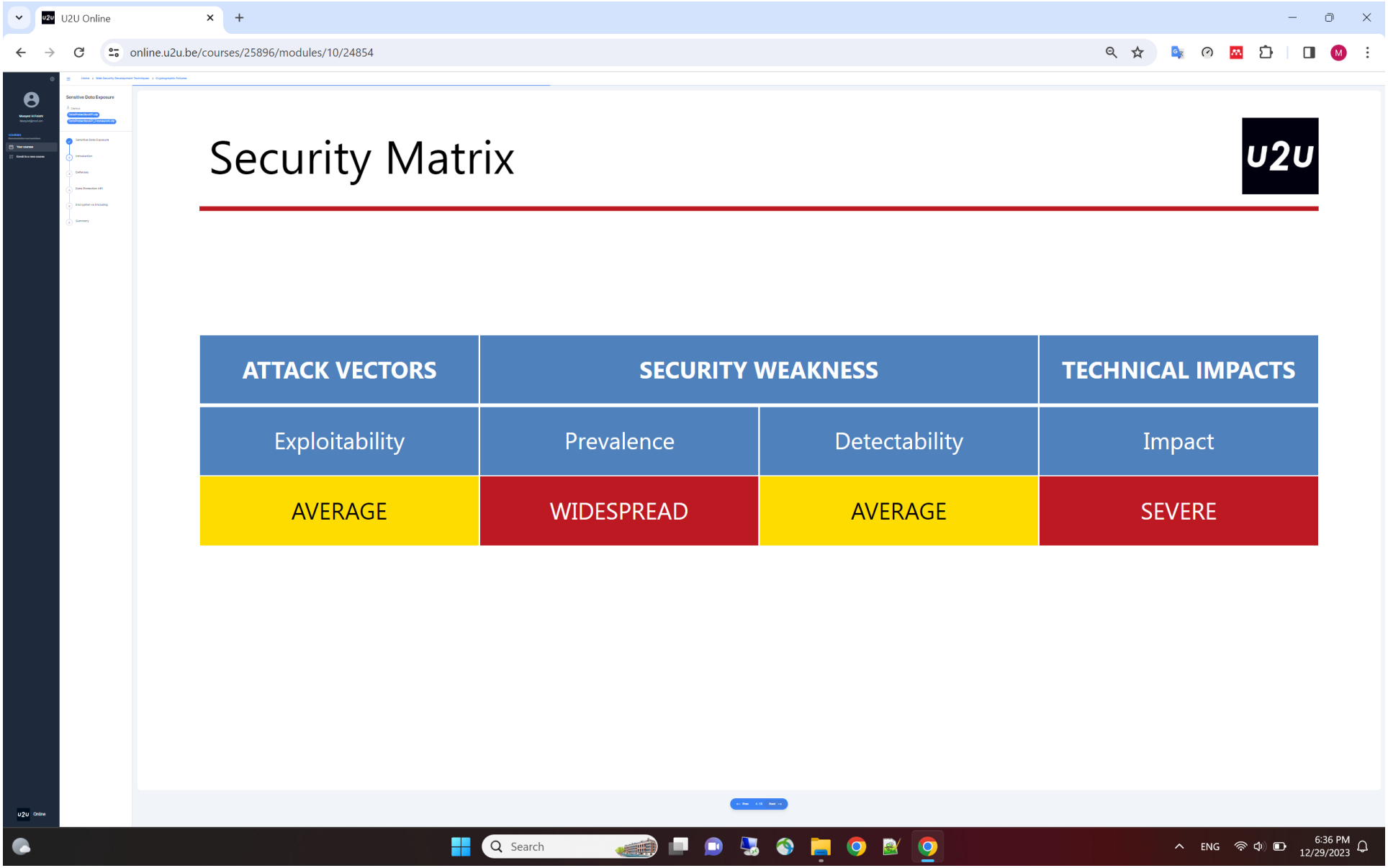
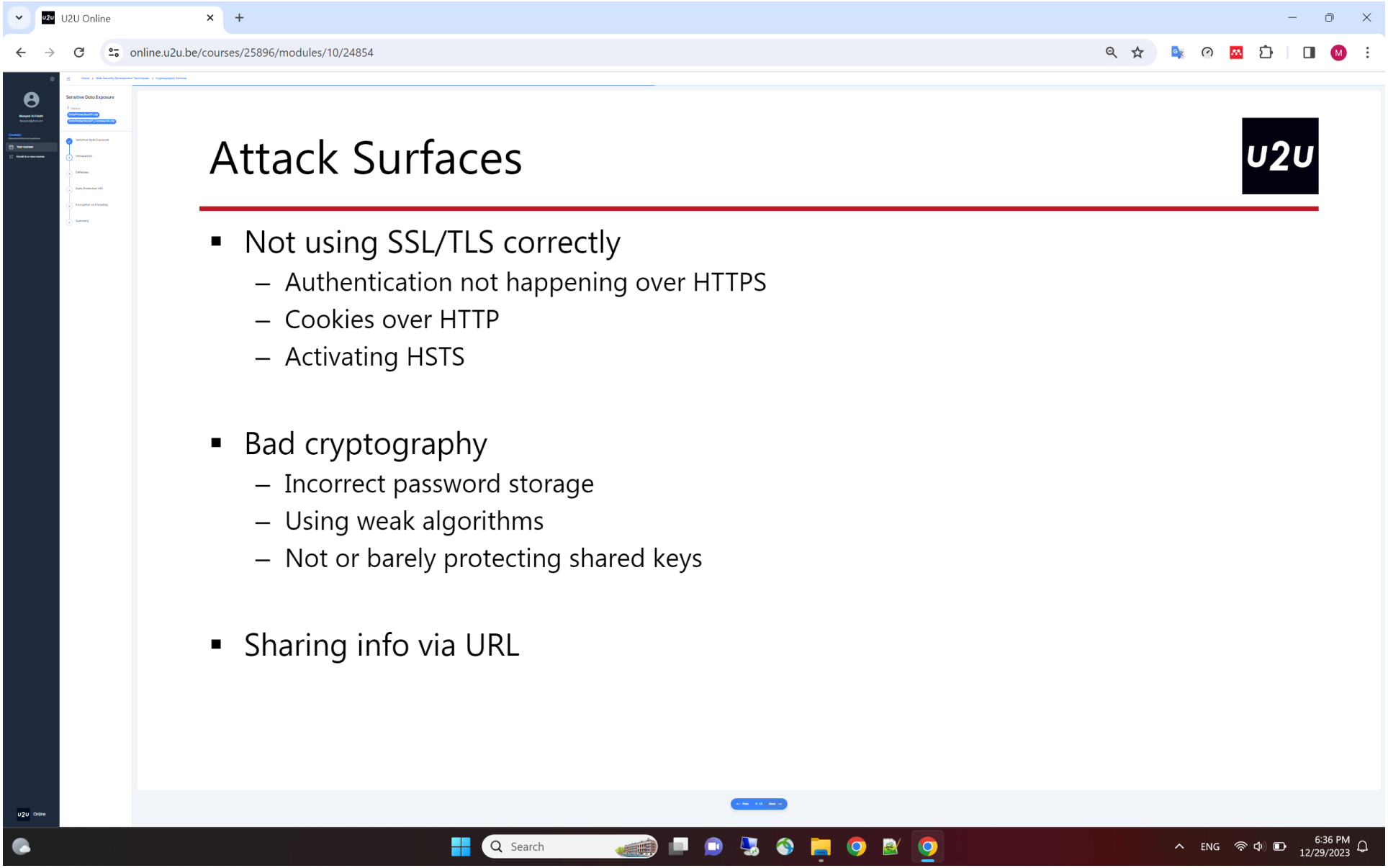

U2U Online
online.u2u.be/courses/25896/modules/10/24854
Developer and IT Training
u2u
Cryptographic Failures
OWASP Web Security Threat #2
Search
ENG
6:35 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/10/24854
Agenda
u2u
Introduction
Defenses
Using Data Protection API
Encryption versus Encoding
Summary
Search
ENG
6:35 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/10/24854
#2: Cryptographic Failures
U2U
Exposing sensitive data
Credit cards
Tax IDs
Authentication Credentials
Showing that sensitive data is not wrong!
As long as it is to the right person
Attackers can try to steal or modify the data if it is weakly protected
Not using https
Insecure cookies
Search
ENG
6:35 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/10/24854
Security Matrix
u2u
ATTACK VECTORS
SECURITY WEAKNESS
TECHNICAL IMPACTS
Exploitability
Prevalence
Detectability
Impact
AVERAGE
WIDESPREAD
AVERAGE
SEVERE
Search
ENG
6:36 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/10/24854
Attack Surfaces
U2U
Not using SSL/TLS correctly
Authentication not happening over HTTPS
Cookies over HTTP
Activating HSTS
Bad cryptography
Incorrect password storage
Using weak algorithms
Not or barely protecting shared keys
Sharing info via URL
Search
ENG
6:36 PM
12/29/2023

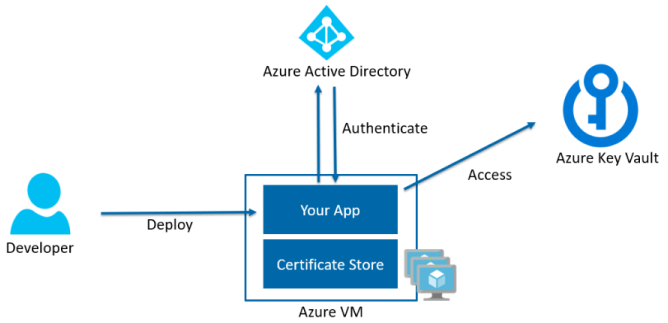
Defenses

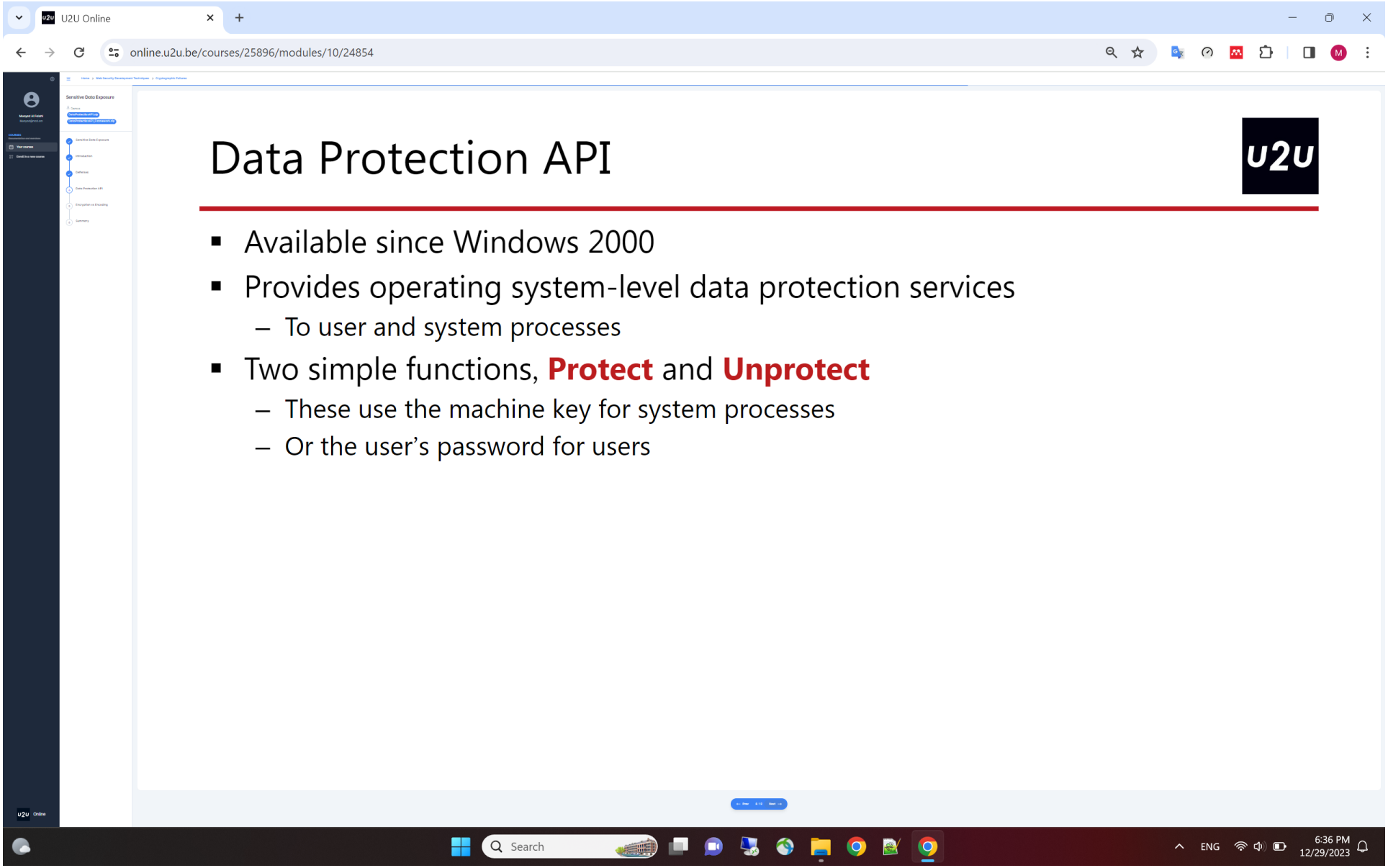
- Don’t collect all that sensitive data
  - You can’t lose what you don’t have!
  - Or only store the hash (with salt!)
- Store secrets in encrypted storage
  - Enable SQL Server Encryption
    - Transparent Data Encryption
    - In combination with extra encryption techniques!
- HTTPS everywhere
  - Not a performance problem any longer!
- Use correct cryptography

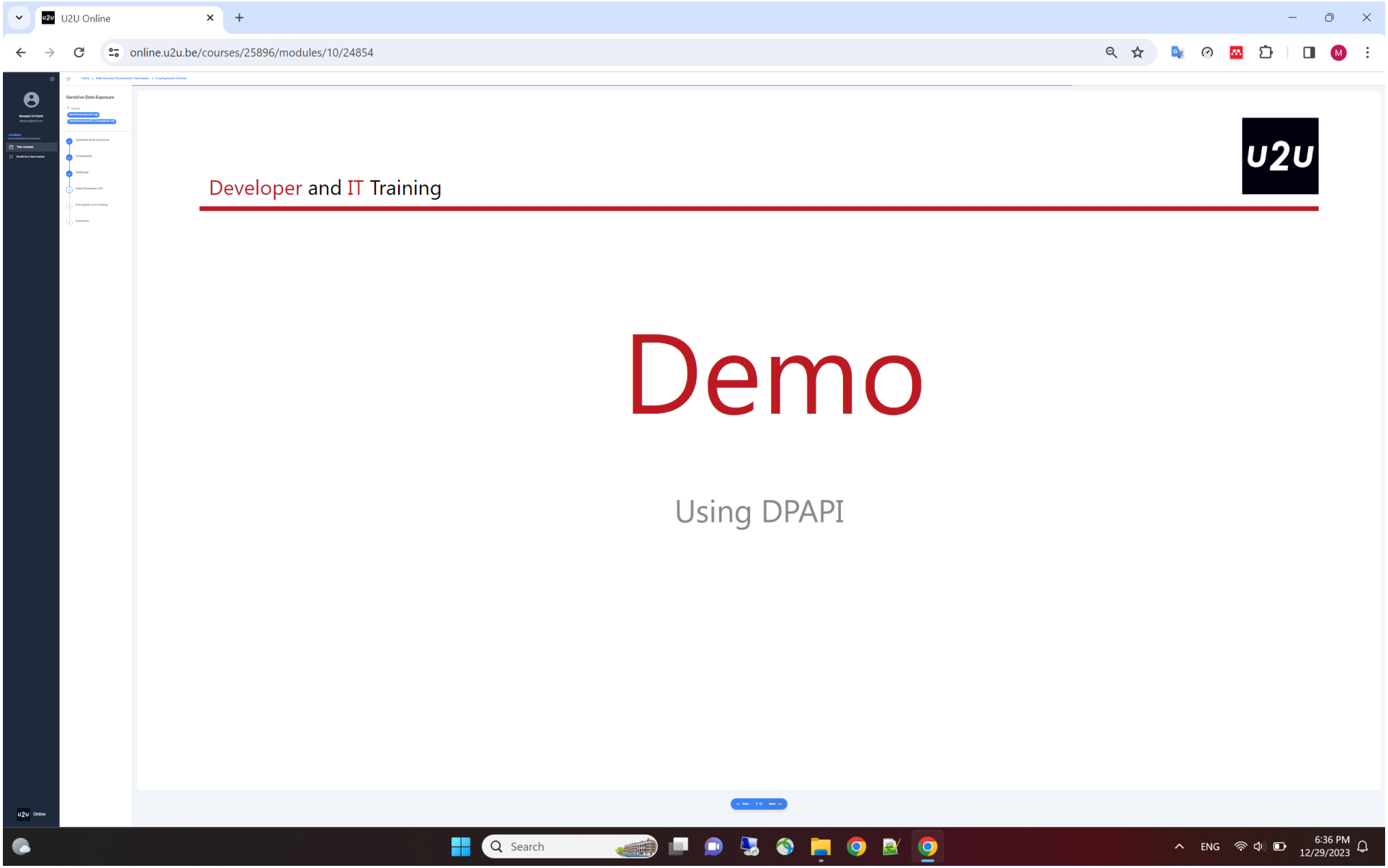
Where to Store Secrets

- Secrets like
  - Some App settings
  - Connection strings
  - Passwords
  - Keys
  - Certificates

- Store them in Azure Key Vault
  - Applications don't store keys directly
  - Automate tasks for certificates (e.g. renewal)
  - Monitor and audit key usage
  - Scales to meet the demands of your apps




U2U Online
online.u2u.be/courses/25896/modules/10/24854
Data Protection API
u2u
Available since Windows 2000
Provides operating system-level data protection services
To user and system processes
Two simple functions, Protect and Unprotect
These use the machine key for system processes
Or the user's password for users
Search
ENG
6:36 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/10/24854
Developer and IT Training
u2u
Demo
Using DPAPI
Search
ENG
6:36 PM
12/29/2023

U2U Online

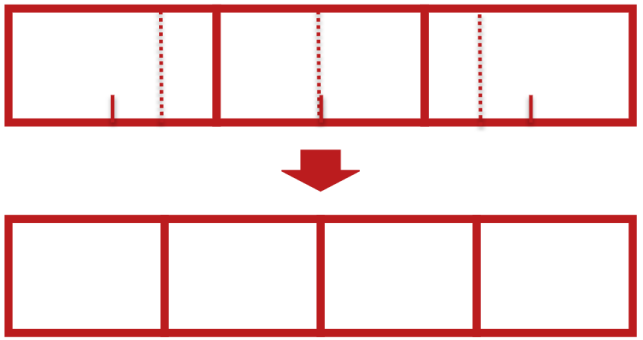
online.u2u.be/courses/25896/modules/10/24854

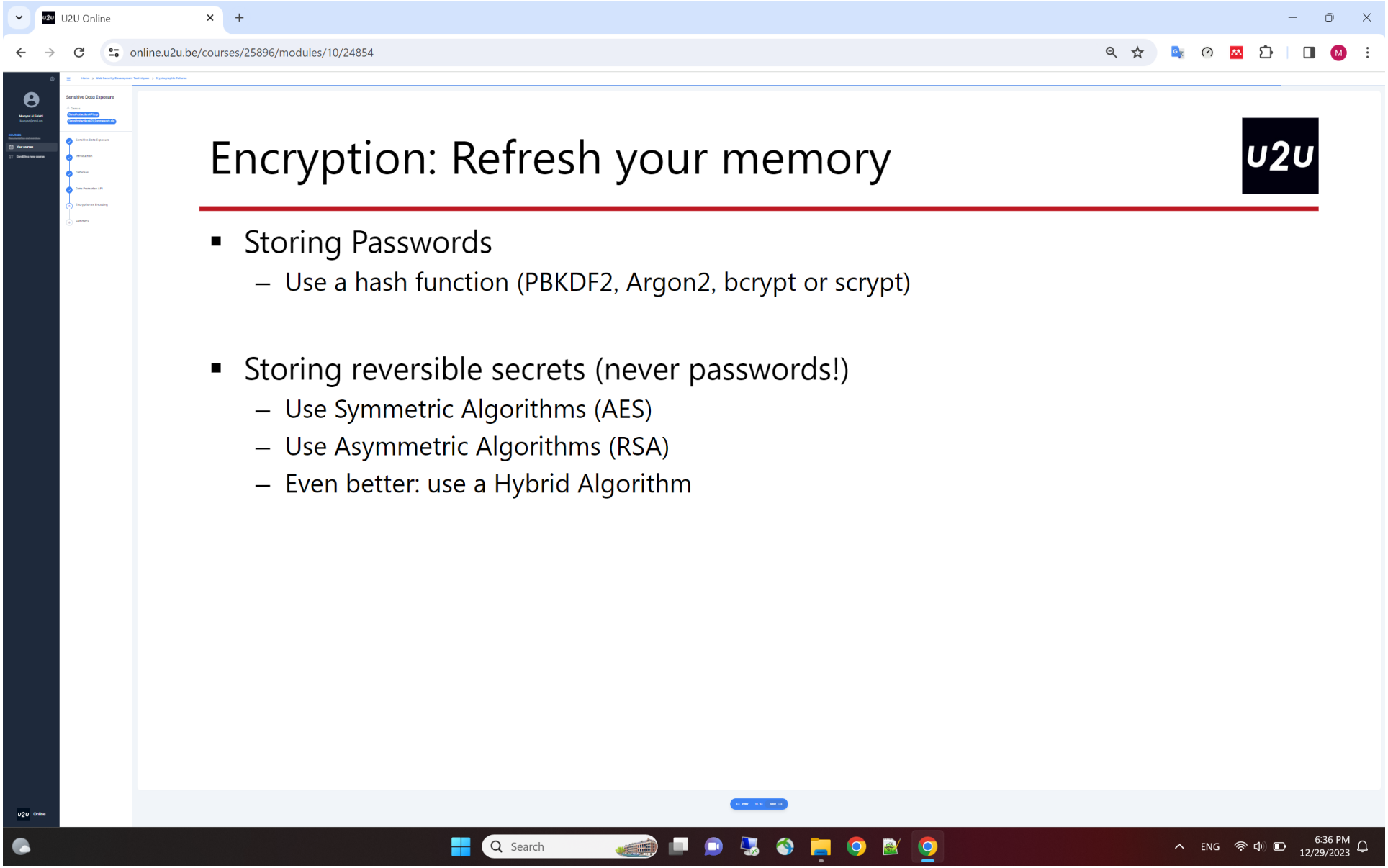
Encryption vs. Encoding

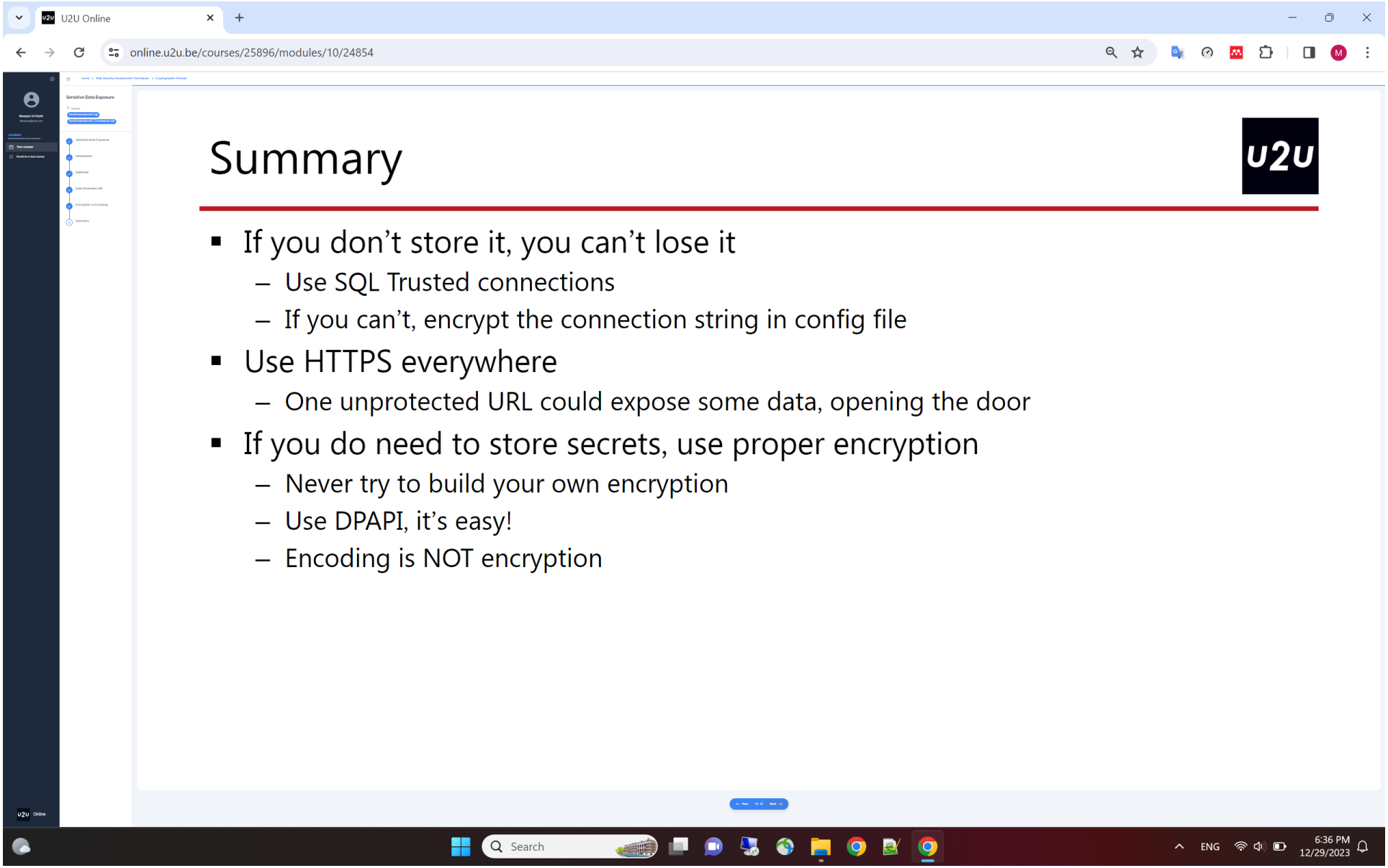
- Encoding != Encryption
- Encryption example: AES

```
Text: Hello @ U2U!          secret key: P@$$w0rd
                    ↓
                0SW%?6G
```

- Encoding example: Base64




U2U Online
online.u2u.be/courses/25896/modules/10/24854
Encryption: Refresh your memory
U2U
Storing Passwords
Use a hash function (PBKDF2, Argon2, bcrypt or scrypt)
Storing reversible secrets (never passwords!)
Use Symmetric Algorithms (AES)
Use Asymmetric Algorithms (RSA)
Even better: use a Hybrid Algorithm
Search
ENG
6:36 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/10/24854
Summary
U2U
If you don't store it, you can't lose it
Use SQL Trusted connections
If you can't, encrypt the connection string in config file
Use HTTPS everywhere
One unprotected URL could expose some data, opening the door
If you do need to store secrets, use proper encryption
Never try to build your own encryption
Use DPAPI, it's easy!
Encoding is NOT encryption
Search
ENG
6:36 PM
12/29/2023