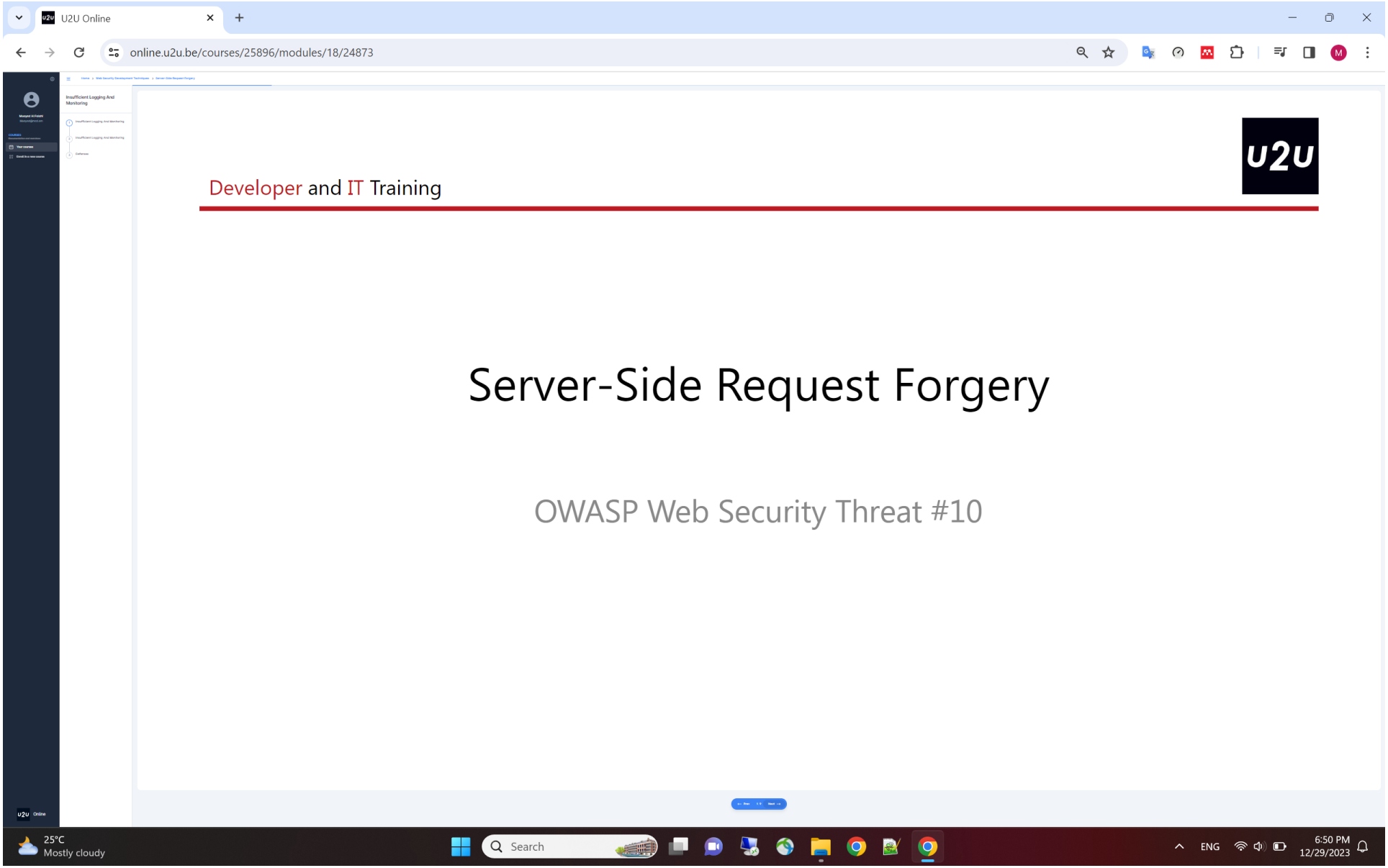
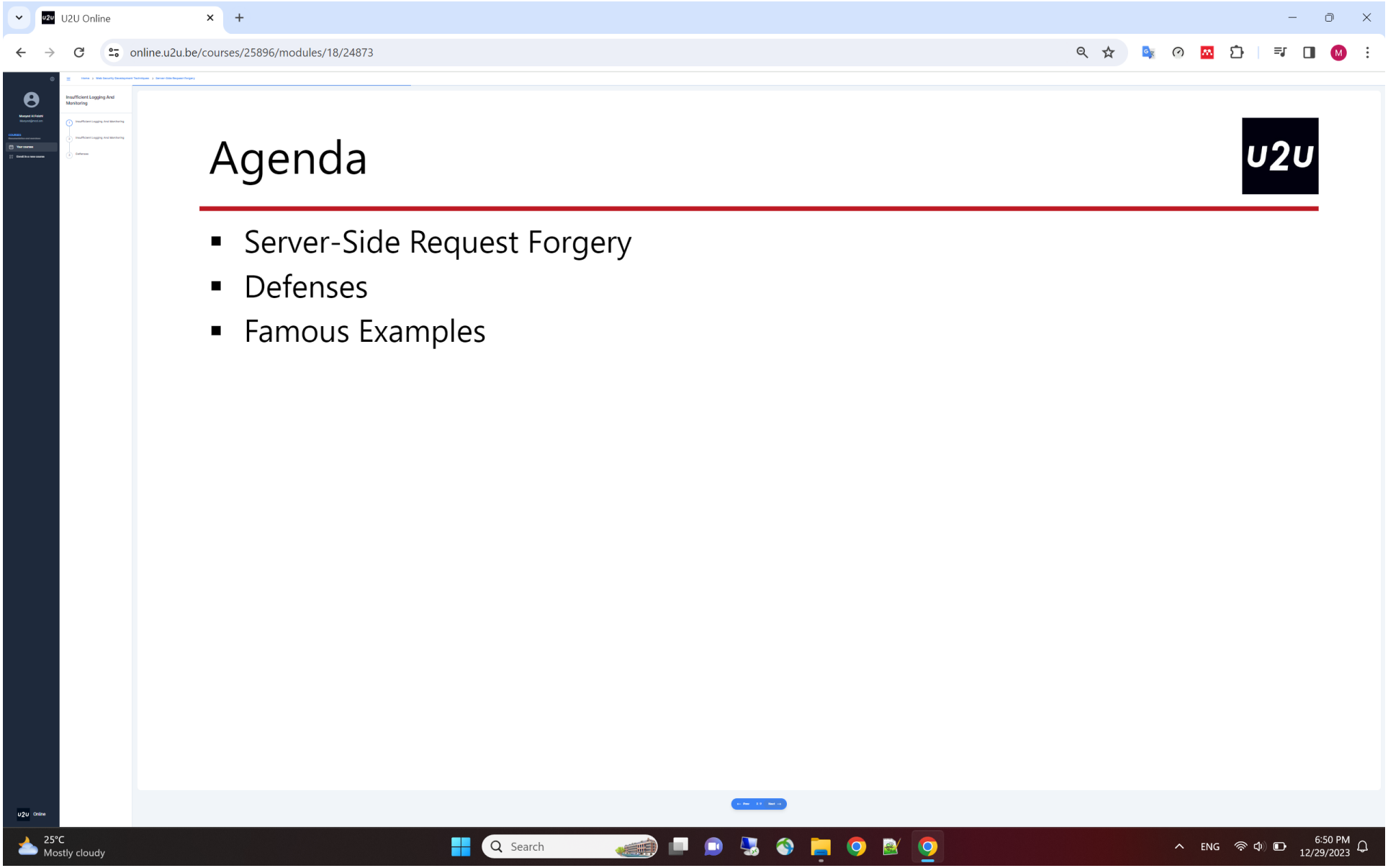
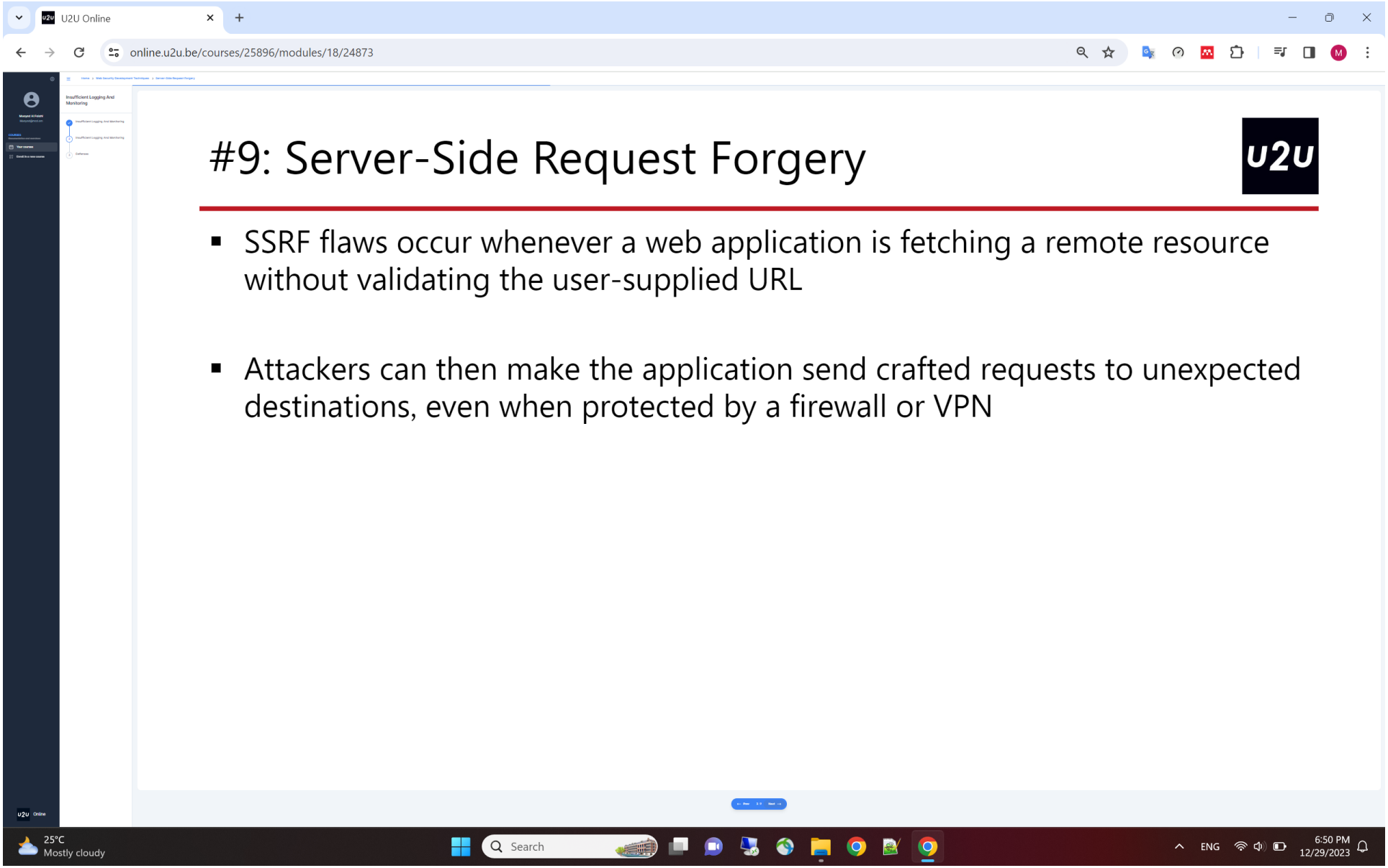
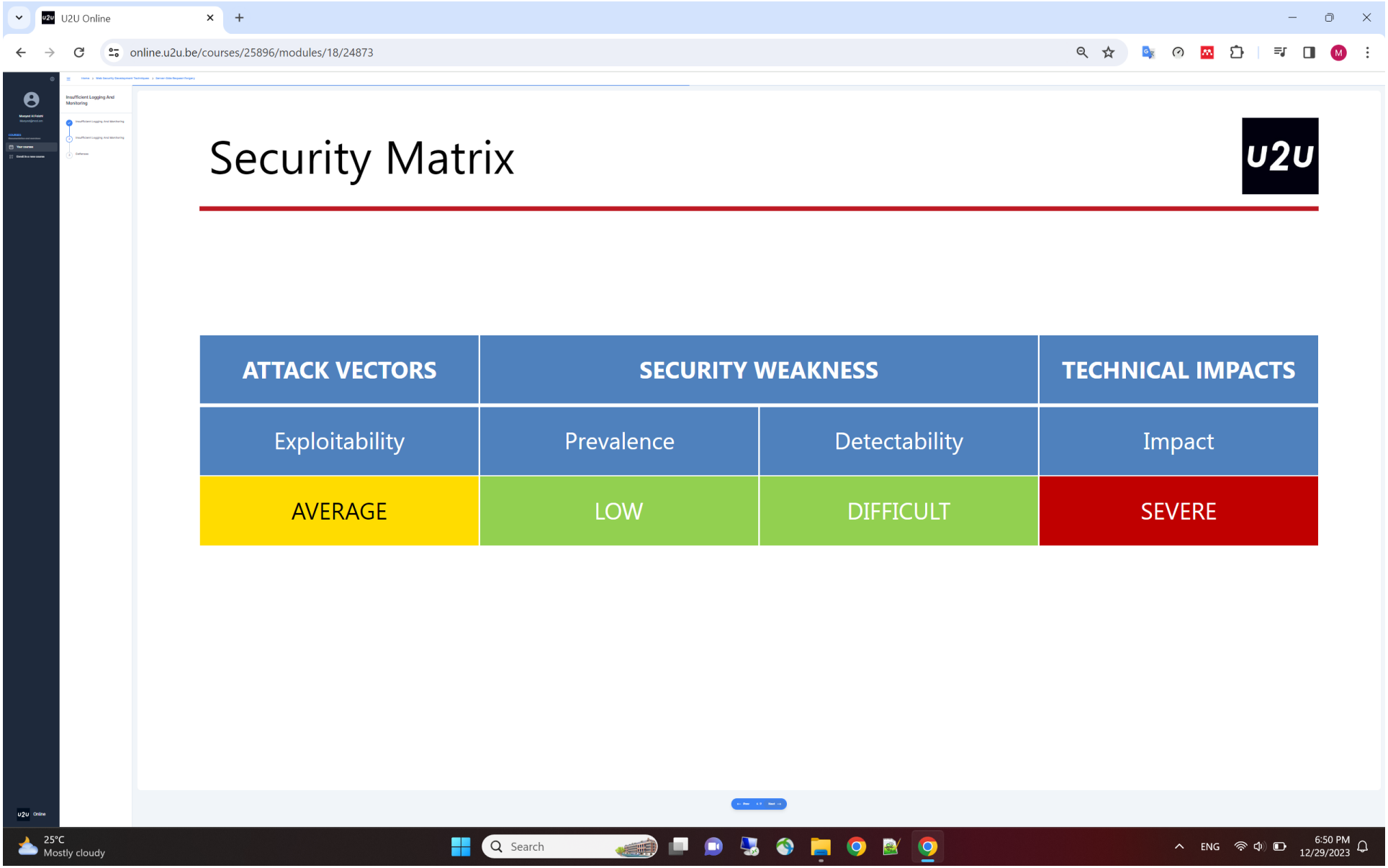
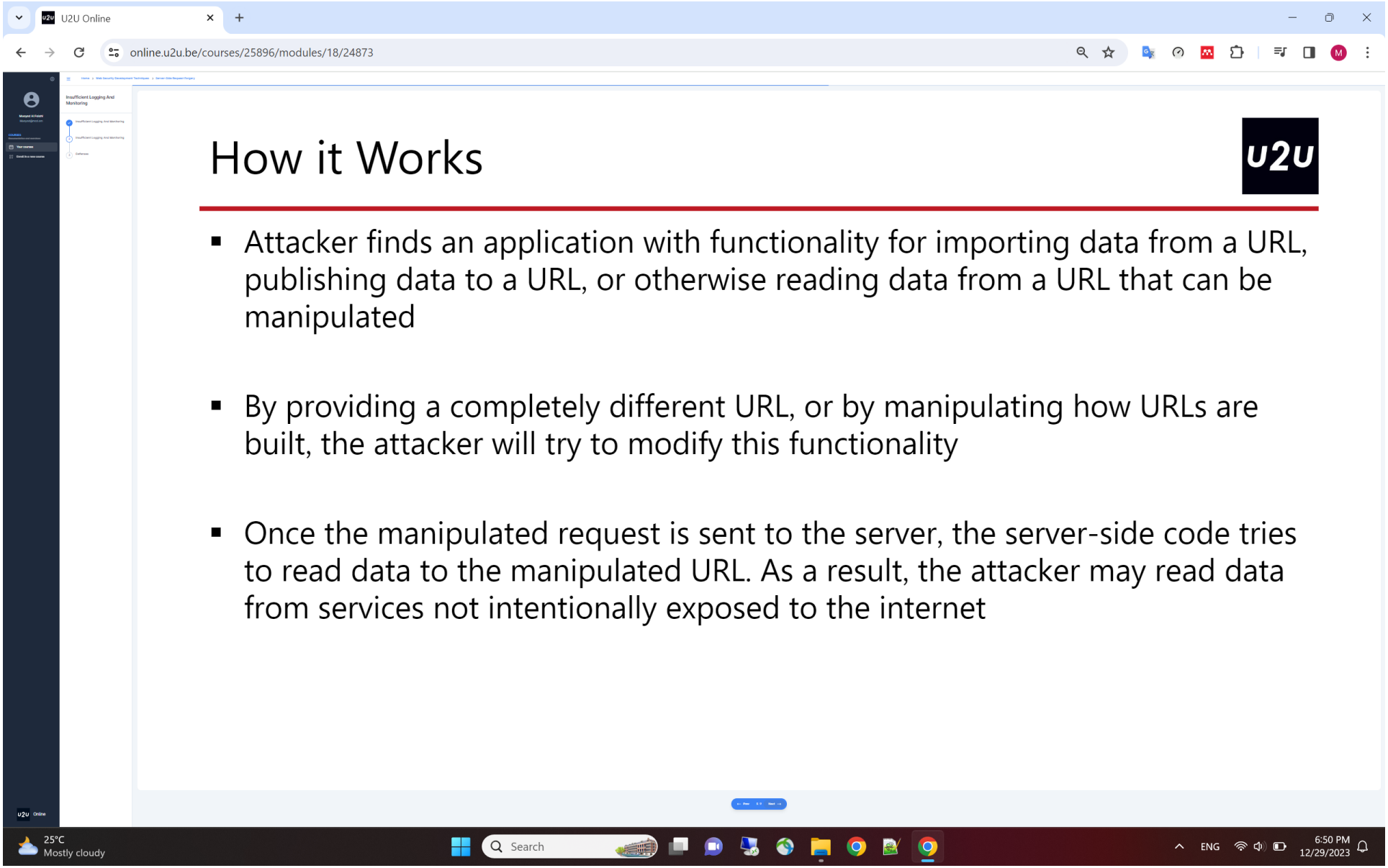
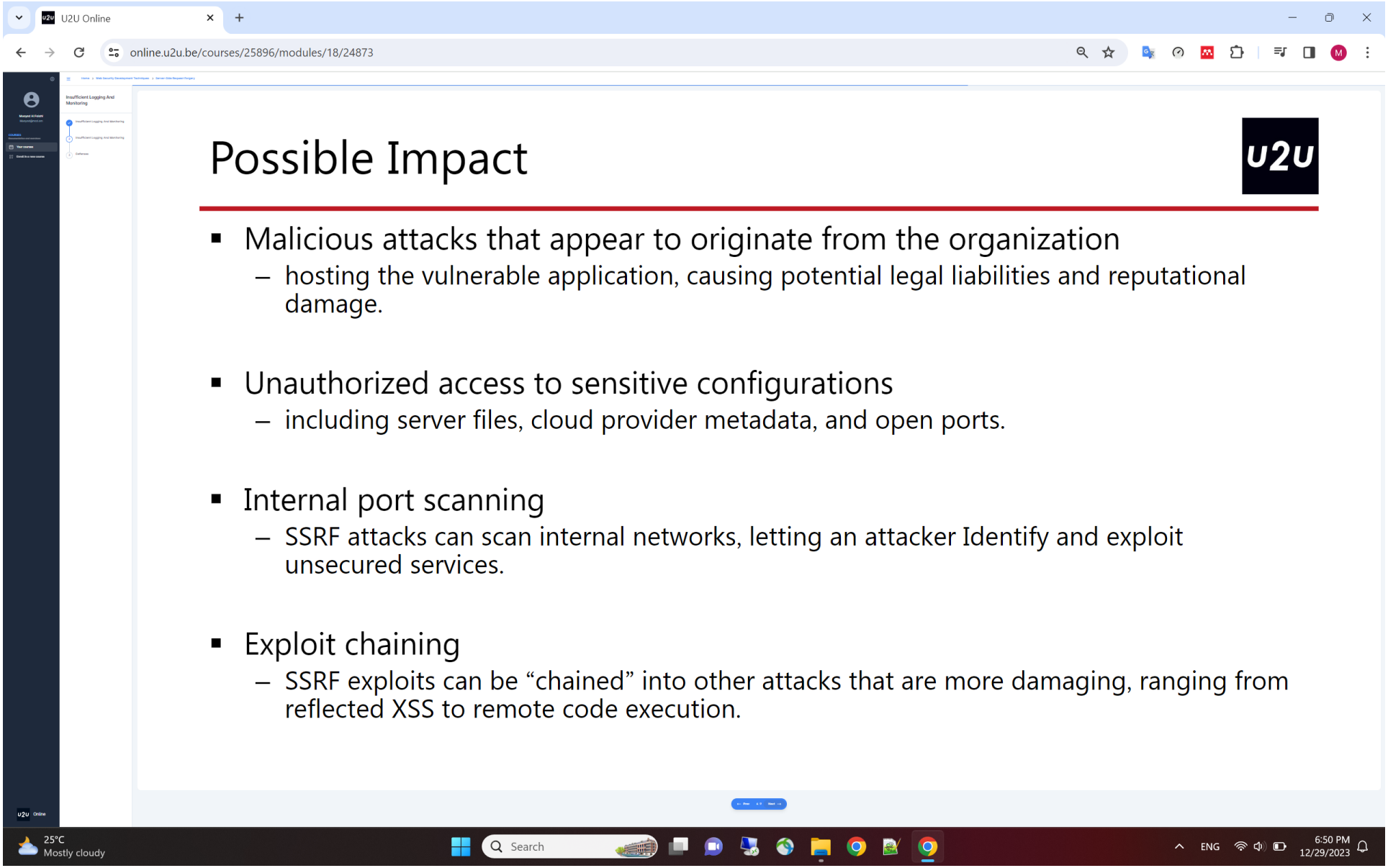

U2U Online
online.u2u.be/courses/25896/modules/18/24873
Developer and IT Training
U2U
Server-Side Request Forgery
OWASP Web Security Threat #10
25°C
Mostly cloudy
Search
ENG
6:50 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/18/24873
Insufficient Logging And Monitoring
Agenda
u2u
Server-Side Request Forgery
Defenses
Famous Examples
25°C
Mostly cloudy
Search
ENG
6:50 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/18/24873
#9: Server-Side Request Forgery
U2U
SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL
Attackers can then make the application send crafted requests to unexpected destinations, even when protected by a firewall or VPN
25°C
Mostly cloudy
Search
ENG
6:50 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/18/24873
Security Matrix
u2u
ATTACK VECTORS
SECURITY WEAKNESS
TECHNICAL IMPACTS
Exploitability
Prevalence
Detectability
Impact
AVERAGE
LOW
DIFFICULT
SEVERE
25°C
Mostly cloudy
Search
ENG
6:50 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/18/24873
How it Works
U2U
Attacker finds an application with functionality for importing data from a URL, publishing data to a URL, or otherwise reading data from a URL that can be manipulated
By providing a completely different URL, or by manipulating how URLs are built, the attacker will try to modify this functionality
Once the manipulated request is sent to the server, the server-side code tries to read data to the manipulated URL. As a result, the attacker may read data from services not intentionally exposed to the internet
25°C
Mostly cloudy
Search
ENG
6:50 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/18/24873
Possible Impact
U2U
Malicious attacks that appear to originate from the organization
– hosting the vulnerable application, causing potential legal liabilities and reputational damage.
Unauthorized access to sensitive configurations
– including server files, cloud provider metadata, and open ports.
Internal port scanning
– SSRF attacks can scan internal networks, letting an attacker Identify and exploit unsecured services.
Exploit chaining
– SSRF exploits can be “chained” into other attacks that are more damaging, ranging from reflected XSS to remote code execution.
25°C
Mostly cloudy
Search
ENG
6:50 PM
12/29/2023

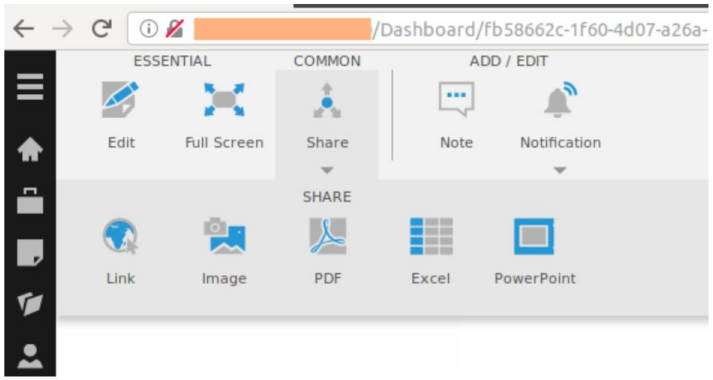
U2U Online

online.u2u.be/courses/25896/modules/18/24873

Examples

SSRF in Dundas BI

Dundas BI is a web-based analytics solution developed by Dundas Data Visualization, Inc. During one of our engagements, we found that this product was being used. After spending some time exploring the features and attack surface of the application, one thing caught our eye. One of Dundas BI features allows you to export what you're seeing in the data dashboard to different formats. For example, the following screenshot shows how it's possible to share the current dashboard as an image:

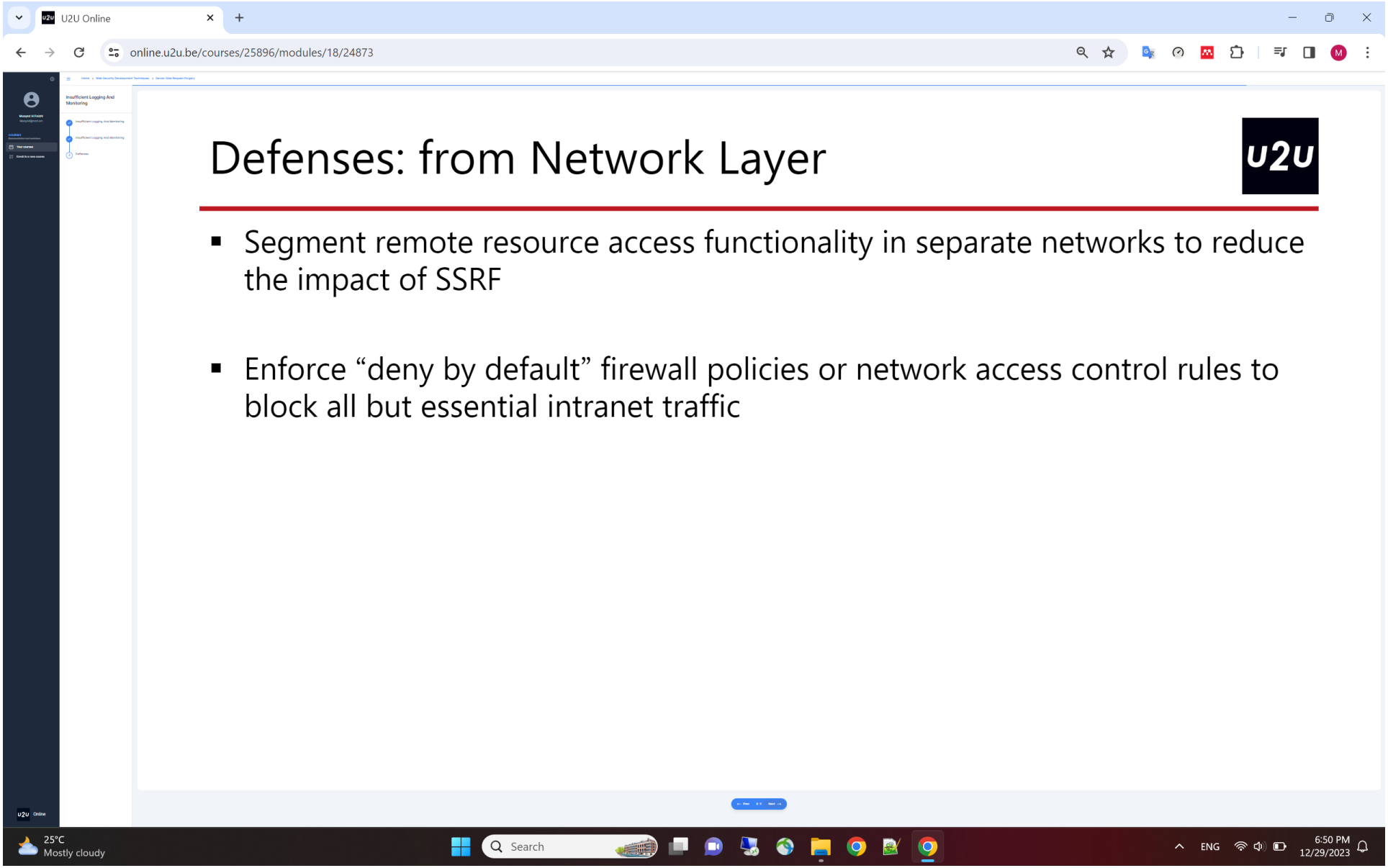


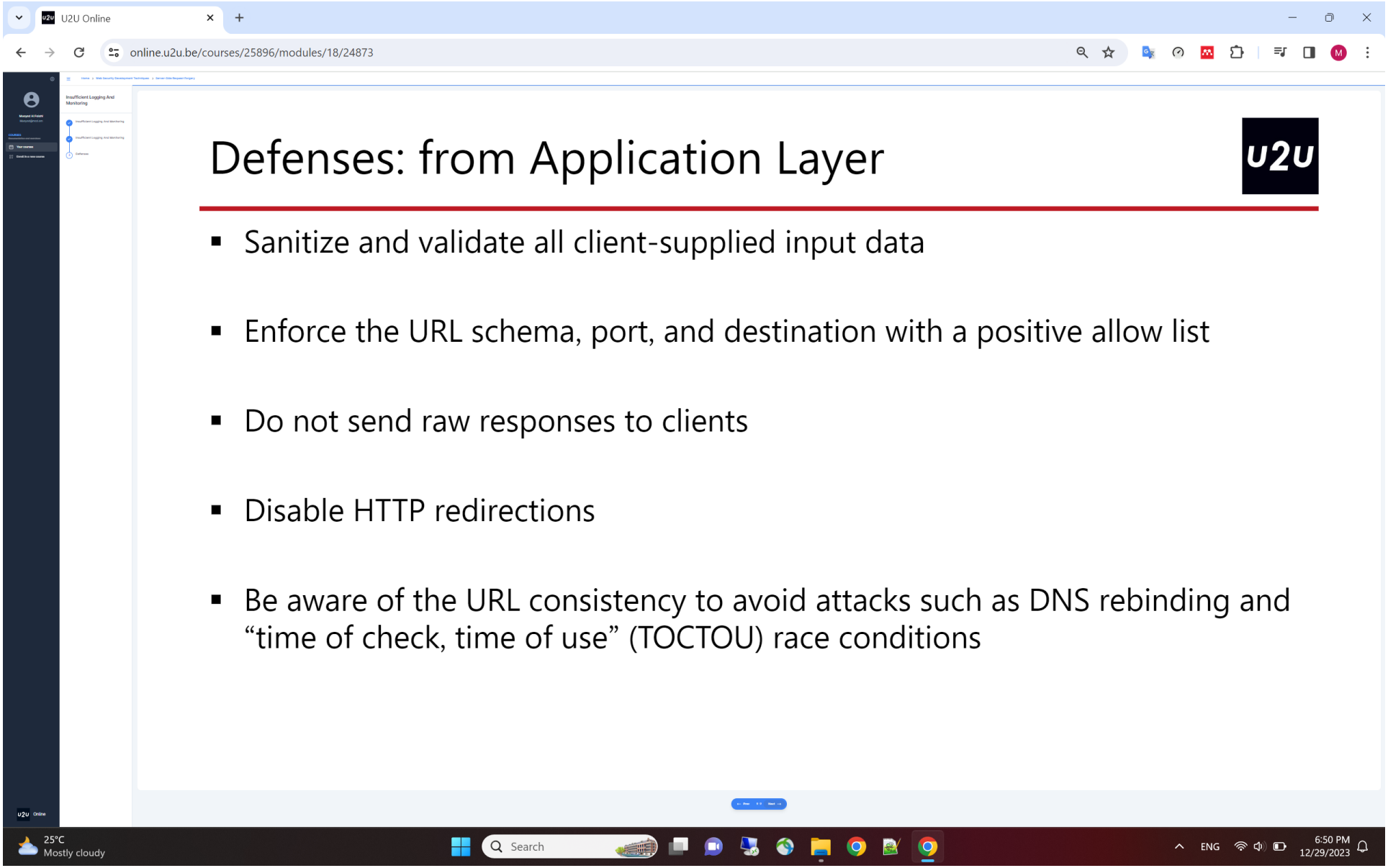
25°C
Mostly cloudy

Search

ENG

6:50 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/18/24873
Insufficient Logging And Monitoring
Defenses: from Network Layer
U2U
Segment remote resource access functionality in separate networks to reduce the impact of SSRF
Enforce “deny by default” firewall policies or network access control rules to block all but essential intranet traffic
25°C
Mostly cloudy
Search
ENG
6:50 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/18/24873
Defenses: from Application Layer
U2U
Sanitize and validate all client-supplied input data
Enforce the URL schema, port, and destination with a positive allow list
Do not send raw responses to clients
Disable HTTP redirections
Be aware of the URL consistency to avoid attacks such as DNS rebinding and "time of check, time of use" (TOCTOU) race conditions
25°C
Mostly cloudy
Search
ENG
6:50 PM
12/29/2023