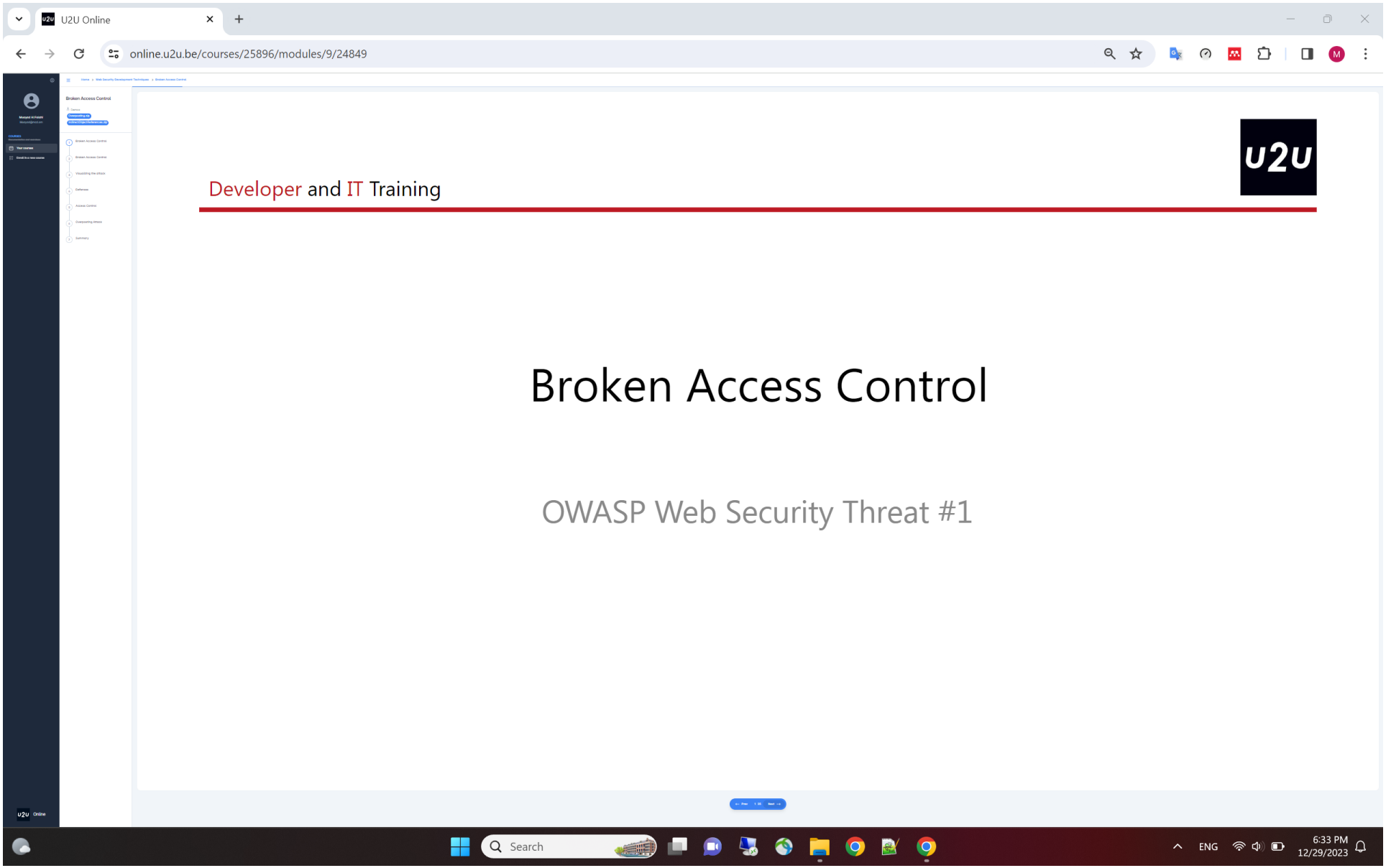
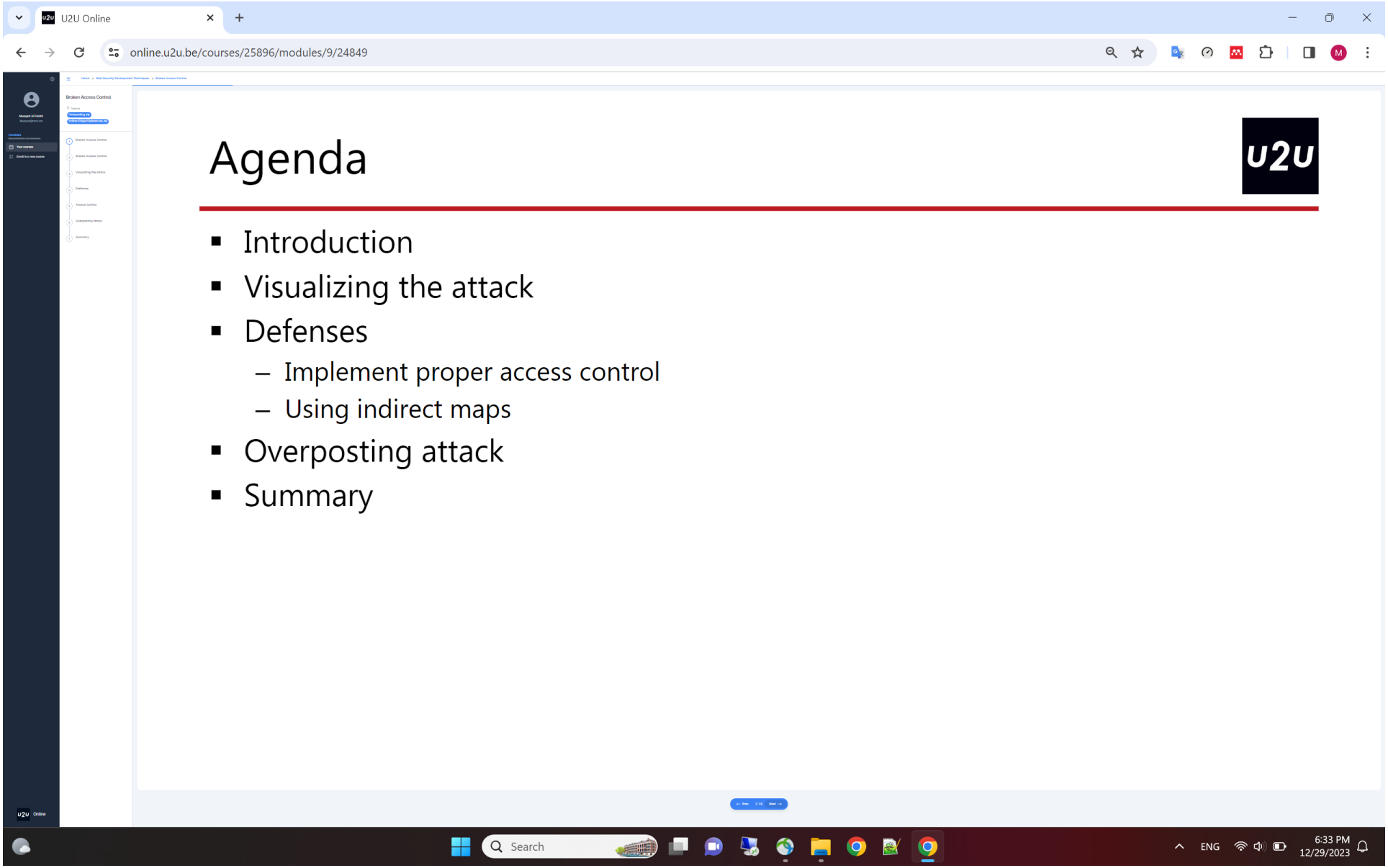
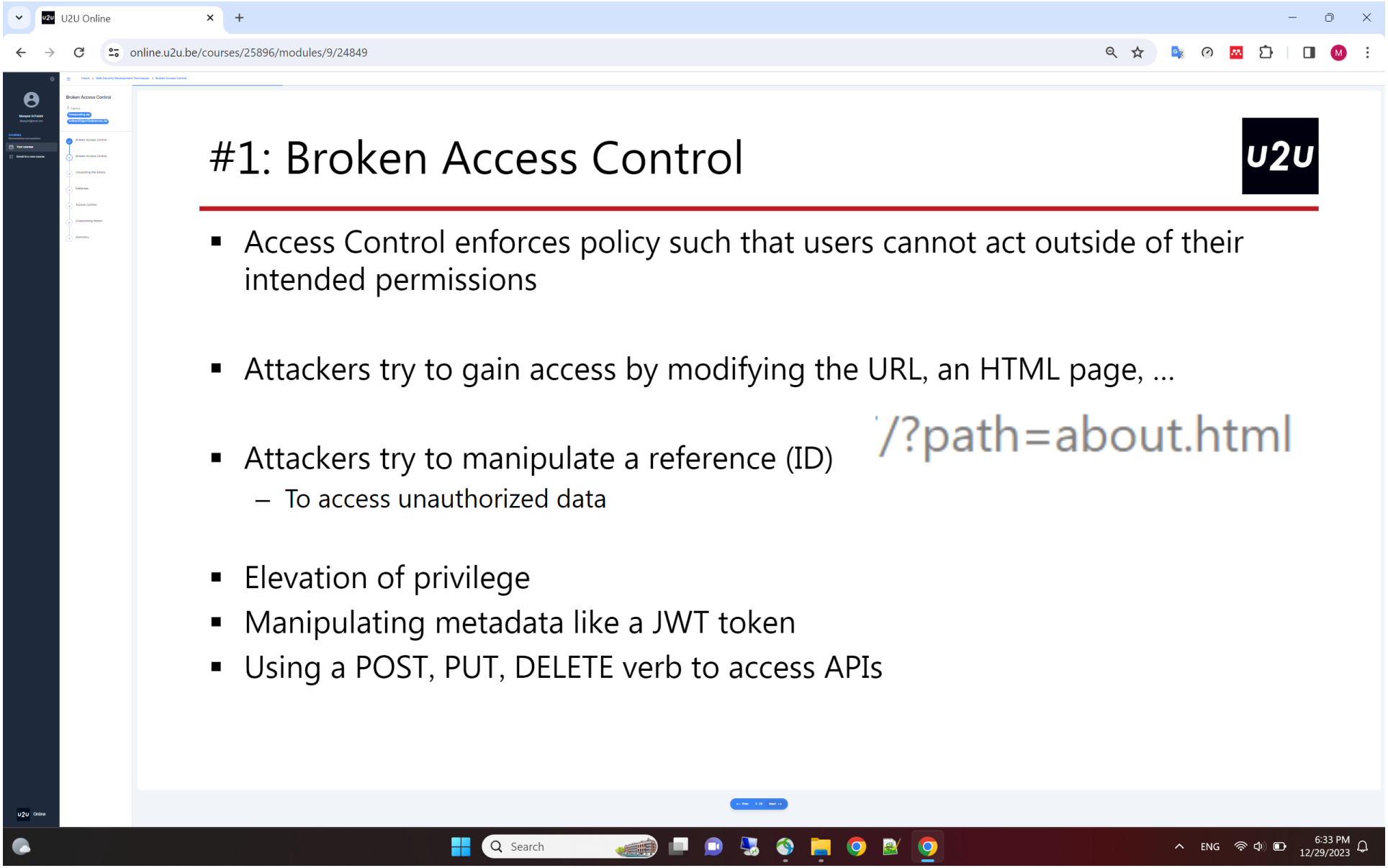
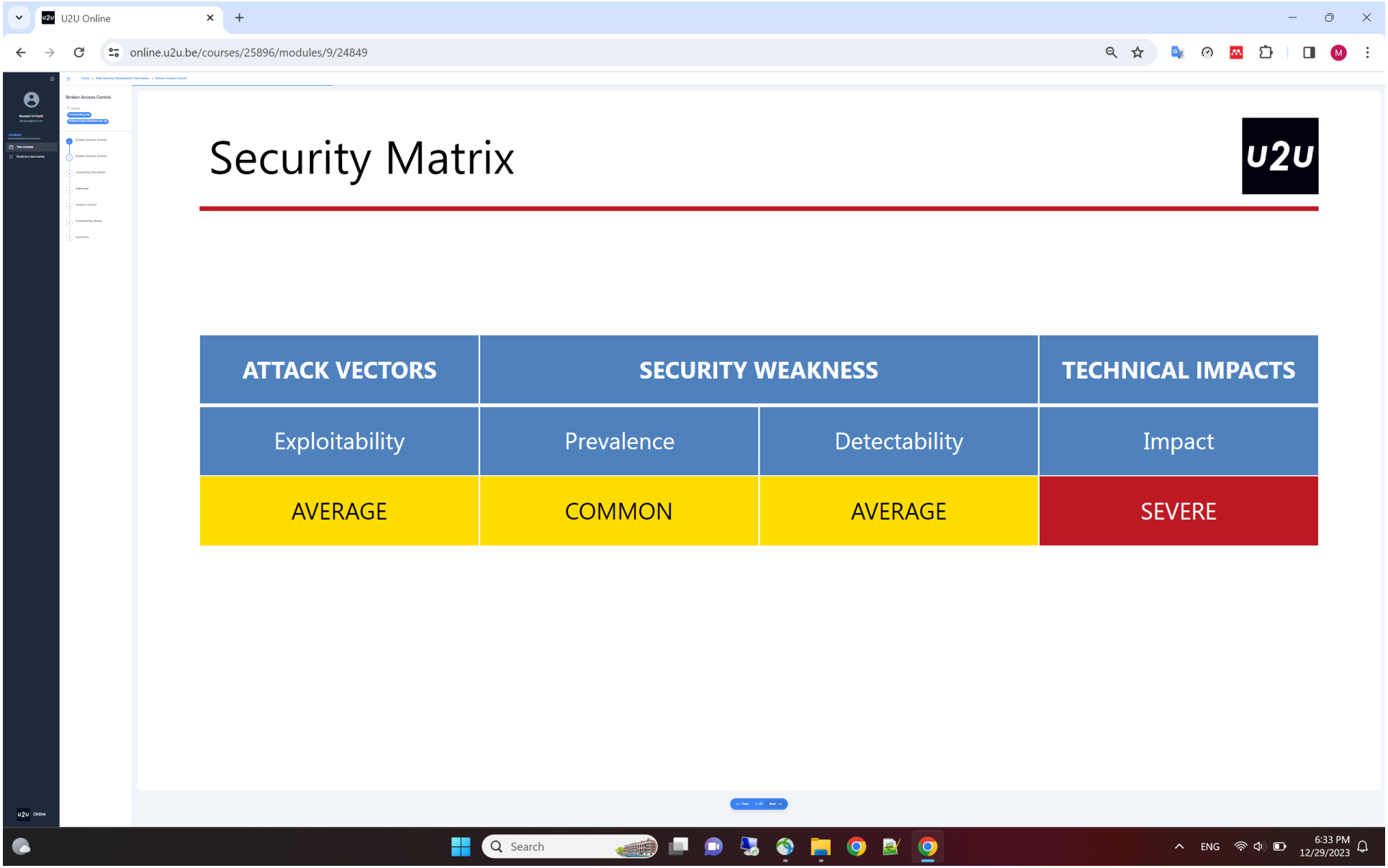
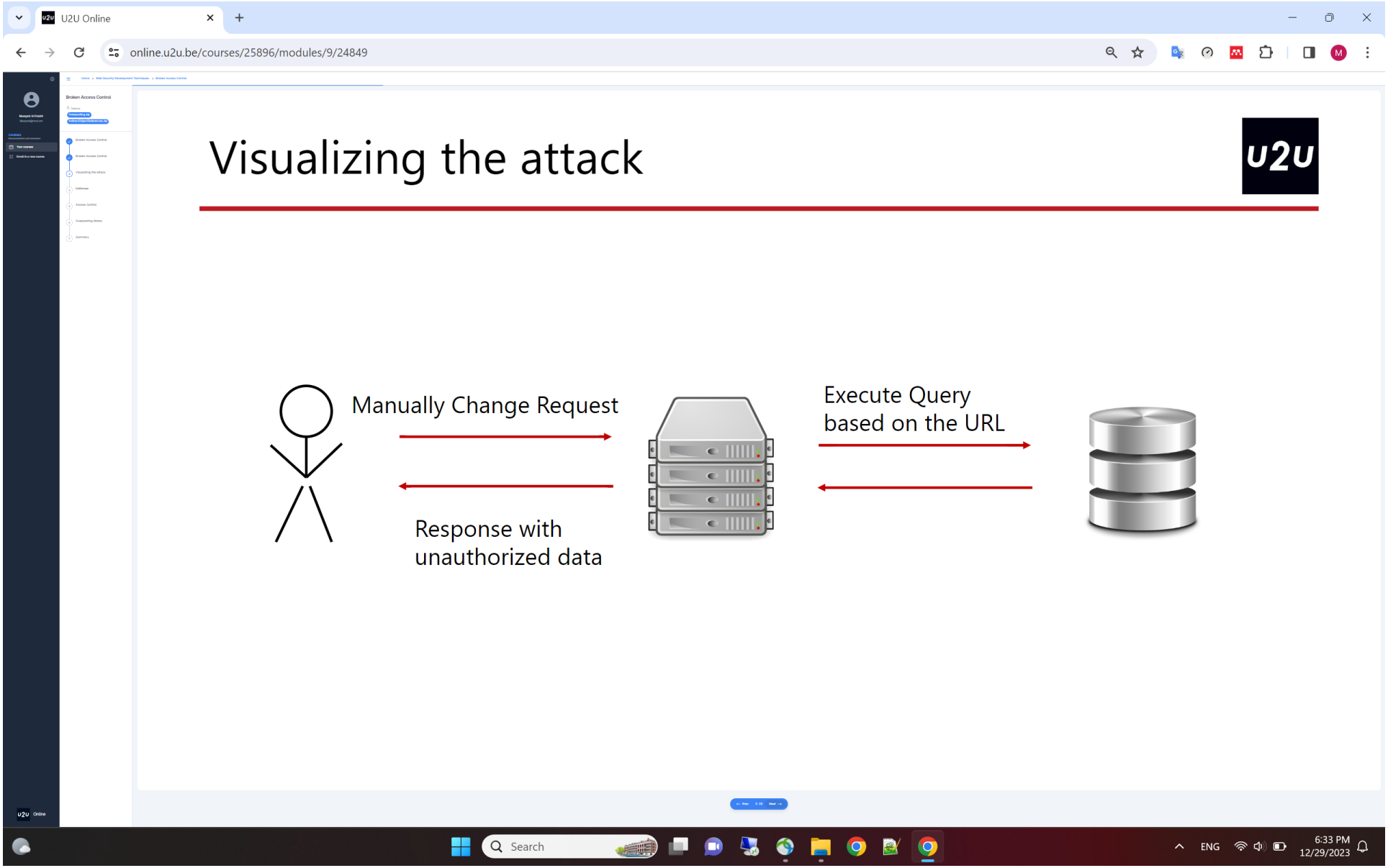
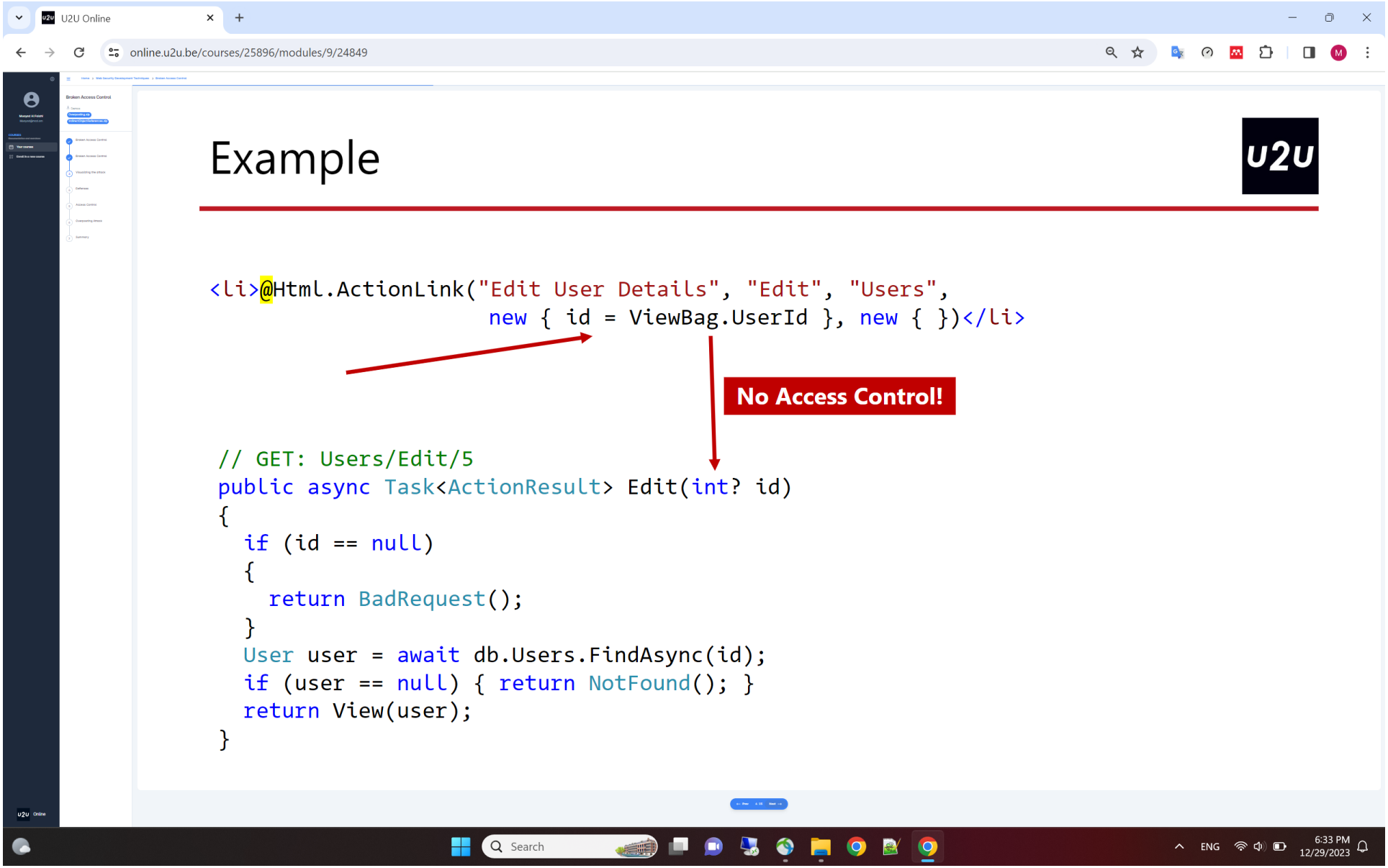

U2U Online
online.u2u.be/courses/25896/modules/9/24849
Broken Access Control
Developer and IT Training
u2u
Broken Access Control
OWASP Web Security Threat #1
Search
ENG
6:33 PM
12/29/2023

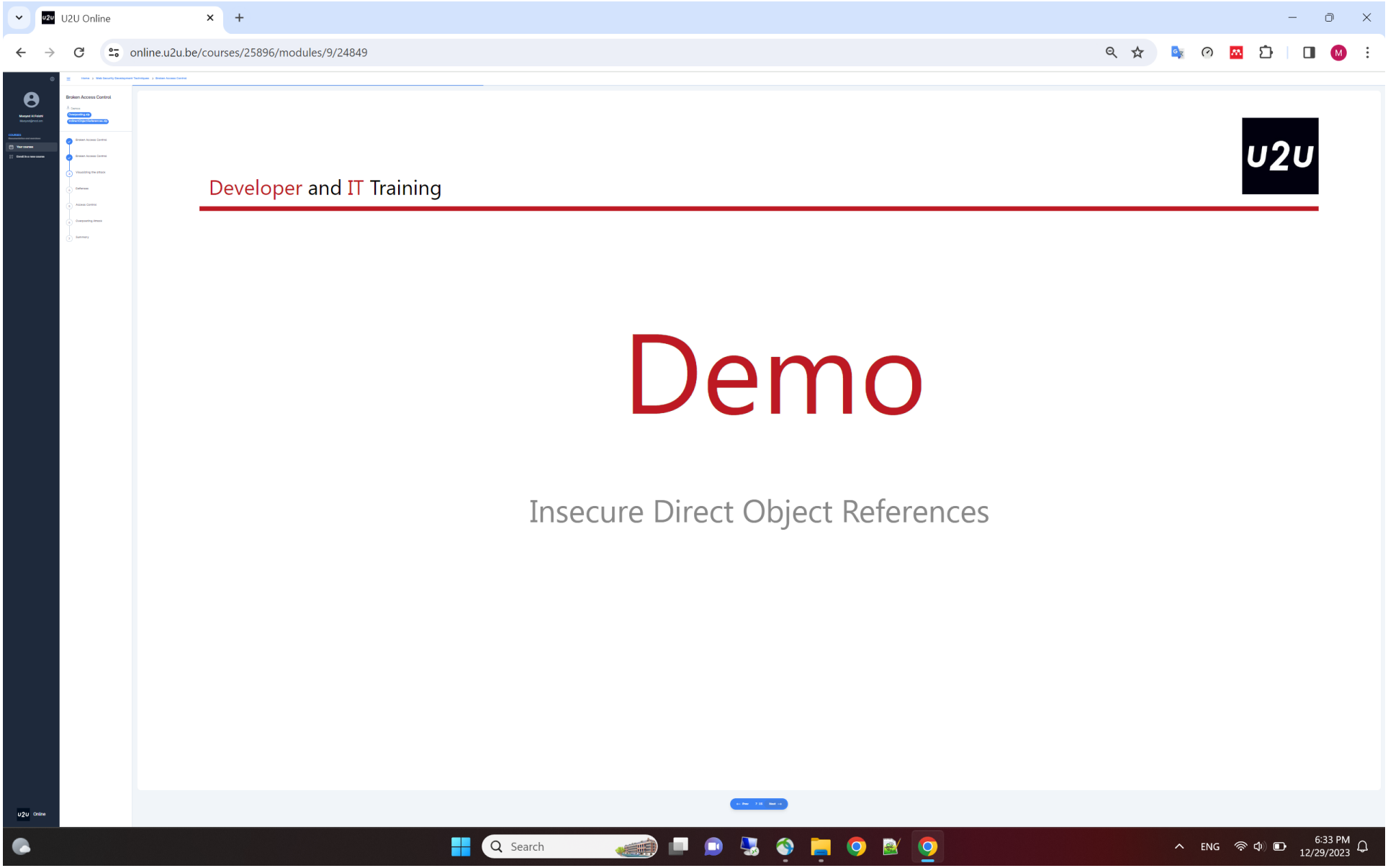

U2U Online
online.u2u.be/courses/25896/modules/9/24849
Agenda
u2u
Introduction
Visualizing the attack
Defenses
Implement proper access control
Using indirect maps
Overposting attack
Summary
Search
ENG
6:33 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/9/24849
#1: Broken Access Control
U2U
Access Control enforces policy such that users cannot act outside of their intended permissions
Attackers try to gain access by modifying the URL, an HTML page, …
'/?path=about.html
Attackers try to manipulate a reference (ID)
To access unauthorized data
Elevation of privilege
Manipulating metadata like a JWT token
Using a POST, PUT, DELETE verb to access APIs
Search
ENG
6:33 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/9/24849
Broken Access Control
Security Matrix
u2u
ATTACK VECTORS
SECURITY WEAKNESS
TECHNICAL IMPACTS
Exploitability
Prevalence
Detectability
Impact
AVERAGE
COMMON
AVERAGE
SEVERE
Search
ENG
6:33 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/9/24849
Visualizing the attack
u2u
Manually Change Request
Response with
unauthorized data
Execute Query
based on the URL
Search
ENG
6:33 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/9/24849
Example
U2U
@Html.ActionLink("Edit User Details", "Edit", "Users",
new { id = ViewBag.UserId }, new { })
No Access Control!
// GET: Users/Edit/5
public async Task<ActionResult> Edit(int? id)
{
if (id == null)
{
return BadRequest();
}
User user = await db.Users.FindAsync(id);
if (user == null) { return NotFound(); }
return View(user);
}
Search
ENG
6:33 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/9/24849
Broken Access Control
Developer and IT Training
u2u
Demo
Insecure Direct Object References
Search
ENG
6:33 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/9/24849

Real-Life Story

U2U

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Security

Citigroup hack exploited easy-to-detect web flaw

Brute force attack exposes 200,000 accounts

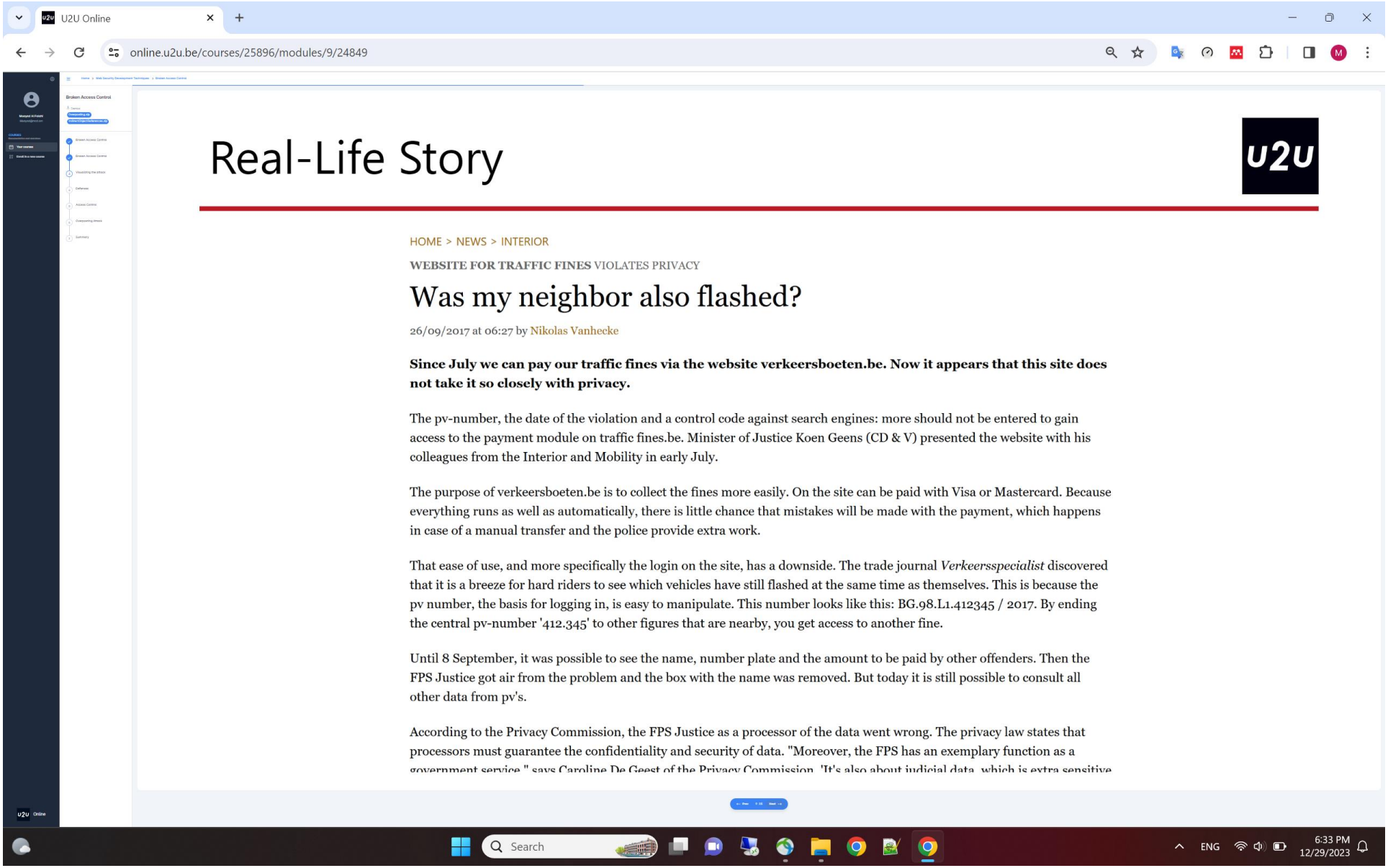
14 Jun 2011 at 21:25, Dan Goodin

Hackers who stole bank account details for 200,000 Citigroup customers infiltrated the company's system by exploiting a garden-variety security hole in the company's website for credit card users, according to a report citing an unnamed security investigator.

The New York Times reported that the technique allowed the hackers to leapfrog from account to account on the Citi website by changing the numbers in the URLs that appeared after customers had entered valid usernames and passwords. The hackers wrote a script that automatically repeated the exercise tens of thousands of times, the *NYT* said in an article published Monday.

Search

ENG 6:33 PM 12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/9/24849
Real-Life Story
U2U
HOME > NEWS > INTERIOR
WEBSITE FOR TRAFFIC FINES VIOLATES PRIVACY
Was my neighbor also flashed?
26/09/2017 at 06:27 by Nikolas Vanhecke
Since July we can pay our traffic fines via the website verkeersboeten.be. Now it appears that this site does not take it so closely with privacy.
The pv-number, the date of the violation and a control code against search engines: more should not be entered to gain access to the payment module on traffic fines.be. Minister of Justice Koen Geens (CD & V) presented the website with his colleagues from the Interior and Mobility in early July.
The purpose of verkeersboeten.be is to collect the fines more easily. On the site can be paid with Visa or Mastercard. Because everything runs as well as automatically, there is little chance that mistakes will be made with the payment, which happens in case of a manual transfer and the police provide extra work.
That ease of use, and more specifically the login on the site, has a downside. The trade journal Verkeersspecialist discovered that it is a breeze for hard riders to see which vehicles have still flashed at the same time as themselves. This is because the pv number, the basis for logging in, is easy to manipulate. This number looks like this: BG.98.L1.412345 / 2017. By ending the central pv-number '412.345' to other figures that are nearby, you get access to another fine.
Until 8 September, it was possible to see the name, number plate and the amount to be paid by other offenders. Then the FPS Justice got air from the problem and the box with the name was removed. But today it is still possible to consult all other data from pv's.
According to the Privacy Commission, the FPS Justice as a processor of the data went wrong. The privacy law states that processors must guarantee the confidentiality and security of data. "Moreover, the FPS has an exemplary function as a
Search
ENG
6:33 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/9/24849

Example from real life

U2U

Apple's Worst Security Breach: 114,000 iPad Owners Exposed

Ryan Tate
06/09/10 03:50PM Filed to: EXCLUSIVE

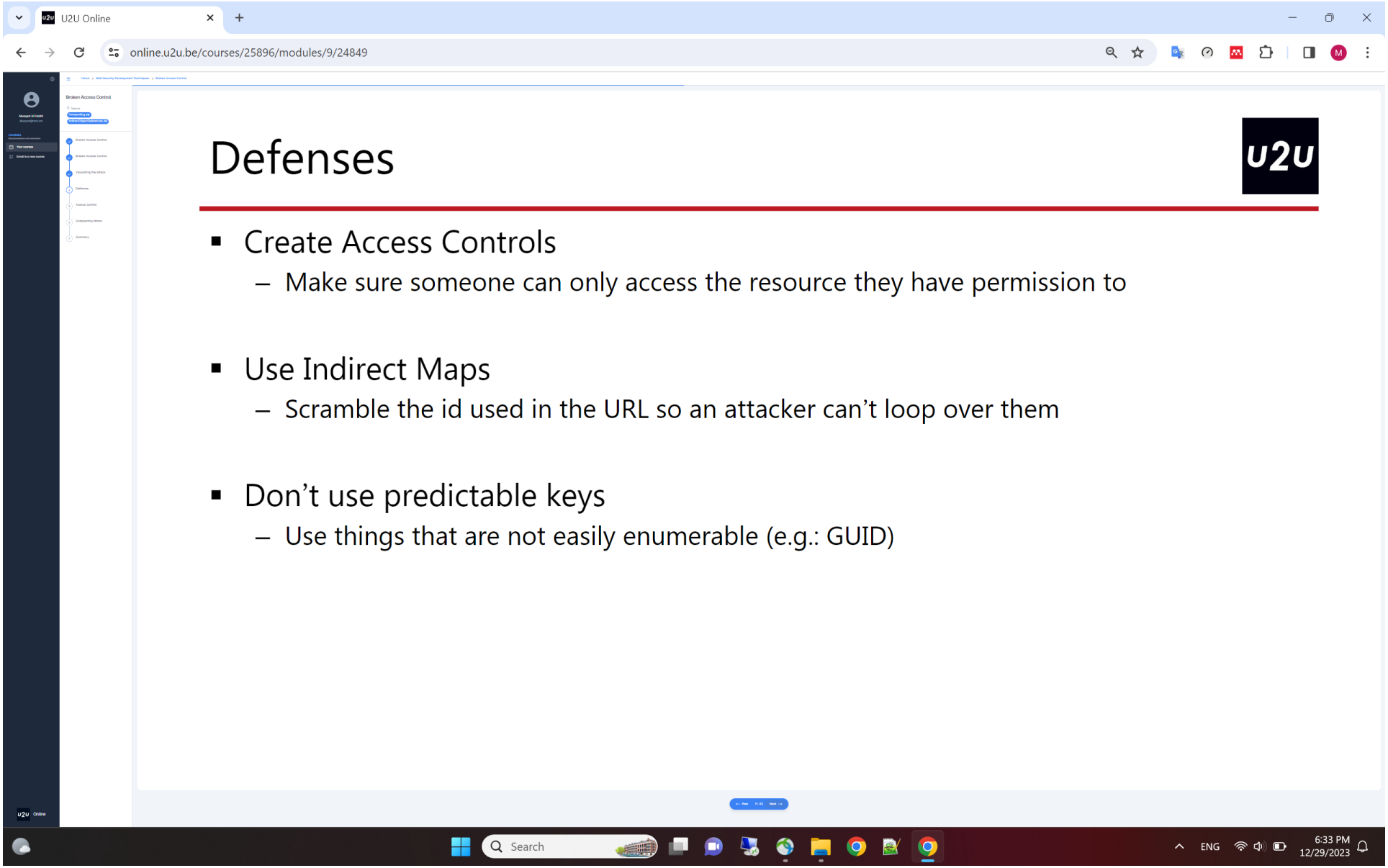
The specific information exposed in the breach included subscribers' email addresses, coupled with an associated ID used to authenticate the subscriber on AT&T's network, known as the ICC-ID. ICC-ID stands for integrated circuit card identifier and is used to identify the SIM cards that associate a mobile device with a particular subscriber.

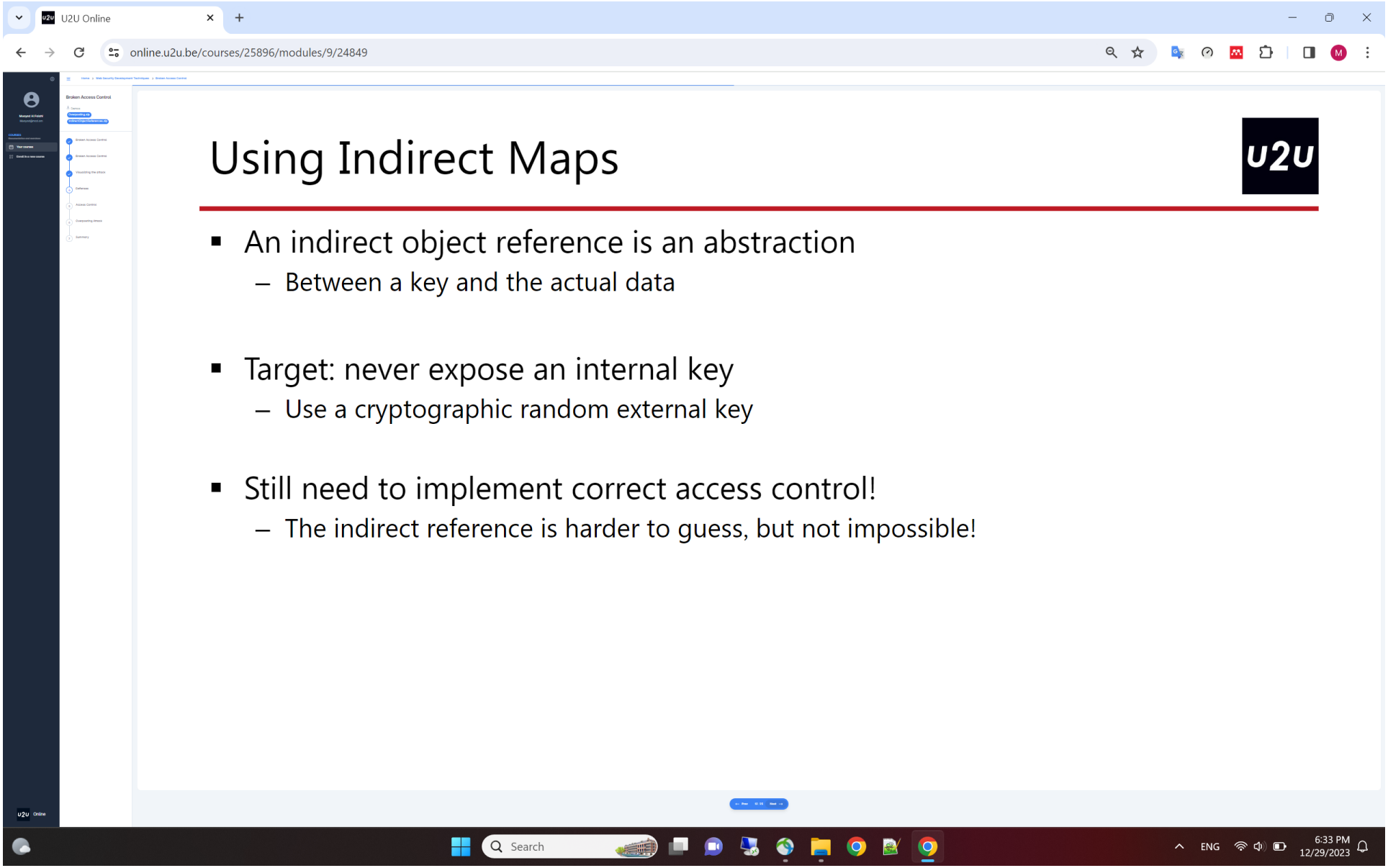
Goatse Security obtained its data through a script on AT&T's website, accessible to anyone on the internet. When provided with an ICC-ID as part of an HTTP request, the script would return the associated email address, in what was apparently intended to be an AJAX-style response within a Web application. The security researchers were able to guess a large swath of ICC IDs by looking at known iPad 3G ICC IDs, some of which are shown in pictures posted by gadget enthusiasts to Flickr and other internet sites, and which can also be obtained through friendly associates who own iPads and are willing to share their information, available within the iPad "Settings" application.

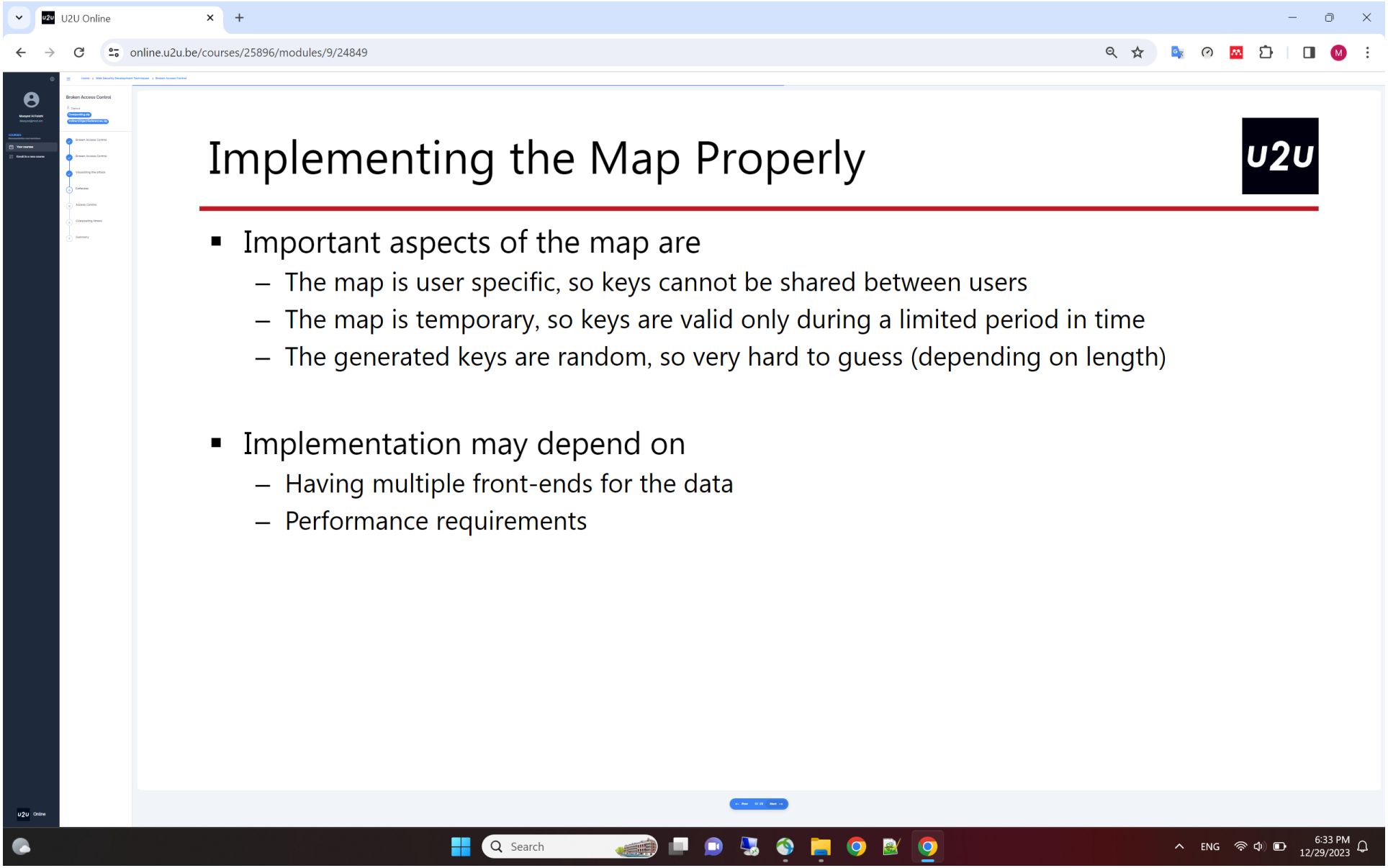
http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed

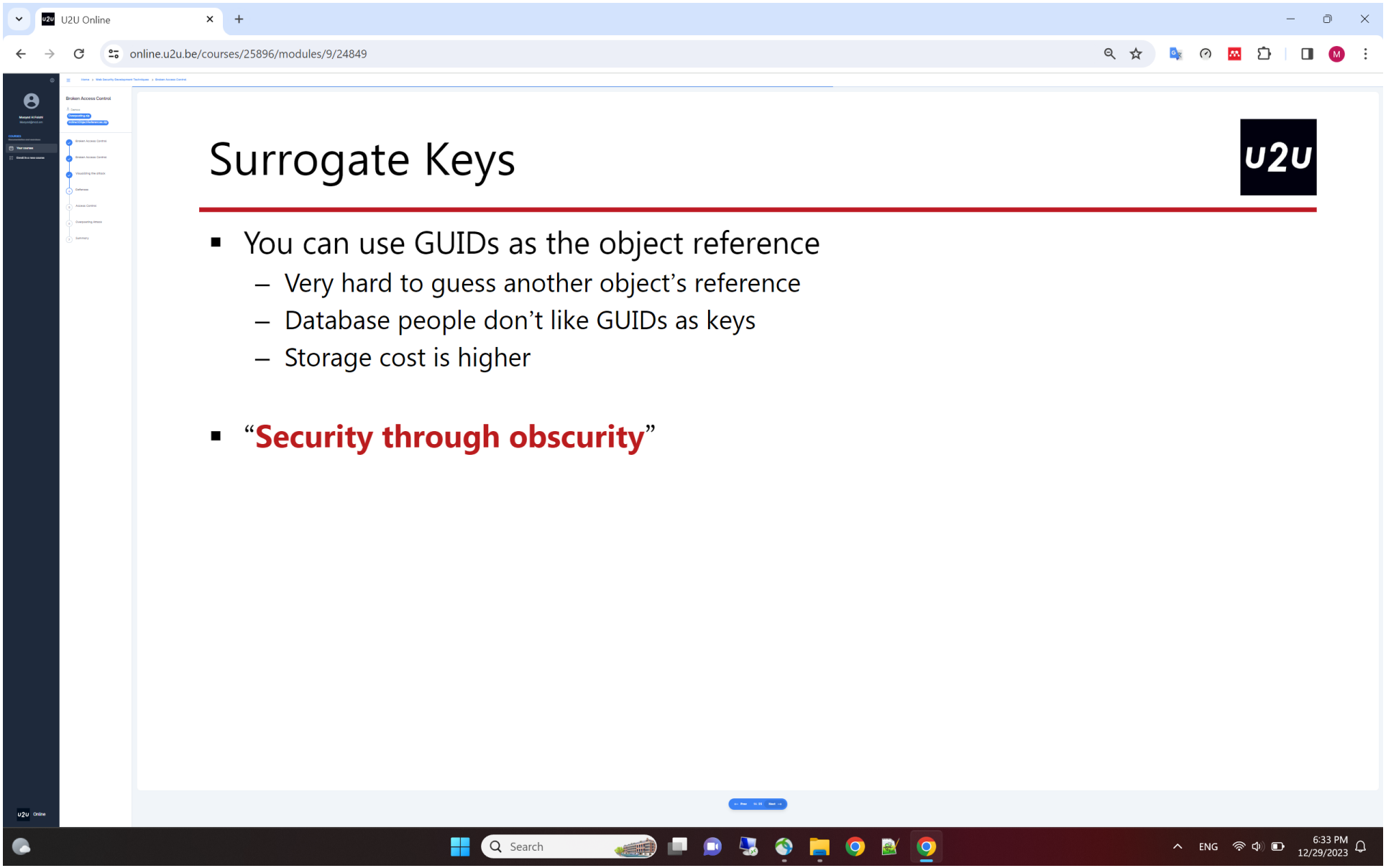
Search

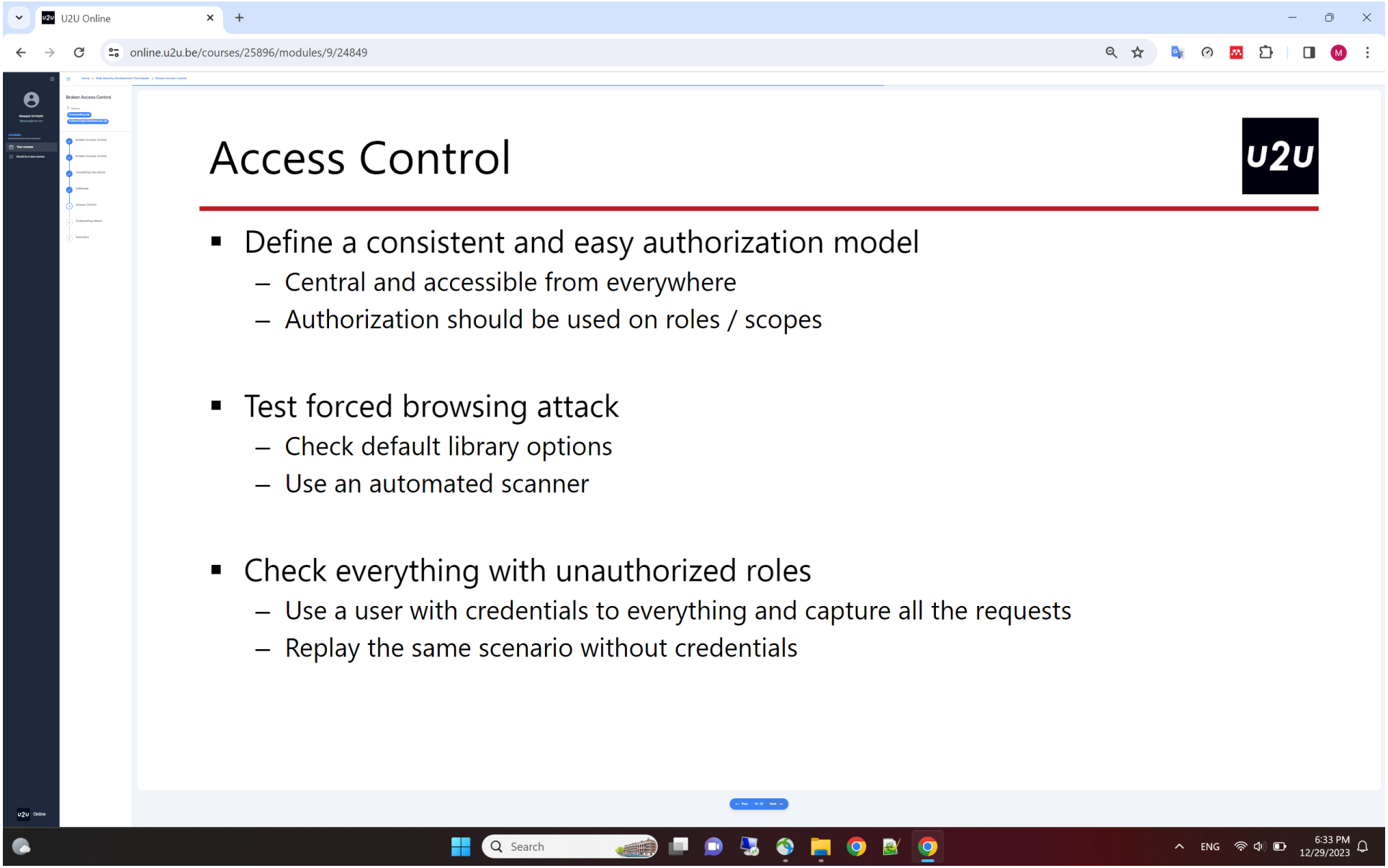
ENG 6:33 PM 12/29/2023

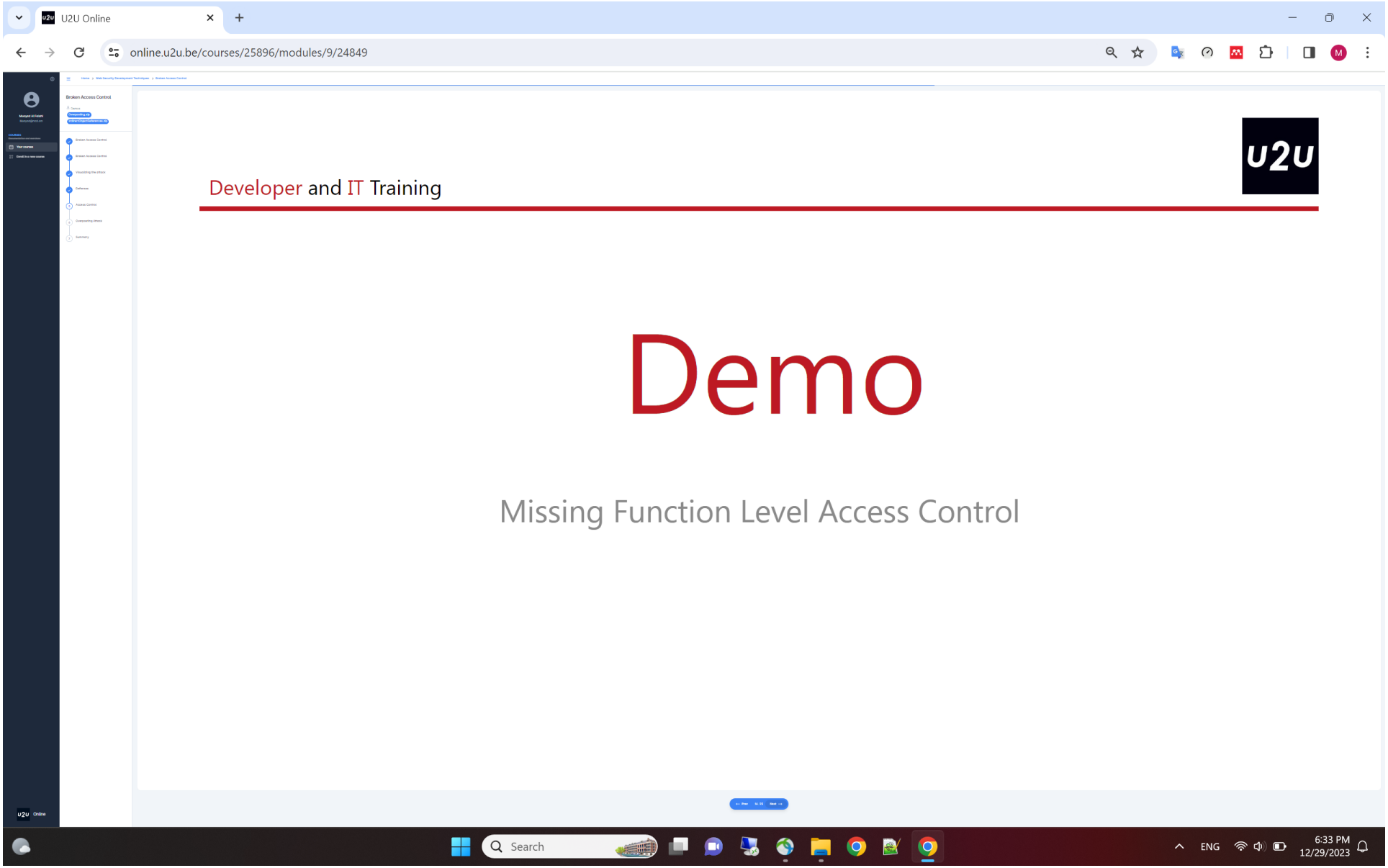

U2U Online
online.u2u.be/courses/25896/modules/9/24849
Broken Access Control
Defenses
u2u
Create Access Controls
Make sure someone can only access the resource they have permission to
Use Indirect Maps
Scramble the id used in the URL so an attacker can't loop over them
Don't use predictable keys
Use things that are not easily enumerable (e.g.: GUID)
Search
ENG
6:33 PM
12/29/2023

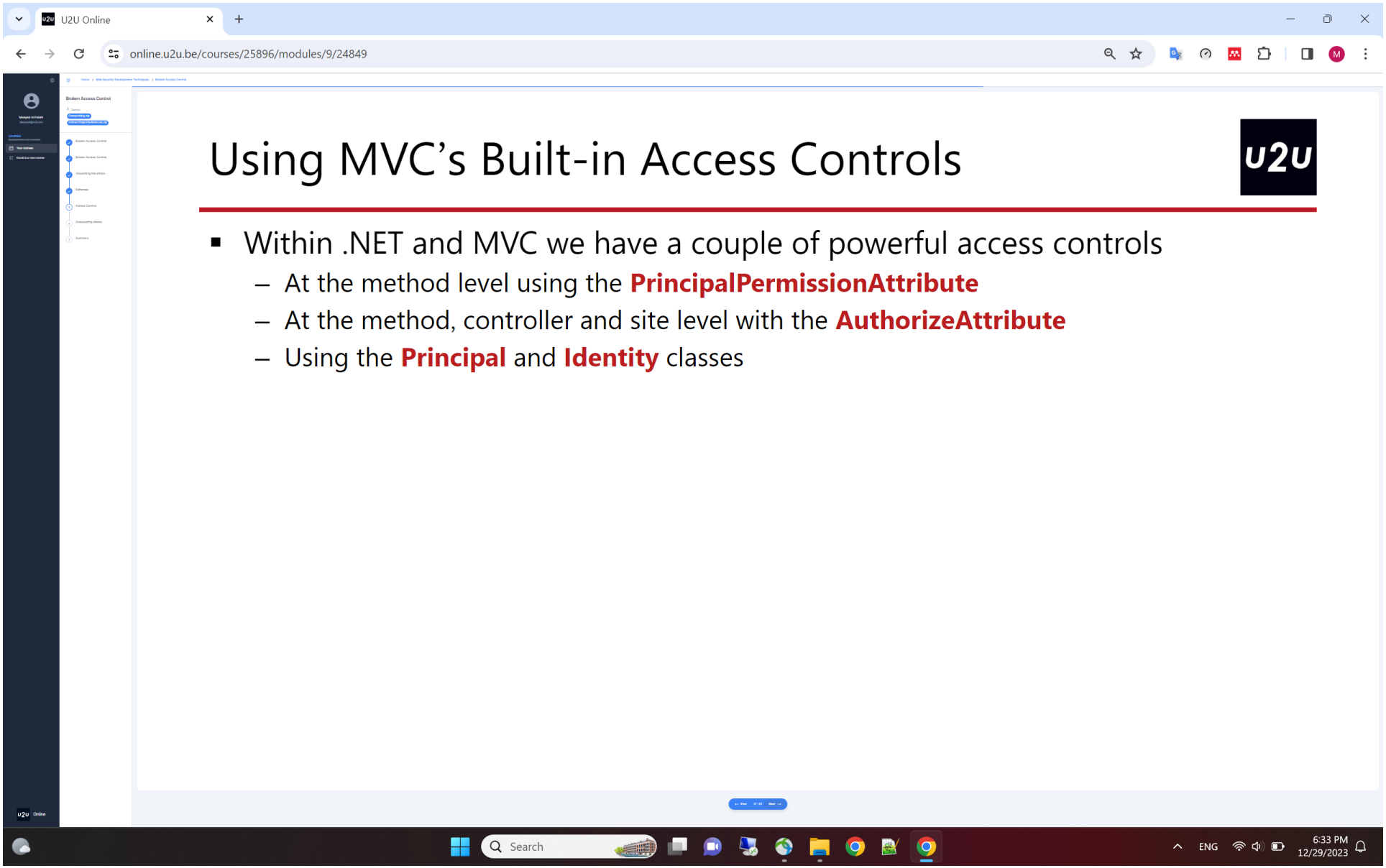

U2U Online
online.u2u.be/courses/25896/modules/9/24849
Broken Access Control
Using Indirect Maps
u2u
An indirect object reference is an abstraction
Between a key and the actual data
Target: never expose an internal key
Use a cryptographic random external key
Still need to implement correct access control!
The indirect reference is harder to guess, but not impossible!
Search
ENG
6:33 PM
12/29/2023

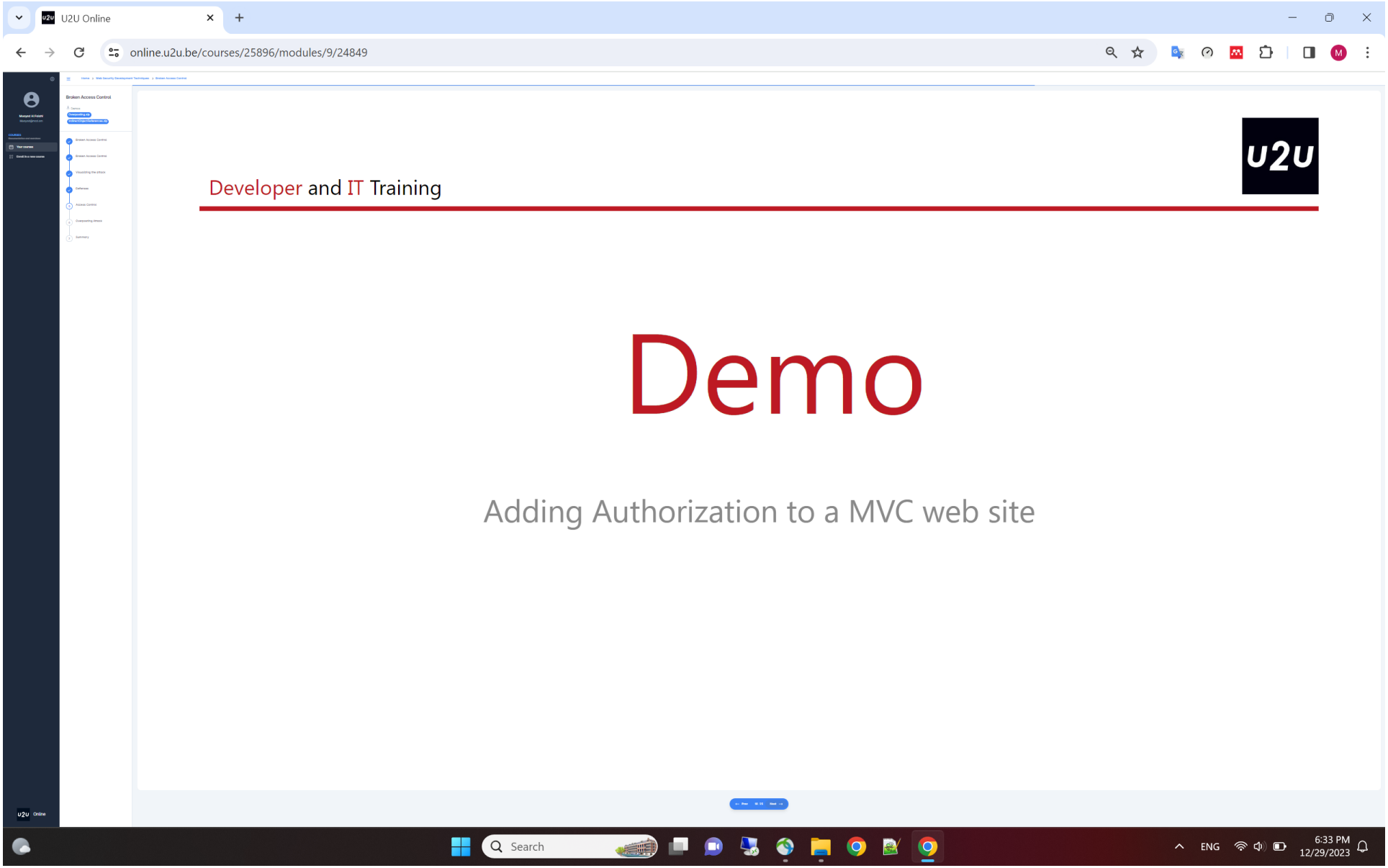

U2U Online
online.u2u.be/courses/25896/modules/9/24849
Implementing the Map Properly
u2u
Important aspects of the map are
The map is user specific, so keys cannot be shared between users
The map is temporary, so keys are valid only during a limited period in time
The generated keys are random, so very hard to guess (depending on length)
Implementation may depend on
Having multiple front-ends for the data
Performance requirements
Search
ENG
6:33 PM
12/29/2023

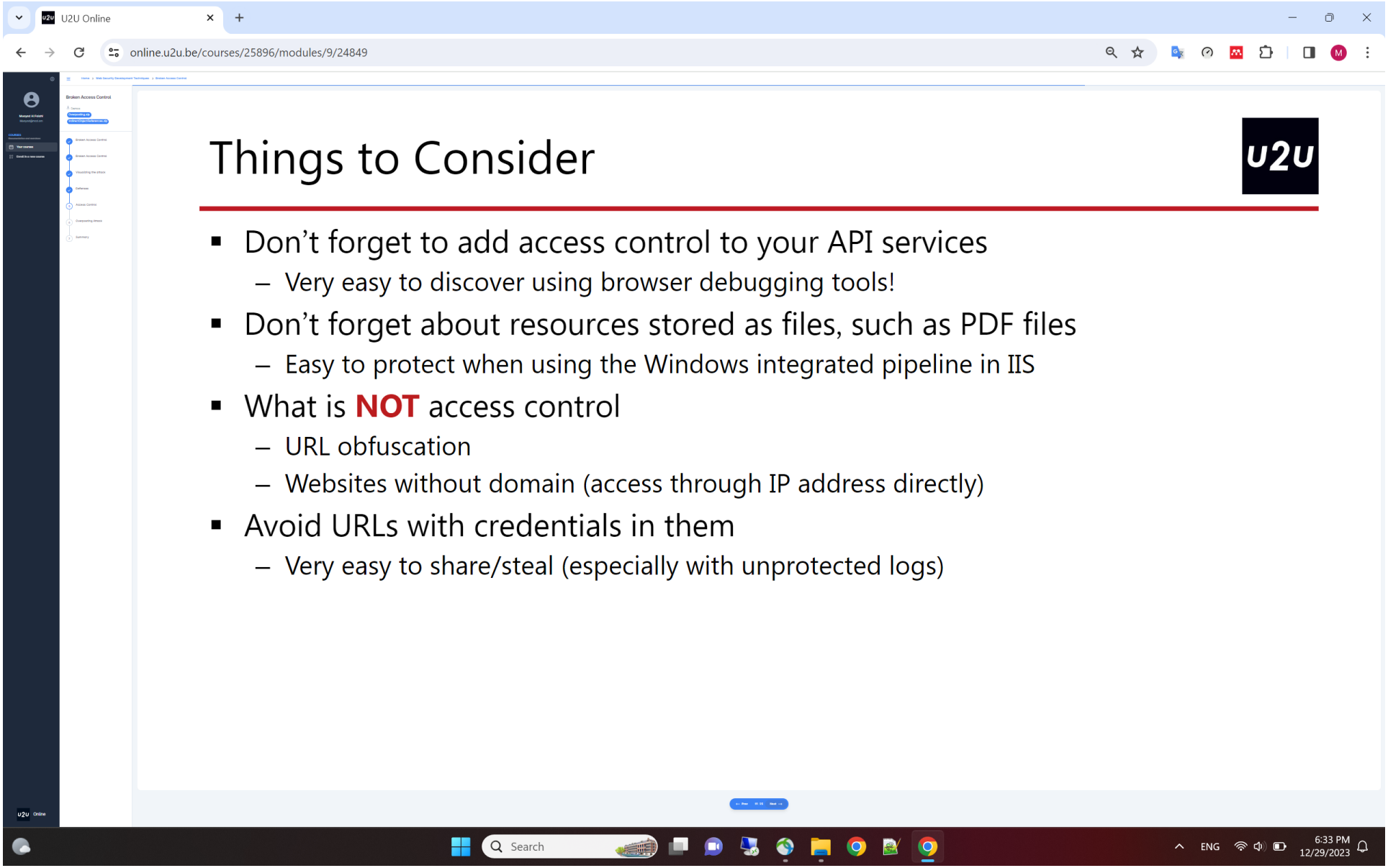

U2U Online
online.u2u.be/courses/25896/modules/9/24849
Broken Access Control
Surrogate Keys
u2u
You can use GUIDs as the object reference
Very hard to guess another object's reference
Database people don't like GUIDs as keys
Storage cost is higher
"Security through obscurity"
Search
ENG
6:33 PM
12/29/2023

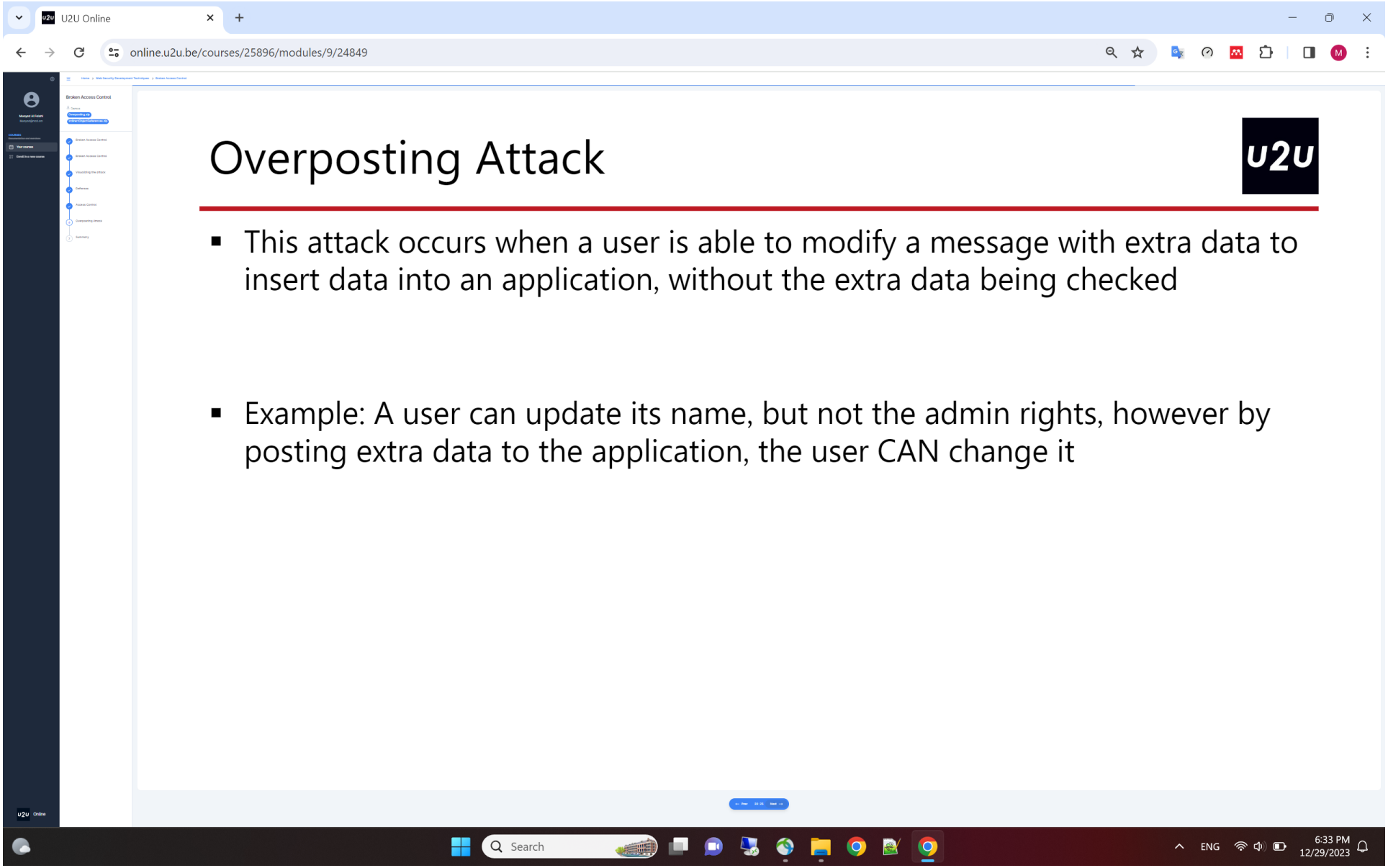

U2U Online
online.u2u.be/courses/25896/modules/9/24849
Access Control
u2u
Define a consistent and easy authorization model
Central and accessible from everywhere
Authorization should be used on roles / scopes
Test forced browsing attack
Check default library options
Use an automated scanner
Check everything with unauthorized roles
Use a user with credentials to everything and capture all the requests
Replay the same scenario without credentials
Search
ENG
6:33 PM
12/29/2023

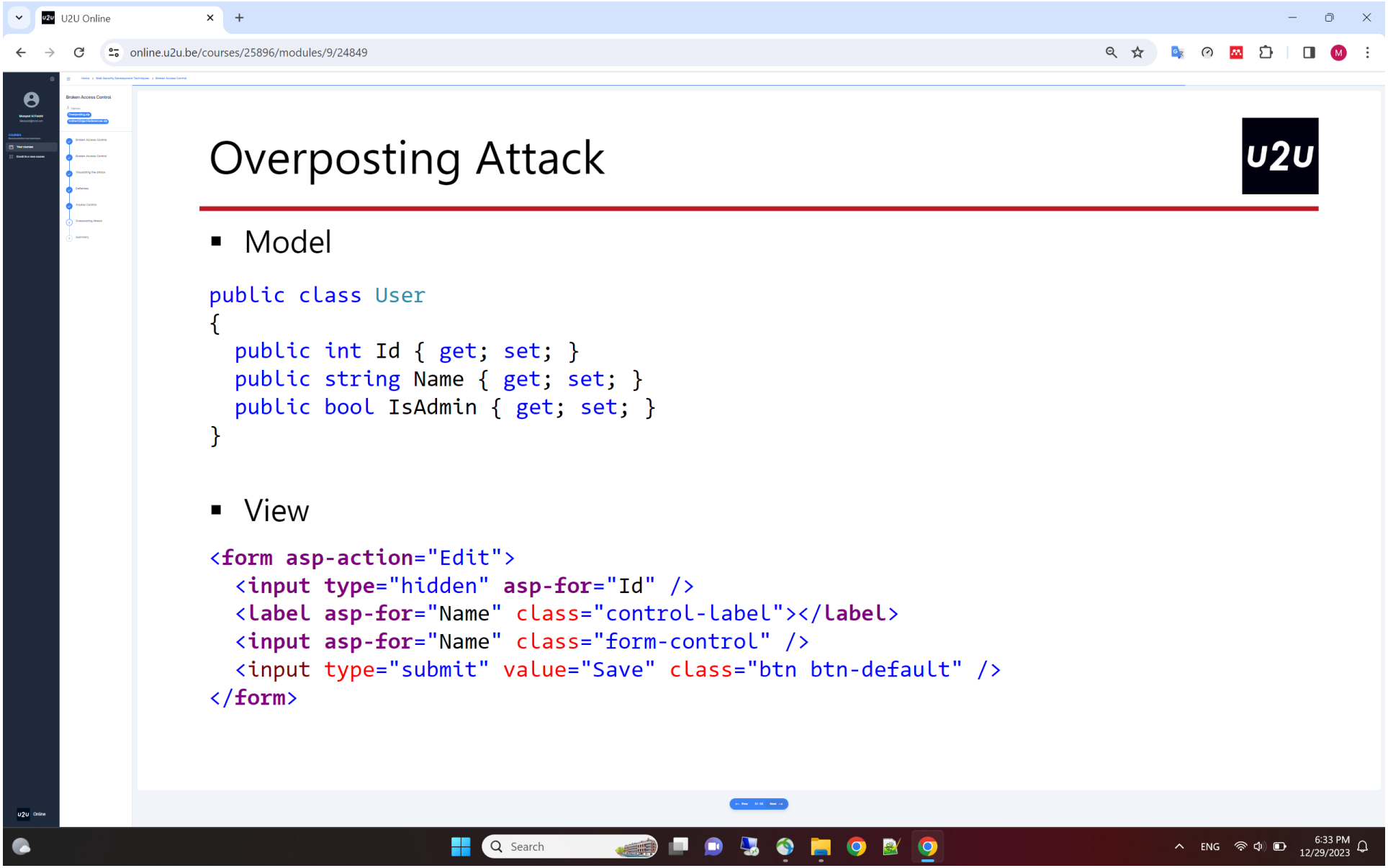

U2U Online
online.u2u.be/courses/25896/modules/9/24849
Broken Access Control
Developer and IT Training
U2U
Demo
Missing Function Level Access Control
Search
ENG
6:33 PM
12/29/2023

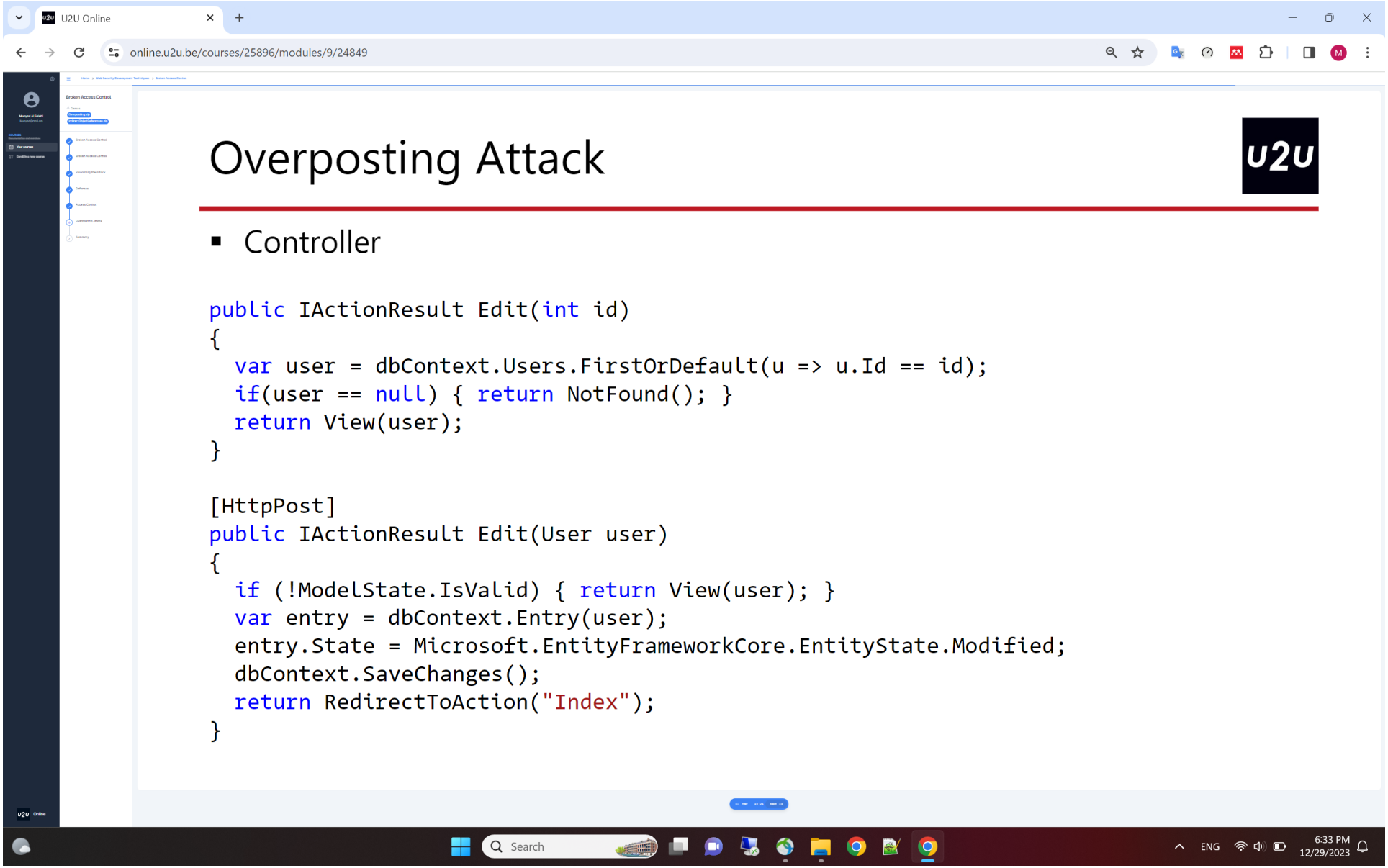

U2U Online
online.u2u.be/courses/25896/modules/9/24849
Using MVC's Built-in Access Controls
u2u
Within .NET and MVC we have a couple of powerful access controls
At the method level using the PrincipalPermissionAttribute
At the method, controller and site level with the AuthorizeAttribute
Using the Principal and Identity classes
Search
ENG
6:33 PM
12/29/2023

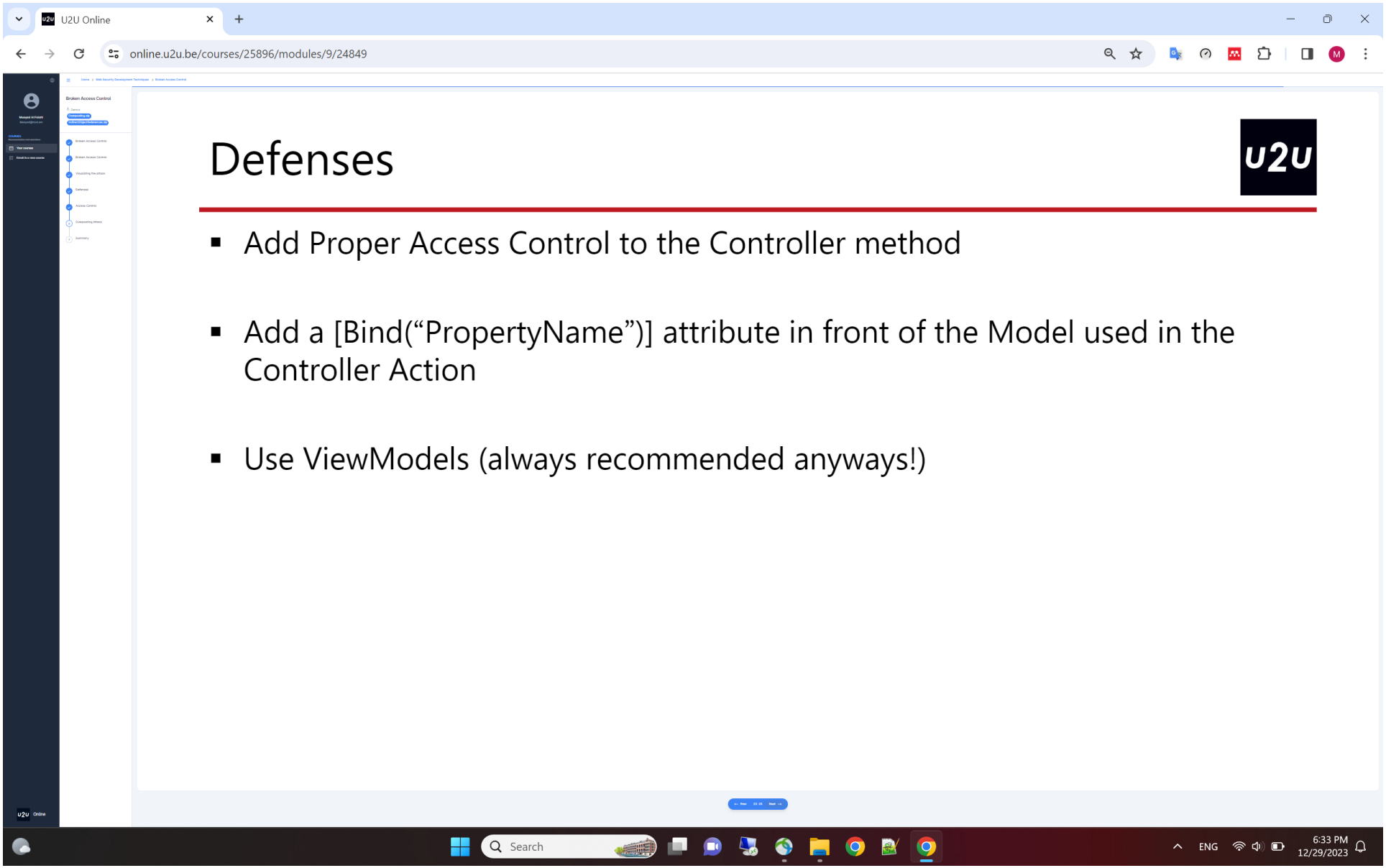

U2U Online
online.u2u.be/courses/25896/modules/9/24849
Broken Access Control
Developer and IT Training
u2u
Demo
Adding Authorization to a MVC web site
Search
ENG
6:33 PM
12/29/2023

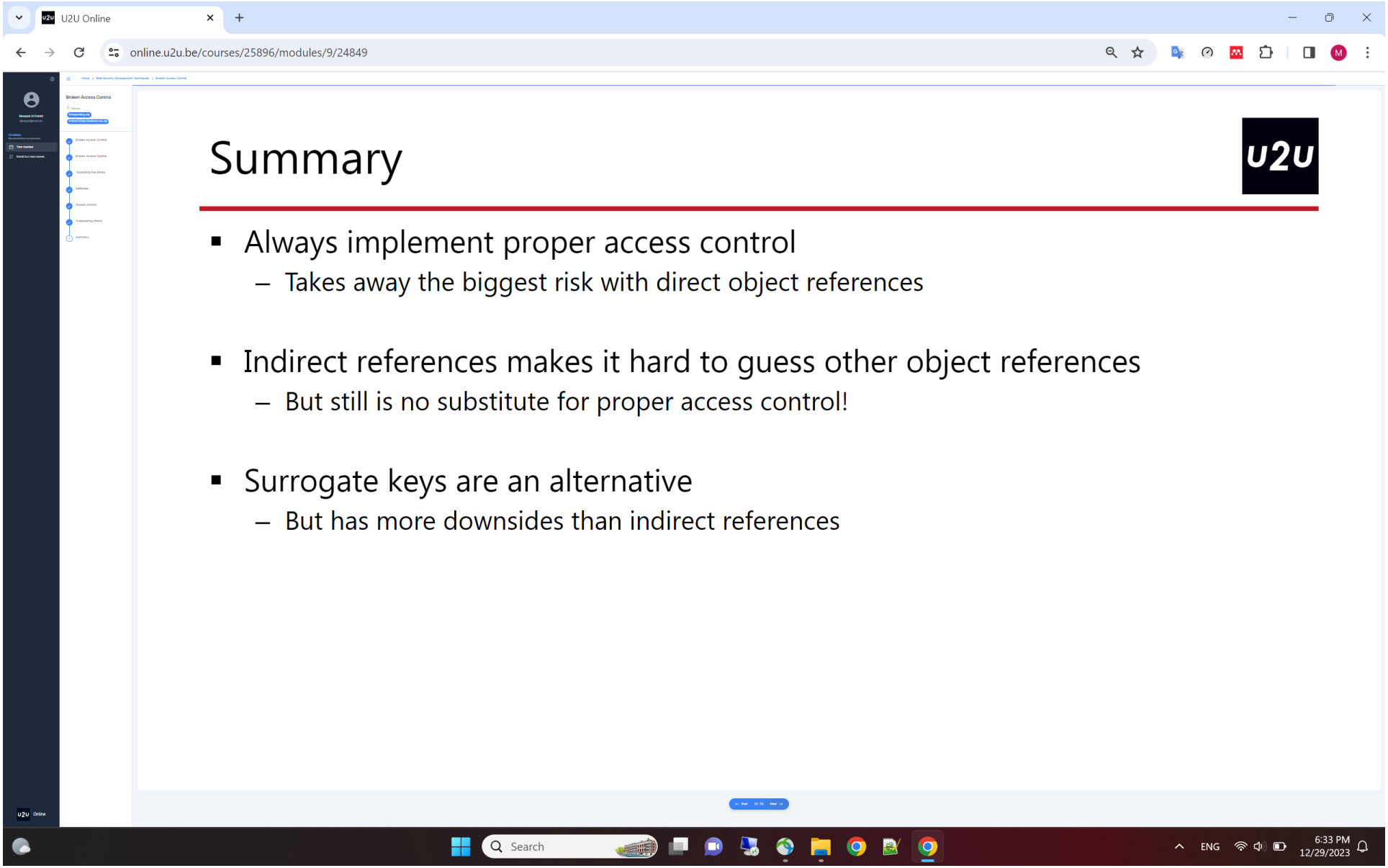

U2U Online
online.u2u.be/courses/25896/modules/9/24849
Broken Access Control
Things to Consider
U2U
Don’t forget to add access control to your API services
Very easy to discover using browser debugging tools!
Don’t forget about resources stored as files, such as PDF files
Easy to protect when using the Windows integrated pipeline in IIS
What is NOT access control
URL obfuscation
Websites without domain (access through IP address directly)
Avoid URLs with credentials in them
Very easy to share/steal (especially with unprotected logs)
Search
ENG
6:33 PM
12/29/2023

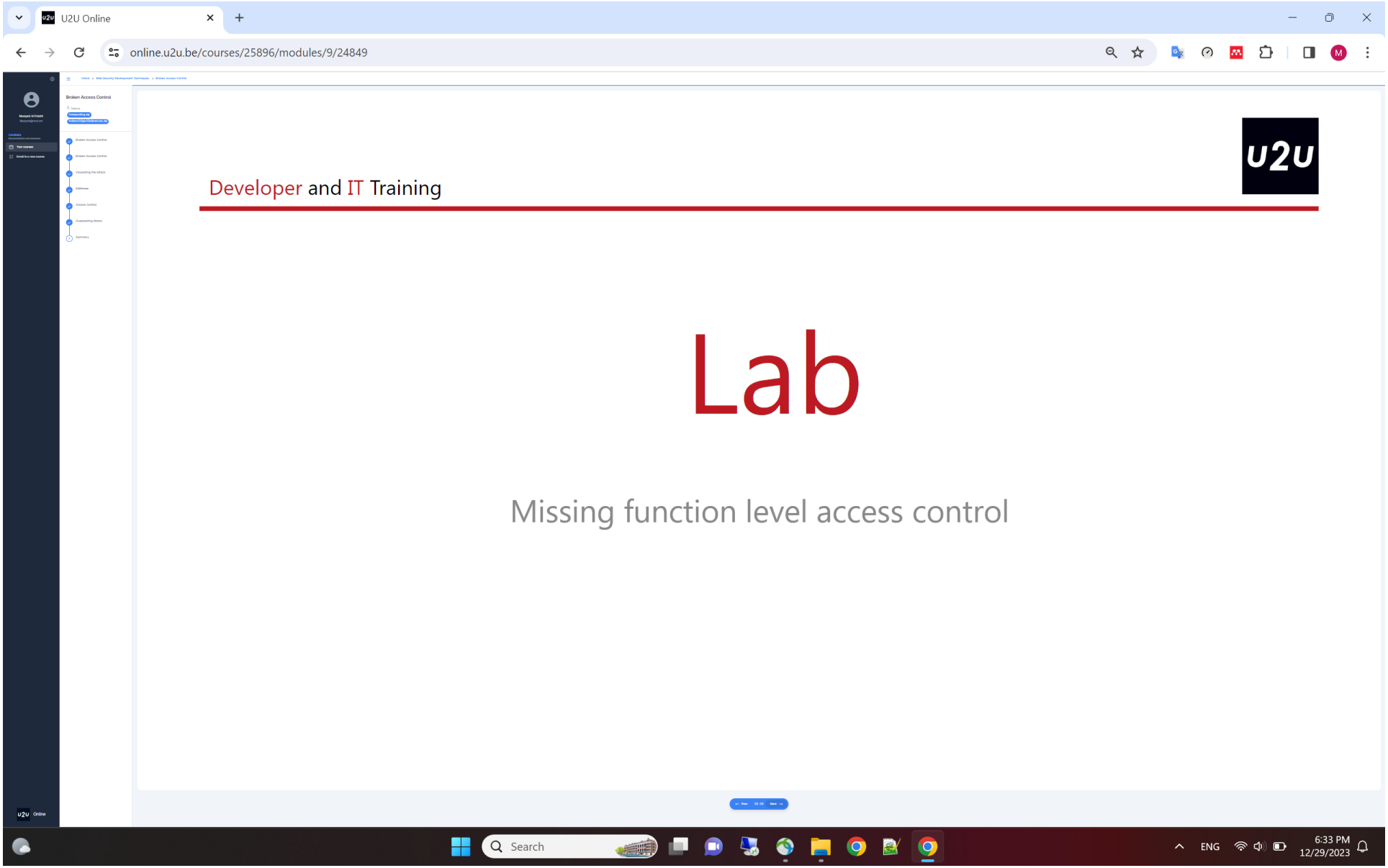

U2U Online
online.u2u.be/courses/25896/modules/9/24849
Broken Access Control
Overposting Attack
U2U
This attack occurs when a user is able to modify a message with extra data to insert data into an application, without the extra data being checked
Example: A user can update its name, but not the admin rights, however by posting extra data to the application, the user CAN change it
Search
ENG
6:33 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/9/24849
Overposting Attack
u2u
Model
public class User
{
public int Id { get; set; }
public string Name { get; set; }
public bool IsAdmin { get; set; }
}
View
<form asp-action="Edit">
<input type="hidden" asp-for="Id" />
<label asp-for="Name" class="control-label"></label>
<input asp-for="Name" class="form-control" />
<input type="submit" value="Save" class="btn btn-default" />
</form>
Search
ENG
6:33 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/9/24849
Overposting Attack
u2u
Controller
public IActionResult Edit(int id)
{
var user = dbContext.Users.FirstOrDefault(u => u.Id == id);
if(user == null) { return NotFound(); }
return View(user);
}
[HttpPost]
public IActionResult Edit(User user)
{
if (!ModelState.IsValid) { return View(user); }
var entry = dbContext.Entry(user);
entry.State = Microsoft.EntityFrameworkCore.EntityState.Modified;
dbContext.SaveChanges();
return RedirectToAction("Index");
}
Search
ENG
6:33 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/9/24849
Broken Access Control
Defenses
u2u
Add Proper Access Control to the Controller method
Add a [Bind("PropertyName")] attribute in front of the Model used in the Controller Action
Use ViewModels (always recommended anyways!)
Search
ENG
6:33 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/9/24849
Summary
u2u
Always implement proper access control
Takes away the biggest risk with direct object references
Indirect references makes it hard to guess other object references
But still is no substitute for proper access control!
Surrogate keys are an alternative
But has more downsides than indirect references
Search
ENG
6:33 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/9/24849
Broken Access Control
Developer and IT Training
u2u
Lab
Missing function level access control
Search
ENG
6:33 PM
12/29/2023