

u2u U2U Online

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

Developer and IT Training

Broken Access Control

OWASP Web Security Threat #1

u2u

The screenshot shows a web browser window titled "U2U Online" with the URL "online.u2u.be/courses/25896/modules/9/24849". The page content is a presentation slide with a dark blue header and footer. The header includes the "u2u" logo, the title "Broken Access Control", and a navigation menu with items like "Home", "About", "Contact", and "Logout". The footer shows system icons for battery, signal, and volume, along with the time "6:33 PM" and date "12/29/2023".

Agenda

- Introduction
- Visualizing the attack
- Defenses
 - Implement proper access control
 - Using indirect maps
- Overposting attack
- Summary

The screenshot shows a web browser window titled "U2U Online" with the URL "online.u2u.be/courses/25896/modules/9/24849". The main content is a slide titled "#1: Broken Access Control" from a course on "Web Security Fundamentals Techniques". The slide lists several points about Broken Access Control:

- 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, ...
- 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

A large watermark or logo for "u2u" is visible in the bottom right corner of the slide content.

u2u U2U Online

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

Home > Web Security Fundamentals Techniques > Broken Access Control

Broken Access Control

Module 9: Broken Access Control

Broken Access Control

Visualizing the attack

Defenses

Attack Goals

Overcoming threats

Summary

Security Matrix

u2u

ATTACK VECTORS	SECURITY WEAKNESS	TECHNICAL IMPACTS
Exploitability	Prevalence	Detectability
AVERAGE	COMMON	AVERAGE
		Impact
		SEVERE

u2u Online

6:33 PM 12/29/2023

U2U Online

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

Home > Web Security Fundamentals Techniques > Broken Access Control

Broken Access Control

Visualizing the attack

Submit

Attack Details

Overcoming attack

Summary

Visualizing the attack

u2u

The diagram illustrates a Broken Access Control attack flow. It shows a user icon interacting with a server stack and a database. A red arrow points from the user to the server, labeled "Manually Change Request". Another red arrow points from the server to the database, labeled "Execute Query based on the URL". A red arrow points back from the database to the server, labeled "Response with unauthorized data".

Manually Change Request

Response with unauthorized data

Execute Query based on the URL

6:33 PM 12/29/2023 ENG

u2u U2U Online

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

Example

No Access Control!

```
<li>@Html.ActionLink("Edit User Details", "Edit", "Users",
    new { id = ViewBag.UserId }, new { })</li>

// 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);
}
```

6

u2u U2U Online

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

Developer and IT Training

u2u

Demo

Insecure Direct Object References

Broken Access Control
Broken Authentication
Broken Session Management
Broken Direct Object References
Broken Cross-Site Scripting
Broken Content Security Policy
Broken Email
Broken Cookies
Overcoming errors
Summary

Developer and IT Training

u2u

Demo

Insecure Direct Object References

u2u Online

6:33 PM 12/29/2023 ENG

U2U Online

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

Real-Life Story

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.

6:33 PM 12/29/2023

u2u U2U Online

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

Real-Life Story

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 government service" says Caroline De Geest of the Privacy Commission. "It's also about judicial data which is extra sensitive."

6:33 PM 12/29/2023

u2u Online

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

Example from real life

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>



6:33 PM 12/29/2023

u2u Online

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

Home > Web Security Fundamentals Techniques > 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)

6:33 PM 12/29/2023

Using Indirect Maps

- 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!

Implementing the Map Properly

- 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

The screenshot shows a web browser window with the URL online.u2u.be/courses/25896/modules/9/24849. The page title is "Surrogate Keys". On the left, there's a sidebar with a navigation tree under "Broken Access Control" and a user profile. The main content area contains the following text:

Surrogate Keys

- 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"**

The bottom of the screen shows a taskbar with various icons and the system tray.

The screenshot shows a web browser window with the URL online.u2u.be/courses/25896/modules/9/24849. The page title is "Access Control". The left sidebar has a navigation tree with nodes like "Broken Access Control", "Broken Access Control", "Visualizing the attack", "Solutions", "Access Control", and "Summary". The right sidebar features a large "u2u" logo. The bottom of the screen shows a Windows taskbar with icons for Start, Search, File Explorer, Task View, Edge, and Google Chrome, along with system status icons.

Access Control

- 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

A screenshot of a web browser window. The title bar says "u2u U2U Online". The address bar shows the URL "online.u2u.be/courses/25896/modules/9/24849". The page content is a course titled "Broken Access Control" from "Developer and IT Training". The main title on the page is "Demo" in large red letters. Below it is the subtitle "Missing Function Level Access Control". The left sidebar shows a navigation menu with "My Courses" and "Courses" sections, and a list of course modules: "Introduction", "Broken Access Control", "Fixing the attack", "Refactor", "Access Control", "Reviewing code", and "Summary". The top right corner features the "u2u" logo. The bottom of the screen shows the Windows taskbar with various pinned icons.

U2U Online

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

Home > Web Security Fundamentals Techniques > Broken Access Control

Broken Access Control

Module 9: Broken Access Control

Broken Access Control

Violating the policy

Summary

u2u

Using MVC's Built-in Access Controls

- 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

6:33 PM 12/29/2023

Developer and IT Training

Demo

Adding Authorization to a MVC web site

Things to Consider

- 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)

U2U Online

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

Home > Web Security Fundamentals Techniques > Broken Access Control

Broken Access Control

- Broken Access Control
- Violating the policy
- Denial
- Abuse
- Overposting attack

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

6:33 PM 12/29/2023

The screenshot shows a web browser window with the URL online.u2u.be/courses/25896/modules/9/24849. The page title is "Overposting Attack". The left sidebar shows a navigation tree under "Broken Access Control". The main content area contains the following text:

Overposting Attack

- 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>
```

The browser's status bar at the bottom right shows the time as 6:33 PM and the date as 12/29/2023.

Overposting Attack

- 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");
}
```

u2u U2U Online

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

Defenses

- 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!)

u2u

The screenshot shows a web browser window with the URL online.u2u.be/courses/25896/modules/9/24849. The page title is "Summary". On the left, there's a sidebar with a navigation tree under "Broken Access Control". The main content area contains the following summary:

- 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

The browser interface includes a search bar, a toolbar with various icons, and a system tray at the bottom showing the date and time (6:33 PM, 12/29/2023).

Developer and IT Training

Lab

Missing function level access control

Broken Access Control

- Broken Access Control
- Broken Access Control
- Violating the object
- Software
- Attack
- Overcoming issues
- Summary

u2u