

u2u U2U Online

online.u2u.be/courses/25896/modules/15/24869

Developer and IT Training

u2u

# Identification and Authentication Failures

## OWASP Web Security Threat #7

25°C Mostly cloudy

Search

1

u2u U2U Online

online.u2u.be/courses/25896/modules/15/24869

Home > Web Security Fundamentals Techniques > Identification and Authentication Attacks

Broken Authentication and Session Management

3. Session

Session Management

Broken Authentication and Session Management

Introduction

Defenses

Password Policies

Summary

# Agenda

---

- Introduction
- Defenses
- Password Policies

u2u

25°C Mostly cloudy

Search

6:46 PM 12/29/2023

## #7: Identification and Authentication Failures

- Authentication and session management not implemented correctly
  - Capture or bypass authentication methods
- Attackers are able to compromise
  - Passwords
  - Keys
  - Session tokens
  - Or other flaws...
- Goal: Impersonate some other user's identity

The screenshot shows a web browser window with the following details:

- Title Bar:** U2U Online
- Address Bar:** online.u2u.be/courses/25896/modules/15/24869
- Page Content:**
  - Section Title:** Not Protecting Authentication Information
  - List:**
    - Unencrypted connections, i.e., not using HTTPS
      - All the information sent can be intercepted
    - Predictable login credentials
    - Session value does not timeout
      - Or does not get invalidated after logout
    - User authentication credentials not protected in storage
    - Session IDs are used in the URL
- Sidebar:** Shows a navigation menu for "Broken Authentication and Session Management" with sections like "Introduction", "Definition", "Session Management", etc.
- Bottom Bar:** Shows system status including weather (25°C, Mostly cloudy), search bar, taskbar icons (File Explorer, Task View, File Explorer, Google Chrome, etc.), and system tray with battery level (6:46 PM, ENG, 12/29/2023).

u2u U2U Online

online.u2u.be/courses/25896/modules/15/24869

Home > Web Security Fundamentals Techniques > Identification and Authentication Issues > Session Management

Broken Authentication and Session Management

2. Session Management

Introduction  
Cookies  
Session Fixation  
Session Hijacking  
Summary

# Security Matrix

u2u

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

25°C Mostly cloudy

Search

6:47 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/15/24869

# Visualizing the Issue

u2u

Request with authentication

Hijacks the request

Request with impersonated identity

25°C Mostly cloudy

Search

6

The screenshot shows a web browser window with the title bar "U2U Online". The address bar contains the URL "online.u2u.be/courses/25896/modules/15/24869". The main content area displays a slide titled "What is Hijacking?". The slide features a bulleted list of attack methods. On the left side of the slide, there is a sidebar with navigation links and a user profile. The bottom of the screen shows a taskbar with various icons and system status indicators.

# What is Hijacking?

- Authentication Cookie gets stolen
  - By using a XSS weakness
  - Reading it from the PC
  - Sniffing it from an insecure connection
- Taking the Session ID (if the Session is used for authentication)
- Account Management System attack
  - Brute force login
  - Using weak credentials like 4 number PIN
  - Password reset exploit (e.g. Security question)

25°C Mostly cloudy 6:47 PM 12/29/2023

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/15/24869](https://online.u2u.be/courses/25896/modules/15/24869). The page title is "Defenses". On the left, there's a sidebar with navigation links like "Introduction", "Cookies", "Session", and "Summary". On the right, there's a large "u2u" logo. The main content area contains a bulleted list of security measures:

- Protect your cookies
  - Use the **HttpOnly** flag
  - Mark the cookie as **Secure**
- Decrease attack window
  - Tradeoff between quick expiration and user friendliness
  - Challenge the user for impacting commands (e.g., Validating a bank transfer)
- Account Management Improvements
  - Lockout policy and Login Rate limit
  - Use Strong passwords
  - Allow Multi-Factor Authentication

At the bottom of the screen, there's a taskbar with icons for weather (25°C, Mostly cloudy), search, file explorer, and browser windows. The system tray shows the date and time (6:47 PM, 12/29/2023) and battery status.

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/15/24869](https://online.u2u.be/courses/25896/modules/15/24869). The page title is "Protecting your Cookies". On the left, there's a sidebar with navigation links like "My profile", "Your courses", and "Logout". The main content area contains a bulleted list and some code snippets.

# Protecting your Cookies

- By setting the HttpOnly flag you prevent JavaScript from reading that cookie
  - Excellent way to protect against cookie theft
- Two ways to do this
  - In web.config
  - In code

```
<system.web>
    <httpCookies httpOnlyCookies="true"/>
```

```
var cookie = new HttpCookie("name", "value");
cookie.HttpOnly = true;
```

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/15/24869](https://online.u2u.be/courses/25896/modules/15/24869). The page title is "Protecting your Cookies". The left sidebar shows a navigation menu with sections like "Introduction", "Cookies", "Session Management", and "Summary". The main content area contains a bulleted list and code snippets. The bottom of the screen shows a taskbar with various icons and system status.

# Protecting your Cookies

- By setting the Secure flag the cookie can only be used in HTTPS sessions
  - Prevents against accidental transfer over HTTP
- Again, you can do this from
  - Web.config
  - Code

```
<system.web>
    <httpCookies requireSSL="true"/>
```

```
var cookie = new HttpCookie("name", "value");
cookie.Secure = true;
```

The screenshot shows a Microsoft Edge browser window with the following details:

- Title Bar:** U2U Online
- Address Bar:** online.u2u.be/courses/25896/modules/15/24869
- Page Content:**
  - Section Header:** Protecting your Cookies
  - List:**
    - In ASP.NET Core, there are no default settings for cookies
    - Use CookieOptions to set flags
      - In your controller
      - In middleware
  - Code Example:**

```
var options = new CookieOptions {
    HttpOnly = true,
    Secure = true,
    MaxAge = TimeSpan.FromMinutes(20),
};
Response.Cookies.Append("u2u", "secret", options);
```
- Bottom Taskbar:**
  - Weather: 25°C Mostly cloudy
  - Search bar
  - Icons for File Explorer, Task View, Taskbar settings, and Google Chrome
  - System tray icons: battery, signal, volume, and date/time (12/29/2023)

u2u U2U Online

online.u2u.be/courses/25896/modules/15/24869

Developer and IT Training

**u2u**

# Demo

Protecting your cookies

25°C Mostly cloudy

Search

6:47 PM 12/29/2023

u2u Online

The screenshot shows a web browser window with the following details:

- Title Bar:** U2U Online
- Address Bar:** online.u2u.be/courses/25896/modules/15/24869
- Page Content:**
  - Section Title:** URL Weaknesses
  - List:**
    - URLs can easily be shared (and thus stolen)
    - URLs are frequently logged
      - In proxies and web logs
      - And logs are not always protected properly!
    - URLs can be retrieved from the browser history
    - Never store anything confidential in the URL!
      - Remember Membership's Cookieless mode?

The browser interface includes a sidebar with user information (Maged Al-Khatib, MagedAlKhatib@gmail.com), a navigation menu for the course, and a bottom taskbar with various icons and system status.

The screenshot shows a web browser window with the following details:

- Title Bar:** U2U Online
- Address Bar:** online.u2u.be/courses/25896/modules/15/24869
- Page Content:**
  - Section Header:** Configuring Session and Auth Cookies
  - List Item:** Decrease the attack window by limiting validity of these cookies
    - Tradeoff between convenience and security
  - Code Snippet:** <sessionState timeout="20" />
  - List Item:** You can also change the cookiename (not to reveal using ASP.NET)
  - Code Snippet:** <sessionState cookieName="MySession" timeout="20" />
- Sidebar:** Shows a navigation menu for "Broken Authentication and Session Management" with sections like "Introduction", "Cookies", "Cookies", "Cookies", and "Summary".
- Bottom Bar:** Shows weather (25°C, Mostly cloudy), search bar, taskbar icons (File Explorer, Task View, File Manager, Google Chrome, etc.), and system status (6:47 PM, ENG, battery, 12/29/2023).

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/15/24869](https://online.u2u.be/courses/25896/modules/15/24869). The page title is "Enforce Strong Passwords". The left sidebar shows a navigation tree under "Broken Authentication and Session Management". The main content area contains a bulleted list of recommendations:

- Don't use passwords, use **passphrases**!
  - A good minimal length today is 20 characters
    - Because humans are very bad at generating “random” passwords
  - For practical purposes enforce at least 8 characters (see NIST guidelines)
- Encourage people to use a **password manager**
  - Avoid using the same password for more than one site (who's not guilty of this!?)
  - Generate real random passwords of sufficient length
- Activate Multi-Factor Authentication
  - Note that SMS services are not considered best practice anymore!

The browser taskbar at the bottom shows the date and time as 12/29/2023, 6:47 PM. The system tray icons include a weather forecast (25°C, Mostly cloudy), a search bar, and various application icons.

u2u U2U Online

online.u2u.be/courses/25896/modules/15/24869

Home > Web Security Fundamentals Techniques > Identification and Authentication Patterns

Broken Authentication and Session Management

3. Session Management

Introduction

Defense

Penetration Testing

Summary

# Checking Password Strength

u2u

- What makes a password strong?
  - Depends on who is talking (problem is the human factor again)
- Don't
  - Limit the length of a password (longer passwords are always better!)
    - A limit to a password length is a **security smell!**
  - Force people to embed special characters (they will substitute things like 'a' with '@')
  - Allow known words (but how do you check against different languages?!)
    - But do check against things like password, 123456, etc.
    - There are known online repositories for helping with this

I changed all my passwords to "incorrect".

So whenever I forget, it will tell me "Your password is incorrect."

25°C Mostly cloudy

Search

6:47 PM 12/29/2023

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/15/24869](https://online.u2u.be/courses/25896/modules/15/24869). The page title is "Summary". On the left, there's a sidebar with a user profile and a navigation menu for the course "Broken Authentication and Session Management". The main content area contains a large heading "Summary" and a bulleted list of best practices:

- Avoid building your own authentication mechanism
  - It is very easy to get this wrong!
- Never store secrets such as session IDs in the URL
- Protect your cookies
  - HttpOnly and Secure
- Timeout your sessions
- Apply strong password policies
  - And never restrict passwords in length

The browser interface includes a top bar with tabs, a search bar, and various icons. At the bottom, there's a taskbar showing the weather (25°C, Mostly cloudy), system icons (Search, File Explorer, Task View, Edge, Google Chrome), and system status (6:47 PM, ENG, battery level, 12/29/2023).