

U2U Online

online.u2u.be/courses/25896/modules/12/24862

Developer and IT Training

U2U

Insecure Design

OWASP Web Security Threat #4

25°C Mostly cloudy

Search

6:40 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/12/24862

Agenda

- Introduction
- Defenses
- Password Policies

u2u

25°C Mostly cloudy

Search

6:40 PM 12/29/2023

The screenshot shows a web browser window with the address bar displaying 'online.u2u.be/courses/25896/modules/12/24862'. The page content is a slide titled '#4: Insecure Design' with the U2U logo in the top right corner. The slide lists two main bullet points: 'What is Insecure design?' and 'How does this happen?'. The first bullet point has two sub-points: 'Risks related to design and architectural flaws' and 'Expressed as **missing** or **ineffective** control design'. The second bullet point has three sub-points: 'Missing domain logic', 'Missing checks for edge cases', and 'Complex interactions between systems could be exploited'. The browser's taskbar at the bottom shows the Windows logo, a search bar, and various application icons. The system tray on the right indicates the date and time as 6:40 PM on 12/29/2023.

U2U Online

online.u2u.be/courses/25896/modules/12/24862

#4: Insecure Design

- What is Insecure design?
 - Risks related to design and architectural flaws
 - Expressed as **missing** or **ineffective** control design
- How does this happen?
 - Missing domain logic
 - Missing checks for edge cases
 - Complex interactions between systems could be exploited

25°C Mostly cloudy

Search

6:40 PM 12/29/2023

The screenshot shows a web browser window with the address bar displaying 'online.u2u.be/courses/25896/modules/12/24862'. The page title is 'Missing Control Design'. The U2U logo is in the top right corner. A sidebar on the left contains a navigation menu with items like 'Introduction', 'Guidelines', and 'Summary'. The main content area features a list of bullet points and a code snippet.

Missing Control Design

- Mechanisms that were supposed to be put in place but were forgotten or omitted for whatever reason
- Example: Sensitive data was supposed to be encrypted for transmission, but the encryption method was never implemented or applied.

```
public Byte[] EncryptSensitiveData(string data)
{
    //TODO: We'll implement this when we feel like it
}
```

The bottom of the image shows a Windows taskbar with the date and time '6:40 PM 12/29/2023' and system status icons.

U2U Online

online.u2u.be/courses/25896/modules/12/24862

U2U

Ineffective Control Design

- Mechanisms that allow for an attack to happen because of insufficient checks
- Example: a method is supposed to update an account owner's balance after withdrawing money, but it doesn't check the sign of the amount that is being withdrawn

```
public void Withdraw(decimal amount)
{
    this.balance -= amount;
}
```

Withdraw Euro

Balance: € 43.54

Amount: -1000 EUR

25°C Mostly cloudy


Search

6:40 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/12/24862

Security Matrix



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

25°C Mostly cloudy

Search


6:40 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/12/24862

Example Scenarios

- New video card or gaming console is released
- E-commerce sites allow botnets to buy all available units
- Scalpers use these botnets to create scarcity and drive up price
- Both hardware manufacturer and e-commerce site suffer terrible publicity



25°C Mostly cloudy

Search

6:40 PM 12/29/2023

The screenshot shows a web browser window with the address bar displaying 'online.u2u.be/courses/25896/modules/12/24862'. The browser's address bar and tabs are visible at the top. The slide content is displayed in a large white area. On the left side of the slide, there is a dark blue sidebar with a user profile icon and a list of course modules. The slide title 'How To Prevent?' is in a large, bold, black font, followed by a red horizontal line. Below the title, the text 'E-commerce site could have implemented anti-botnet measures' is displayed. Underneath this text is a bulleted list with three items: 'Strong Captcha', 'IP blocking', and 'Limiting the amount of units that can be bought in one purchase'. The U2U logo is in the top right corner of the slide. The Windows taskbar is visible at the bottom of the screen, showing the search bar, task view button, and several application icons. The system tray on the right shows the date and time as 6:40 PM on 12/29/2023.

U2U Online

online.u2u.be/courses/25896/modules/12/24862

How To Prevent?

E-commerce site could have implemented anti-botnet measures

- Strong Captcha
- IP blocking
- Limiting the amount of units that can be bought in one purchase

U2U

25°C Mostly cloudy


Search


6:40 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/12/24862

Example Scenarios





We can try to verify your identity using your secret questions

When you set up your Yahoo account, you selected and answered two secret questions.
Answer both questions correctly to access your account.

Question 1 of 2

What is the first name of your oldest niece?

Last updated June 09, 2010

25°C Mostly cloudy

Search

6:40 PM 12/29/2023

The image is a screenshot of a web browser displaying a U2U Online course. The browser's address bar shows the URL `online.u2u.be/courses/25896/modules/12/24862`. The slide content is titled "How to Prevent?" and features a list of security recommendations. The U2U logo is in the top right corner of the slide. The browser's taskbar at the bottom shows the Windows Start button, a search bar, and various application icons. The system tray indicates a temperature of 25°C, mostly cloudy weather, and the time 6:40 PM on 12/29/2023.

How to Prevent?

- Don't use security questions!
 - Questions don't prove identity since more than one person can know the answer
- Safer alternatives
 - URL Tokens (sent via email)
 - PINs (sent via side-channel like SMS)
 - Offline backup codes (like a PUK code for your SIM card)
- *Note: Using multiple mechanisms in series can significantly improve security in these types of situations*

The image is a screenshot of a web browser displaying a U2U Online course. The browser's address bar shows the URL `online.u2u.be/courses/25896/modules/12/24862`. The course content is a slide titled "How to Prevent" with the U2U logo in the top right corner. The slide lists four bullet points regarding secure development practices. The browser's taskbar at the bottom shows the Windows logo, a search bar, and various application icons. The system tray indicates a temperature of 25°C, mostly cloudy weather, and the time 6:40 PM on 12/29/2023.

U2U Online

online.u2u.be/courses/25896/modules/12/24862

How to Prevent

- Establish and use a secure development lifecycle with AppSec professionals to help evaluate and design security and privacy-related controls
- Establish and use a library of secure design patterns or paved road ready to use components
- Use threat modeling for critical authentication, access control, business logic, and key flows
- Write unit and integration tests to validate that all critical flows are resistant to the threat model

25°C Mostly cloudy

6:40 PM 12/29/2023

The screenshot shows a web browser window with the address bar displaying `online.u2u.be/courses/25896/modules/12/24862`. The page content includes a sidebar on the left with a navigation menu containing 'Introduction', 'Courses', and 'Summary'. The main content area features the title 'Summary' in a large font, followed by a red horizontal line. Below the line, the text reads: 'Security isn't something you can think about after you build an application, it should be incorporated in every aspect and mainly the design.' The U2U logo is visible in the top right corner of the content area. The browser's address bar and various extension icons are visible at the top. The Windows taskbar at the bottom shows the date and time as 6:40 PM on 12/29/2023, along with weather information (25°C, Mostly cloudy) and several application icons.

U2U Online

online.u2u.be/courses/25896/modules/12/24862

Summary

Security isn't something you can think about after you build an application, it should be incorporated in every aspect and mainly the design.

U2U

25°C Mostly cloudy

Search

6:40 PM 12/29/2023