

u2u U2U Online

online.u2u.be/courses/25896/modules/8/24848

Web Security Threats

Developer and IT Training

OWASP Security Top 10 Threats

26°C Mostly sunny

Search

1

3:24 PM 12/29/2023

u2u U2U Online

online.u2u.be/courses/25896/modules/8/24848

Web Security Threats

OWASP

Broken Access Control

Cryptographic Failures

Injection

Insecure Design

Security Misconfiguration

Vulnerable and Outdated Components

Identification and Authentication Failures

Software and Data Integrity Failures

Security Logging and Monitoring Failures

Server-Side Request Forgery

OWASP Juice Shop

Denial-of-Service

Agenda

u2u

26°C Mostly sunny

Search

3:24 PM

u2u U2U Online

online.u2u.be/courses/25896/modules/8/24848

Web Security Threats

What is OWASP?

u2u

- The Open Web Application Security Project
  - Publishes a top 10 security issues every couple of years
- Open community dedicated to help organizations
  - Non-profit organization
  - Technology agnostic
- OWASP publishes free and open
  - Application security tools
  - Complete books on security testing, development, ...
  - Cutting edge research
  - ...
- <https://www.owasp.org>



26°C Mostly sunny

Search

3:24 PM

u2u U2U Online

online.u2u.be/courses/25896/modules/8/24848

Web Security Threats

Top 10 OWASP Security Issues

u2u

- First Released in 2003
  - Updates in 2003, 2004, 2007, 2010, 2013, 2017 and 2021
- Goals
  - Raise awareness about application security
  - Identify some of the most critical risks facing organizations

**OWASP Top 10**  
The Ten Most Critical Web Application Security Risks



26°C Mostly sunny

Search

3:24 PM 12/29/2023

u2u U2U Online

online.u2u.be/courses/25896/modules/8/24848

# OWASP Top 10 2017 vs 2021

u2u

2017

A01:2017-Injection  
A02:2017-Broken Authentication  
A03:2017-Sensitive Data Exposure  
A04:2017-XML External Entities (XXE)  
A05:2017-Broken Access Control  
A06:2017-Security Misconfiguration  
A07:2017-Cross-Site Scripting (XSS)  
A08:2017-Insecure Deserialization  
A09:2017-Using Components with Known Vulnerabilities  
A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control  
A02:2021-Cryptographic Failures  
A03:2021-Injection  
A04:2021-Insecure Design  
A05:2021-Security Misconfiguration  
A06:2021-Vulnerable and Outdated Components  
A07:2021-Identification and Authentication Failures  
A08:2021-Software and Data Integrity Failures  
A09:2021-Security Logging and Monitoring Failures\*  
A10:2021-Server-Side Request Forgery (SSRF)\*

(New)

\* From the Survey

26°C Mostly sunny

Search

3:24 PM

u2u U2U Online

online.u2u.be/courses/25896/modules/8/24848

How We Will Discuss Each Risk **u2u**

Overview of the risk

Understanding the risk

Defenses

Real-life examples

26°C Mostly sunny

Search

3:24 PM 12/29/2023

The screenshot shows a web browser window titled "U2U Online" with the URL "online.u2u.be/courses/25896/modules/8/24848". The page displays a list of "Current Top 10" security threats, which includes:

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery
- **Bonus: Denial-of-Service**

The browser interface includes a sidebar with user information (Maged Al-Hajri, Maged@Gmail.com) and navigation links (Web Security Threats, Overview, Checklist, Issues, Details, Summary). The bottom of the screen shows a taskbar with various icons and system status indicators.

u2u U2U Online

online.u2u.be/courses/25896/modules/8/24848

Web Security Techniques > Critical Security Top 10 Threats

Web Security Threats

- Web Security Threats
- Cross-Site Scripting (XSS)
- Cross-Site Scripting (XSS) - DOM
- SQLi
- CSRF

u2u

# Security In Depth Principle

Treasure

26°C Mostly sunny

Search

3:24 PM 12/29/2023

u2u U2U Online

online.u2u.be/courses/25896/modules/8/24848

Web Security Techniques > OWASP Juice Shop

# OWASP Juice Shop

u2u

- Demo application containing tons of vulnerabilities
- Notifies you when you solved a challenge and keeps track on a scoreboard

The diagram illustrates the architecture of the OWASP Juice Shop application. It is divided into three main components: Browser, Server, and File System.

- Browser:** Contains a Google icon and a Frontend section with Angular (A) and Material (IUP) components. A dashed arrow labeled "OAuth 2.0" points from the Google icon to the Frontend.
- Server:** Contains a Node.js logo and an express component. It also includes Sequelize (blue cube) and finale-rest (blue box) components. A dashed arrow labeled "socket.io" points from the Frontend to the Server. Another dashed arrow labeled "NoSQL" points from the Server to a red circle labeled "DB".
- File System:** Contains a Content Folder (grey folder icon) and an SQLite database (blue cylinder with a pen icon).

Dashed arrows indicate communication between the Frontend and Server, and between the Server and Database. The Server also has a "Dynamic API" connection to the SQLite database.

26°C Mostly sunny 3:24 PM ENG 12/29/2023

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/8/24848](https://online.u2u.be/courses/25896/modules/8/24848). The page title is "#11: DDoS?". The content area contains the following list:

- **Distributed Denial of Service**
  - An attack used to deny usage of a certain service (website, webservice, app,...)
- **Botnets are most commonly used for DDoS**
  - Compromised machines will send requests at will to a target
- Attacks can range from very small to 1100 Gbps and upwards

The browser interface includes a sidebar with user information (u2u Online), a navigation bar with back, forward, search, and refresh buttons, and a status bar at the bottom showing weather (26°C, Mostly sunny), system icons (battery, signal, volume), and the date/time (3:24 PM, 12/29/2023).

u2u U2U Online

online.u2u.be/courses/25896/modules/8/24848

Web Security Threats

- Web Security Trends
- OWASP
- CWE/CSS
- XSS
- Summary

# Security Matrix

u2u

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

26°C Mostly sunny

Search

3:24 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/8/24848

DoS attack

u2u

Attack this website!

HELP!

target.website.org

Could you give me resource x?  
Could you give me resource x?  
Could you give me resource x?

26°C  
Mostly sunny

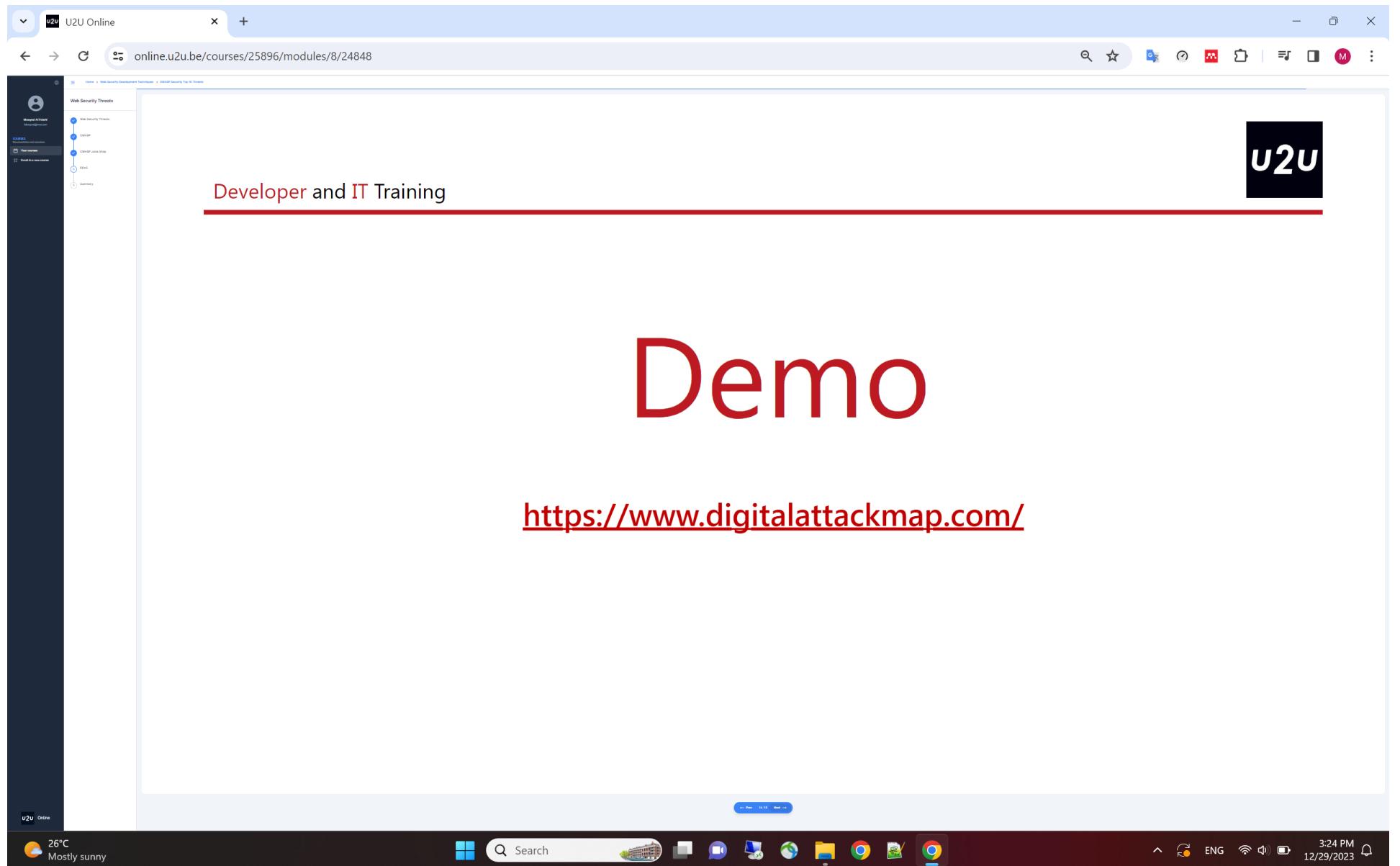
Search

3:24 PM

The screenshot shows a web browser window with the URL [online.u2u.be/courses/25896/modules/8/24848](https://online.u2u.be/courses/25896/modules/8/24848). The page title is "Defenses?". The left sidebar shows a navigation menu with "Web Security Threats" selected. The main content area contains a list of mitigation strategies:

- This one is very hard to protect against!
- Ask your administrators to help block IP-ranges that are potentially bad
- Use Automated Mitigation tools
  - Do blocking and control the flow for you
- Use a Third-Party Provider that helps you
  - Cloudflare, Akamai, ...

The browser interface includes a search bar, a toolbar with various icons, and a system tray at the bottom showing weather (26°C, Mostly sunny), a date (12/29/2023), and a time (3:24 PM).



The screenshot shows a web browser window with the title bar "u2u U2U Online". The address bar contains the URL "online.u2u.be/courses/25896/modules/8/24848". The main content area displays a course summary titled "Summary". On the left, there's a sidebar with a user profile picture and the name "Maarten Klaasen". Below the profile is a navigation menu with items like "Your courses" and "Send this course invite". A vertical sidebar on the left lists "Web Security Threats" with categories: "OWASP", "Broken Access Control", "Cryptographic Failures", "Injection", "Insecure Design", "Security Misconfiguration", "Vulnerable and Outdated Components", "Identification and Authentication Failures", "Software and Data Integrity Failures", "Security Logging and Monitoring Failures", "Server-Side Request Forgery", and "Denial-of-Service". The right side of the screen features a large "u2u" logo. At the bottom, there's a taskbar showing the date and time (3:24 PM, 12/29/2023), weather (26°C, Mostly sunny), and various system icons.

# Summary

---

- OWASP
- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery
- Denial-of-Service