

u2u U2U Online

online.u2u.be/courses/25896/modules/1/24839

Web Security Development Techniques

Developer and IT Training

u2u

Web Security Development Techniques

For Developers



26°C Mostly sunny

Search

1

u2u U2U Online

online.u2u.be/courses/25896/modules/1/24839

Web Security Development Techniques

u2u

Agenda

- Web Security Development Techniques
- Security, a many pronged word
- Defense in Depth
- Testing (hopefully) secure applications
- Bug Bounties and Code Reviews
- The Ten Immutable Laws of Security

26°C Mostly sunny

Search

3:05 PM 12/29/2023

The screenshot shows a web browser window titled "U2U Online" with the URL "online.u2u.be/courses/25896/modules/1/24839". The main content area displays a slide titled "Current OWASP Top 10" with a red horizontal line below it. To the right of the title is a large "u2u" logo. On the left, there is a sidebar with a user profile and a navigation menu. The main content area contains a bulleted list of ten security vulnerabilities. At the bottom of the screen, there is a taskbar with various icons and a system tray showing the date and time.

Current OWASP Top 10

- 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- Vulnerable and Outdated Components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

26°C Mostly sunny 3:05 PM 12/29/2023

u2u Online

online.u2u.be/courses/25896/modules/1/24839

Web Security Development Techniques

Mengel Ariswandi
Mengel@u2u.be

COURSES

My courses

Create new course

Web Security Development Techniques

State Security Development Techniques

Web Security

Identity - A never ending quest

Refactor in Depth

Building (RESTful) services

Microservices

My favorite code review

Java security best practices

Java security code review

Types of hackers

- Script Kiddies
 - No hacking skills
 - Run scripts downloaded from internet
 - In it for the fun of it
- Hacktivist (Anonymous, LulzSec)
 - Varying degrees of skills
 - Politically motivated
- Cyber Criminals
 - For gain \$\$\$, €€€, ¥¥¥, ₩₩₩
 - Ransomware
- Cyber warfare
 - Government funded
 - Presidential election 2016 ☺



Search

26°C Mostly sunny

ENG ENG

3:05 PM 12/29/2023

The screenshot shows a web browser window with the URL online.u2u.be/courses/25896/modules/1/24839. The page title is "Security, a many pronged word". On the left, there's a sidebar with a user profile and a navigation tree under "Web Security Development Techniques". The main content area contains a bulleted list about the多义性 of security. The browser has a standard toolbar at the top and a taskbar at the bottom showing weather, search, and system icons.

Security, a many pronged word

- Security has a lot of overloaded meanings
 - Non-disclosure
 - Making sure that your secrets cannot be read by another party, secure communication
 - Authentication
 - Who is the current user?
 - Authorization
 - What can the authenticated user do?
 - Data-tampering
 - Ensuring that data cannot be modified by non-privileged users

The screenshot shows a web browser window with the URL online.u2u.be/courses/25896/modules/1/24839. The page title is "The STRIDE Security model". The left sidebar shows a navigation tree under "Web Security Development Techniques" with nodes like "Web Security", "Security of every present asset", "Defense in Depth", "Testing (Inspection) review", and "Bug Bounties and Code Review". The right sidebar has a "u2u" logo. The bottom taskbar shows the weather (26°C, Mostly sunny), a search bar, and various application icons.

The STRIDE Security model

- **S**poofing identity
 - Using another user's authentication information
- **T**ampering with data
 - Unauthorized changes to persistent data, such as database, audit logs
- **R**epudiation
 - Users who deny performing a certain action
- **I**nformation disclosure
 - Exposure of data to individuals who are not supposed to have access to it
- **D**enial of service
 - Making a web server unavailable or unusable
- **E**levation of Privilege
 - Unprivileged user gains privileged access

The screenshot shows a web browser window with the URL online.u2u.be/courses/25896/modules/1/24839. The main content area displays a slide titled "Mitigation Techniques" with a list of seven bullet points. The sidebar on the left shows a user profile and a navigation menu. The bottom of the screen shows a taskbar with various icons and system status.

Mitigation Techniques

- Apply good access control
- Run with least privilege
- Use cryptography
- Don't store secrets
- Validate data, internal and external
- Don't tell the attacker anything

26°C Mostly sunny 3:06 PM 12/29/2023

The screenshot shows a web browser window with the URL online.u2u.be/courses/25896/modules/1/24839. The page title is "Security Through Obscurity". On the left, there's a sidebar with user information and a navigation tree for "Web Security Development Techniques". A large red horizontal bar spans the width of the slide. On the right, there's a "u2u" logo. Below the title, there are two lists of bullet points. The first list discusses the concept of security through obscurity. The second list provides historical context, mentioning Auguste Kerckhoffs and his principle.

Security Through Obscurity

- Believing that if the flaws are not known, that will be sufficient to prevent a successful attack.

"Rogues are very keen in their profession, and know already much more than we can teach them."

- Auguste Kerckhoffs already wrote about this in 1883
 - Kerckhoffs principle: *A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.*

26°C Mostly sunny 3:06 PM 12/29/2023

The image shows a screenshot of a web browser window. The URL bar at the top displays "online.u2u.be/courses/25896/modules/1/24839". The main content area of the browser shows an aerial photograph of Caerphilly Castle, a massive medieval castle with extensive earthworks and a double-motte design. The castle is surrounded by a moat and features multiple concentric walls and towers. The surrounding landscape includes green fields, a road, and some modern buildings. On the far right of the browser window, there is a black vertical bar with the white text "u2u" in a bold, sans-serif font. The overall layout suggests a learning platform or course page.

u2u U2U Online

online.u2u.be/courses/25896/modules/1/24839

Web Security Development Techniques

u2u

Defense in depth

- Medieval castles applied this principle
- Defend a system against any particular attack using several independent methods
 - Multi-factor authentication
 - Firewalls
 - Encryption and hashing
 - Logging and auditing
 - ...

26°C Mostly sunny

Search

3:06 PM 12/29/2023

u2u U2U Online

online.u2u.be/courses/25896/modules/1/24839

Testing (hopefully) secure applications

- Security testing is different
 - You will see if the user can spoof another user's identity
 - That the user cannot tamper with data
 - ... STRIDE ...
- Think of security as a product feature
 - Who wants to use an insecure product anyway?

26°C Mostly sunny

Search

3:06 PM 12/29/2023

Role playing Marge, Homer and Bart

- You need to **assume three roles** while testing



Marge is the user who does her job correctly and uses the system for its intended purposes



Homer is the user who fills in data you would never suspect out of laziness/stupidity



Bart is the user who tries to exploit the system, either out of plain evilness, or for gain

26°C Mostly sunny

Search

3:06 PM

Building the test plan

- Decompose the application into its components
- Identify component interfaces
 - HTTP requests, configuration, database access, files, LDAP
- Rank interfaces by their relative vulnerability
 - Prioritize which interfaces to test first
- Find security problems by injecting faulty data
 - Data that is of the wrong type, length, contents, special cases

Almost free testing, use a bounty plan

- Offer people prices for finding security problems in your application
 - And give them credit, ethical hackers like publicity!

APPLE'S FINALLY OFFERING BUG BOUNTIES—WITH THE HIGHEST REWARDS EVER

Microsoft Launches Office Insider Program Bug Bounty

Office Insider Program members can now receive rewards of between \$500 and \$15,000 for finding vulnerabilities in the Microsoft Office suite.

Code Reviews

- Code reviews help expose problems
 - Especially in rarely executed code
- Search for dangerous APIs
 - Automated code reviews are very good at this

u2u U2U Online

online.u2u.be/courses/25896/modules/1/24839

Web Security Development Techniques

Module 1: Web Security Development Techniques

1. Web Security Fundamentals

2. Web Security Development

3. Web Security

4. Security: A very popular word

5. OWASP's 10

6. Testing: Inspect, review, understand

7. Bug Bounties and Code Review

8. The Ten Immutable Laws of Security

The Ten Immutable Laws of Security

■ Break any of these laws and you will be pwned!

CATS: ALL YOUR BASE ARE BELONG
TO US.

26°C Mostly sunny

Search

3:06 PM 12/29/2023

u2u U2U Online

online.u2u.be/courses/25896/modules/1/24839

#1

**If a bad person can persuade you to run a program on your computer,
it's not your computer anymore!**

- A program running on your computer can do a lot of things
 - Install a virus (even ransomware), or a backdoor
 - Send rude messages
 - Install a keylogger
 - ...
- Never run (or even download) a program from an untrusted source!



26°C Mostly sunny

Search

3:06 PM 12/29/2023

#2

**If a bad person can alter the operating system on your computer,
it's not your computer anymore!**

- Make sure the operating system files are well protected
 - Don't run as an Administrator all the time

26°C Mostly sunny

Search

3:06 PM 12/29/2023

#3

**If a bad person has unrestricted physical access to your computer,
it's not your computer anymore!**

- Physical access can result in all kinds of damage
 - Unplug your computer
 - Replace the BIOS chip, or replace the hard drive
 - Install extensions (<https://hakshop.com/>)
- Always protect a computer proportionate to its value
 - Don't put your server beneath someone's desk!
 - Encrypt the file system on your laptop

26°C Mostly sunny

Search

3:06 PM 12/29/2023

#4

**If you allow a bad person to upload programs to your website,
it's not your website anymore!**

- If you run a website, you need to limit what users can do
- Only run code on your website you can trust
 - Written by you, or someone you trust

u2u Online

26°C Mostly sunny

Search

3:06 PM 12/29/2023

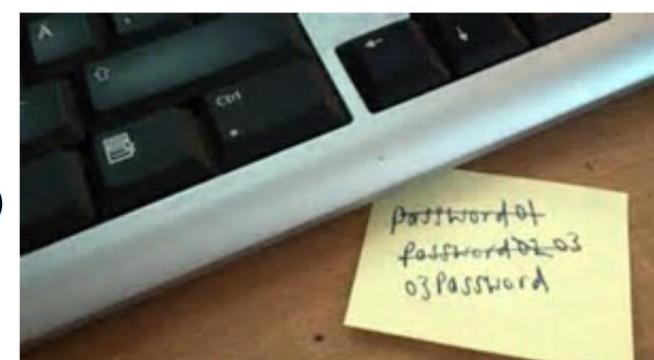
u2u U2U Online

online.u2u.be/courses/25896/modules/1/24839

#5

Weak passwords trump strong security

- Any bad person who gets your password can do anything you can
 - And it will be in your name!
- Always use strong passwords that are complex
 - And have a different password for each account
 - Use a password manager to help with this
 - Don't write it down!
 - [http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf\(ch 5.1.1\)](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf(ch 5.1.1))



26°C Mostly sunny

Search

3:06 PM 12/29/2023

#6

A machine is only as secure as the administrator is trustworthy

- Administrators have a lot of power on a machine
- When hiring system administrators, check their references
 - Do a background check
- Take steps to keep honest people honest
 - Keep logs of who enters/leaves the server room
 - Implement a two-person rule
 - Don't use the built-in Administrator account, give each admin their own account
 - Store audit data on WORM (Write Once Read Many) devices

26°C Mostly sunny

Search

3:06 PM

u2u U2U Online

online.u2u.be/courses/25896/modules/1/24839

#7

Encrypted data is only as secure as the decryption key

- Use offline storage for keys
 - Passwords used to generate keys should be very strong!
- Don't put the key under the doormat ☺



26°C Mostly sunny

Search

3:06 PM 12/29/2023

#8

An out-of-date virus scanner is only marginally better than no virus scanner

- Keep anti-virus software up-to-date!
 - Update virus definition files
 - But also the virus scanner itself!

u2u Online

26°C Mostly sunny

Search

3:06 PM 12/29/2023

#9

Absolute anonymity isn't practical, in real life or on the web

- People can learn a lot about you from discussions in real life.
 - Your accent will reveal where you are from
- Same thing on the internet
 - Your IP-address will reveal where you are from
 - Google can deduce a lot from how you search

u2u Online

26°C Mostly sunny

Search

3:06 PM 12/29/2023

u2u U2U Online

online.u2u.be/courses/25896/modules/1/24839

#10

Technology is not a panacea

- Technology does not offer a risk-free world
 - Perfect security does not exist
 - All software has bugs
- Sometimes hackers will fall back on social engineering



SOCIAL ENGINEERING SPECIALIST
Because there is no patch for
human stupidity

26°C Mostly sunny

Search

3:06 PM 12/29/2023