

U2U Online

online.u2u.be/courses/25896/modules/16/24871

Developer and IT Training

U2U

Software and Data Integrity Failures

OWASP Web Security Threat #8

25°C Mostly cloudy

Search

6:48 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/16/24871

Software and Data Integrity Failures

Agenda

- Software and Data Integrity Failures
- Defenses
- Famous Examples

u2u

25°C Mostly cloudy

Search

6:48 PM 12/29/2023

The image is a screenshot of a web browser displaying a U2U Online course slide. The browser's address bar shows the URL `online.u2u.be/courses/25896/modules/16/24871`. The slide itself has a dark blue sidebar on the left with a navigation menu. The main content area is white and features the title **#8: Software and Data Integrity Failures** in a large black font, followed by a red horizontal line. Below the title is a bulleted list of three points. The U2U logo is in the top right corner of the slide. The bottom of the image shows a Windows taskbar with various icons and system information.

U2U Online

online.u2u.be/courses/25896/modules/16/24871

#8: Software and Data Integrity Failures

- Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations
- Often, assumptions are made related to software updates, critical data, and CI/CD pipelines without verifying integrity
- This can lead to downloading and running malicious code, tampering with sensitive data, massive distribution of spyware,...

25°C Mostly cloudy

6:48 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/16/24871

Visualizing an Attack

Let's look for vulnerabilities

I use a vulnerable cookie/header/...

Let's modify that data and try to gain access

vulnerable.website.org

25°C Mostly cloudy

Search

6:48 PM 12/29/2023

The screenshot shows a web browser window with the address bar displaying 'online.u2u.be/courses/25896/modules/16/24871'. The page content is a slide titled 'Examples: Insecure Deserialization' with the U2U logo in the top right corner. The slide lists two scenarios related to insecure deserialization. The left sidebar of the browser shows a navigation menu with options like 'Home', 'Web Security Fundamentals', 'Software and Data Integrity', 'Network Security', 'Defenses', and 'Practical Exercises'. The Windows taskbar at the bottom shows the date as 12/29/2023 and the time as 6:48 PM.

Examples: Insecure Deserialization

- **Scenario #1:** A React application calls a set of Spring (Java) Boot microservices. Being functional programmers, they tried to ensure that their code is immutable. The solution they came up with is serializing user state and passing it back and forth with each request. An attacker notices the "R00" Java object signature, and uses the Java Serial Killer tool to gain remote code execution on the application server
- **Scenario #2:** A PHP forum uses PHP object serialization to save a "super" cookie, containing the user's user ID, role, password hash, and other state:
a:4:{i:0;i:132;i:1;s:7:"**Mal**";i:2;s:4:"**user**";i:3;s:32:"b6a8b30e05022f8f3c88bc960";}
An attacker changes the serialized object to give themselves admin privileges:
a:4:{i:0;i:1;i:1;s:5:"**Alice**";i:2;s:5:"**admin**";i:3;s:32:"b6a8b30e05022f8f3c88bc960"};

The screenshot shows a web browser window with the address bar displaying 'online.u2u.be/courses/25896/modules/16/24871'. The page features a dark blue sidebar on the left with a navigation menu. The main content area has a white background with the title 'Defenses' in a large, bold, black font. Below the title is a red horizontal line. The content consists of three bullet points, each with a square icon. The first bullet point is 'Use .NET to serialize and deserialize data', followed by two sub-points: 'The .NET framework is pretty secure for serializing and deserializing' and 'Keep note of .NET security blogs (just in case)'. The second bullet point is 'Taking over a computer by injecting machine code into a message is pretty hard in .NET'. The third bullet point is 'Services that use other frameworks', followed by three sub-points: 'Restrict or monitor incoming and outgoing network connectivity', 'Isolate and run code in low privileged environments', and 'Enforce strict type constraints for properties'. The U2U logo is in the top right corner of the content area. The Windows taskbar is visible at the bottom, showing the time as 6:48 PM on 12/29/2023.

U2U Online

online.u2u.be/courses/25896/modules/16/24871

Defenses

- Use .NET to serialize and deserialize data
 - The .NET framework is pretty secure for serializing and deserializing
 - Keep note of .NET security blogs (just in case)
- Taking over a computer by injecting machine code into a message is pretty hard in .NET
- Services that use other frameworks
 - Restrict or monitor incoming and outgoing network connectivity
 - Isolate and run code in low privileged environments
 - Enforce strict type constraints for properties

25°C Mostly cloudy 6:48 PM 12/29/2023

The screenshot shows a web browser window with the address bar displaying 'online.u2u.be/courses/25896/modules/16/24871'. The page content is titled 'Defenses' and features a list of four bullet points. The U2U logo is in the top right corner of the page. The browser's taskbar at the bottom shows the Windows logo, a search bar, and several application icons. The system tray on the right indicates the time is 6:48 PM on 12/29/2023.

Defenses

- If you need to deserialize cookies, headers or other input (viewstate,...)
 - Make sure the input is clean and cannot be tampered with
- Implement integrity checks (digital signatures)
- Logging deserialization exceptions and failures
- Monitoring deserialization, alerting if a user deserializes constantly

The screenshot shows a web browser window displaying a U2U Online course page. The browser's address bar shows the URL `online.u2u.be/courses/25896/modules/16/24871`. The page has a dark blue sidebar on the left with a navigation menu. The main content area has a white background with a red horizontal line below the title. The title is 'Examples: Supply Chain Attack' in a large, black, sans-serif font. To the right of the title is the U2U logo, which consists of the letters 'u2u' in white on a dark blue square background. Below the title, there are two bullet points, each starting with a square icon. The first bullet point is 'Scenario #1: Attacker breaches update server for an application, and starts issuing malicious updates. Application users then download and install the malicious update, systems get infected'. The second bullet point is 'Scenario #2: Many home routers, set-top boxes, device firmware, and others do not verify updates via signed firmware. Unsigned firmware is a growing target for attackers and is expected to only get worse. This is a major concern as many times there is no mechanism to remediate other than to fix in a future version and wait for previous versions to age out.' At the bottom of the browser window, there is a Windows taskbar with a search bar, several application icons, and a system tray showing the date and time as 6:48 PM on 12/29/2023.

U2U Online

online.u2u.be/courses/25896/modules/16/24871

Examples: Supply Chain Attack

- **Scenario #1:** Attacker breaches update server for an application, and starts issuing malicious updates. Application users then download and install the malicious update, systems get infected
- **Scenario #2:** Many home routers, set-top boxes, device firmware, and others do not verify updates via signed firmware. Unsigned firmware is a growing target for attackers and is expected to only get worse. This is a major concern as many times there is no mechanism to remediate other than to fix in a future version and wait for previous versions to age out.

25°C Mostly cloudy

Search


6:48 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/16/24871

Software and Data Integrity Features

Famous examples



PayPal Servers Compromised via Well-Known Java Deserialization Bug

PayPal addresses issue after security researcher broke into their servers and took data files just to prove his point

Jan 26, 2016 09:28 GMT · By Catalin Cimpanu · Share: [Twitter](#) [Facebook](#) [LinkedIn](#) [Reddit](#) [Google+](#)

Michael "Artspl0it" Stepankin, an independent security researcher, has discovered a critical security flaw in PayPal's Manager interface that allowed him to execute malicious code on PayPal's servers, an issue which would have enabled him to take full control of PayPal's infrastructure.

The bug is an exploitation of the [Java deserialization issue](#) that's been around for over a year, but only this past autumn came to the forefront of the infosec community.

The problem relies on the way developers handle user-supplied serialized data in Java, and can be found in different open source Java libraries.

Java insecure coding practice exposed PayPal's servers

The researchers that discovered this flaw also published a tool that automatically generates the malicious code needed to exploit this vulnerability via the Apache Commons Collections Java library.

Mr. Stepankin used this tool to create a malicious Java serialized object, which he then fed into one of the forms present in the PayPal Manager Web interface, which he discovered that PayPal's devs failed to protect.

"I realized that it's a Java serialized object without any signature and it's handled by the

25°C Mostly cloudy

Search

6:48 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/16/24871

U2U


Famous examples

Wide-ranging SolarWinds probe sparks fear in Corporate America

By Christopher Bing, Chris Prentice and Joseph Menn on Sep 11, 2021 11:28AM

Over liability for unreported cyber incidents.

A US Securities and Exchange Commission investigation into the SolarWinds Russian hacking operation has dozens of corporate executives fearful information unearthed in the expanding probe will expose them to liability, according to six people familiar with the inquiry.



25°C Mostly cloudy

Search

ENG

6:48 PM 12/29/2023