

U2U Online

online.u2u.be/courses/25896/modules/18/24873

Developer and IT Training

U2U

Server-Side Request Forgery

OWASP Web Security Threat #10

25°C Mostly cloudy

Search

6:50 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/18/24873

Insufficient Logging And Monitoring

u2u

Agenda

- Server-Side Request Forgery
- Defenses
- Famous Examples

25°C Mostly cloudy

Search

6:50 PM 12/29/2023

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/18/24873`. The page has a dark blue sidebar on the left with a user profile icon and a list of course modules. The main content area is white and features the title **#9: Server-Side Request Forgery** in a large black font, followed by a red horizontal line. Below the title, there are two bullet points. In the top right corner of the content area, there is a black square logo with the white text 'u2u'. The bottom of the image shows a Windows taskbar with various icons, including the Start button, search bar, and several application icons. The system tray on the right shows the date and time as 6:50 PM on 12/29/2023.

U2U Online

online.u2u.be/courses/25896/modules/18/24873

#9: Server-Side Request Forgery

- SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL
- Attackers can then make the application send crafted requests to unexpected destinations, even when protected by a firewall or VPN

u2u

25°C Mostly cloudy

Search

6:50 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/18/24873

U2U

Insufficient Logging And Monitoring

Insufficient Logging And Monitoring

Insufficient Logging And Monitoring

Overview

Security Matrix

ATTACK VECTORS	SECURITY WEAKNESS		TECHNICAL IMPACTS
Exploitability	Prevalence	Detectability	Impact
AVERAGE	LOW	DIFFICULT	SEVERE

25°C Mostly cloudy

Search

ENG

6:50 PM 12/29/2023

The screenshot shows a web browser window with the address bar displaying 'online.u2u.be/courses/25896/modules/18/24873'. The page features a dark blue sidebar on the left with a user profile icon and a navigation menu. The main content area has a white background with the title 'How it Works' in a large, bold, black font. Below the title is a red horizontal line. 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 and line is a list of three bullet points. 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.

How it Works

- Attacker finds an application with functionality for importing data from a URL, publishing data to a URL, or otherwise reading data from a URL that can be manipulated
- By providing a completely different URL, or by manipulating how URLs are built, the attacker will try to modify this functionality
- Once the manipulated request is sent to the server, the server-side code tries to read data to the manipulated URL. As a result, the attacker may read data from services not intentionally exposed to the internet

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/18/24873`. The course title is 'Insufficient Logging And Monitoring'. The slide content is as follows:

Possible Impact

- Malicious attacks that appear to originate from the organization
 - hosting the vulnerable application, causing potential legal liabilities and reputational damage.
- Unauthorized access to sensitive configurations
 - including server files, cloud provider metadata, and open ports.
- Internal port scanning
 - SSRF attacks can scan internal networks, letting an attacker Identify and exploit unsecured services.
- Exploit chaining
 - SSRF exploits can be “chained” into other attacks that are more damaging, ranging from reflected XSS to remote code execution.

The Windows taskbar at the bottom shows the date and time as 6:50 PM on 12/29/2023, along with weather information (25°C, Mostly cloudy) and various system icons.

U2U Online

online.u2u.be/courses/25896/modules/18/24873

U2U

Examples

SSRF in Dundas BI

Dundas BI is a web-based analytics solution developed by Dundas Data Visualization, Inc. During one of our engagements, we found that this product was being used. After spending some time exploring the features and attack surface of the application, one thing caught our eye. One of Dundas BI features allows you to export what you're seeing in the data dashboard to different formats. For example, the following screenshot shows how it's possible to share the current dashboard as an image:

ESSENTIALCOMMONADD / EDIT

EditFull ScreenShare

NoteNotification

SHARE

LinkImagePDFExcelPowerPoint

Export

more help

EDIT

25°C Mostly cloudy

Search

6:50 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/18/24873

Defenses: from Network Layer

- Segment remote resource access functionality in separate networks to reduce the impact of SSRF
- Enforce “deny by default” firewall policies or network access control rules to block all but essential intranet traffic

25°C Mostly cloudy

Search


6:50 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/18/24873

Insufficient Logging And Monitoring

Defenses: from Application Layer



- Sanitize and validate all client-supplied input data
- Enforce the URL schema, port, and destination with a positive allow list
- Do not send raw responses to clients
- Disable HTTP redirections
- Be aware of the URL consistency to avoid attacks such as DNS rebinding and “time of check, time of use” (TOCTOU) race conditions

25°C Mostly cloudy

Search

6:50 PM 12/29/2023