CSOC 1030: Assignment #2

July 14, 2023

**Prepared By**: *Ashish Kishor Hedau*

Table of Contents

[Sensitive File Exposure in YorkU station login page directory 2](#_Toc137283759)

[Description 2](#_Toc137283760)

[Impact 2](#_Toc137283761)

[Recommendations 2](#_Toc137283762)

[Steps to Reproduce 3](#_Toc137283763)

# Sensitive File Exposure in YorkU station login page directory

## Description

The assessed web application “<http://10.5.30.20>” was found to be protected by login type functionality having users to submit username and password to get the access to YorkU Broadcast Station. The web application denies access to a directory named “/access” but allows access to a specific file within it, “/access/README”. This misconfiguration enabled us to discover and access the README file, exposing sensitive information contained within it. Proper access controls and configuration reviews are necessary to address this vulnerability and prevent unauthorized disclosure of confidential data.

## Impact

An attacker can brute force the directories for the web application in scope, resulting in access to /access/README file. The information in the file **included the Login ID and Password** which should not be publicly exposed. The attacker then could log into the YorkU Broadcast Station and could potentially do malicious actions.

## Recommendations

To fix this vulnerability, the administrators of the web application need to check and change the server’s access control settings. They should make sure that the permissions for accessing files and directories are set up correctly. This means that unauthorized users or anonymous requests should not be able to access sensitive resources.

## Steps to Reproduce

The target application was found to be protected by a **Login Page** that required users to submit the E-mail address and password before accessing the content on the site, as pictured below:

![A screenshot of a computer

Description automatically generated]()

To search for exposed files and directories, we ran the brute force tool “**dirsearch**” on the web application in Scope.

![A screenshot of a computer

Description automatically generated]()

We found the robots.txt file which provides instructions to search engines like “Google” regarding which pages or directories of the website they are allowed to access and crawl.

![A computer screen with text and images

Description automatically generated]()

Opening the **robots.txt** file in browser revealed interesting data. We were curious about the **Disallow: /access/** path as it could contain directories which are not supposed to be seen but are exposed due to lack of access controls.

![A screenshot of a computer

Description automatically generated]()

We again ran the directory brute force attack on the web application in scope but this time we added the **/access** path to the URL as shown in the image below resulting in a **200 code for /access/README** shown in green font.

![A screen shot of a computer

Description automatically generated]()

We downloaded the README file from the browser to see the contents and it had the credentials for the login page as seen below in the image.

![A computer screen with white text

Description automatically generated]()

By providing credentials to the login page, we got from the README file above, we were successfully able to access the YorkU Broadcast Station.

![A screenshot of a computer

Description automatically generated]()