AMRIUNIX (https://amriunix.com/)

Alfresco Reset Password Add-on - 0day Vulnerabilities

This post is as much about the penetration testing process and the 0-day approach as it is about the vulnerability. I discovered a 0-day vulnerability in one of the most used plugin (https://www.flex-solution.com/page/alfresco-solution/alfresco-reset-password-add-on) for Password Reset on Alfresco (https://www.alfresco.com/) Content Services framework.

TL;DR

I was performing a penetration test recently and really hadn't found much on the scoped server. So i start by reviewing the application components hoping to find 0-day vulnerabilities, and indeed i found an intrusting third-party component in the application which seems to be vulnerable.

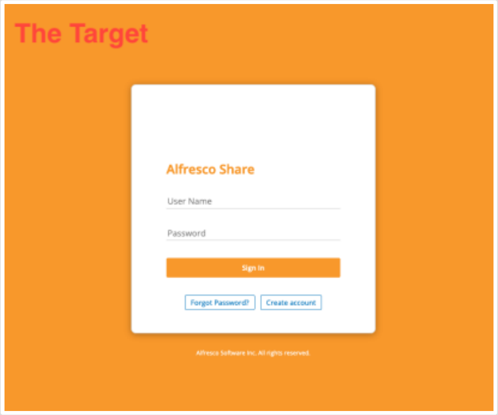
The 0-day Approach

In order to take the 0-day approach, first thing is to simulate the target environment and the easiest way is by using docker, so i found this nice docker-compose file on github acs-community-deployment (https://github.com/ALfresco/acs-community-deployment) to deploy the entire Alfresco Content Services (Community Edition) on my lab environment.

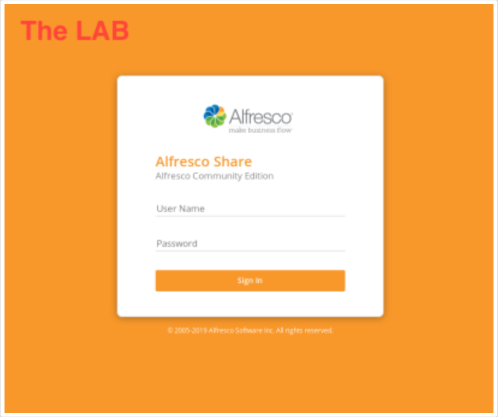
Components discovery

After deploying Alfresco on my lab, I start by comparing the one on the target environment with the one my lab and i quickly figure out that there is no `Create account` and `Forget Password?` buttons by default on my lab !

The Target Server



The Lab Server


The LAB
Alfresco
make business flow
Alfresco Share
Alfresco Community Edition
User Name
Password
Sign in
© 2005-2019 Alfresco Software Inc. All rights reserved.

Next, I start by analyzing the HTTP requests going from my browser to the server when i click on the `Forget Password?` button and i found out that all requests is being sent to `/share/proxy/alfresco-noauth/com/flex-solution/reset-password` .

With a quick google search i figure out that the `Forget Password?` button is being handled by a plugin called Alfresco Reset Password add-on (https://github.com/FlexSolution/AlfrescoResetPassword)

Vulnerabilities discovery

Blind-boolean-based CMIS-SQL Injection

`Alfresco Reset Password add-on` is using CMIS-SQL (https://hub.alfresco.com/t5/alfresco-content-services-hub/cmis-query-language/ba-p/289736) to query data from Alfresco, which is `a read-ony` query language for SELECT statement and with limited functions (like, UPPER, LOWER, etc...).