Tushar Jadhav Follow

Dec 26, 2021 · 2 min read · Listen

Save

CVE-2021-40579

Insecure direct object references (IDOR)

👨‍💻 Discovered by **Tushar Jadhav**

Profile: https://www.linkedin.com/in/tushar-jadhav-7a43b4171/

📄 **Vulnerable version: 1.0**

🔗 **Vendor Homepage:** https://www.sourcecodester.com/

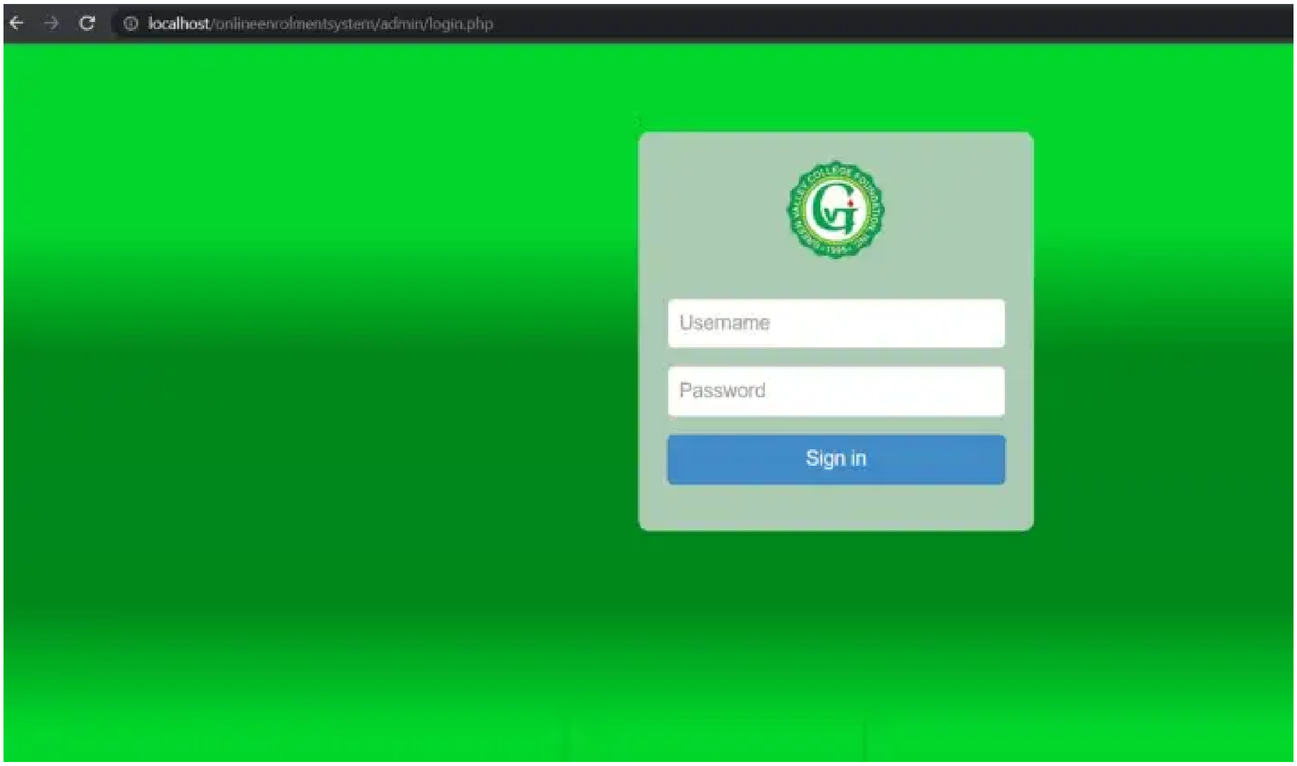
Product: Online *Enrollment Management System* in PHP and *Paypal Payment System*

Vulnerability Title: Insecure direct object references (IDOR)

Detailed description: Found this vulnerability in the id parameter. Lead to business logic also, Anyone can download admission confirmed and paid invoice without any authentication.

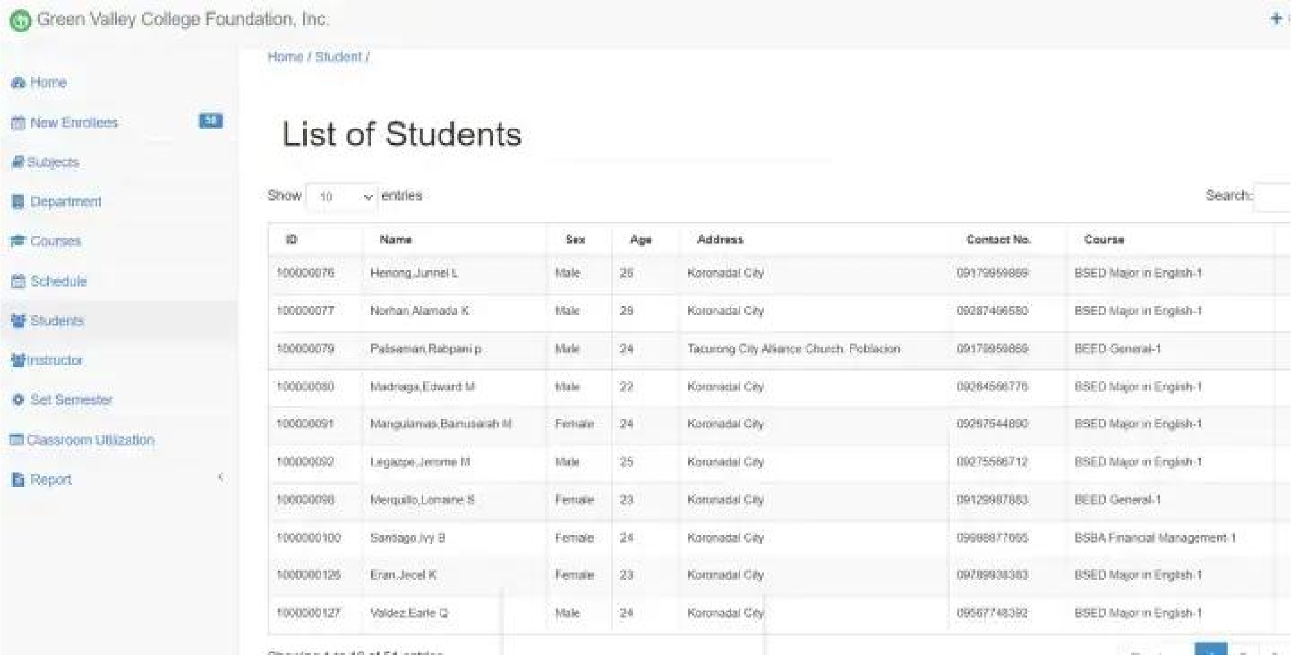
Steps-To-Reproduce:

1. Login into the Online Enrollment Management System admin panel.



Admin Login Page

2. Now go to the Students You can List Of Students, Where we can confirm the admission and payment.

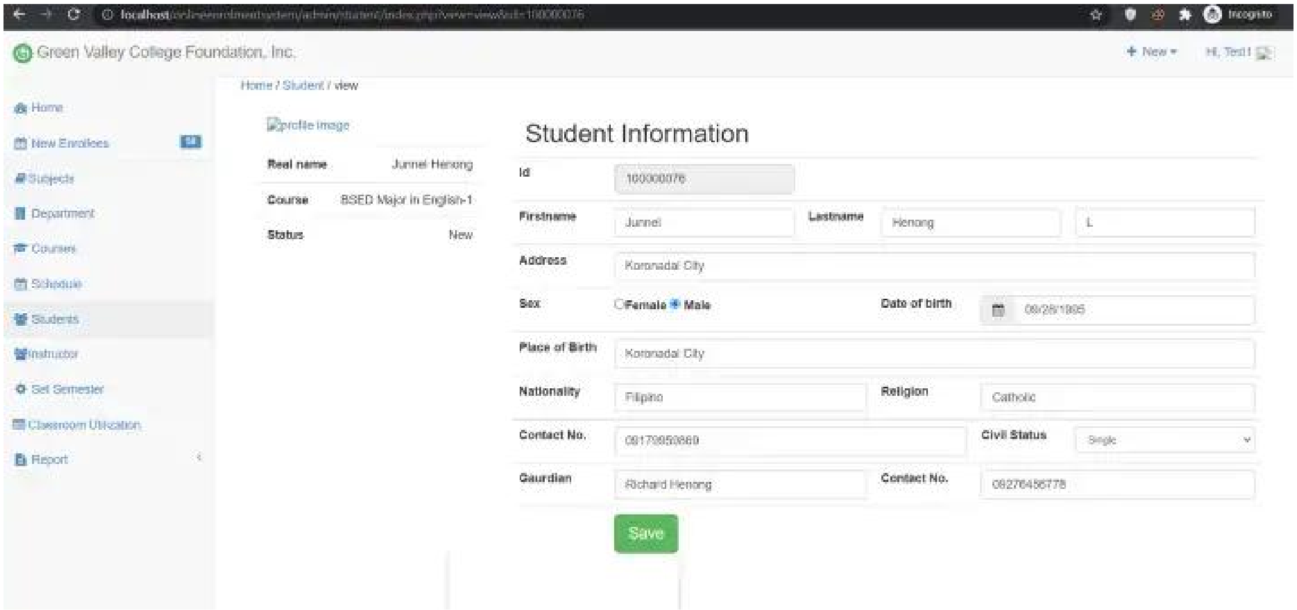


List of Students

Show 10 entries Search:

ID	Name	Sex	Age	Address	Contact No.	Course
100000076	Henong,Junnel L	Male	26	Koronadal City	09179959869	BSED Major in English-1
100000077	Norhan,Alamada K	Male	26	Koronadal City	09287496580	BSED Major in English-1
100000079	Palsaman,Rabpani p	Male	24	Tacurong City Alliance Church, Poblacion	09179959869	BEED General-1
100000080	Madriaga,Edward M	Male	22	Koronadal City	09284566776	BSED Major in English-1
100000091	Mangulamas,Bainusarah M	Female	24	Koronadal City	09267544890	BSED Major in English-1
100000092	Legazpe,Jerome M	Male	25	Koronadal City	09275586712	BSED Major in English-1
100000098	Merquillo,Lorraine S	Female	23	Koronadal City	09129987883	BEED General-1
1000000100	Santiago,Ivy B	Female	24	Koronadal City	09998877095	BSBA Financial Management-1
1000000126	Eran,Jecel K	Female	23	Koronadal City	09789938383	BSED Major in English-1
1000000127	Valdez,Earle Q	Male	24	Koronadal City	09567748392	BSED Major in English-1

3. Every form Has a Specific ID where We can change parameters and admission confirmed we can see the receipt.



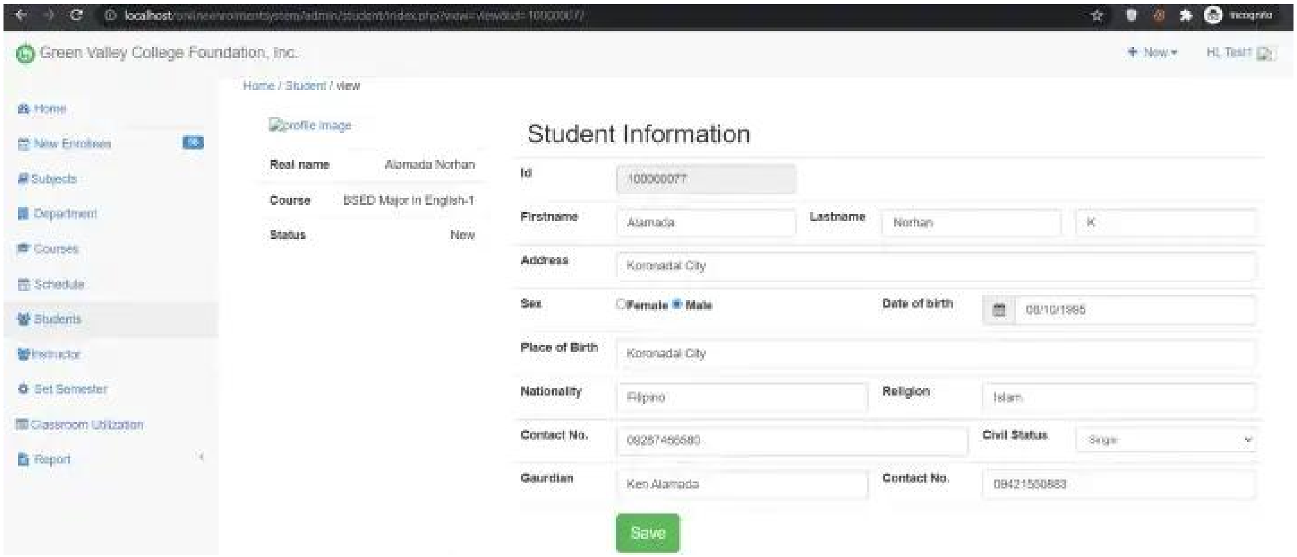
Real name	Junnel Henong
Course	BSED Major in English-1
Status	New

Student Information

Id	100000076			
Firstname	Junnel	Lastname	Henong	L
Address	Koronadal City			
Sex	○Female ● Male	Date of birth	08/28/1995	
Place of Birth	Koronadal City			
Nationality	Filipino	Religion	Catholic	
Contact No.	09179959869	Civil Status	Single	
Gaurdian	Richard Henong	Contact No.	09276456778	

User_Id

4. As I changed the id I can see another user’s All PII details also and I’m able to confirm The Admission.

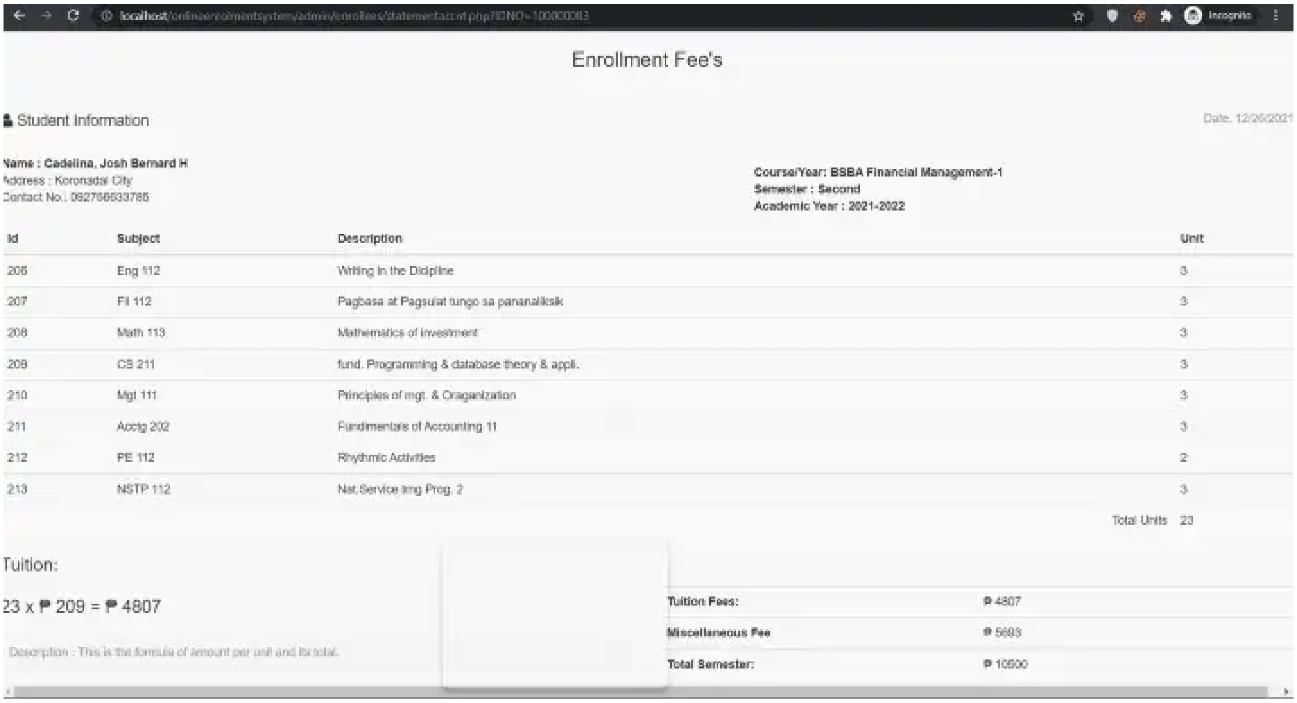


Real name	Alamada Norhan
Course	BSED Major in English-1
Status	New

Student Information

Id	100000077			
Firstname	Alamada	Lastname	Norhan	K
Address	Koronadal City			
Sex	○Female ● Male	Date of birth	08/10/1995	
Place of Birth	Koronadal City			
Nationality	Filipino	Religion	Islam	
Contact No.	09287466580	Civil Status	Single	
Gaurdian	Ken Alamada	Contact No.	09421560883	

5. This vulnerability contains On Different locations. Also with that, we will get an admission receipt that we have paid money and admission confirmed.


localhost/onlineenrolmentsystem/admin/enrollees/statementaccnt.php?IDNO=100000083
Incognito

Enrollment Fee's

Student Information

Date: 12/26/2021

Name : Cadelina, Josh Bernard H
Address : Koronadal City
Contact No.: 092766633785

Course/Year: BSBA Financial Management-1
Semester : Second
Academic Year : 2021-2022

Id	Subject	Description	Unit
206	Eng 112	Writing in the Dicipline	3
207	Fil 112	Pagbasa at Pagsulat tungo sa pananaliksik	3
208	Math 113	Mathematics of investment	3
209	CS 211	fund. Programming & database theory & appl.	3
210	Mgt 111	Principles of mgt. & Oraganization	3
211	Acctg 202	Fundimentals of Accounting 11	3
212	PE 112	Rhythmic Activities	2
213	NSTP 112	Nat.Service trng Prog. 2	3
		Total Units	23

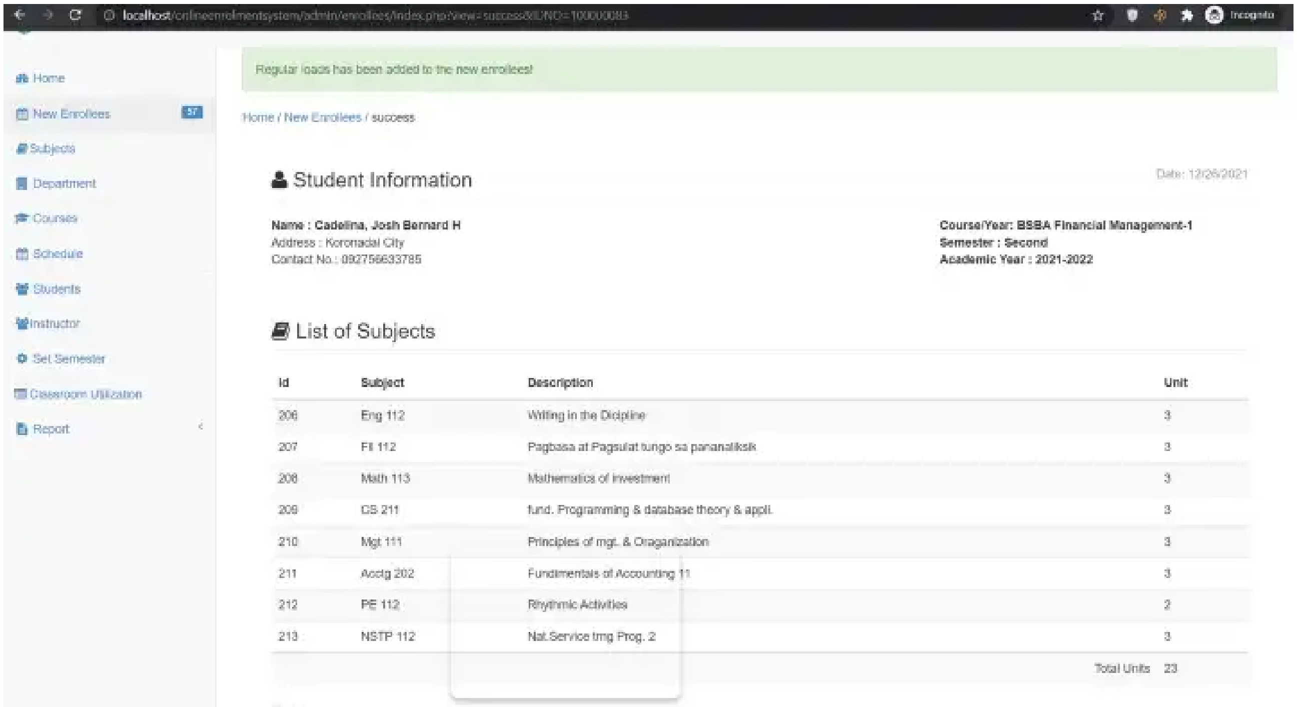
Tuition:

23 x ₱ 209 = ₱ 4807

Description : This is the formula of amount per unit and its total.

Tuition Fees:	₱ 4807
Miscellaneous Fee	₱ 5693
Total Semester:	₱ 10500

6. This is the interesting part, In this case, if anyone knows their form id they can download their receipt without any authentication or fuzz the id parameter.



Regular loads has been added to the new enrollees!

Home / New Enrollees / success

Student Information

Date: 12/26/2021

Name : Cadelina, Josh Bernard H
Address : Koronadal City
Contact No.: 092756633785

Course/Year: BSBA Financial Management-1
Semester : Second
Academic Year : 2021-2022

List of Subjects

Id	Subject	Description	Unit
206	Eng 112	Writing in the Dicipline	3
207	Fil 112	Pagbasa at Pagsulat tungo sa pananaliksik	3
208	Math 113	Mathematics of investment	3
209	CS 211	fund. Programming & database theory & appl.	3
210	Mgt 111	Principles of mgt. & Oraganization	3
211	Acctg 202	Fundimentals of Accounting 11	3
212	PE 112	Rhythmic Activities	2
213	NSTP 112	Nat.Service trng Prog. 2	3
		Total Units	23

Thanks For Reading !!!

Vapt Bug Bounty Bugs Hacking Cve