Security Bug report

Respected Sir/Ma’am,

I have identified a critical security flaw that demands immediate attention. The flaw is allowing any malicious actor to reset passwords of the students that have an account there. Once the password is reset the malicious actor can log into the portal as the victim user and make changes and view sensitive information of the victim.

The information that is exposed includes:

1. Students’ Mark-Sheets
2. Students’ Admits
3. Students’ Application Form

Security Bug report

Explanation and remediation of the security issue:

The bug(security issue) exists in the reset password functionality. The functionality can be broken down into two steps:

1. Entering the roll number or the registered phone number to receive and confirm the OTP.
2. Allow the user to enter a new password.

The OTP is checked properly only to redirect the user to the new password entering page. The OTP validity is not checked when the user enters a new password(in the 2nd step). This is where the bug arises. A malicious user can simply send a POST request with the roll number and a new password to “/setPassword” and reset that respective student’s password.

To fix the issue it is advised to send the OTP in the POST request to “/setPassword” endpoint, that way if the OTP is incorrect the password will not get updated. Alternatively a cookie can be sent to the user if they successfully verify the OTP sent to them. After that if

the valid cookie is not present while setting the new password, the password will not get updated.

About me:

My name is Ashutosh Dutta, I am a 1st year BCA student in JB college (Autonomous). Carrier wise I work as a security researcher (freelance) who finds security vulnerabilities for MNCs that have bug bounty programs. I happen to find this bug coincidently while changing my student account's password. I have not leaked any data of any student but I might have changed some of the student's password while verifying this bug. The students should not have any problem resting the password and I assure you there accounts are 100% safe with no other changes.

Note: I would like to keep my identity as a freelance security researcher private when in college.

Email: marvelmaniac@wearehackerone.com

Linkedin: https://linkedin.com/in/marvelmaniac