OTP Bypass in Kalvium Admissions

Vulnerability Report: OTP Bypass in `admissions.kalvium.com` at `/signup` Endpoint

Summary

A critical OTP bypass vulnerability has been identified in the `/signup` endpoint of `admissions.kalvium.com`. This flaw allows an attacker to create an account for any user without requiring a valid OTP, enabling unauthorized access.

Vulnerable Endpoint

- **Domain:** `admissions.kalvium.com`
- **Endpoint:** `/signup`

Description

The OTP verification mechanism in the signup process is bypassable, which means:

1. An attacker can register an account using any phone number.
2. The OTP validation step can be skipped, allowing the attacker to complete registration without providing a valid OTP.

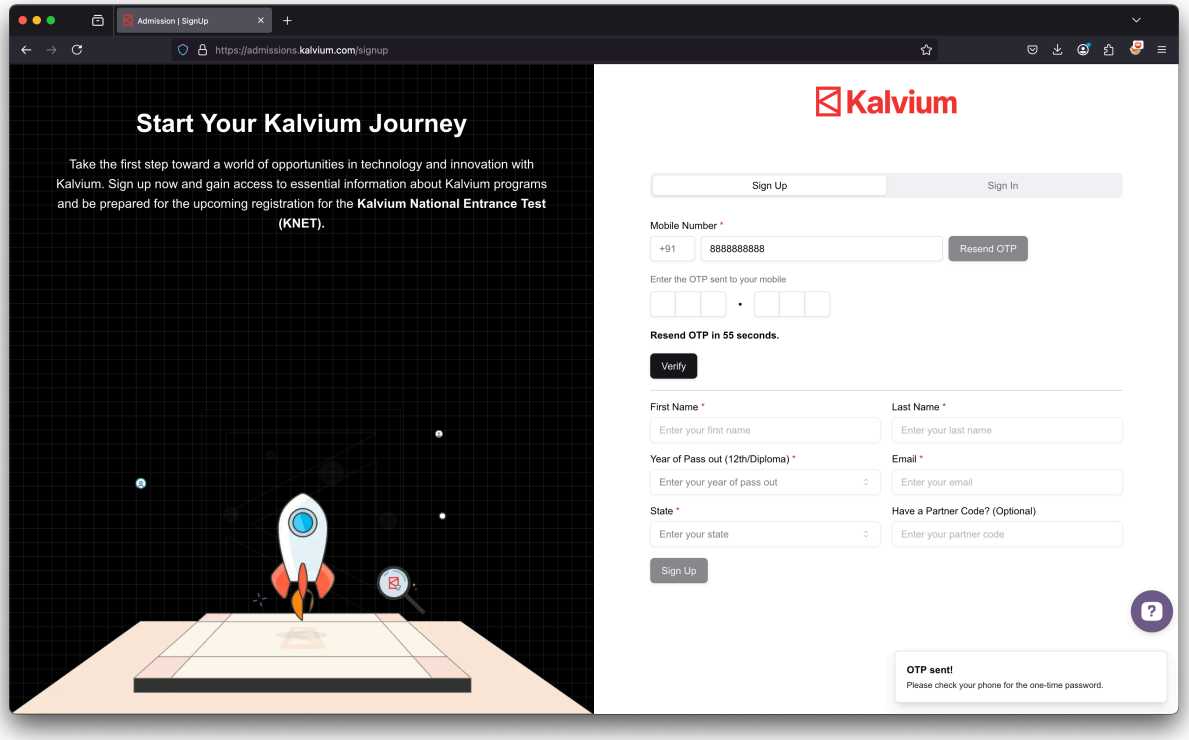
Steps to Reproduce

1. Navigate to `https://admissions.kalvium.com/signup`.
2. Enter a valid phone number for signup.
3. Capture the request using a proxy tool like Burp Suite.
4. Modify the OTP validation response to bypass verification

5. The account gets created without a valid OTP, allowing an attacker to access the system.

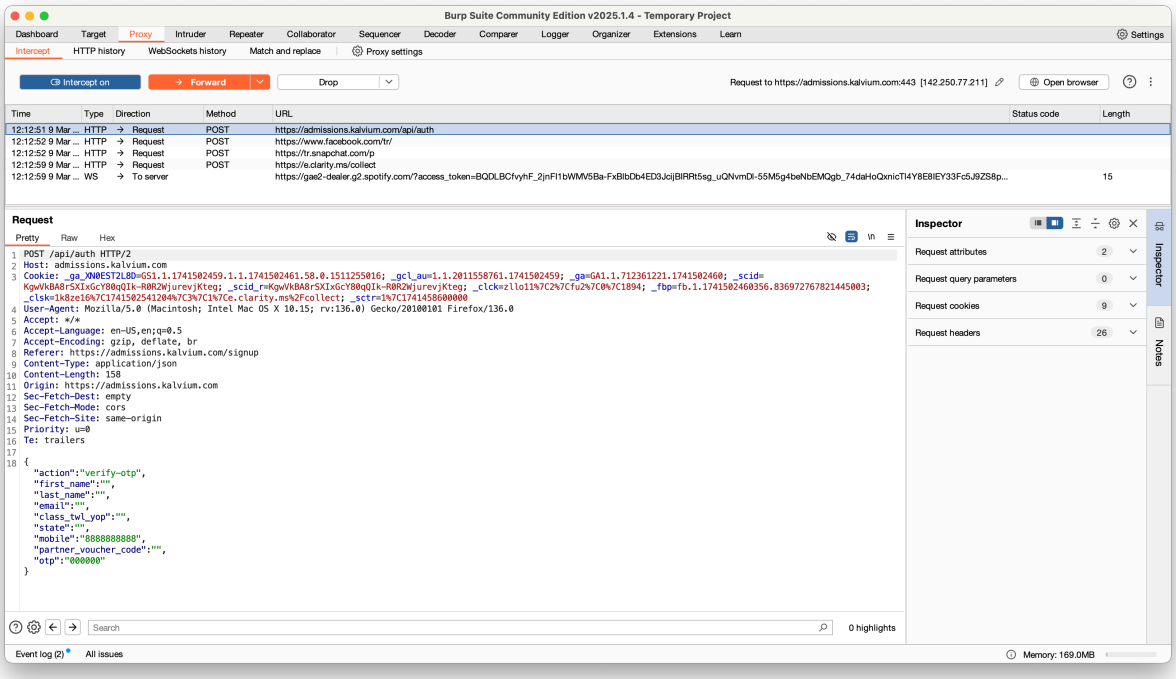
Screenshots

I am Creating an account for phone number +91 88888 88888:

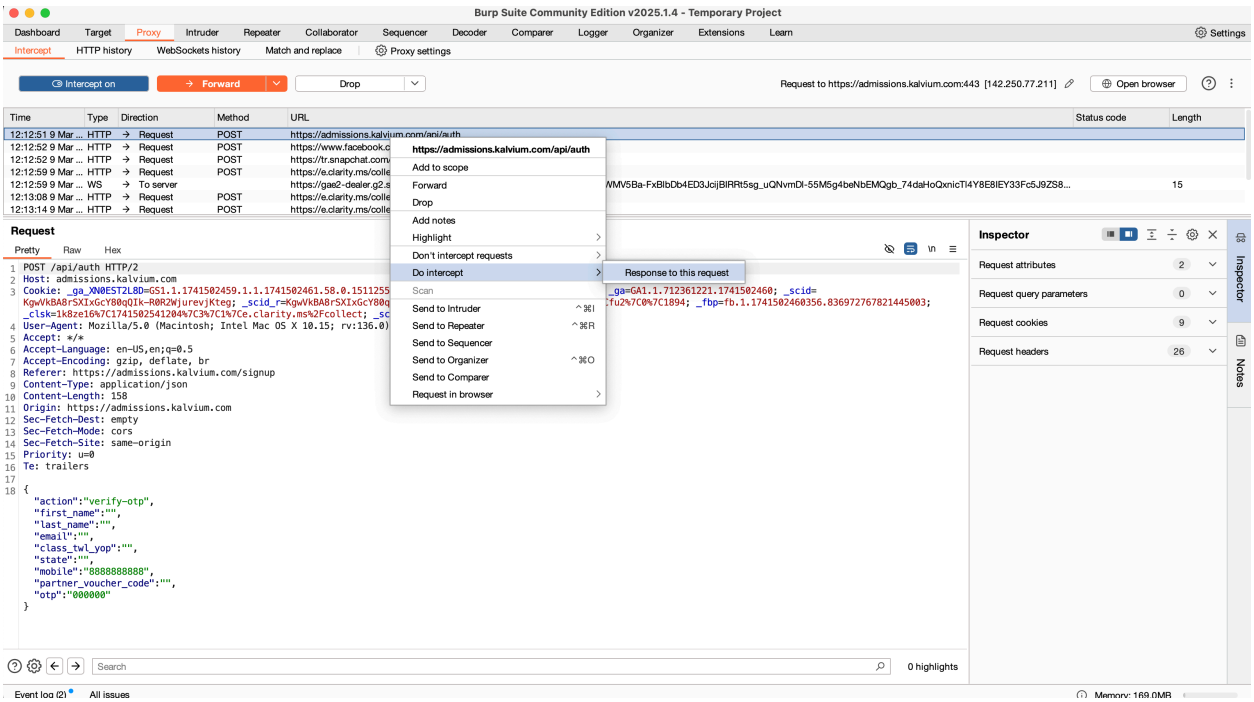


Capturing the OTP request using Burp:

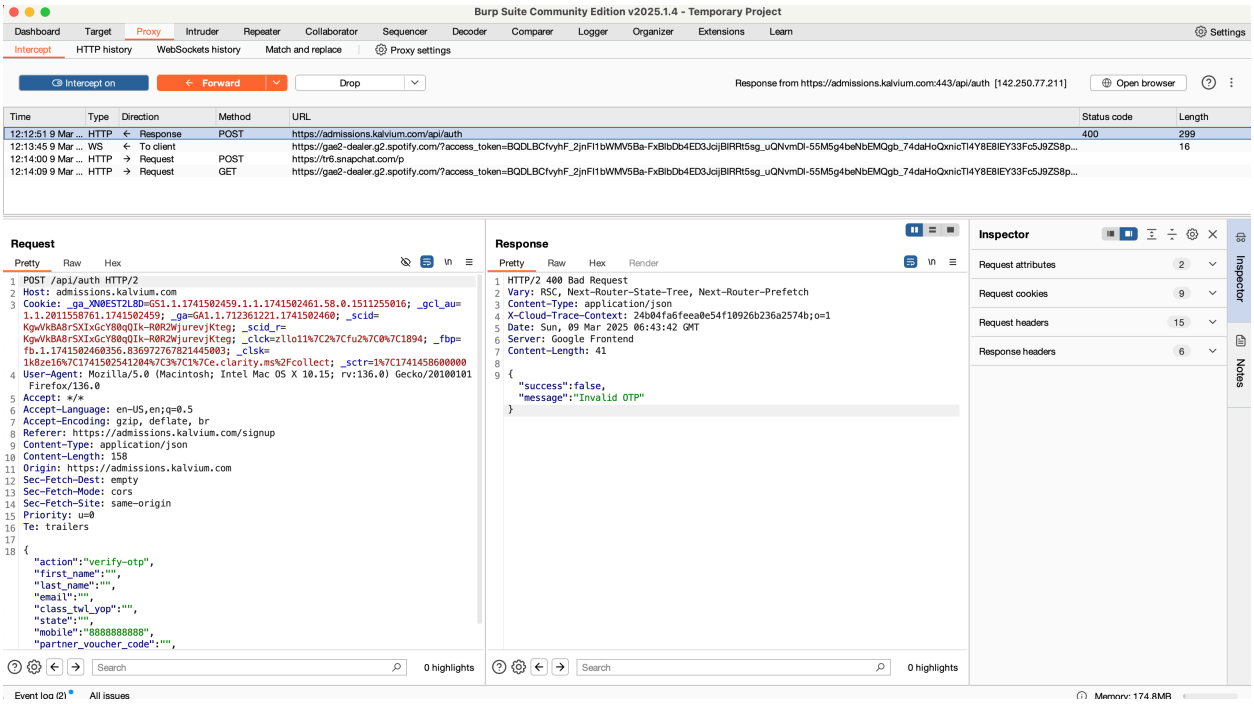
- Here you can see the otp is “000000”



Manipulating the Response:

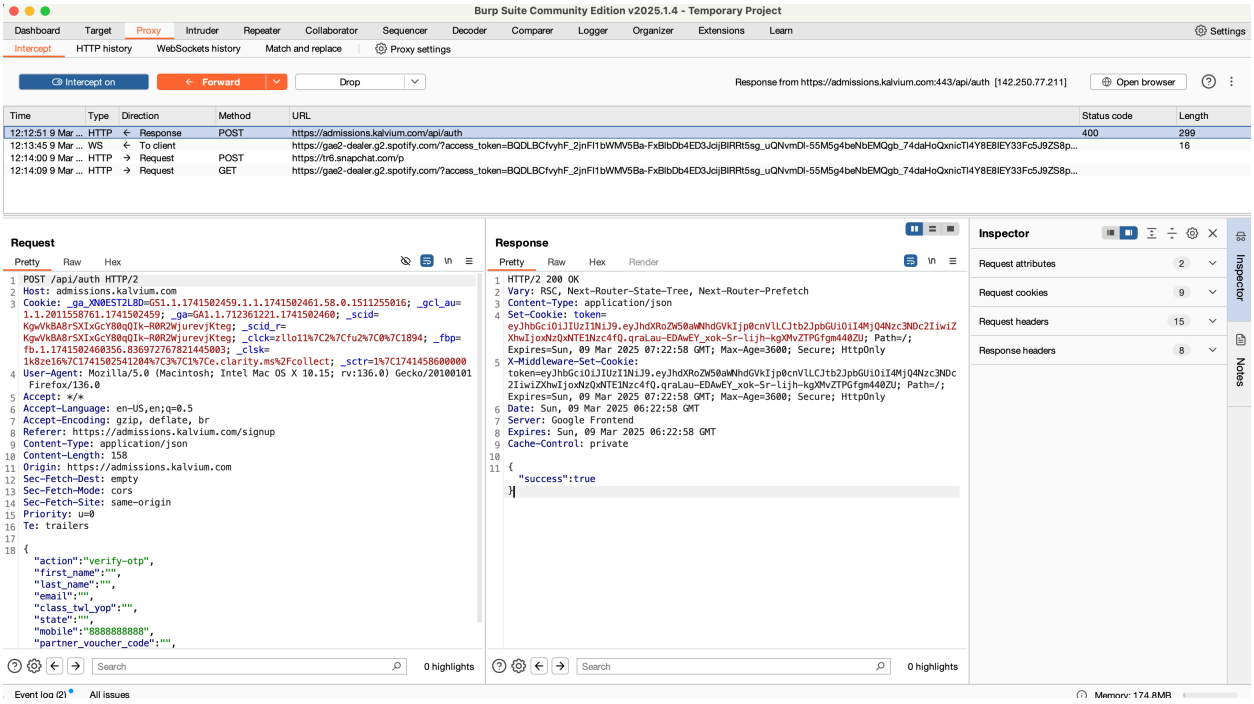


The Actual Response:

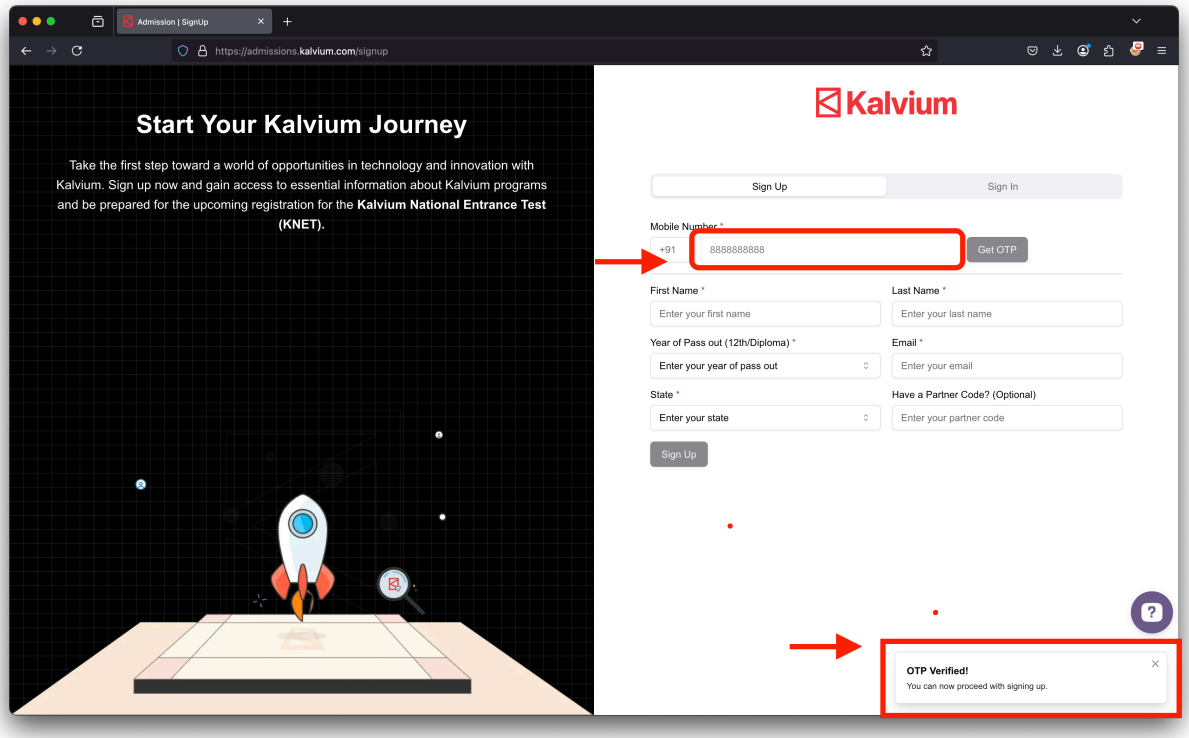


Modified Response:

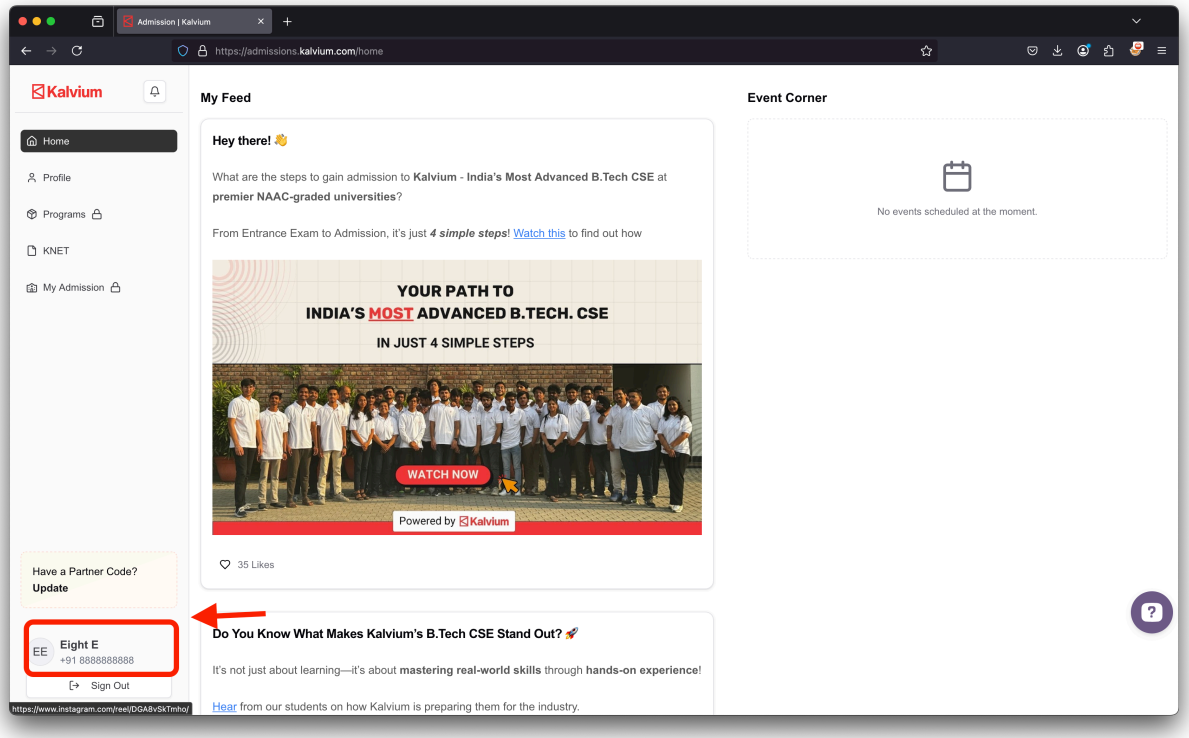
- e.g success: true



You Can see the OTP is verified:



Attacker Logged in Successfully:



Recommendation

- Implement strict server-side OTP validation before allowing account creation.
- Use rate-limiting to prevent automated attacks.
- Enforce re-validation of OTP at multiple stages to ensure security.
- Monitor logs for suspicious account creation patterns.

Conclusion

This vulnerability poses a significant risk and should be addressed immediately. A patch should be deployed to prevent attackers from bypassing OTP verification and gaining unauthorized access.