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

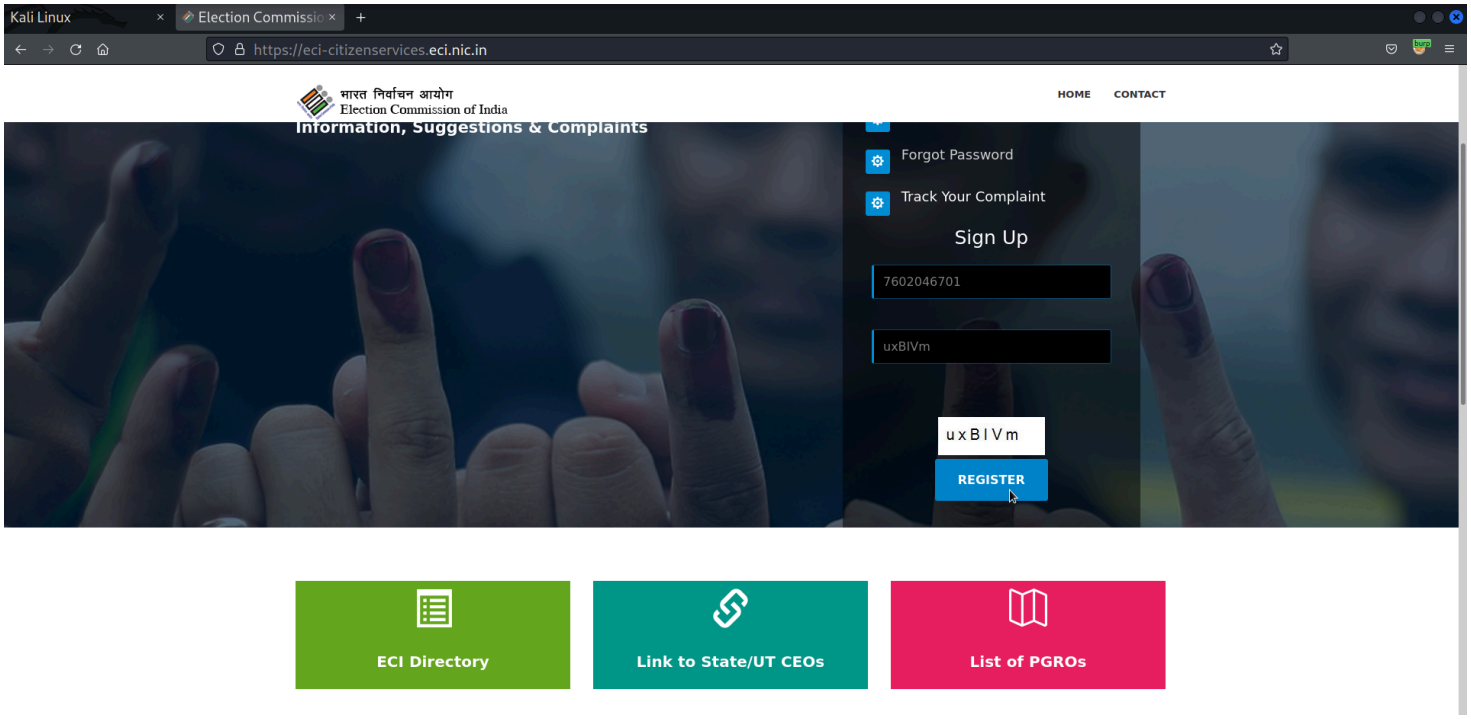
Sign up OTP bypass:

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.

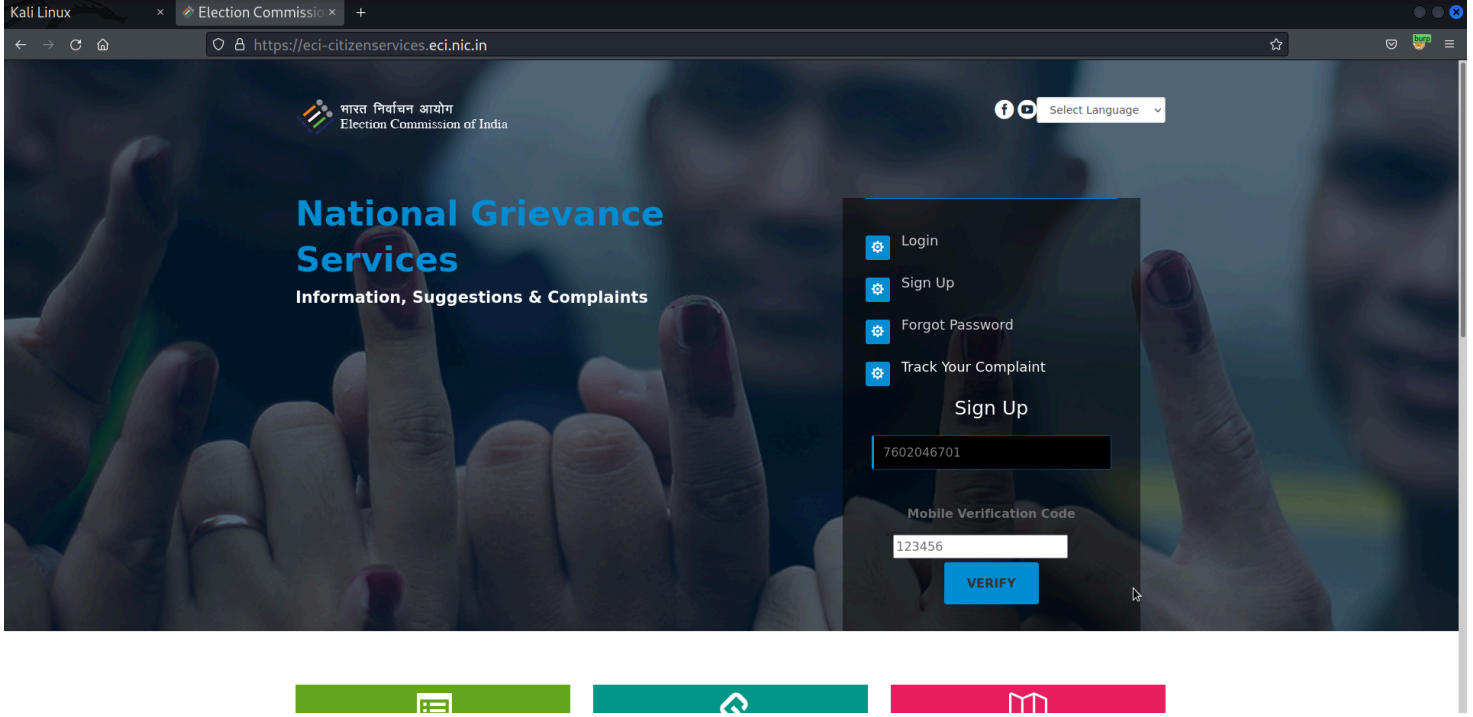
Summery:
Upon singing up on *https://eci-citizenservices.eci.nic.in/* with a valid phone number we receive a 6 digit OTP. By intercepting the OTP validation form we can bruteforce the 6 digit code which is in range (000,000-999,999). So any attacker with enough time can guess the right OTP and sign up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

Steps To Reproduce:

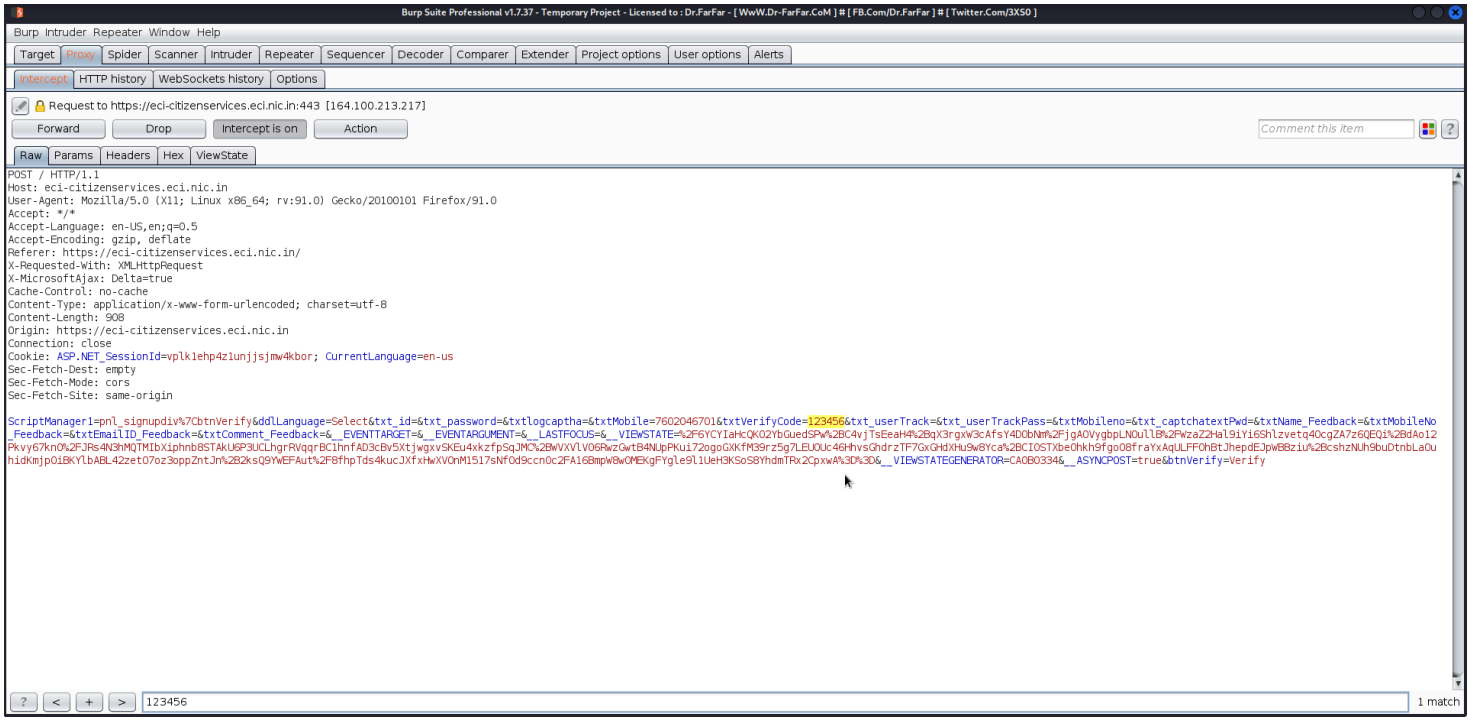
1. Go to https://eci-citizenservices.eci.nic.in/ and click on sigh up. Enter valid phone number and captcha. Then click **REGISTER**.



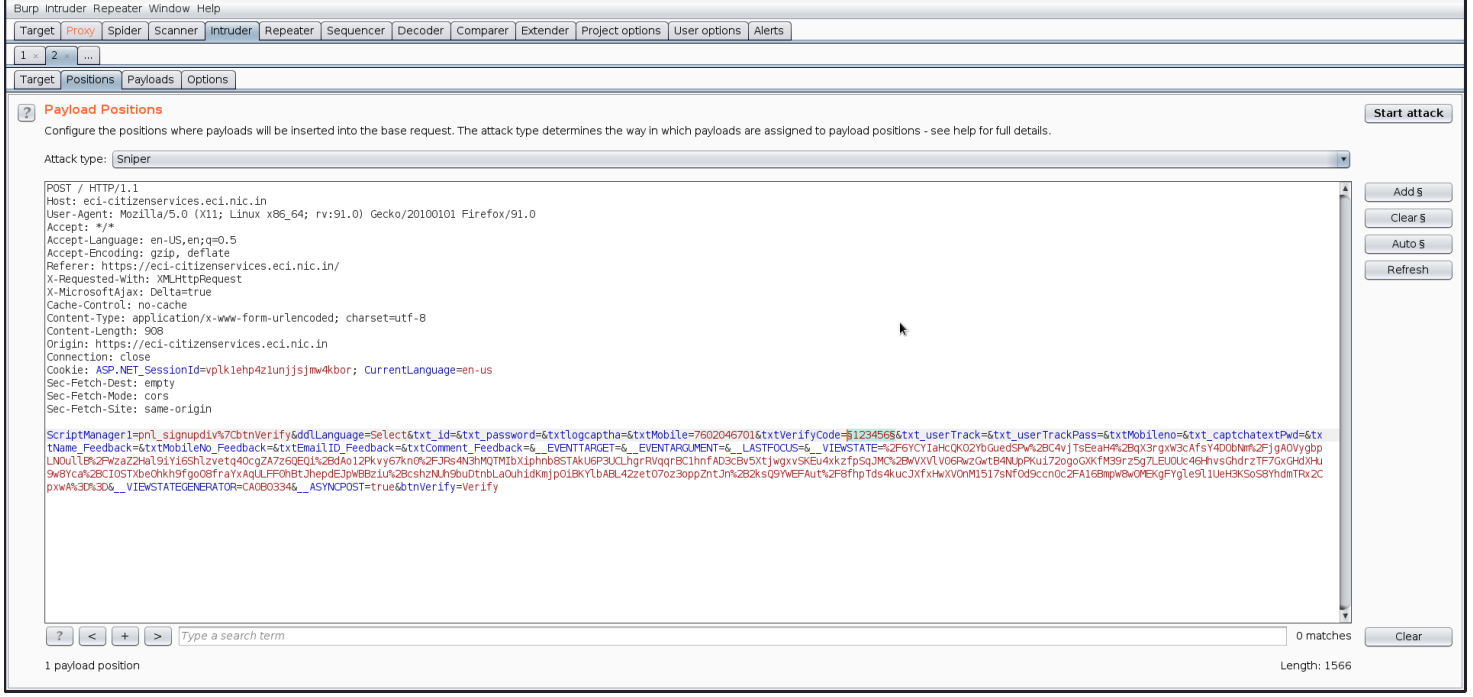
2. OTP will be sent to the victim's phone number. Submit 123456 in the verification form and click on verify after turning the interception on.



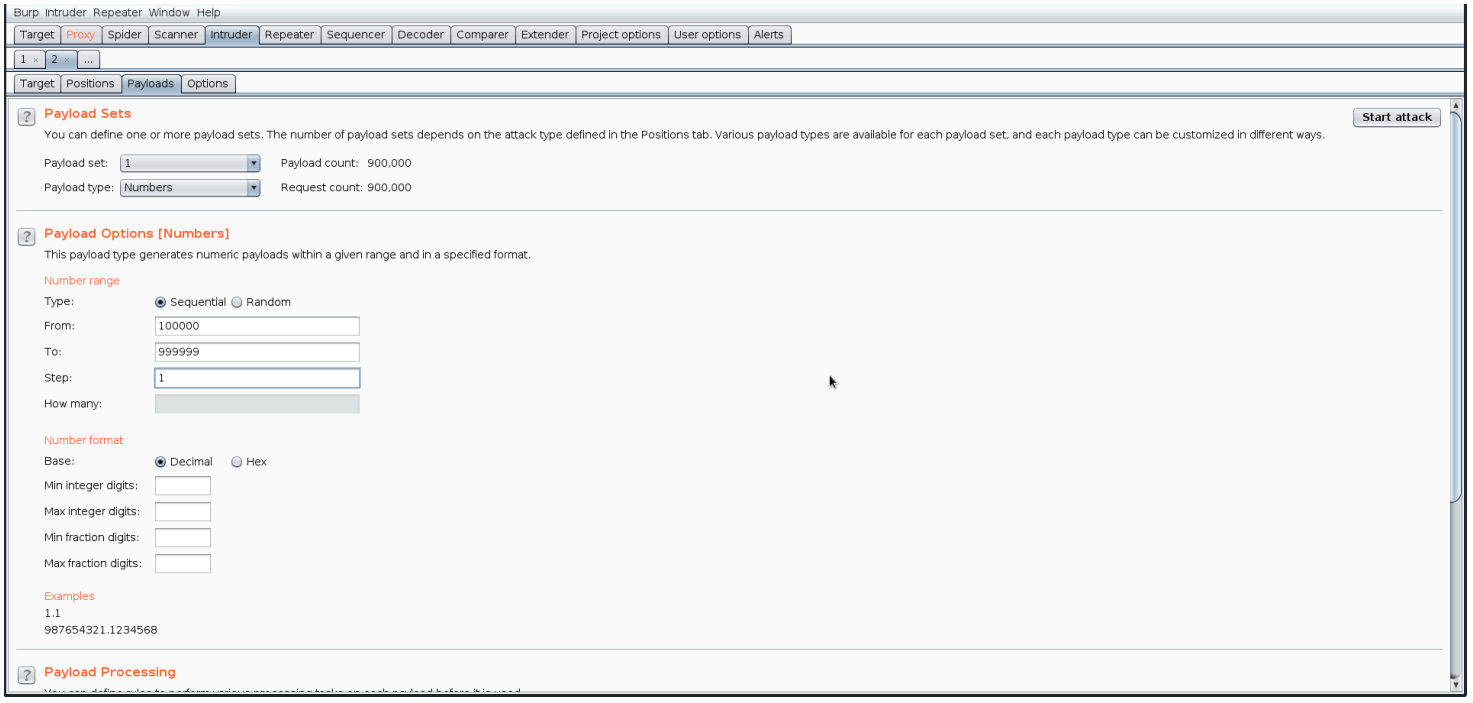
3. Intercept the verification request.(Do not turn the interception off yet.)



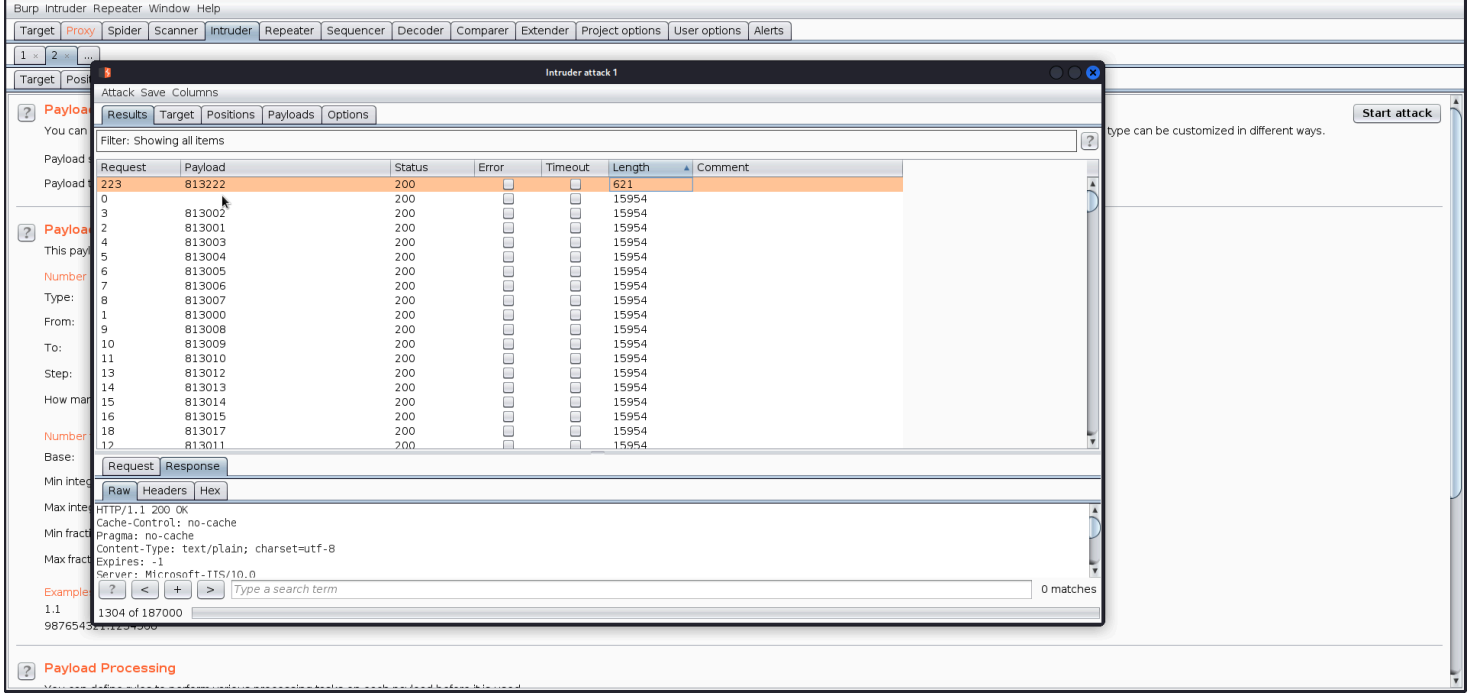
4. Send the request to intruder and select the position where 123456(or whatever number you've chosen) is highlighted.



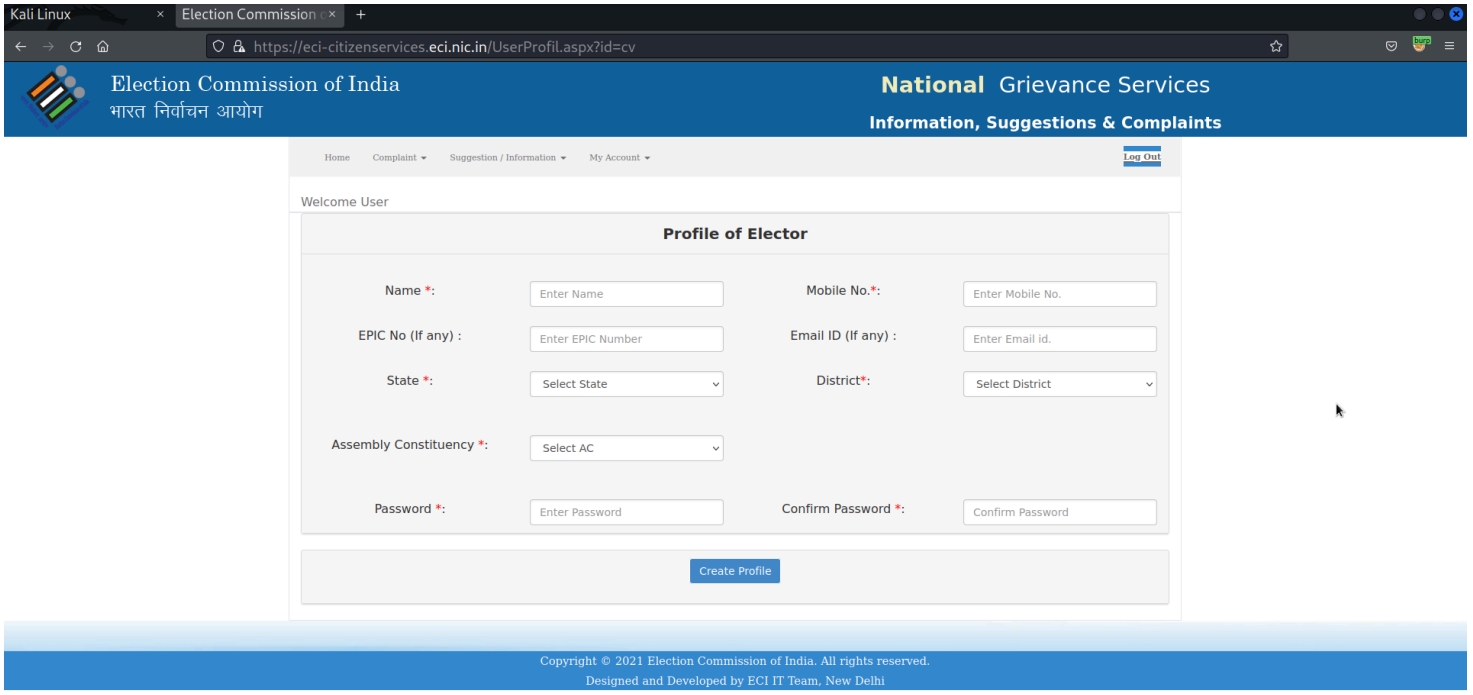
5. Select Number payload. For testing purpose when otp is known use a small range in which the OTP is present otherwise use range 000,000-999,999 and use step: 1. Start the attack.



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.



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



Impact:

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

Mitigation

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