Abusing functions for bug bounty

ADITYA SHENDE

whoami

ADITYA SHENDE

-Proud Indian

-Bug Bounty Hunter

-Listed in top 100 researchers on Bugcrowd

-Trader and investor

Functions ? What ? Type ?

BASIC

What we can do on website or how it works

AUTHENTICATED

In this type we need to use our credentials to perform activities or changes

NON-AUTHENTICATED

Simple opposite of authenticated, In which we dot need to provide creds or identity

What to check ?

Always check whole website as normal user.

No need to use burpsuite all time.

Functions are easy to understand

REGISTER FUNCTION

Creating new user in site as per function

LOGIN FUCNTION

Providing creds to access registered account

ACCOUNT SETTINGS

Most buggy section with multiple functions

WEB APP + ANDROID APP

For checking activity reflections in both

Register account

-Creating account on web + android with same id

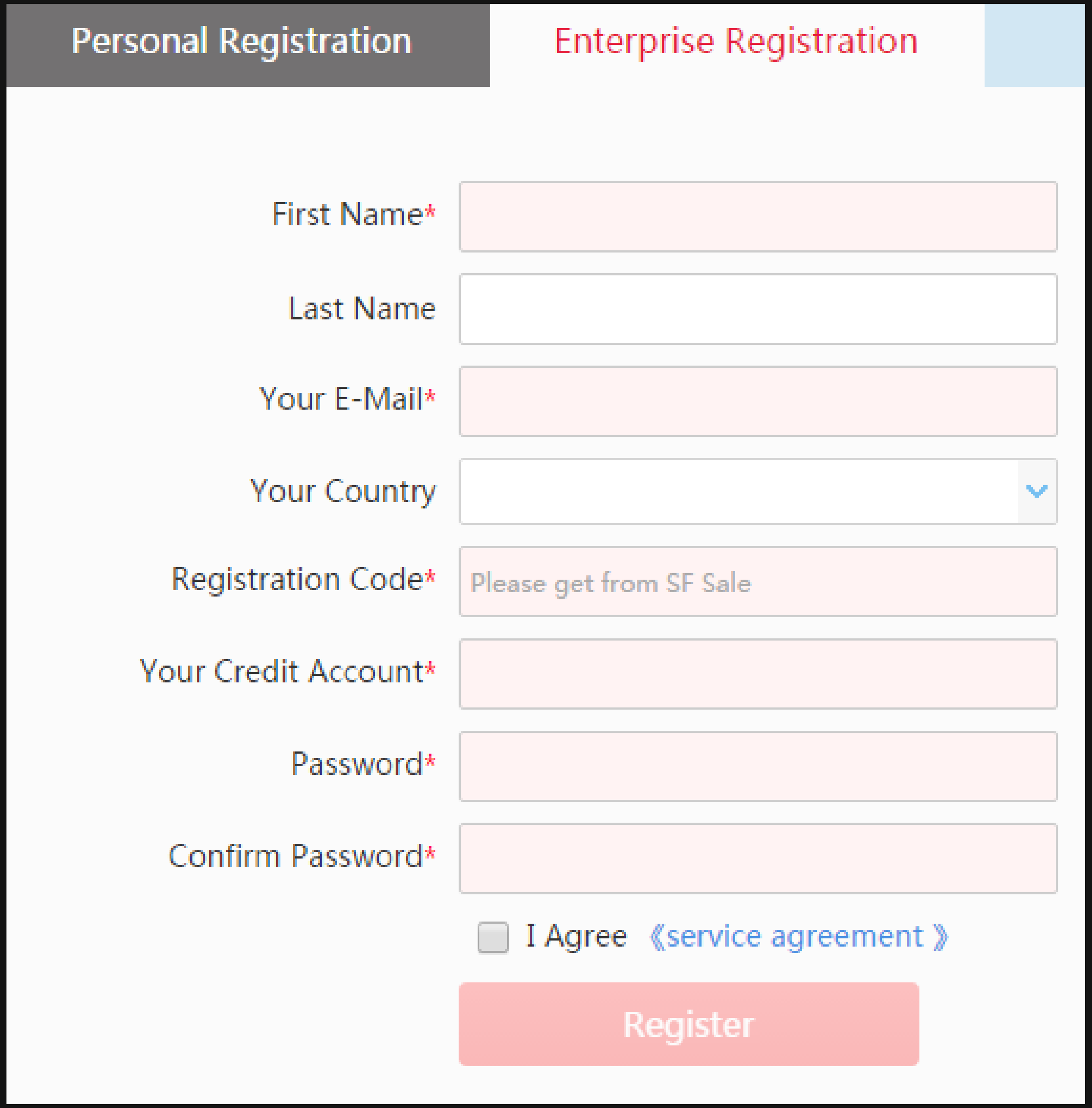
-Crafting id for takeover

hacker@gmail.com@target.com

-Username + reset function with collaborator link username@collaborator.net

-Creating account with company mail addresses to gain extra authorities.

Use hunter.io



Personal Registration | Enterprise Registration

First Name*

Last Name

Your E-Mail*

Your Country

Registration Code* Please get from SF Sale

Your Credit Account*

Password*

Confirm Password*

□ I Agree 《service agreement》

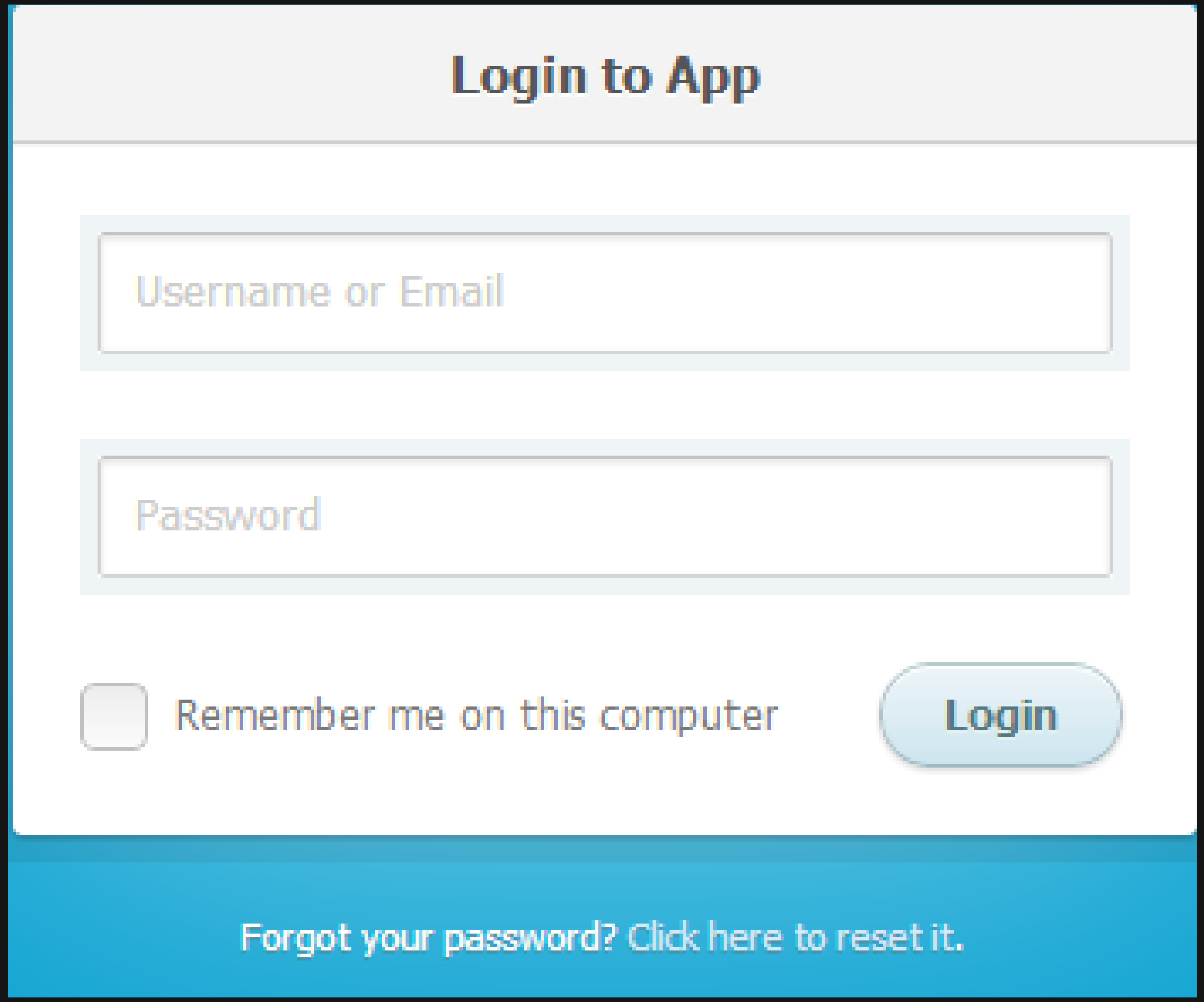
Register

Account Login

-Using multiple usernames at a time. "aditya","victim": It may give you weird response or error disclosing information.

-As usual perfoming Long DOS attack but ever tried "username=z||ping+-c+10+0.0.0.0 |" for time delay resposne

-Sending reset link with email :
1. victimusername@site.com
2.victimusername@collaboratorlink.net to gain link in SMTP conversation.


Login to App
Username or Email
Password
□ Remember me on this computer
Login
Forgot your password? Click here to reset it.

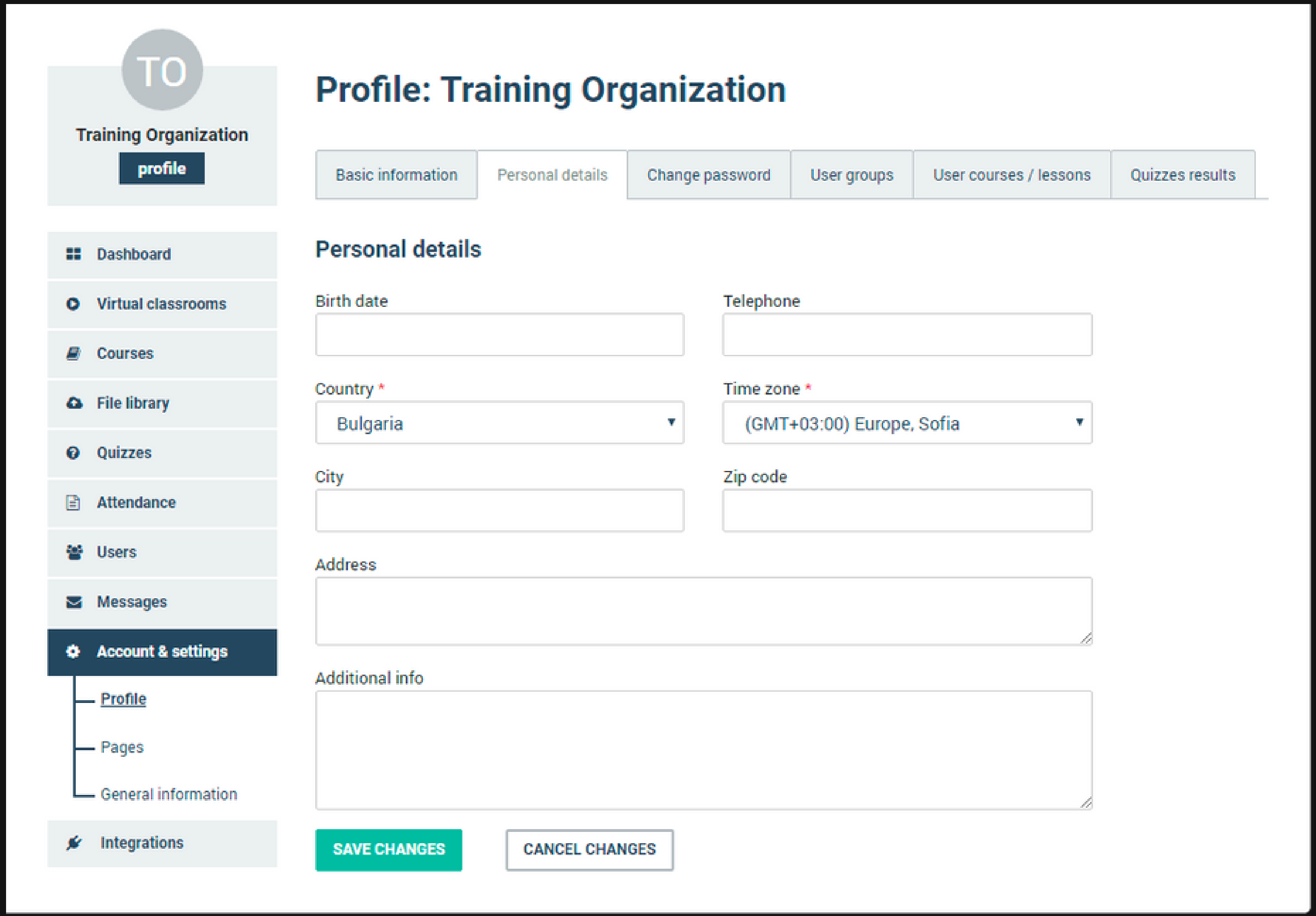
Account Settings

-Multiple functions: Add link, Attach file, Add number, Password functions, email functions etc.

-Using null payloads everywhere to get weird response, time delay, Blind SSRF, IDOR's, Long DOS everywhere

-Try to perform same actions without log in.

Opening sensitive URL like site.com/uvsgkushdjnxlj2s1a/account-settings.



Profile: Training Organization

Personal details

Birth date:

Telephone:

Country *: Bulgaria

Time zone *: (GMT+03:00) Europe, Sofia

City:

Zip code:

Address:

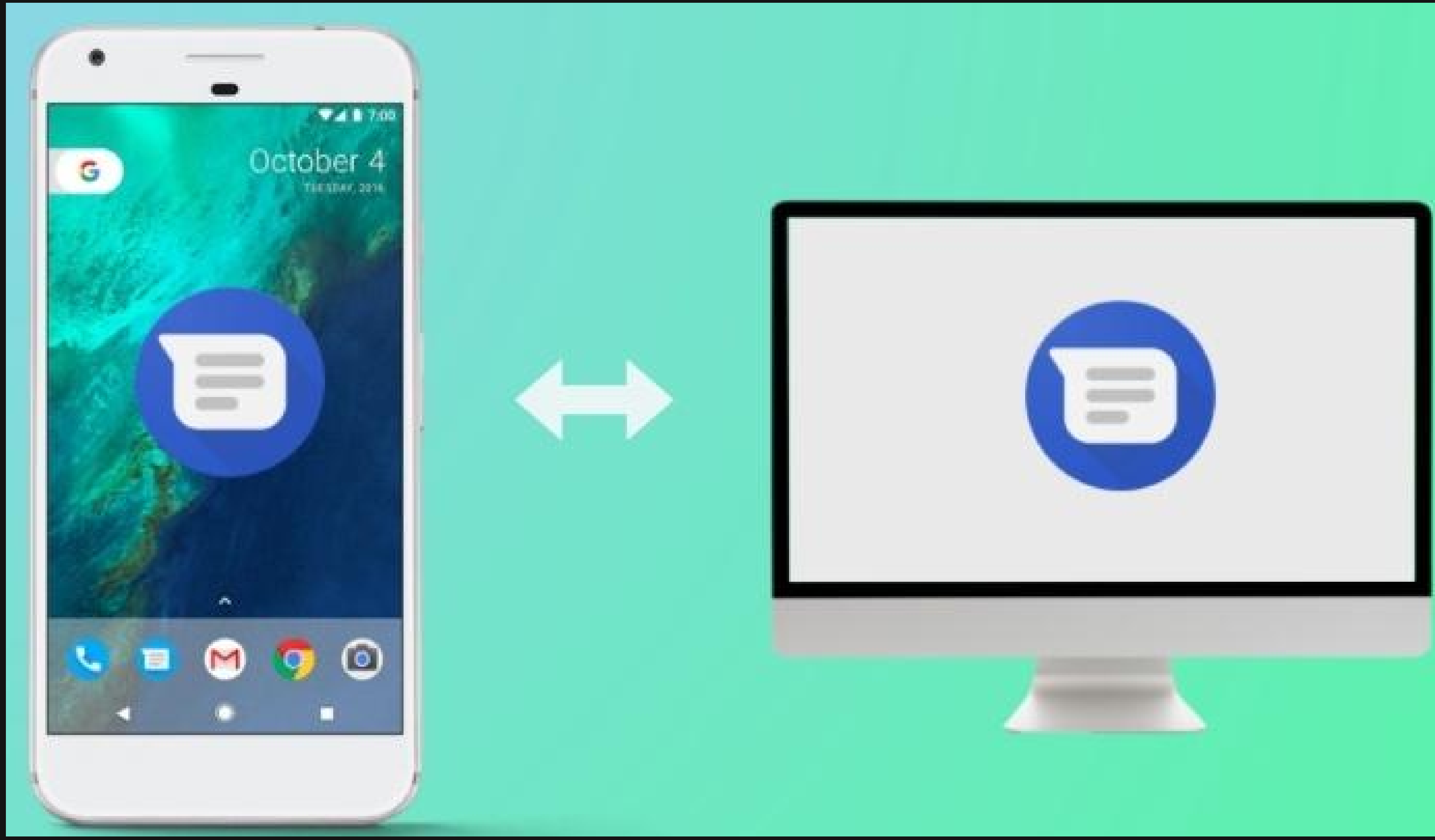
Additional info:

Web + Android app

-Creating account with same email-id on web and android app.

-Bypassing it with response tampering(mostly works) in web app.

-For verification do some changes into android app and verify it with web app Example: Updating name, number, data change, deleting account.



Burnout and time management

FUSTRATION

Getting duplicates is okay, You found valid bug just need to increase speed

SCREENSHOTS

Don't focus on money . Learning always leads to $$$$. Better ignore screenshots.

TIME

Read 2 hours daily. Increase your report ratio and finally do not compare.

THANK YOU