Vishal Bharad Follow
Mar 21, 2020 · 2 min read · Listen

Account Takeover Via Modifying Email ID — Codeigniter Framework Through 3.0.0

Hello Members, I am **Vishal Bharad.** Works as **Security Researcher** and pursuing **OSCP.** Here I am Back with another Interesting blog on **Full Account Takeover Via Modifying Email ID.**

> *Vulnerable Product — Codeigniter 3.0.0 (Authentication) Web Application Framework*
>
> *Vulnerability Type — Insecure Permissions*
>
> *Affected Component — Login page form.*
>
> *Attack Type — Remote*
>
> *Impact Escalation of Privileges — true*

Here in Authentication Library there are many Simple, Fast and Lightweight auth codeigniter.

Feature:
-Add user
-Delete user
-Ban, Unban user
-Register new user sent to email token
-Forget password
-**Role user level — Vulnerable Feature**
-Edit user profile
-Gravatar user profile
-Recaptcha by Google
-And much more

> *Core Authentication Features*

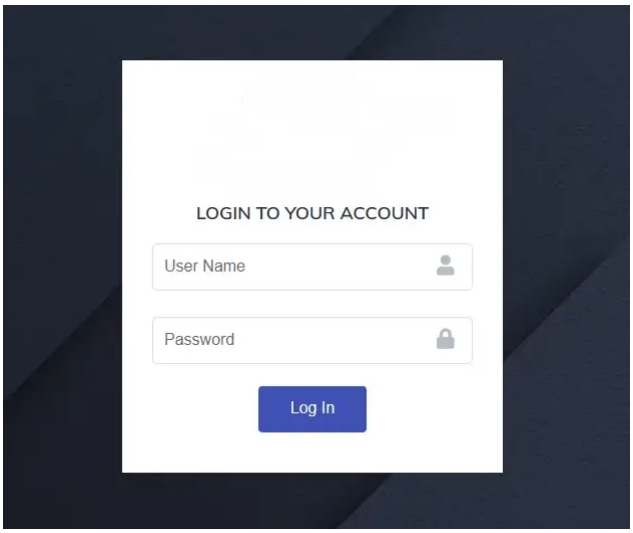
- User Authentication *(User Login)*
- **Access Granted by Level / Role — Vulnerable Feature**
- **Access Granted by Role Group — Vulnerable Feature**
- ACL for Finer Controlled Permissions
- Limits Failed Login Attempts
- Limits Login to a Single Device *(Default)*
- Deny Access by IP *(Requires Local Apache Configuration File)*
- Persistent Login *(Remember Me) (Turned Off by Default)*
- Forgotten Password and Username Recovery

Tools Used for this Vulnerability:

1. ***BurpSuite***

Steps to Reproduce:

It Starts With Login Page which is as shown in Below Image.

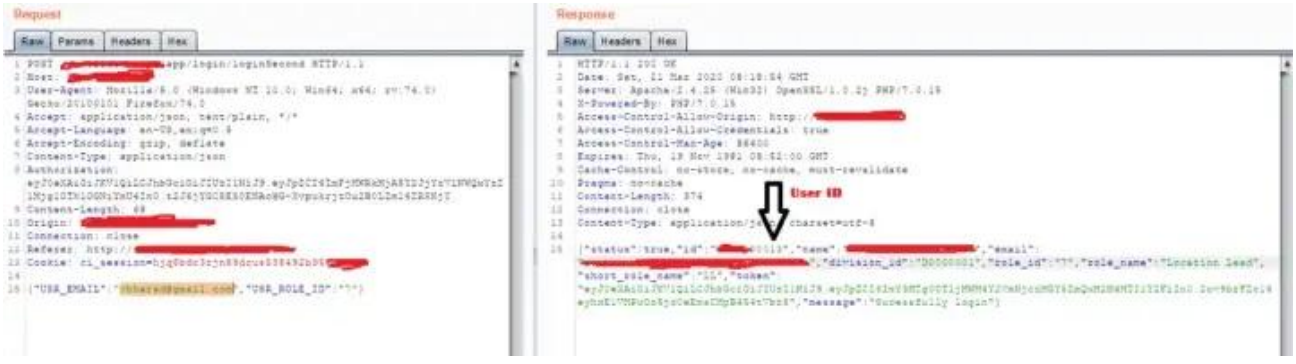


Login Page

1. There are two account abc@gmail.com and xyz@gmail.com.
2. Attacker can log in with abc@gmail.com account and He got an page to select role of the user.

User Role After Login

3. while selecting role capture the request in Burp suite.
4. Now You got an Email ID to and User Role in Request.

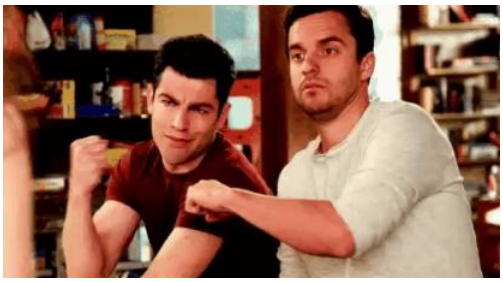


Attackers Email ID with Response.

5. Change the Email id to victim mail id i.e xyz@gmail.com and forward the request.

Victim Email ID with Response.

6. Boom….. You can now able to login with an any victims account.



Thank You

Looking forward to share more blogs

Best Regards

Vishal Bharad

Linkedin Profile : https://www.linkedin.com/in/vishal-bharad-b476b388/