

Forum:[Hack Forums](#)

Thread: [\[MoneyMasters Tutorial \] Authentication Bypass via OTP exposure \[Tutorial \]](#)

SIM-5172123 - April 17, 2022, 4:10 pm

Hello HF Member's

Today i come with tutorial that most of you looking for it

Tutorial Sponsored By
[Money Masters](#)

Authentication Bypass via OTP exposure

what is authentication bypass ?

Authentication Bypass is vulnerability which can be found on all kind of platforms . Attackers can bypass the control mechanisms which are used by the underlying application's like OTP, Captcha, 2FA, Email verification etc.

An Attacker can perform a complete Account takeover of Victim.

Reasons behind the vulnerability :

for authentication bypass there is many reasons behind it so i will only talk about OTP exposure.

some applications reveal the otp/vc in the respons it self and this mean that if you can catch the respons you will be able to bypass OTP/VC

How to avoid authentication bypass ?

do full authentication penetration testing on your application " pc , mobile , web , etc.."

Practice Time

Required Tools :

i will be using Brup suite in this tutorial and you are free to use any tool that make you feel comfort as long as it can intercept requests and responses

Note : i will not show targets address

Open your Burpsuite

Spoiler [\(Click to View\)](#)

make sure the intercept is off , and lunch the embedded Chromium browser in burp

Spoiler [\(Click to View\)](#)

after you lunch it sucessfully you can now open your targeted site and go to login page

then open intercept

Spoiler [\(Click to View\)](#)

now go to the login page and type the number you wish to bypass it otp and type the number then press login

Spoiler [\(Click to View\)](#)

now the interesting part back to burp-suite you will see the Post request with your number and token id

Spoiler [\(Click to View\)](#)

now press on Action >> Do Intercept > Response to this request

Spoiler [\(Click to View\)](#)

then press Forward and you are done

Spoiler [\(Click to View\)](#)

as you can see i intercepted the OTP successfully

i hope you like this tutorial and waiting for your feed back
Don't hesitate to correct me if you see anything wrong Knowledge is power

Blazin - April 17, 2022, 5:07 pm

Not a bad concept, but keep in mind this would only work for badly programmed API/websites.
You won't see that in anything like Twitter, FB, SC, etc

I thought you had found an actual bypass but instead the server is just programmed badly and sends the code to the user and checks it locally instead of server side.

It is good for badly programmed websites though.

SIM-5172123 - April 17, 2022, 5:13 pm

(Apr 17, 2022 05:07 PM)Blazin Wrote: [CITE](#) Not a bad concept, but keep in mind this would only work for badly programmed API/websites.
You won't see that in anything like Twitter, FB, SC, etc

I thought you had found an actual bypass but instead the server is just programmed badly and sends the code to the user and checks it locally instead of server side.
there is no way to bypass secured otp unless you are in the same pool of the sms provider else

,you can just look into programmers mistakes i will try to make more better tutorial on more better ways to get around OTP and accounts take over

but thanks for your answer really appreciate your opinion

SIM-2501407 - April 17, 2022, 7:03 pm

(Apr 17, 2022 05:13 PM)Sec.Mod Wrote: [\[CITE\]](#) there is no way to bypass secured otp unless you are in the same pool of the sms provider else ,you can just look into programmers mistakes i will try to make more better tutorial on more better ways to get around OTP and accounts take over

but thanks for your answer really appreciate your opinion

If you do not mind me asking, what is your native language? Not trying to be rude, but I noticed misspellings in some of your words.

I, myself, am horrible with foreign languages, so props to you for even knowing English.

SIM-5172123 - April 17, 2022, 7:11 pm

(Apr 17, 2022 07:03 PM)Educational Purposes Wrote: [\[CITE\]](#) If you do not mind me asking, what is your native language? Not trying to be rude, but I noticed misspellings in some of your words.

I, myself, am horrible with foreign languages, so props to you for even knowing English.

arabic is my native i know my english sucks but i try to make some progress please correct me to make the guide look more better

SIM-2501407 - April 17, 2022, 7:23 pm

(Apr 17, 2022 07:11 PM)Sec.Mod Wrote: [\[CITE\]](#) arabic is my native i know my english sucks but i try to make some progress please correct me to make the guide look more better

Sure, I'll help make grammar and spelling corrections. I'll make some corrections to this thread tomorrow afternoon

SIM-5172123 - April 19, 2022, 1:22 pm

(Apr 19, 2022 01:03 PM)shatter Wrote: [\[CITE\]](#) This is really misleading thread and none of what you said exists as a vulnerability per say. It's really intercepting the POST requests and you need to be client side to do this. The actual vulnerability that you're posting about is if you were able to intercept this token as third party or someone who should not be intercepting it.

You're literally posting about the functionality of the intercept feature on Burp Suite, this is a laughably poor quality post intended to market as something of value.

WTF are you saying ! are you high man ?!

this thread say " Authentication Bypass via OTP exposure "

i hope you noticed "exposure" also you should read what Blazin mentioned then you will understand what is the difference between server side bypass and client side bypass i never said i do server side bypass as it's just not possible to "bypass" you should do more than this to get over OTP

you also seem lack of knowledge as this functionality not only in Burp-suite, and i show kind of information disclosure vulnerability that lead to account take over if you want more specific title lol

actuly i see your post is very LQ don't post shit on my topic please if you have respectful opinion that can add to the topic you are welcome if not then search for other thread to shit post it

SIM-5172123 - April 19, 2022, 2:06 pm

(Apr 19, 2022 01:40 PM)shatter Wrote: [\[CITE\]](#) via a post request essentially

that's what i said

also

<https://portswigger.net/burp/documentation/desktop/tools/proxy/getting-started-intercept>

yeah dude i have an "authentication bypass" to any application login if i have the password in cleartext that's how authentication works

omg you still try hard to make a point that doesn't exist XD i already mentioned it's exposed you moron and i show to people how they can use this vulnerability " Via/Using " Tool , still posting shit

Horse - April 19, 2022, 2:08 pm

great post very informative hope to see more post by you buddy !

SIM-5172123 - April 19, 2022, 2:19 pm

(Apr 19, 2022 02:08 PM)shatter Wrote: [\[CITE\]](#) exposed in the post request i ensure you if you login to any site it'll expose your credentials with intercept on

>doesn't understand web requests

>doesn't understand authentication

>doesn't understand how tool works

>makes thread showing off how to AuDiT iNsECuRE ApPlicAtIoNs

>???

looks like you didn't understand the tutorial then , in the post i made i was register new account and the site require to send OTP to my mobile as verification step but the programmer didn't do the verification task using thierd party insted he send the OTP using script , and handle the requests in unsafe way that expose data

so please read before comment or just fuck off

SIM-5172123 - April 19, 2022, 2:57 pm

(Apr 19, 2022 02:39 PM)shatter Wrote: [\[CITE\]](#) So it's an information disclosure vulnerability that is not exploitable unless actually chained with another vulnerability such as a XSS since OTP are single use...

It's not an authentication bypass as you stated, you still need credentials.

Not about what I want...

You're misidentifying the vulnerability altogether.

? no i am not and it's authentication bypass , let me explain we might also chat if you want maybe you are correct and maybe i am but don't just attack without understand .

let's say you only know user phone number nothing more , by this vulnerability you can verify you are the owner of the account and take over the full account with only phone number so it's considered authentication bypass and i will make it more clear in next tutorials about Account take over

SIM-5172123 - April 19, 2022, 3:05 pm

(Apr 19, 2022 03:00 PM)shatter Wrote: [\[CITE\]](#) That sounds like a misconfiguration in the

authentication if you can reset the user credential by only the phone number prompt.

I understand the premise and either scenarios require more information than the vulnerability to perform the compromise.

exactly that's why i called it exposure and didn't stop at bypass , you disclose information's that makes you able bypass verification steps

it's so simple i hope everything understandable now and sorry for my bad english maybe it's the reason for this misunderstanding

WntdArt - May 1, 2022, 11:53 am

Yep Burpsuite is a super cool for stuffs like this but I agree with @Blazin it only really works for sites with poor security.

SIM-5172123 - May 1, 2022, 12:21 pm

(May 1, 2022 11:53 AM)WntdArt Wrote: [\[CITE\]](#) Yep Burpsuite is a super cool for stuffs like this but I agree with @Blazin it only really works for sites with poor security.

well i might agree with that but the reality against that ! ex: search for Authentication Bypass vulnerability writeup's you will find hundreds like this in big sites reported

donboss007 - June 28, 2022, 6:38 pm

safsafsafsaf????saaFFFFFFFFFFFFFFFFFFFFFFFFF

Tteppy. - June 29, 2022, 3:58 pm

great post very informative hope to see more post by you buddy !

Ufopw - July 9, 2022, 9:45 am

sir is there a discord address where i can reach you i have questions thank you

millier88 - July 27, 2022, 2:06 pm

are you working for portswigger?

SIM-3956520 - August 8, 2022, 6:17 am

If you do not mind me asking, what is your native language?

qqnsoldier - August 14, 2022, 4:21 am

this won't work in 99% of the cases

the best way is the request a new password method