

Forum:[Hack Forums](#)

Thread: [OTP Bypass Techniques](#)

#AfterDark - August 20, 2024, 10:06 pm

Sure feels good to be back on HF! Here's my contribution for being back to this amazing community.

This will demonstrate several methods to bypass OTP (One-Time Password) verification during account registration or login processes using BurpSuite. These techniques can potentially lead to unauthorized access to user accounts, resulting in account takeover. This guide is intended for educational purposes to help you understand common vulnerabilities and improve your skills in penetration testing.

Method 1: Response Manipulation During RegistrationRegister an Account:

Register an account with a mobile number and request an OTP.

Capture the Request:

Enter an incorrect OTP and capture the request in BurpSuite.

Intercept the Response:

In BurpSuite, go to the "Proxy" tab and intercept the response to the OTP verification request.

The response will look like:

```
Code {"verificationStatus":false,"mobile":"9072346577","profileId":"84673832"}
```

Change the response to:

```
Code {"verificationStatus":true,"mobile":"9072346577","profileId":"84673832"}
```

In BurpSuite, edit the intercepted response directly in the "HTTP history" tab.

Forward the Response:

Forward the modified response by clicking on the "Forward" button.

Outcome:

You will be logged into the account.

Method 2: Response Manipulation During LoginGo to the login page and request an OTP.

Capture the Request:

Enter an incorrect OTP and capture the request in BurpSuite.

Intercept the Response:

In BurpSuite, intercept the response to the OTP verification request.

The response will indicate an error (e.g., incorrect OTP).

Modify the Response:

Change the response to indicate success (e.g., replace {"status":"error"} with {"status":"success"}).

Forward the Response:

Forward the modified response by clicking on the "Forward" button.

Outcome:

You will be logged into the account.

Method 3: Intercept and Modify Response StatusRegister two accounts with any two mobile numbers, entering the correct OTP initially.

Capture the Request:

Intercept your request in BurpSuite.

Intercept the Response:

Click on "Action" -> "Do intercept" -> "Intercept response to this request".

Check the Response:

Check the response message for a status, e.g., status:1.

Repeat with Incorrect OTP:

Follow the same procedure with the other account but enter an incorrect OTP this time.

Capture and Modify:

Intercept the response to the request and note the message status, e.g., status:0.

Change the status to status:1.

Forward the Response:

Forward the modified response by clicking on the "Forward" button.

Outcome:

If you are logged in, you have successfully bypassed authentication.

Method 4: Bypass OTP in Registration Forms Using RepeaterCreate an account with a non-existent

phone number.

Intercept the Request:

Intercept the request in BurpSuite.

Use Repeater:

Send the request to the repeater by right-clicking on the request and selecting "Send to Repeater".

Modify the Phone Number:

Go to the Repeater tab and change the non-existent phone number to your phone number.

Use Received OTP:

If you receive an OTP on your phone, use that OTP to register the non-existent number.

Method 5: No Rate LimitingCreate an account.

Capture the Request:

When the application asks for the OTP, enter an incorrect OTP and capture the request in BurpSuite.

Use Repeater:

Send this request to the Repeater by right-clicking on the request and selecting "Send to Repeater".

Check for Rate Limiting:

Set up a payload on the OTP value and repeat the request.

If there is no rate limit, wait for a 200 OK or 302 Found status code.

Outcome:

If you receive a 200 OK or 302 Found status code, you have bypassed the OTP.

Additional Test Cases for Bypassing OTPDefault OTPs:

Test common default OTPs like 111111, 123456, 000000.

Leaked OTP in Response:

Capture the request in BurpSuite and check the response for any leaked OTP.

Old OTP Validity:

Check if an old OTP is still valid by attempting to reuse it.

Ecca - August 20, 2024, 11:19 pm

Hm, interesting, how common would you say is it for this to be exploitable?

D707 - August 20, 2024, 11:37 pm

Sorry for nob question,

What do you mean by 'capture'? Taking screenshot or else?

Oxyd - August 21, 2024, 9:51 am

(Aug 20, 2024 11:37 PM)DZ07 Wrote: [\[CITE\]](#) Sorry for nob question,

What do you mean by 'capture'? Taking screenshot or else?

He means intercepting requests.

You should read Burp Suite documentation, it might give you some valuable information.

<https://portswigger.net/burp/documentation/desktop/getting-started/intercepting-http-traffic>

Pp1llast - August 21, 2024, 10:59 am

What are some sites this works successfully with?

D707 - August 21, 2024, 3:22 pm

(Aug 21, 2024 09:51 AM)Oxyd Wrote: [\[CITE\]](#) He means intercepting requests.

You should read Burp Suite documentation, it might give you some valuable information.

<https://portswigger.net/burp/documentation/desktop/getting-started/intercepting-http-traffic>

Thanks, friend.

#AfterDark - August 21, 2024, 4:41 pm

(Aug 20, 2024 11:19 PM)Ecca Wrote: [\[CITE\]](#) Hm, interesting, how common would you say is it for this to be exploitable?

Quite common actually! The trick is identifying the correct endpoint. I have come across quite a few that do the OTP logic on the client side. Using burp you can easily manipulate it.

Now with the big boys such as Okta, OAuth and others its a little trickier, but then again depends on how it is configured.

At the end of the day. nothing is 100% secure ;) #hacktheplanet

(Aug 21, 2024 09:51 AM)Oxyd Wrote: [\[CITE\]](#) He means intercepting requests.

You should read Burp Suite documentation, it might give you some valuable information.

<https://portswigger.net/burp/documentation/desktop/getting-started/intercepting-http-traffic>

Correct! And thank you Oxyd.

Portswigger got some really good Labs on Bug bounties as well that I would highly recommend.

tongken665 - August 24, 2024, 4:43 am

VERY INTERESTING and will look up more this software

Money- - August 24, 2024, 6:38 pm

Good methods but very common ones. Is mostly used in bug bounties and pentesting but yea pretty much all the public checklist and articles have these.

01Hidden10 - August 25, 2024, 5:02 am

Very intersting , should try

Kaleb - August 25, 2024, 5:05 am

Actual cool high quality thread. Wonder how many of these work on bigger websites. I was reading a recent paper about Russian Twitter bots powered by LLMs and during the registration they had some sort of bypass for verification of the accounts.

DramaKing - August 26, 2024, 7:02 am

How does one even capture an SMS OTP request in BurpSuite?? ? And how are SMS OTPs done client-side?

#2 sounds like one is supposed to capture a response to the incorrect OTP, and repeat it back to the server after changing the false response to true. ?

Money- - August 26, 2024, 7:10 am

(Aug 26, 2024 07:02 AM)DramaKing Wrote: [\[CITE\]](#) How does one even capture an SMS OTP request in BurpSuite?? ? And how are SMS OTPs done client-side?

#2 sounds like one is supposed to capture a response to the incorrect OTP, and repeat it back to the server after changing the false response to true. ?

You can , Websites or mobile application just turn on burp suite when you register an account after entering the mobile field.

It will capture the OTP being sent.

#2 Capture the response of the false OTP and modify the response to a correct one.

Usually this is done by first checking what does the correct response looks like and then you navigate back to the false one to try it out to prove the vulnerability.

Right click on the request and click intercept response then from there you can modify the response and forward it to the server via Burp Suite.

These are all bug bounty checklist or pentest checklist for OTP test cases , well just the common ones.

I done these before in my bug hunt journey as well as my pentest engagements.

=====

Btw man , your signature you found those public wifis and submit it on that site wigi.net etc?

DramaKing - August 26, 2024, 7:16 am

(Aug 26, 2024 07:10 AM)Money- Wrote: [\[CITE\]](#) Btw man , your signature you found those public wifis and submit it on that site wigi.net etc?

Okay then. Have to do my own testing then. Yes, I've been on wigle, since before I started my pentest journey.

Money- - August 26, 2024, 7:21 am

(Aug 26, 2024 07:16 AM)DramaKing Wrote: [\[CITE\]](#) Okay then. Have to do my own testing then. Yes, I've been on wgle, since before I started my pentest journey.

I sent you a convo previously btw , you read or you just dint bother replying lol?

cam667 - October 28, 2024, 3:42 pm

wow engineer really and I would never think I think I will try on Skype maybe it will work

diabloshulu - November 7, 2024, 9:02 pm

Oh yeah! This is the tutorial I was looking for, although I've seen it elsewhere. But I'm not sure who sent out such technology first, but I'm sure you are the first!

hayaletthikayesi - November 21, 2024, 7:49 pm

Can it be used in online games?