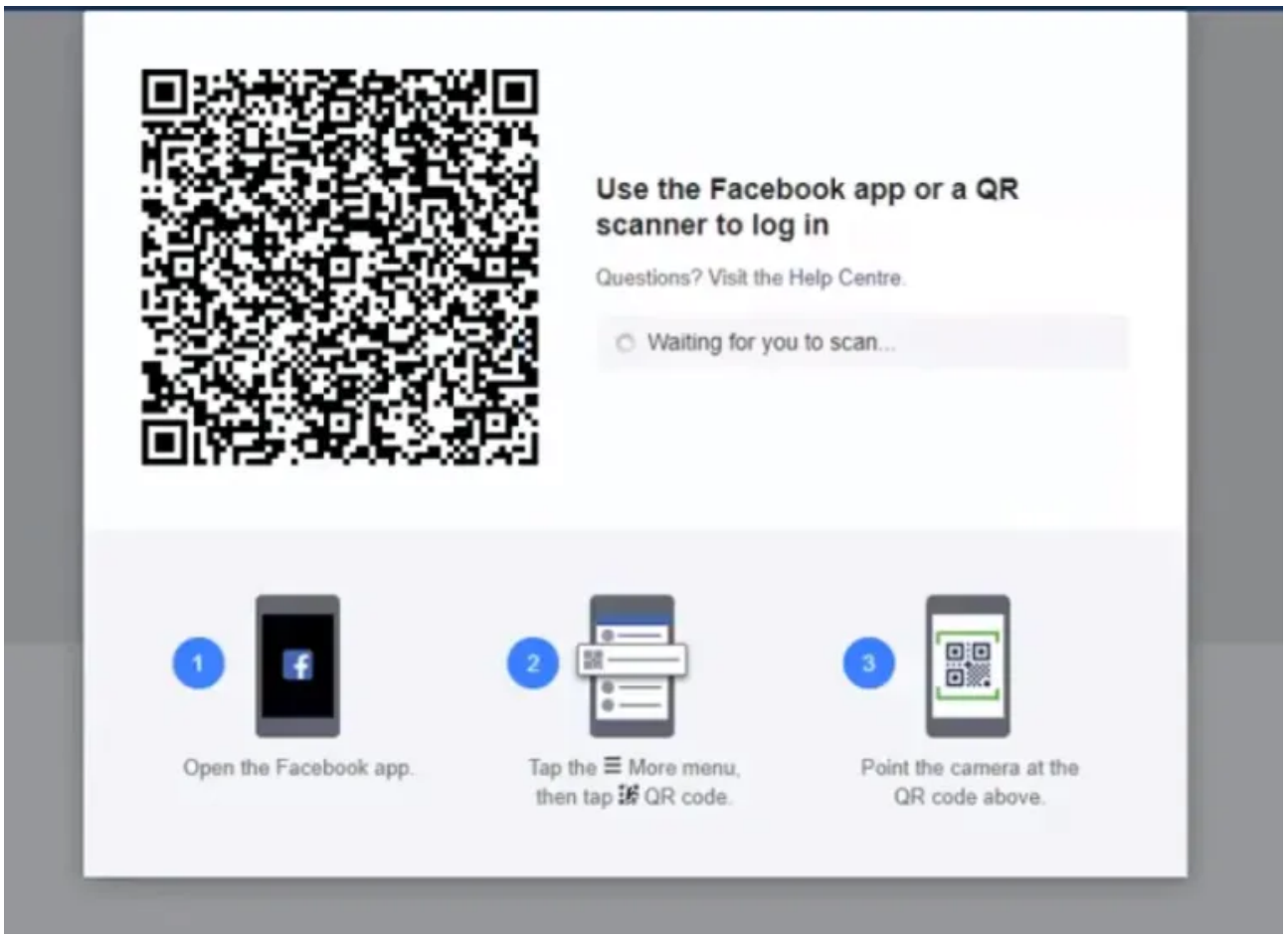
HOW I WAS ABLE TO TAKEOVER FACEBOOK ACCOUNT | Bug Bounty Poc

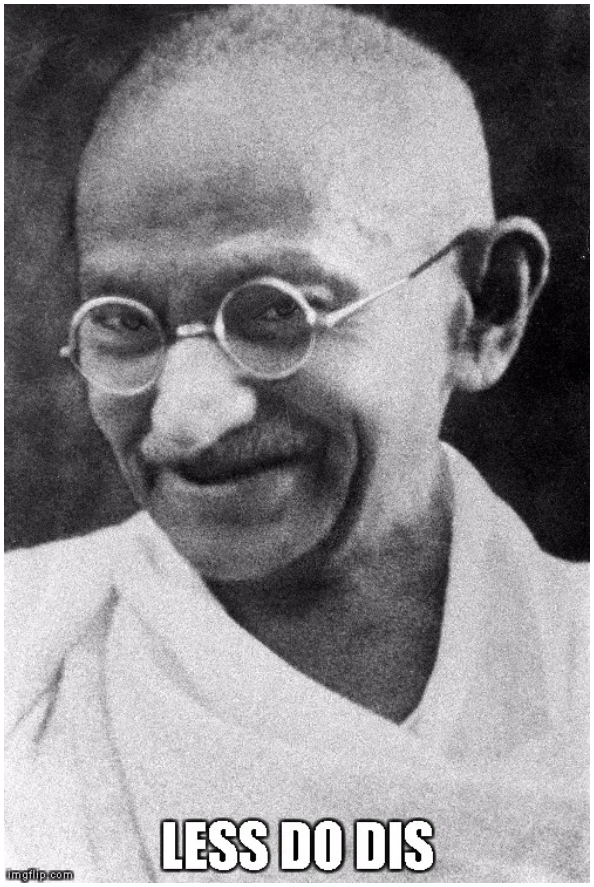
December 10, 2017 | | BugBounty POC

HOW I WAS ABLE TO TAKEOVER FACEBOOK ACCOUNT | Bug Bounty Poc

hey all here is ameer hamza, Facebook has recently introduced login with phone functionality if you have forgotten your password. however I was able to exploit it which leads to access the facebook account.login with phone button pops a qr code to scan :



so i thought why not try to break it ?



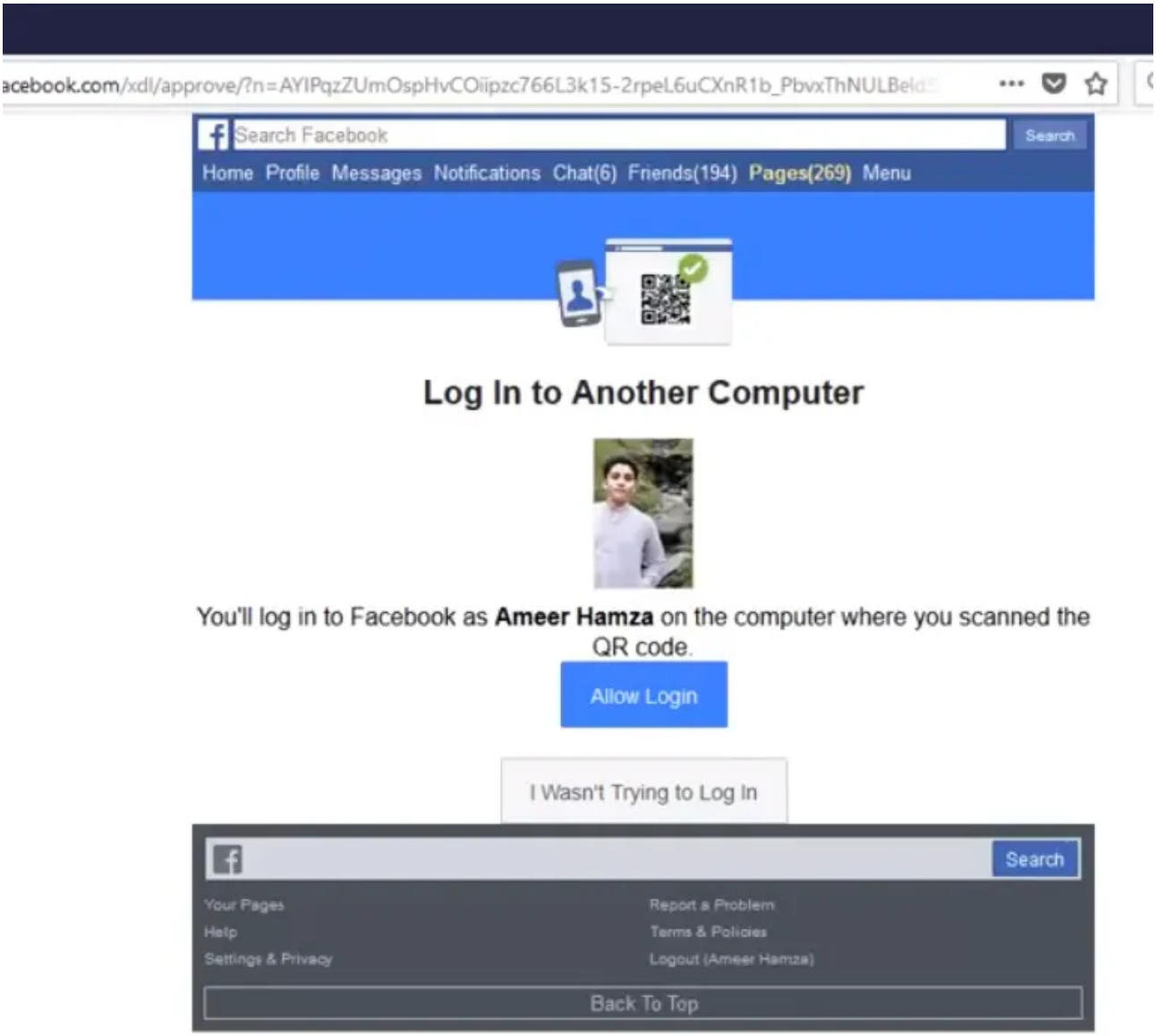
firstly i tried to decode the qrcode using QrCode Decoder here is what i got :

Decode Succeeded

Raw text	https://m.facebook.com/xdl/approve/?n=AYK8pQLRNK7UtXH77qI48xUnEHXb0rf2ySjUTHVjA6H-pU5gkI1JPYzit6wCp2z1tTNKZbXScD4MUshQuaP5M9H9j0e_x2ZK0ee9jkjLvv5-sQ&d=AYItt0ByoBCJEFQNGwike6sOHJyPJvDTCOruRgesi-7vvdIm4T3g22-FUW0f0Jph6gPYE3t10SddJ-rS7fg-z9VI&ext=1512136729&hash=AYKa_wmq-7CeeTac
Raw bytes	40 02 b6 87 47 47 07 33 a2 f2 f6 d2 e6 66 16 36 56 26 f6 f6 b2 e6 36 f6 d2 f7 86 46 c2 f6 17 07 07 26 f7 66 52 f3 f6 e3 d4 15 94 b3 87 02 00 f2 9e 6b 38 b7 90 01 19 d1 61 20 dc dd c5 24 d0 e1 e1 55 b9 15 21 61 88 c1 c9 98 c9 e5 4d a9 55 51 21 59 a0 04 d9 20 b5 c1 54 d5 9d ad 24 c5 29 41 65 e9 a5 d0 d9 dd 0d c0 c9 e8 c5 d1 51 39 2d 09 89 61 4d 8d 10 d1 35 55 cd a1 45 d5 84 80 34 6a 7c ec 19 00 06 9a 8c 19 57 de 0c 96 92 cc 19 59 4e 5a 9a da 93 1d 9d 8d 4b 5c d4 49 99 0f 58 56 52 5d 1d 0c 18 9e 5b c8 04 1f b6 ca af 60 da 00 26 3b b4 b5 b2 9b 39 a7 a4 25 3c a0 25 3b 22 2a 21 a7 b9 3a a9 33 b2 b9 b4 96 9b bb 3b 32 24 b6 9a 2a 19 b3 99 19 16 a3 2a ab 98 33 18 25 38 34 1b 33 a8 2c a2 99 ba 18 98 29 b2 32 25 16 b9 29 9b b3 33 96 bd 1c ab 24 93 32 bc 3a 1e 88 05 12 e6 ad 41 28 00 2c 4c d0 c2 e6 d0 7a 82 b2 96 c2 be ee da e2 5a 6e 86 ca ca a8 c2 c6 00 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec
Barcode format	QR_CODE
Parsed Result Type	URI
Parsed Result	https://m.facebook.com/xdl/approve/?n=AYK8pQLRNK7UtXH77qI48xUnEHXb0rf2ySjUTHVjA6H-pU5gkI1JPYzit6wCp2z1tTNKZbXScD4MUshQuaP5M9H9j0e_x2ZK0ee9jkjLvv5-sQ&d=AYItt0ByoBCJEFQNGwike6sOHJyPJvDTCOruRgesi-7vvdIm4T3g22-FUW0f0Jph6gPYE3t10SddJ-rS7fg-z9VI&ext=1512136729&hash=AYKa_wmq-7CeeTac

the url i got was : https://m.facebook.com/xdl/approve/?n=AYK8pQLRNK7UtXH77qI48xUnEHXb0rf2ySjUTHVjA6H-pU5gkI1JPYzit6wCp2z1tTNKZbXScD4MUshQuaP5M9H9j0e_x2ZK0ee9jkjLvv5-sQ&d=AYItt0ByoBCJEFQNGwike6sOHJyPJvDTCOruRgesi-7vvdIm4T3g22-FUW0f0Jph6gPYE3t10SddJ-rS7fg-z9VI&ext=1512136729&hash=AYKa_wmq-7CeeTac

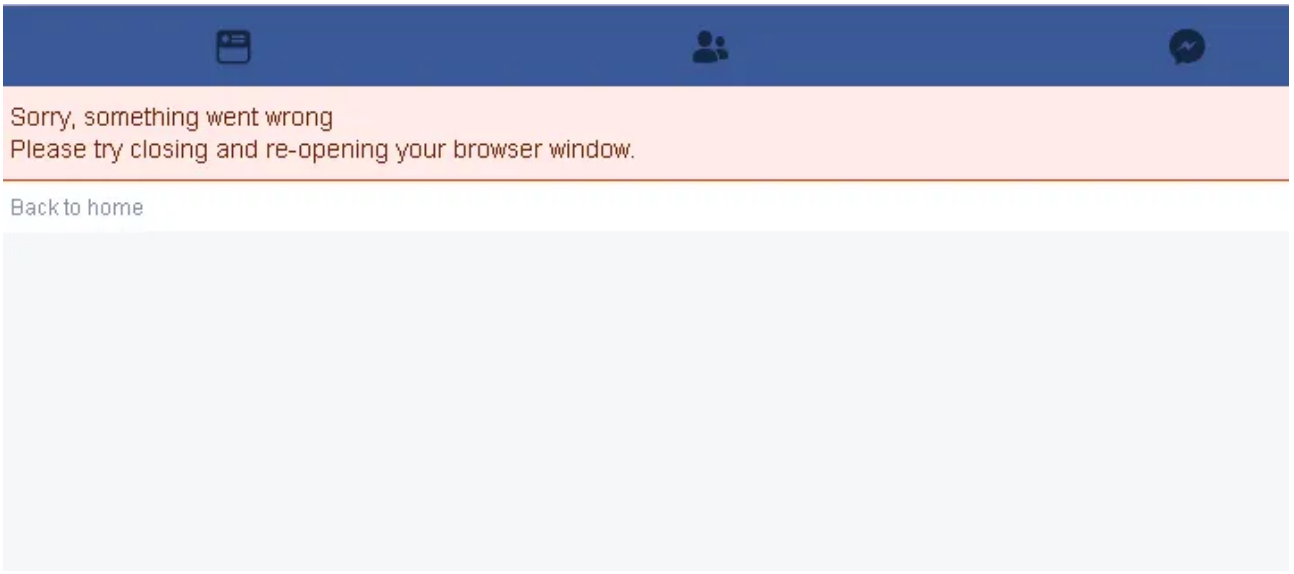
open the url these are the options I got :



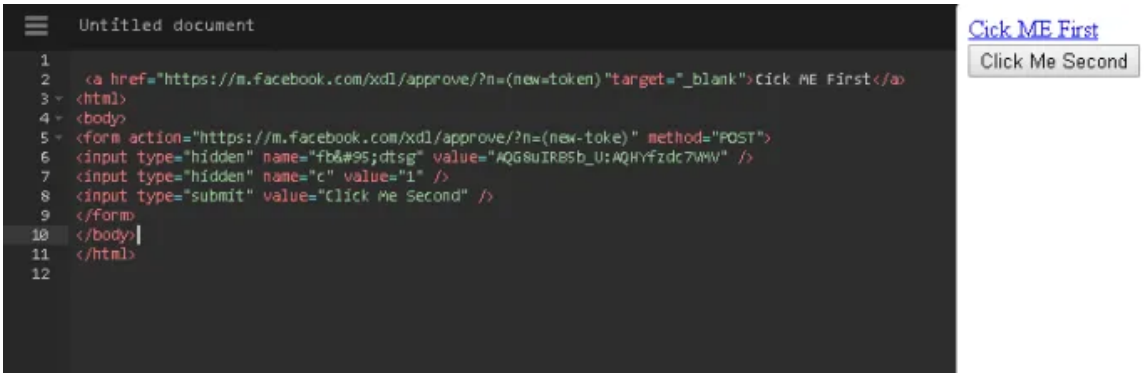
just capture the request and send it to repeater while dropping the request too so that the code don’t get expired ,changed the fb_dtsg value to AQG8uIRB5b_U:AQHYfzdc7AB from AQG8uIRB5b_U:AQHYfzdc7VMV and it just got accepted ! 😀 (no screenshot available -_-)

Didn’t thinking for a while to create a csrf form :

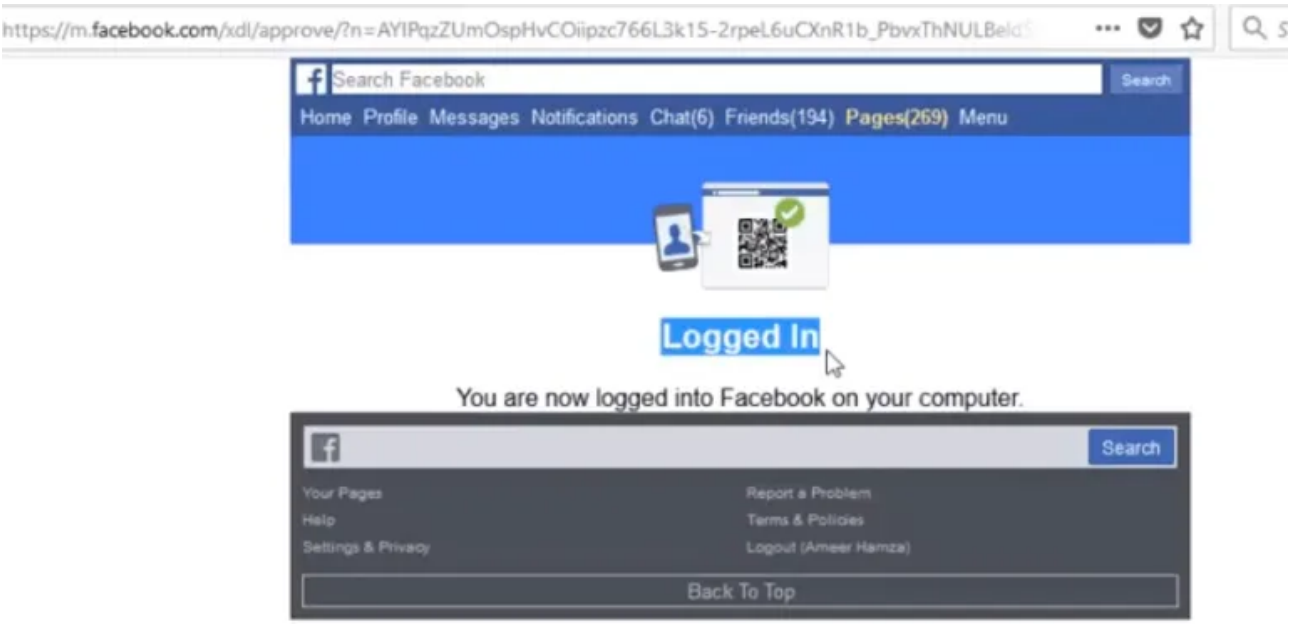
Shit! the request got aborted :/ :



for understanding all the shit qr code does. monitored all the request again and after 2 to 3 hours of brainfuc*k hence, came to know that its important for the victim to open the link first so that the fb server could detect it as scanning the qr code . i quickly made the csrf form again :



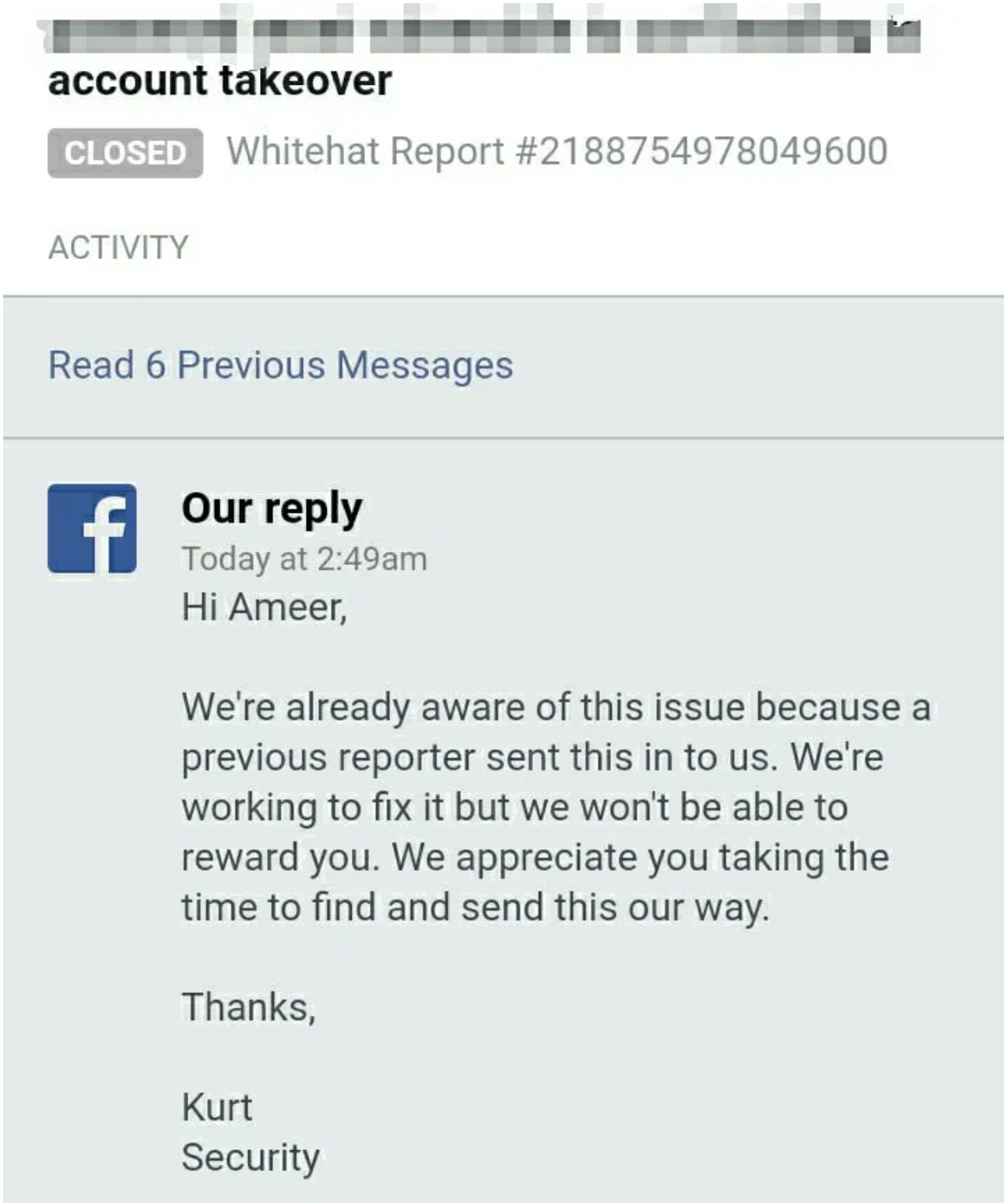
and here comes the response 😀 :



I was like :

tested it on 2,3 accounts and hopefully this bug was legit ! and here is the poc I made:

after three days of waiting and 4 any update replies this got duplicated 🙁 :



Bug : Qr code's allow login/i wasn't trying to login form was vulnerable to csrf

Impact : this security issue leads any attacker to gain access of the victims account.

Reward : n/a

That's all fellas ! Hope you enjoyed my write up , Thanks to Muhammad Khizer Javed

Best Regards, Ameer
Hamza

Share this:

Like this:

Loading...

How I was able to Download Any file from Web server!
January 27, 2018
In "BugBounty POC"

Unrestricted File Upload to RCE | Bug Bounty POC
December 19, 2017
In "BugBounty POC"

IDOR User Account Takeover By Connecting My Facebook Account with victims Account
September 16, 2018
In "BugBounty POC"

About the Author

‹ My Guide to Basic Recon? | Bug Bounties + Recon | Amazing Love story.

Unrestricted File Upload to RCE | Bug Bounty POC ›

3 thoughts on “HOW I WAS ABLE TO TAKEOVER FACEBOOK ACCOUNT | Bug Bounty Poc”

Kartik singh

December 10, 2017, 4:36 pm

I have reported it last month, that’s why you have got it duplicate. Anyways nice blog.

★ Loading...

Edit this comment Reply

Sidharth B

December 10, 2017, 4:52 pm

Good job man

★ Loading...

Edit this comment Reply

Jacob

November 21, 2018, 7:34 pm

I’m confused… you have to already have access to the account in order to get the qr code , so what exactly was the attack here? You used the login to login to an account you already had access to?

★ Loading...

Edit this comment Reply

Leave a Reply

Enter your comment here...

ADS

Search ... Search

CATEGORIES

BugBounty POC

News

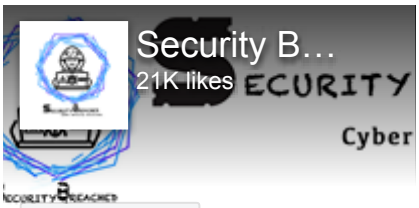
Tutorials

Uncategorized

BLOG STATS

100,114 hits

SECURITY BREACHED



Like Page

Be the first of your friends to like this

FOLLOW ME ON TWITTER

M. Khizer Javed
@KHIZER_JAVED47

Replying to @KHIZER_JAVED47

I'm on Payoneer from 2016 when i joined @Bugcrowd it really helped me get a huge amount of money easily and effectively. So i hope maybe @Hacker0x01 can do something about it? 😇

Dec 6, 2019

M. Khizer Javed
@KHIZER_JAVED47

Replying to @KHIZER_JAVED47

I see @Payoneer as good alternate payment method to Paypal, BTC & Bank transfer as, in bank transfer i have so many issues mainly the bank i use actually asked me hell lot of questions because payment was coming from Hackerone. Hacker in name lol system got an alerted.

Dec 6, 2019

M. Khizer Javed
@KHIZER_JAVED47

Hey @Hacker0x01 any Plans to add some new Payment Methods? Mainly @Payoneer It's pretty useful for many of us who don't have a direct @PayPal account due to country restrictions and on direct bank transfer many questions are asked. @jobertabma maybe take it as request? 🙂

Dec 6, 2019

USERONLINE

1 User Online

ADS