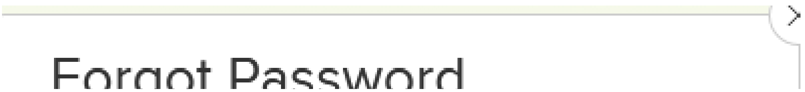
Avinash Jain (@logicbomb_1) Follow
Feb 3, 2018 · 3 min read

#BugBounty—“I don’t need your current password to login into your account” - How could I completely takeover any user’s account in an online classified ads company.

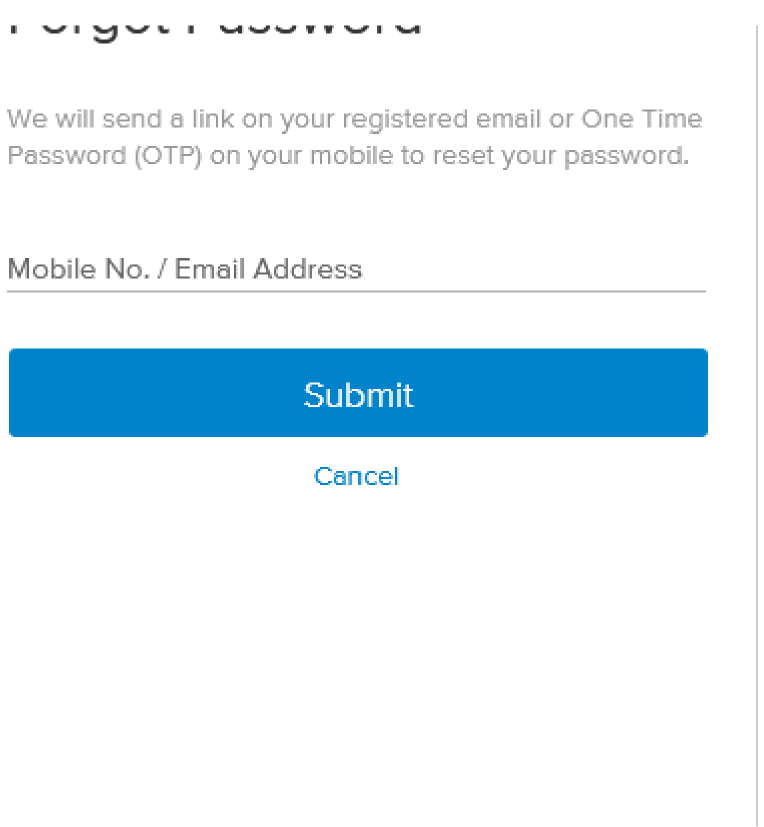
Hi Guys,

“*User account compromise*” ! Yes, you read right . This was an excellent vulnerability which I have found recently during my bug bounty hunting in India’s most popular online classified ads company.

“An **OTP** is more **secure** than a static password, especially a user-created password, which is typically weak” and we all agree to this but what if someone could bruteforce it and what if someone could bypass OTP authentication? That what makes it vulnerable and targeting the same , I carried out this critical piece of hunt. Let’s see into the details —



Forgot Password



Forgot Password

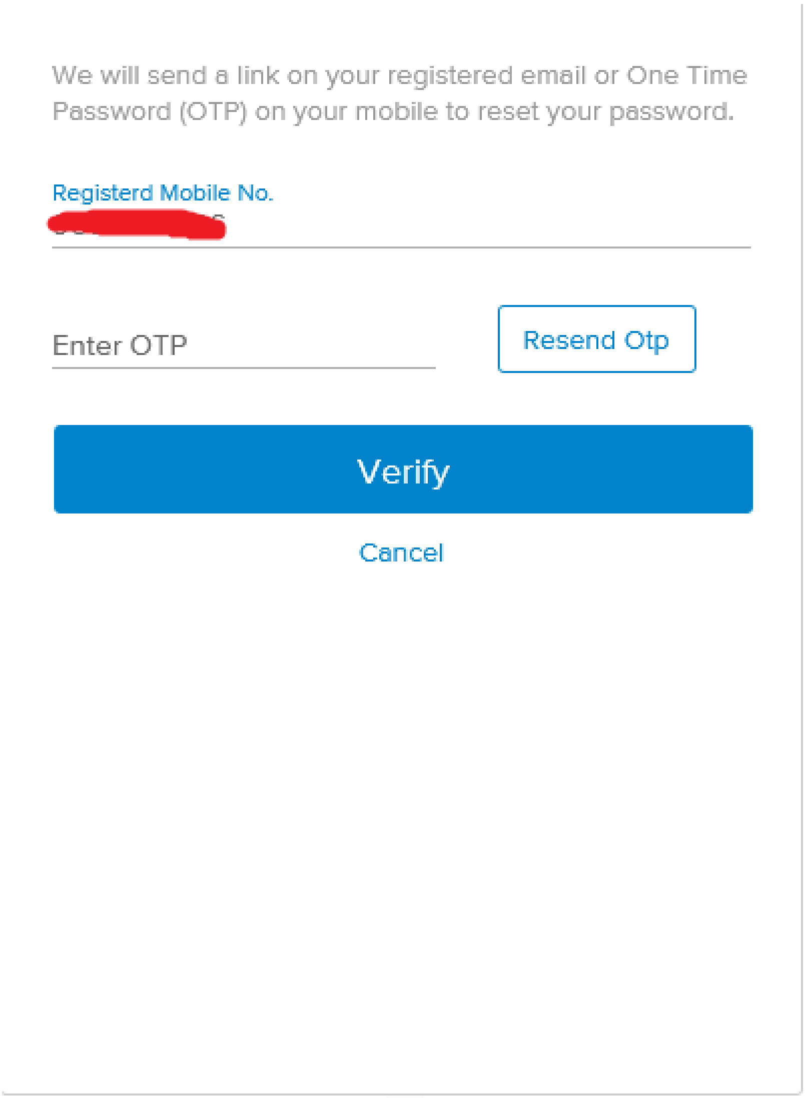
We will send a link on your registered email or One Time Password (OTP) on your mobile to reset your password.

Mobile No. / Email Address

Forgot Password Page

While browsing through the website for some vulnerabilities , I went to the "Forget Password" functionality where it asked me to enter the registered mobile number .

Forgot Password



We will send a link on your registered email or One Time Password (OTP) on your mobile to reset your password.

Registerd Mobile No.

[redacted]

Enter OTP

OTP Verification Page

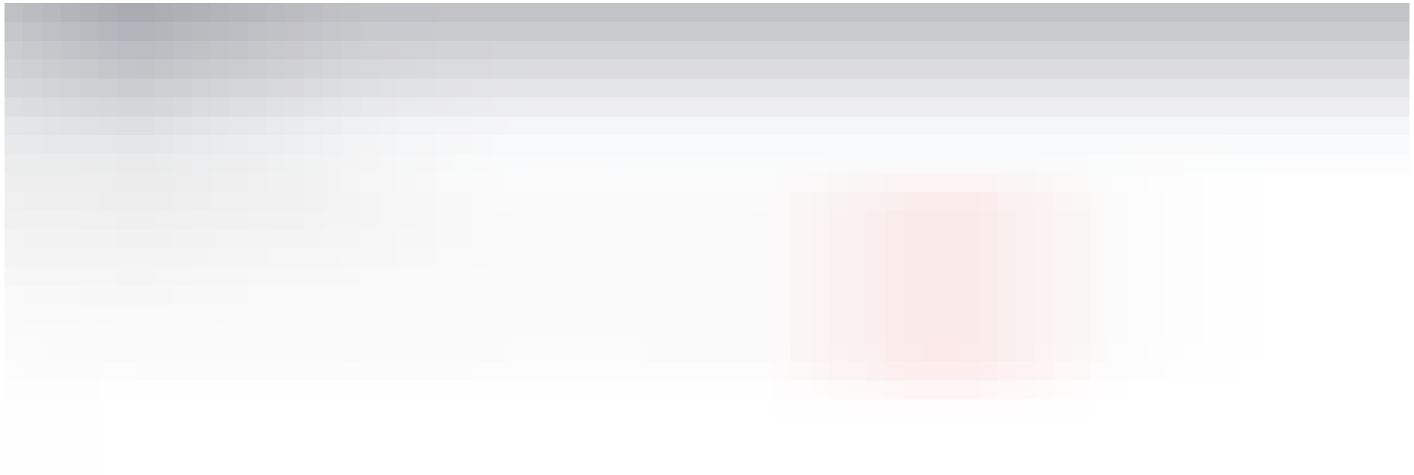
and as I entered the number , it sent me an OTP and after filing the right OTP in the form , it redirected me to “New password page” where I was allowed to set a new password for my account.

I firstly jumped into the most common and basic attack to bypass OTP— bruteforcing attack to see if there is any rate limiting or captcha being implemented but as I phrased it “most common and basic” , so it was not going to help me and captcha was also implemented there after 3 consecutive wrong attempts.

Let’s dive into this more. When I entered the wrong OTP, I got the following as the response —

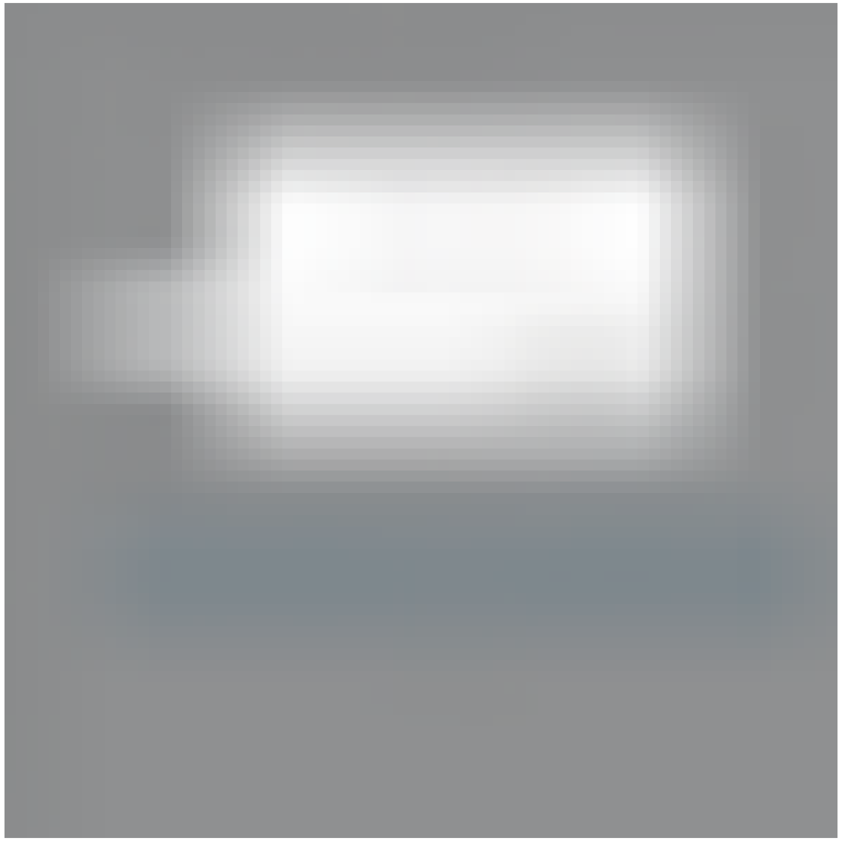
Wrong OTP HTTP Response

Notice status parameter as “401” which means “ Unauthorized Error response” and that was obvious too as I entered the wrong OTP. Now to check whether it is just based on client side validation , I tried to bypass it . Captured the response , changed the “status” json parameter value to “200” and forwarded the response -



Changed HTTP Response

But some validation was there and it throws me the error message-

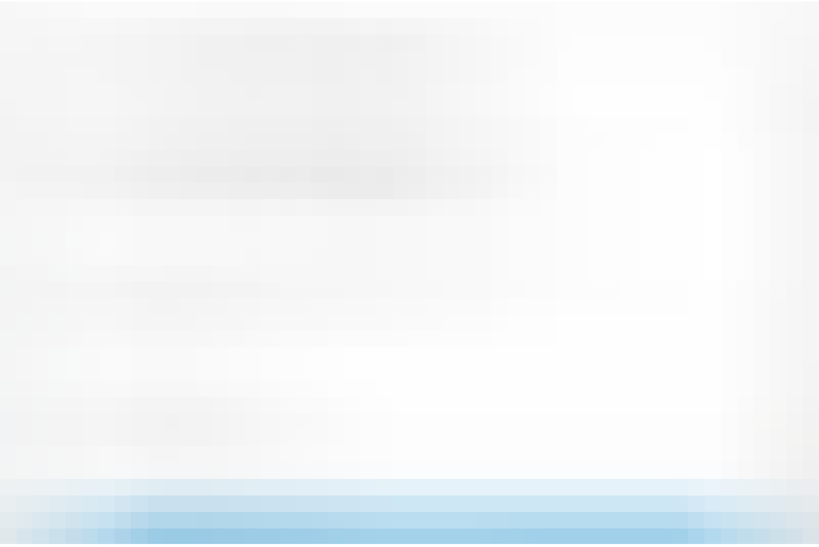


Invalid OTP Error Message

Might be the other parameters are causing the validation error so this time I removed all the json parameters and added the success parameter with the value to “true” so now the response json looks like —

Modified HTTP Response

and this time I was redirected to “Set Password Page” :D -



Forgot Password Page

I was able to set a new password for the user and using the changed password I was able to successfully login into the user's account. This is how I could bypass OTP authentication and set a new password for the user and able to completely compromise his account using his mobile number.

Report details -

07-Jan-2018—Bug Reported to the concerned company.

27-Jan-2018—Bug was marked fixed.

03- Feb-2018—Re-tested and confirmed the fix.

28-Feb-2018— Rewarded by the company .

This was all about this interesting finding. ☺

Thanks!

~Logicbomb (https://twitter.com/logicbomb_1)

Security Bug Bounty Vulnerability Hacking Penetration Testing

852 claps

8

Avinash Jain (@logicbomb_1)

Follow

Lead Infrastructure Security Engineer @groferseng | DevSecops | Part time BugBounty Hunter | Acknowledged by Google, NASA, Yahoo, United Nations, BBC etc.

InfoSec Write-ups

Follow

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. #sharingiscaring

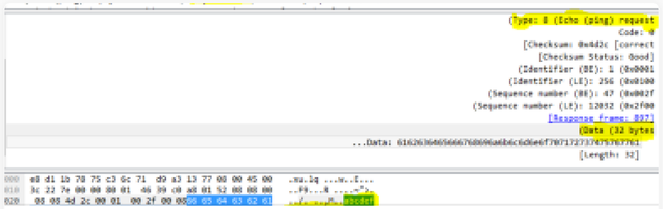
More from InfoSec Write-ups

Writing a Password Protected Bind Shell (Linux/x64)

0x0FFB347

Mar 8 · 5 min read

246



```
(Type: 8 (Echo (ping) request
                         Code: 0
     [Checksum: 0x4d2c [correct
       [Checksum Status: Good]
   (Identifier (BE): 1 (0x0001
  (Identifier (LE): 256 (0x0100
 (Sequence number (BE): 47 (0x002f
(Sequence number (LE): 12032 (0x2f00
             [Response frame: 897]
                   (Data (32 bytes
...Data: 6162636465666768696a6b6c6d6e6f707172737475767761
                     [Length: 32]

e8 d1 1b 78 75 c3 6c 71  d9 a3 13 77 08 00 45 00   ..xu.lq ...w..E...
3c 22 7e 00 00 00 01  46 39 c0 a8 01 52 00 00 00   ..F9...R ......
08 00 4d 2c 00 01  00 2f 00 00 66 65 64 63 62 61   ..M,.../..abcdef
```

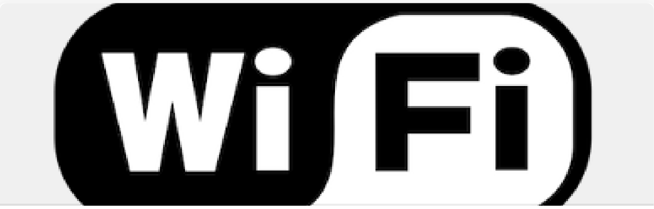
More from InfoSec Write-ups

Ping Power — ICMP Tunnel

Nir Chako

Dec 17, 2018 · 8 min re

488



More from InfoSec Write-ups

How to Make a Captive Portal of Death

Trevor Phillips

Dec 18, 2018 · 6 min re

280

Responses

Write a response…

Applause from Avinash Jain (@logicbomb_1) (author)

Imran Parray
Feb 5, 2018

it proves that you didn’t need only technical skills to be a good hacker rather u need a hacker mindset to hack anything….

22

Conversation between Ak1T4 and Avinash Jain (@logicbomb_1).

Ak1T4
Feb 4, 2018

where do you get the “success”:”true” params?

14

1 response

Avinash Jain (@logicbomb_1)
Feb 4, 2018

It was by general observation in various application.

70

Conversation with Avinash Jain (@logicbomb_1).

Rafael Fidelis
Feb 13, 2018

> An OTP is more secure than a static password

If you can explain what’s is “OTP” before will be a good thing. Nice hacking, thanks for sharing

12

1 response

Avinash Jain (@logicbomb_1)
Feb 13, 2018

OTP is one time password , the code that is sent on the mobile phone for verification.

13

Conversation with Avinash Jain (@logicbomb_1).

Yugesh Rathour
Mar 2, 2018

Hey Avinash, It’s a very interesting find. What additional controls can be placed to mitigate this kind of issues? I too, myself came across a variant of OTP bypass similar to this issue.

1 response

Avinash Jain (@logicbomb_1)
Mar 2, 2018

Thanks for appreciation Yugesh. The mitigation here is simple, there was no server side validation hence server side validation for the OTP should be implemented in this case. You can dm to my twitter any time. ☺

1

Conversation between Avinash Jain (@logicbomb_1) and Manoj.

Manoj
Mar 18, 2018

Great job Avinash !!!

How do you know that using “200" is going to work ?

1 response

Avinash Jain (@logicbomb_1)
Mar 18, 2018

Thanks Manoj for the appreciation. Through this, I was checking whether it is just based on client side. When the browser gets the following success response, it will throw you to next successive page if there is no server side validation.

1

1 response

Manoj
Mar 19, 2018

Yes…and using token validation will mitigate this problem.…actually this problem will never happen

1

Conversation with Avinash Jain (@logicbomb_1).

Manoj
Mar 21, 2018

So ….Did you got rewarded??

1 response

Avinash Jain (@logicbomb_1)
Mar 21, 2018

Yup. You can see the report details at the end of the blog. ☺

1 response

Manoj
Mar 21, 2018

Nope..There it was mentioned reward awaiting for now.. anyways good work 👏 …one more thing I think you have removed DM for your Twitter account 🙄

1 response

Avinash Jain (@logicbomb_1)
Mar 21, 2018

so I have 2 things to edit, this post and DM setting. Thanks Manoj ☺

1

Show all responses