

Forum:[Hack Forums](#)

Thread: [Facebook Password reset vulnerability allowed hackers to hijack any FB account](#)

c00perzz - March 7, 2016, 9:58 pm

Quote:Hacking Facebook is one of the most sought queries on Google search because a lot of Facebook accounts are valuable. So much so that security researchers spend their valuable time and resources to hunt for vulnerabilities in Facebook in search of that elusive big break. One such ethical researcher, Anand Prakash has hit a jackpot with hacking Facebook. He has found a critical vulnerability in Facebook which could have allowed him to hack into any FB account without a sweat.

The vulnerability which Prakash found, resides in the way Facebook's beta pages handle 'Forgot Password' requests. Normally, when you forget your password, Facebook gives you an option to get back into your FB account using 'Forgot Password' option which then sends a 6 digit code on your phone number/email address to your mobile phone. After you enter this code in the window, you are able to access your FB account and reset your password.

Prakash decided to test the vulnerability in Facebook's Forgot Password mechanism. He tried to brute force the 6 digit code in the 'Forgot Password' window but since Facebook has placed a limit of 12 attempts he was unsuccessful and locked out after 12 attempts.

He then turned his attention to Facebook's beta pages, [beta.facebook.com](#) and [mbasic.beta.facebook.com](#) and found that the rate limit was missing on forgot password endpoints in these two pages. Once he found that there was no limitation, he could brute force into any Facebook account without worrying about the limits.

Vulnerable request:

```
POST /recover/as/code/ HTTP/1.1 Host: beta.facebook.com
lsd=AVoywo13&n=XXXXX
```

Brute forcing the "n" successfully allowed Prakash to set new password for any Facebook user.

[Video: <https://youtu.be/U3Of-jF1nWo>]

Prakash reported the issue to the Facebook's security team on 22nd Feb 2016. Facebook immediately acknowledged the severity of the vulnerability and issued a fix on 23rd Feb. It also awarded Prakash a bug bounty of \$15,000 which is among the top bounties by the networking giant.

<http://www.techworm.net/2016/03/facebook-password-reset-vulnerability-allowed-hackers.html>

Roytoy - March 7, 2016, 10:07 pm

Seems that it goes without saying that there should be a limit.

Mr. Robot - March 7, 2016, 10:09 pm

This is exactly when people shouldn't share knowledge lol

L3TM3IN - March 8, 2016, 1:39 am

(Mar 7, 2016 11:09 PM)Mr. Robot Wrote: [\[CITE\]](#) This is exactly when people shouldn't share knowledge lol

This is exactly when fuckers like you don't even read the whole thing
he reported it to facebook weeks ago and received 15k usd bounty