IDOR IN PASSWORD RESET FORM:

FACEBOOK URL TAMPERING AND SQL INJECTION

DESCRIPTION OF THE VULNERABILITY
Facebook URL tampering by unknown telegram number.

SUMMARY

In my Telegram I got a facebook link in which offering 500 R's in paytm by loving in phishing by asking details, (receive a message or link asking for personal information, which may or may not look suspicious) . [These information provides the attacker all they need to gain access to your Facebook account. You could receive an email telling you that there is a problem with your Facebook account and that you need to log in to correct the issue].

SQL injection is a web security that allows an attacker to interfere with the quaries that an application makes to its database.
The impact SQL injection can have on a business is far-reaching. A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database,

STEPS TO IDENTIFY / REPRODUCE TO SECURE YOUR DEVICE
Do not believe on false claims send by unknown use non VPN browser which shows secure or unsecure logos on google url webpage

How to Get secure from them

These emails have a convenient link to follow that leads to a Facebook lookalike site. Once the you land on this imposter website, you are prompted to log in. When you do, the hacker harvests your credentials. Pay careful attention to the uniform resource locator (URL) to be certain you are going to www.Facebook.com. Anything else is likely to be a fake.

How do I Identified that:-
It has an offer of 500 rs in red smaller design that originally that facebook doesn't have. And these link I have got from an unknown number.

I have installed a phone software which protects me from internet surfing which shows that an unsecure link do you want to open but I opened the link. By the red smaller design I realised that It's a URL tampering

SQL
Payloads

Voice Based Sql Injection

It is a sql injection attack method that can be applied in applications that provide access to databases with voice command. An attacker could pull information from the database by sending sql queries with sound.

WEBSITE
https://www.trustedsec.com

URL TAMPERED MODULE

1) Starting Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social - Engineer Toolkit for similar versions
5) Update SET configuration
6) Help, Credits, and About(information)
7) Finallt Exit the Social-Engineer Toolkit
set

IMPACT ON SQL INJECTION

Admin account takeover vulnerability for database system

Just like a data breach can be the result of a SQL injection vulnerability.

USING BURP TO EXPLOIT SQL INJECTION VULNERABILITIES : UNION OPERATOR
Once you have established that a database is vulnerable to SQL injection, it is often useful to exploit the vulnerability to demonstrate any potential implications. A successful SQL injection exploit can potentially read sensitive data from the database, modify database data, execute administration operations on the database and in some cases issue commands on the operating system.

The UNION operator is used in SQL to combine the results of two or more SELECT statements. When a web application contains a SQL injection vulnerability that occurs in a SELECT statement, you can often employ the UNION operator to perform an additional query and retrieve the results.

MIGRATION (CONCLUSION)

Don't trust the user inputs.