Name: Syeda Nowshin Ibnat

ID: 17183103020

Intake: 39 Section: 02

Dept. of CSE, BUBT

Semester: Fall 2021-2022

Home Work - 3

1 No Q Ans:

Solⁿ: From the scenario given on the question we understand that Mr. Anisuzz is a victim of phishing attack. The tools and services such as HiddenEye, Gophish, shellphish etc. enhance the ability to detect and stop phishing attack. Phishing attacks are of the most common security challenges that both individuals and companies face in keeping their information secure. Whether it's getting access to passwords, credit cards, or other sensitive informations, hackers are using email, social media, phone calls and any form of communication they can to steal valuable data.

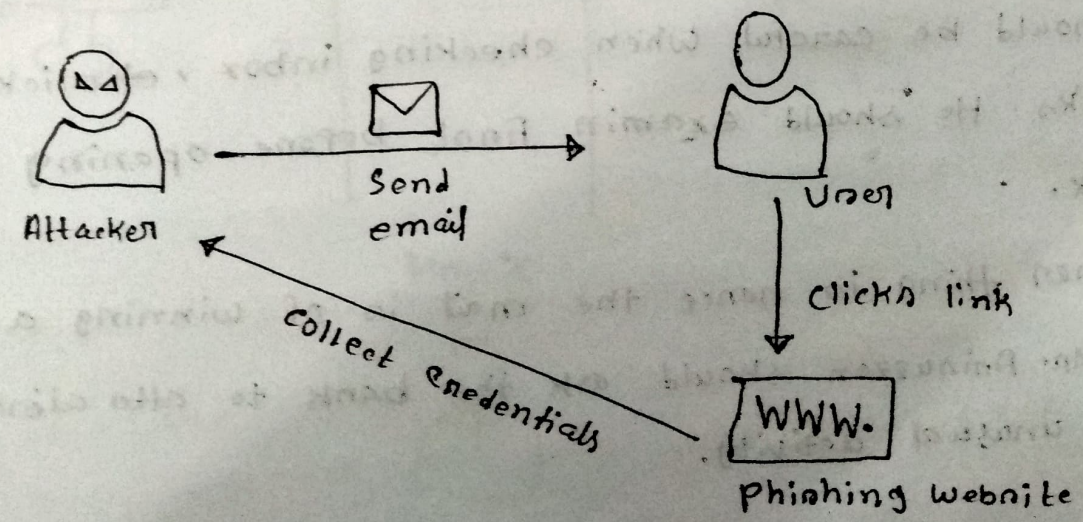

Figure: Phishing attack

The potential countermeasures Mr. Anisuzzan may take ~~to~~ :-

1. change passwonds:- Mr. Anisuzzan should ~~log in~~ change the passwond of the real LinkdIn site.

2. Scan computer for virus: It's a good idea to scan his computer for viruses and malware.

3. Watch out for warning signs of identity theft: If he had revealed any financial information or other ~~sen~~ sensitive data like social security numbers, he needs to watch for signs of ~~idenoity~~ identity theft.

4. Contact with the organization: Report the phishing scheme to his email provider.

5. Protect against future phishing schemes: Mr. Anisuzzan should be careful when checking inbox, ~~eh~~ clicking links. He should examin first before opening ~~an~~ a link.

Another thing is hence the mail is of winning a lottery so Mr. Anisuzzan should ask the bank to ~~atto~~ alert of any unusual activity.

Q No Q Ans:

Soln: From the scenario given in question we understand that Bob and Shella are the victims of a man in the middle attack. A MITM attack is a form of cyber-attack where a user is introduced with some kind of meeting between the two parties by a malicious individual, manipulates both parties, and achieves access to the data that the two people were trying to deliver to each other. Some popular MITM tools are: Bettercap, Proxy.py, Burpsuit etc.

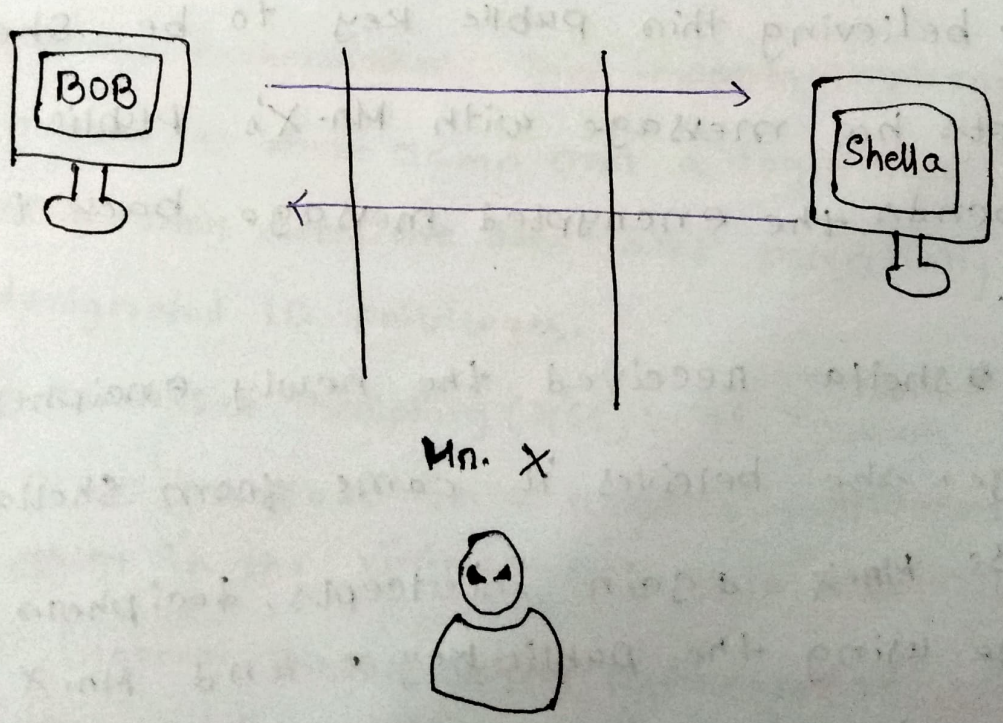

Figure: MITM attack

Suppose Bob wishes to communicate with Shella. Meanwhile, Mr. X wishes to intercept the conversion to eavesdrop and optionally ~~to~~ deliver a false message to ~~sh~~ Shella.

1. First, Bob ~~is~~ asks ~~s~~ Shella for her public key. If Shella sends her public key to Bob, but Mr. X is able to intercept it, a MITM attack can begin.

2. Mr. X sends Shella a forged message that appears to originate from Bob but instead ~~includes~~ includes Mr. X's public key.

3. Bob, believing this public key to be Shella's, encrypts her message with Mr. X's public key and sends the encrypted message back to Shella.

4. When ~~s~~ Shella received the newly enciphered message, she beleives it came from Shella. Whenease, Mr. X again intercepts, deciphers the message using the public key ~~-~~ and Mr. X achieved his goal ~~-~~ by doing this.

3 NO Q Ans

Soln: Web applications are everywhere ~~Now~~ a ~~days~~ today, and they are used to control just about everything we can imagine. A web application attack is any attempt by a malicious acton to compromise the security of a web-based application. Some common web application attacking tools are CookieDigger, WebScarab, Wzaf etc.

Security issues against web application attacks can be:-

1. Injection attacks: A web app that is vulnerable to ~~ize~~ injection attacks accepts untrusted data from an input field without any proper sanitation.

2. Broken Authentication: This improper implementation allows hackers to make claims over a lagitimate user's identity, access their sensitive data and potentially exploit the designated ID privileges.

3. Cross-site scripting (XSS): It involves injecting malicious code in a website application to execute them in the victims' browsers eventually.

4. Insecure Direct Object Reference (IDOR): Through manipulation URL, an attacker gain access to database

belonging to other users.

5 Security Misconfiguration: ~~The~~ This is the most common web application security issue found across web applications. ~~The~~ This ~~Vuln~~ vulnerability exists because developers and administrators "Forget" to change some default settings such as default passwords, usernames etc.

4 No Q Ans:

Soln: Yes, it is possible for the web app to prevent SQL Injections. SQL injection is a basic attack used to ~~eather~~ either gain unauthorized access to a database or to ~~retrive~~ retrieve information directly from the database. There are some popular tools used in SQL injection such as SQLMap, SQL ninja, BSQL hacker etc.

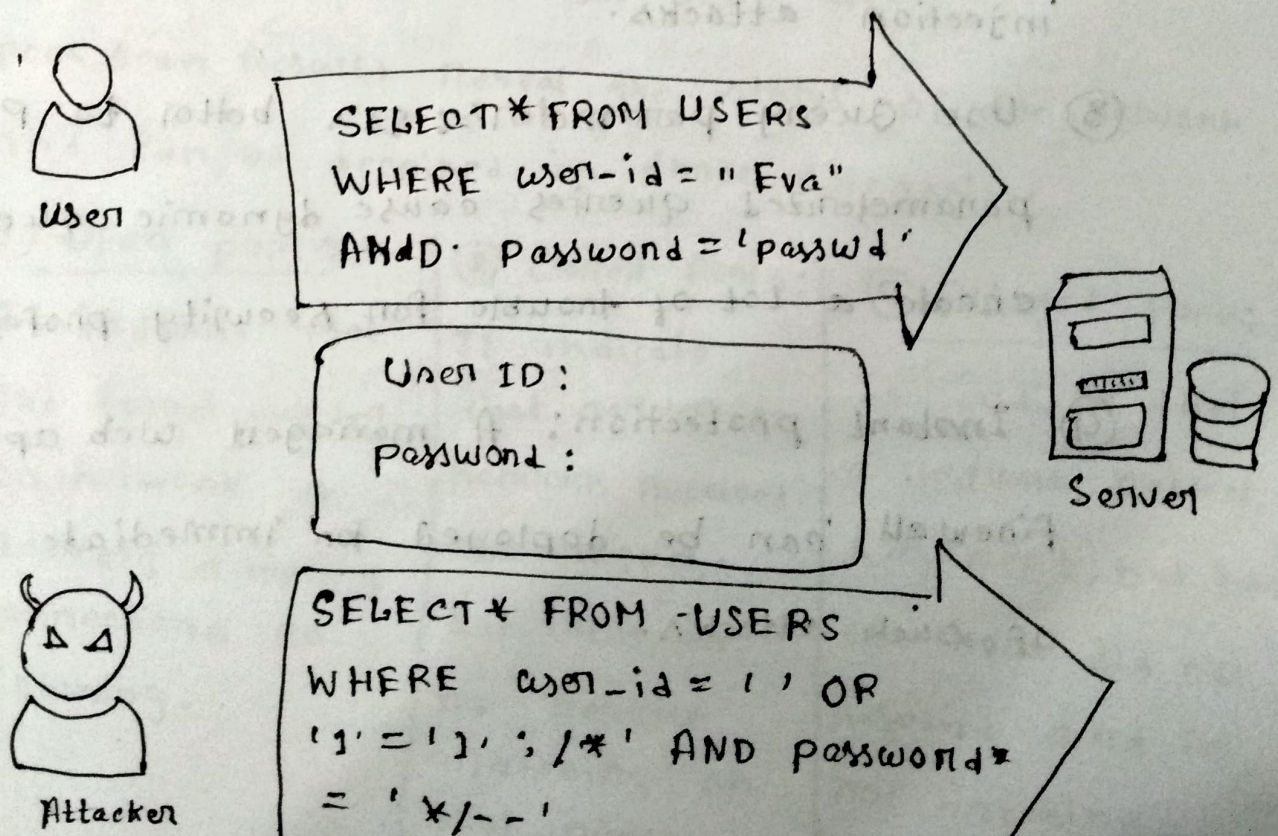

Figure: SQL Injection Attack

To prevent SQL Injections in the web app, some necessary actions ~~can~~ has to be taken:

1. Continuous Scanning and Penetration Testing:

The automated web application scanner has been the best choice ~~for~~ to point out vulnerabilities. Web security professional should explore manual testing with the help of a security vendor.

2. Restrict privileges: ~~For~~ enforcing specific privileges to specific accounts helps prevent blind SQL injection attacks.

3. Use Query parameters: It's better to prepare parameterized queries cause dynamic queries create a lot of trouble for security professionals.

4. Instant protection: A managed web application firewall can be deployed for immediate mitigation of such attacks.