CSCE 5560 Security Commerce Fall 2022

University of North Texas

CSCE 5560 Hacking Project Proposal

Catherine Dockendorf

Matthew Wilson

Divya Abburi

Santoshini Girkati

Sushan Sainju

10/17/2022

Hacking Project Proposal

Malicious Hyperlink that lead to SQL Injection Attacks

Catherine Dockendorf Matthew Wilson Divya Abburi

Santoshini Girkati Sushan Sainju

I. PROBLEM

Cybersecurity is a serious issue and threats of malicious hyperlinks and SQL injection attacks are threats that users encounter possibly more frequently if not for spam filters and malicious link scanners.

SQL Injection is the method of sending SQL (short for Structured Query Language) commands to a database without proper authorization. This method can be used on websites that don't check a user's typed inputs to make sure the inputs are legitimate. From this concept, we propose a hacking project that begins with a malicious hyperlink that leads to the exposure of the victim's credentials. In a general sense, we will send an email to a victim, which would lead to an SQL database being vulnerable to injection.

II. METHOD

The project starts with an email that contains a convincing but malicious hyperlink. This is the start of a phishing attack. When the email is opened and the hyperlink is clicked, this leads to a simple but fake or dummy website. The dummy website uses a fake token that will allow the bypass of security. The HTML and CSS are also setup to edit or add the external elements that are not originally from the website.

The website page contains a login form which will prompt the user for a username and password. This assumes that there will be an SQL server database setup in the background to store the credential information. The JavaScript is also setup in a way that security encryption such as authentication token may be attained using already available implementations such as libraries in the Java Script library.

The site by design will not properly check the username and password text fields. This will allow us to use SQL injection to send commands to the database and gain access to data we shouldn't have access to. This will lead to a data breach.

To prevent this data breach, the web developer needs to program all the text inputs to be checked for against SQL injection commands and make sure that every possible exception input is covered.

The variation that will give novelty to our implementation is that, a script is then downloaded in the background which will enable windows remote desktop and give the attacker access.

With the login info and remote access, the attacker can use SQL injection to query for info relating to the login. This info will be unencrypted personal information like passwords in the form of plain text.

III. RESULT

We will use SQL injection on an insecure database to gain unauthorized access to data and create a data breach.

Knowing that SQL injection attacks are a serious issue in website security, developers must consider this when designing websites.

The novelty we propose to attain in this group is how much of data can we gather once our dummy website is breached and propose what we can do to strengthen the security.

This hacking project will drill into security programming concepts and further strengthen the user requirement of making sure to as much as possible, cover every exception case known to cause exploitation. It is a good supplement and application to the course.