Assignment 6

DDL Injection and API Hooking

Submitted by: M Zeeshan Zafar

Submitted to: M Bilal Majid

Introduction

In the realm of cybersecurity, understanding the various techniques and methods employed by attackers is crucial for protecting sensitive information and maintaining system integrity. Two such techniques are DDL Injection and API Hooking. This assignment explores these methods, their historical context, and their impacts on modern computing environments.

DDL Injection

DDL (Data Definition Language) injection involves the manipulation of the database structure through SQL injection attacks. This type of attack allows an adversary to create, modify, or delete database schema elements such as tables, indexes, and views. The term was first coined in the early 2000s when web applications began to heavily rely on dynamic database queries.

Historical Background: The concept of SQL injection dates back to the late 1990s, with DDL injections emerging as databases became more complex and integral to web applications. The infamous 'SQL Slammer' worm in 2003 was one of the first major incidents highlighting the potential of SQL-based attacks.

Example of DDL Injection:

- DROP TABLE Customers; --

If executed, this command would delete the Customers table from the database, leading to data loss.

Prevention Techniques:

- Use prepared statements and parameterized queries.

- Implement proper input validation.
- Regularly update and patch database management systems.

DDL Injection

Common DDL Injection Commands

Command	Description
CREATE	Creates a new table, view, index, or other database object.
ALTER	Modifies an existing database object.
DROP	Deletes an existing database object.
RENAME	Renames an existing database object.

Assignment 6: DDL Injection and API Hooking

API Hooking

API Hooking is a method used to intercept function calls, messages, or events passed between software components. This technique is widely used in both legitimate software development and malware. By hooking into API calls, developers can modify the behavior of applications without altering their source code.

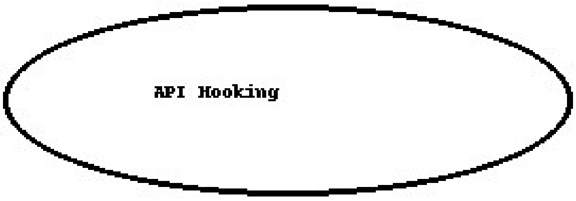
Historical Background: The concept of hooking dates back to the early 1990s, with its roots in debugging and performance monitoring tools. It became more prominent with the advent of Windows operating systems, which exposed a rich set of APIs that could be hooked into for various purposes.

Example of API Hooking:

- Hooking the 'ReadFile' API in Windows to monitor or modify file read operations.

Prevention Techniques:

- Employ code signing and integrity checks.
- Use runtime detection tools to identify unusual API calls.



Conclusion

Understanding DDL Injection and API Hooking is vital for both cybersecurity professionals and developers. These techniques, while powerful tools for attackers, also serve legitimate purposes in software testing and security research. By implementing proper security measures and staying informed about the latest threats, we can mitigate the risks associated with these techniques.

References

1. OWASP. (2024). SQL Injection. Retrieved from https://owasp.org/www-community/attacks/SQL_Injection

2. Microsoft Docs. (2024). Hooking. Retrieved from https://docs.microsoft.com/en-us/windows/win32/api/debugger/using-the-debugging-tools-api

3. TechNet. (2024). SQL Slammer Worm. Retrieved from https://technet.microsoft.com/en-us/library/sql-slammer-worm