**Experiment 9**

**Aim:** Perform SQL injection

**Theory:**

**Injection Attacks:**

Injection attacks are a type of security vulnerability that occur when an attacker is able to inject malicious code or commands into a computer system or application. Injection attacks refer to a broad class of attack vectors. In an injection attack, an attacker supplies untrusted input to a program. This input gets processed by an interpreter as part of a command or query. In turn, this alters the execution of that program.

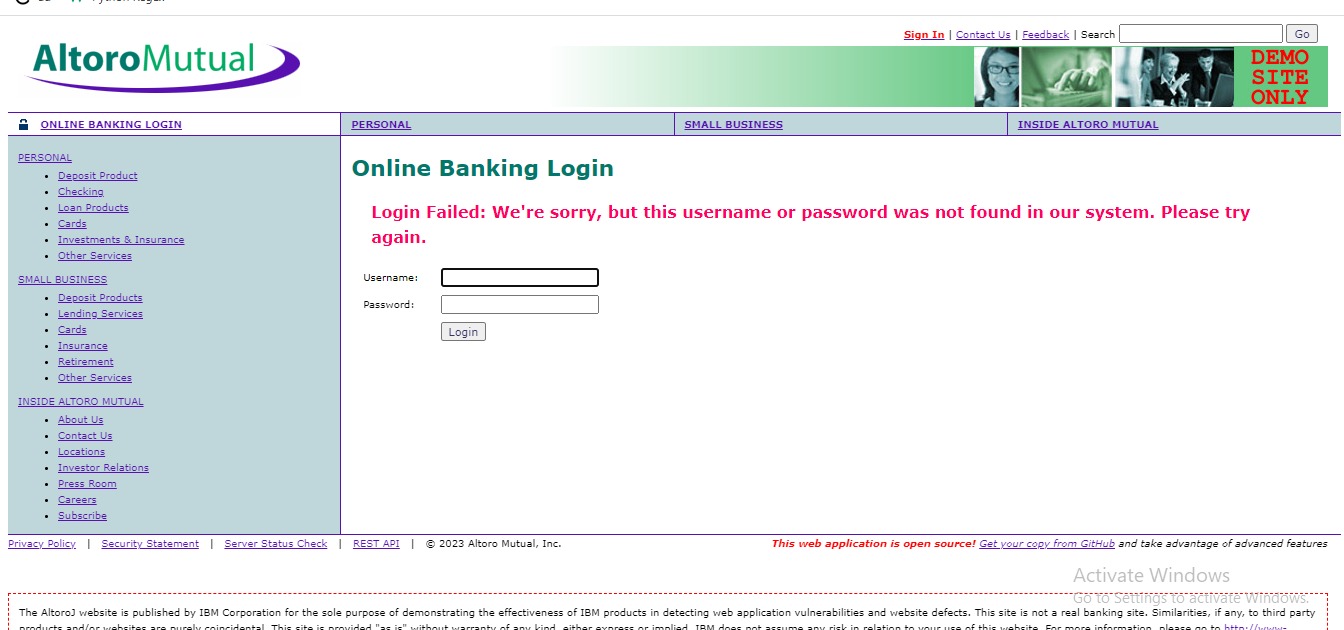
The oldest and most harmful attacks against web applications are injections. These may result in data loss, data integrity loss, data theft, service denial, and total system compromise. Insufficient user input validation is typically the main cause of injection vulnerabilities. The huge attack surface of injection vulnerabilities makes them extremely terrifying. Moreover, injection attacks are a form of vulnerability that is well known. This indicates that there are numerous trustworthy tools that are readily available for free that enable even novice attackers to automatically exploit these vulnerabilities.

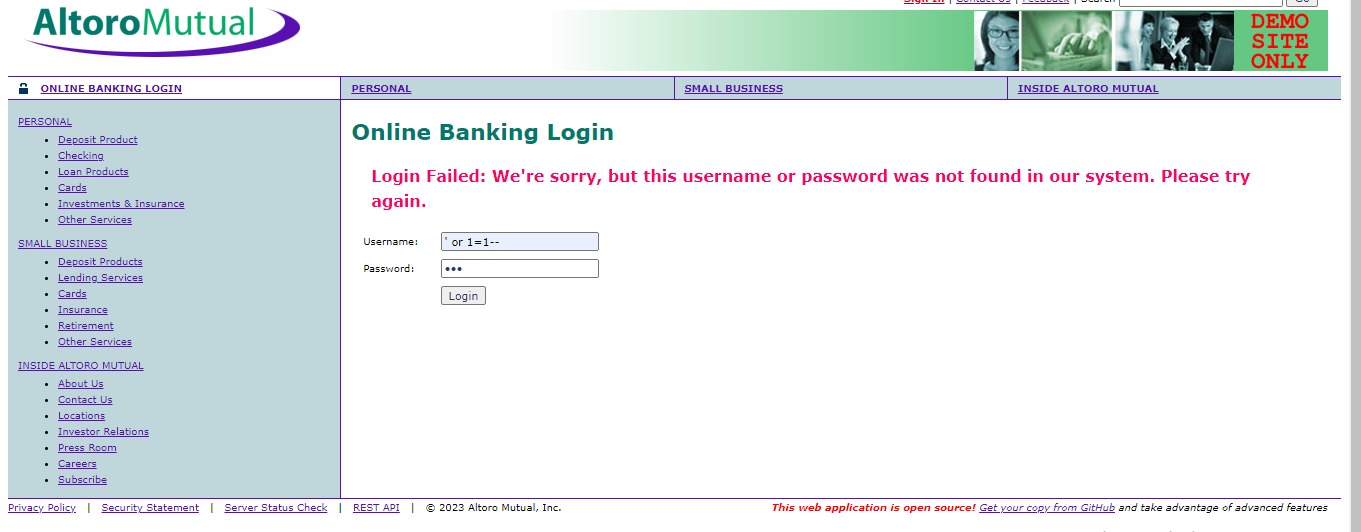
**Types of Injection Attacks:**

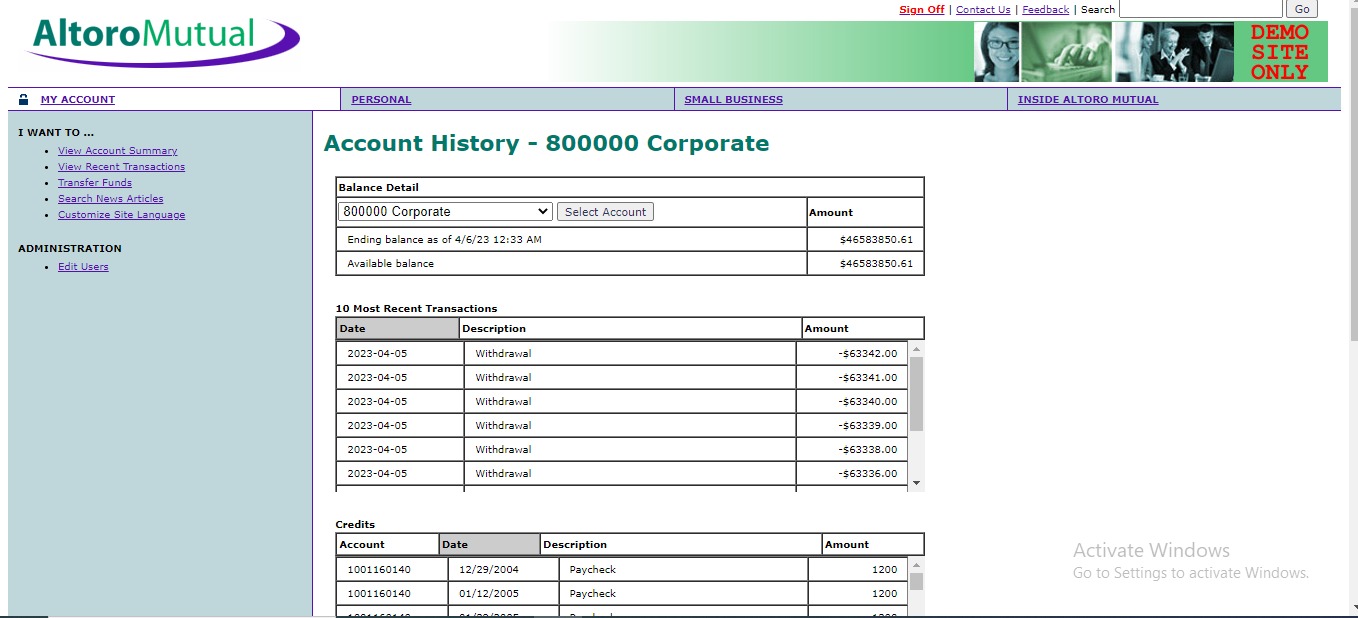
* Code Injection
* CRLF Injection
* Cross-site Scripting (XSS)
* Email Header Injection
* Host Header Injection
* LDAP Injection
* OS Command Injection
* SQL Injection (SQLi)
* Blind XPath Injection

## Threat Modeling

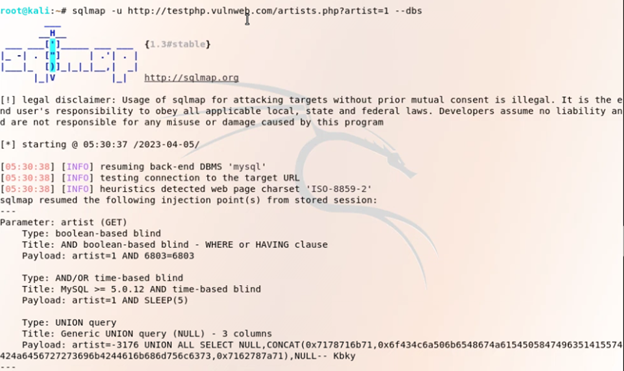
* SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.
* SQL Injection is very common with PHP and ASP applications due to the prevalence of older functional interfaces. Due to the nature of programmatic interfaces available, J2EE and ASP.NET applications are less likely to have easily exploited SQL injections.
* The severity of SQL Injection attacks is limited by the attacker’s skill and imagination, and to a lesser extent, defense in depth countermeasures, such as low privilege connections to the database server and so on. In general, consider SQL Injection a high impact severity.

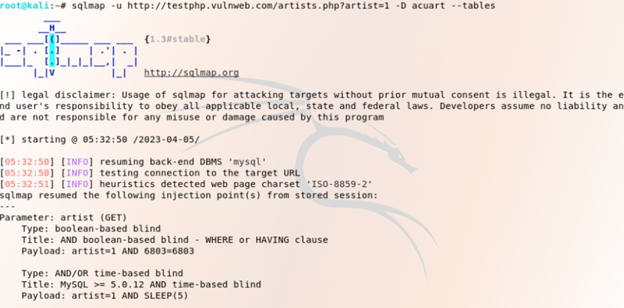




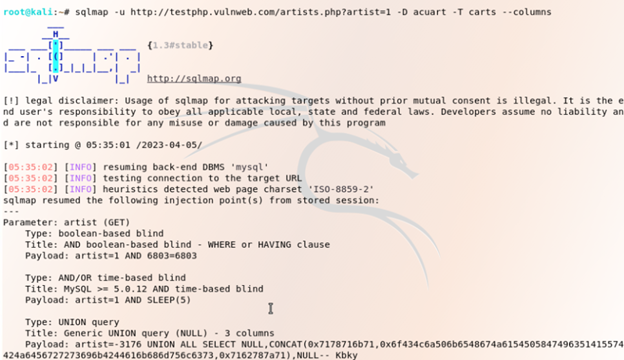


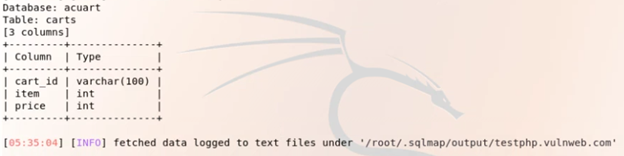


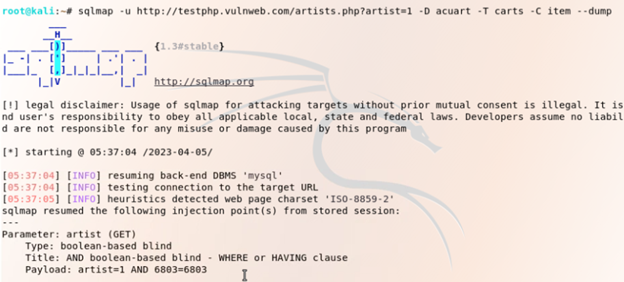


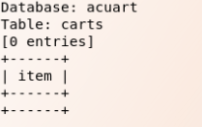












**Conclusion:** We learned about the Injection Attacks and their types and how they can be used by personnel with bad intentions to exploit an organization and get access to important information.

For Faculty Use

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Correction Parameters** | **Formative Assessment [40%]** | **Timely completion of Practical [ 40%]** | **Attendance / Learning Attitude [20%]** |  |
| **Marks Obtained** |  |  |  |