SQL Injection Vulnerability, Prevention Methodologies and Testing Techniques for Web Applications

# Problem Domain

In the cyber world that we all live in, technology driven systems have become an inseparable part of our lives. This growing impact has also left our systems vulnerable to attacks. Injections are a serious threat and always make it to top 10 ten in the OWASP list. This study focuses on SQL injection detection, prevention methodologies and evaluation of testing and scanning tools towards building secure applications. SQLi is the act of injecting malicious SQL code with the intent of getting confidential data and control over the database server.

# Threat model

The simulation of the threat model was performed using Microsoft’s STRIDE Model which measures the system threats against spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege.

The STRIDE threat modelling was performed using Microsoft SDL TMT and threatmodeler, starting with diagramming the system components, assets, and the data flow as shown in Figure 1. As stated by Toulope [4], “Each of the threats identified required inputs for the mitigation measures for the different scenarios.”

Diagram, schematic

Description automatically generated

Figure 1: Diagrammatic Representation of Data Flow

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Attacks | S | T | R | I | D | E |
| SQL Injection | **X** | **X** |  | **X** |  | **X** |

Figure 2: STRIDE Analysis for SQLi [4, pg. 43]

‘X’ represents the areas that apply to the attacks of type SQL injections [4].

##### 

##### Thread Model Description automatically generated with medium confidence

Figure 3: Threat Model for Web Application

Graphical user interface, application

Description automatically generated

Figure 4: Threats and Mitigation

##### Graphical user interface, text, application Description automatically generated

Figure 5: Security Requirements

##### References

|  |  |
| --- | --- |
|  | Hu, H. (2017). Research on the technology of detecting the SQL injection attack and non-intrusive prevention in WEB system. AIP Conference Proceedings, 1839(1). <https://doi.org/10.1063/1.4982570> |

1. Dalai, A. K., & Jena, S. K. (2017). Neutralizing SQL Injection Attack Using Server Side Code Modification in Web Applications. Security and Communication Networks, 2017, 1–12. <https://doi.org/10.1155/2017/3825373>
2. M. Abu Kausar, M. Nasar and A. Said, "SQL Injection Detection and Prevention Techniques in ASP.NET Web Application," *The International Journal of Recent Technology and Engineering (IJRTE),* vol. Vol.8 (3), pp. p.7759-7766, 2019. <https://doi.org/10.35940/ijrte.C6319.098319>

[4] Awojana, Tolulope Bukola. (December 2018). *Threat Modelling and Analysis of Web Application Attacks* (Master's Thesis, East Carolina University). Retrieved from the Scholarship. (<http://hdl.handle.net/10342/7049>.)