

**Finding Name:** SQL Injection

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | | **Role** | | **Project** | | **Quality Assurance** | | **Is this a re-tested Finding?** | |
| KHUSHLEEN KAUR DHINDSA | SCR | Team Member | | ONTRACK | | Roocha Thakkar | | Yes | |
|  |  | |  | |  | |  | |  | |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

SQL injection is a technique which targets insertion of malicious SQL instructions in the entry fields and is caused by lack of sanitization of user inputs. This susceptibility gives interlopers access to subsequent modification of queries, that may ultimately lead to data compromises, unauthorized data modification and unauthorized system access. Fundamentally, custom-written programs with high-grade protection software are indeed the efficient instrument of minimizing risks.

**Risk Rating**  
Impact: Major  
Likelihood: Moderate

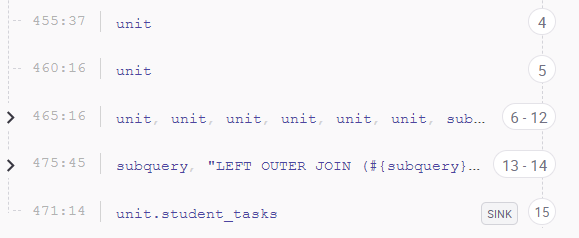
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

SQL injection allows hackers to perform SQL queries at own will. This may give an opening to attackers to manipulate, access, or completely compromise the application and its data—very criminals' favourite spot.

**Affected Assets**

****

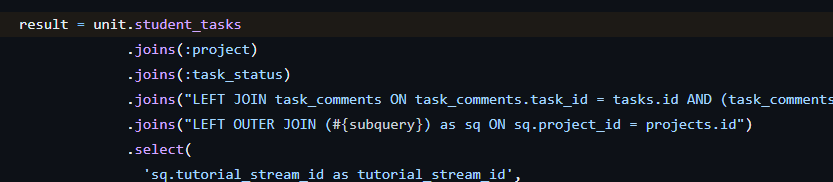
**A screenshot of a computer

Description automatically generated** **A screenshot of a computer

Description automatically generated**

**Evidence**

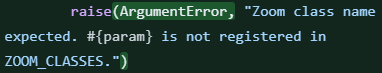
While inspecting the security using the Synk system, the system highlighted the potential danger of user inputs being uncensored and then plugged into SQL queries, which could present a problem when the created code is executed. This exploit was used in the trials which included SQL injection through bad codes lines, consequently, mismanaged data exposure and activity.

****

**Remediation Advice**

To mitigate SQL injection vulnerabilities:

* Avoid including user inputs directly in SQL commands or constructing queries via string concatenation.
* Use parameterized queries and prepared statements.
* Enforce strong typing and strict input validation.
* Adopt secure coding practices and utilize libraries designed to prevent SQL injection.



A screenshot of a computer program

Description automatically generated

**Achievements**

* Corrected the representation of achievements to reflect true contributions to AppAttack and HardHat projects.
* Improved communication with project stakeholders to clarify requirements and report findings.
* Participated in workshops and online courses to enhance SQL injection testing skills.

**References**

***What is SQL Injection (SQLi) and How to Prevent Attacks*. (2024, January 9). Acunetix. https://www.acunetix.com/websitesecurity/sql-injection/#:~:text=SQL%20Injection%20(SQLi)%20is%20a,to%20bypass%20application%20security%20measures.**

***SQL injection*. (n.d.). https://www.w3schools.com/sql/sql\_injection.asp**

**Contact Details**

Name: KHUSHLEEN KAUR

Email: s222342024@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.