Security risk document

1. Executive Summary

The security assessment of RealtyHub was conducted to evaluate its handling of the OWASP Top 10 security risks. The assessment revealed several strengths in mitigating certain risks, but also identified areas of concern that require immediate attention. The report provides detailed findings, risk ratings, and actionable recommendations to enhance the overall security posture of the application.

2. Introduction

The website RealtyHub manages accommodations and housings and lets users post and purchase houses or apartments. Its purpose is to give the users a reliable website for housing. It is crucial to assess and address the OWASP top 10 security risks since this website will be accessible to a wide variety of users and I need to ensure the application’s resilience against common vulnerabilities.

3. Methodology

The assessment followed a comprehensive methodology that included a combination of manual code reviews, automated vulnerability scanning, and penetration testing techniques. Various security tools and expert knowledge were utilized to gather accurate findings and assess the application's security controls effectively.

4. Scope

The assessment focused on evaluating the security of RealtyHub with regards to its core modules, APIs, and database interactions. The assessment excluded third-party components and infrastructure elements outside the application's direct control.

5. Risk Assessment

In this section, each OWASP Top 10 risk is assessed individually. For each risk, the report provides the following details:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attack type | Likelihood | Impact | Risk | Action |
| A01: Broken Access Control | Moderate | High | users act outside of their intended permissions | Use of role base authentication and deny all access by default |
| A02: Cryptographic Failures | High | High | third-party entity exposes sensitive data | Plain text passwords should always be converted into cipher text or encrypt them |
| A03: Injection | Moderate | High | send data to an application in a way that will change the meaning of commands | use of prepared statements with variable binding |
| A04: Insecure Design | low | Low | critical design and architectural flaws in web applications that hackers can exploit | N/A |
| A05: Security Misconfiguration | Unlikely | Moderate | security controls that are inaccurately configured or left insecure, putting your systems and data at risk | N/A |
| A06: Vulnerable and Outdated Components | Moderate | Low | component that is no longer being supported, making it susceptible to security vulnerabilities | I am using the latest versions of java and other tools. |
| A07: Identification/Authentication Failures | High | Moderate | can allow malicious actors to compromise keys, passwords, and session tokens | Risk allowed |
| A08: Software and Data Integrity Failures | Moderate | Moderate | infrastructure that does not protect against integrity violations | libraries and dependencies, such as npm, are consuming trusted repositories |
| A09: Security Logging and Monitoring Failures | Unlikely | Low | The absence of telemetry that could help network defenders detect and respond to hostile attempts to compromise a system | Risk allowed |
| A10: Server-Side Request Forgery | Moderate | Moderate | accessing resources that it was not intended to access | Restrict request protocols |

6. Conclusion

In conclusion, the application RealtyHub has the required security needs for A01, A02, A03 and A10 which are the most preeminent cases in most of the applications but lacks in other departments.