**Security and Privacy Analysis Report for Go NZ**

Project Summary: The Security and Analysis for travel company website GoNZ was conducted to assess that the website protects and secure the data of user’s and company and maintain proper authorisation to access the required data by authorized user only. Additionally, identification of potential thread from third party to access content illegally by SQL injection, Cross-Site Request Forgery, Phishing, Brute Force Attacks etc.

**Findings and Recommendations:**

**Authentication and Authorization:**

* **Finding:** The website uses standard username/password authentication without implementing additional security layers.
* **Recommendation:** Implement multi-factor authentication (MFA) like Django-otp to enhance user account security.

**Data Protection:**

* **Finding:** Sensitive data is stored without encryption.
* **Recommendation:** for storage and transmission, utilize encryption mechanisms to protect sensitive data.
  + For data in transit Use HTTPS protocol and use SSL/TSL certificates.
  + For storage use Django’s built in encryption by specifying “encrypt = True” in model field that store sensitive data

**Input Validation and Secure Coding:**

* **Finding:** Input validation is inadequate, which may lead to vulnerabilities such as SQL injection and Cross-Site Scripting (XSS).
* **Recommendation:** Implement input validation using Django's form validation and validation decorators or “csrf\_token” to prevent injection attacks.

**Secure APIs:**

* **Finding:** APIs lack proper authentication and authorization mechanisms.
* **Recommendation:** U**t**ilize Django REST framework to build secure APIs.

**Infrastructure Security:**

* **Finding:** Lack of essential security measures in server and database configuration.
* **Recommendation:** use virtual environment to isolate your application and dependency

**Third-Party Dependencies:**

* **Finding:** The project uses third-party libraries and components without proper evaluation of their security.
* **Recommendation:** Keep third-party dependencies up to date and monitor for security vulnerabilities. Use python tool like “safety” and “pyup” to scan vulnerabilities.

**Privacy Analysis:**

* **Finding:** lack of transparency about informing user about data collection, usage, and sharing practices.
* **Recommendation:** create a visible and easily accessible section to display privacy policy of data handling and security and keep them updated and revise time to time.

**GDPR Compliance:**

* **Finding:** lack of access for user to edit or delete personal data.
* **Recommendation:** Implement features that allow users to exercise their GDPR rights over their personal data. Give them control of their personal data and access to edit or delete data.

**Cookie and Tracking Policy:**

* **Finding:** Lacks of information provided to user about cookie and tracking policy.
* **Recommendation:** cerate and display a clear cookie and tracking policy, pop-up notification while accessing the website and obtain user consent where necessary.

**Conclusion:** The Security and Privacy Analysis for the GoNZ travel website detects areas which required improvements to ensure the secure handling of user data, protect user privacy, and prevent unauthorized access.

**Action Plan:**

* Implement MFA for user accounts before production stage.
* Encrypt sensitive data during storage and transmission before production stage.
* Enhance input validation and employ secure coding practices crsf\_token applied with Django form .
* Secure APIs not required at this stage.
* Regularly update and secure servers and databases.
* Evaluate and update third-party dependencies for security.
* Update privacy policy to transparently communicate data practices before production stage.
* Develop GDPR-compliant features for user data rights before production stage.
* Create a clear cookie and tracking policy and obtain user consent before production stage.

**Contact Information:** For inquiries about this analysis report, please contact Vijendra Singh.

20th August 2023

Vijendra Singh

Roll No: 20220756

Email:20220756@mywhitecliffe.com