Security Policy

Supported Versions

We release patches for security vulnerabilities. Which versions are eligible for receiving such patches depends on the CVSS v3.0 Rating:

Version	Supported
2024.0.1	:white_check_mark:
< 2024.0.1	:x:

Reporting a Vulnerability

If you discover a security vulnerability within this project, please follow these steps:

1. **Do not** open an issue on GitHub.
2. Send an email to hunsakerconsulting@gmail.com with the details of the vulnerability.
3. Include the following information in your email:
   - A description of the vulnerability.
   - Steps to reproduce the vulnerability.
   - Any potential impact or exploit scenarios.
   - Your contact information.

We will respond to your report within 72 hours with an acknowledgment and will work with you to understand and resolve the issue as quickly as possible.

Security Best Practices

To ensure the security of your deployment, please follow these best practices:

- **Keep Dependencies Updated**: Regularly update your dependencies to the latest versions to ensure you have the latest security patches.
- **Use HTTPS**: Always use HTTPS to encrypt data in transit.
- **Environment Variables**: Store sensitive information such as API keys and database credentials in environment variables, not in your codebase.
- **Access Control**: Implement proper access control mechanisms to restrict access to sensitive parts of your application.
- **Regular Audits**: Conduct regular security audits and code reviews to identify and fix potential vulnerabilities.

Contact

For any security-related inquiries, please contact hunsakerconsulting@gmail.com.

Thank you for helping to keep our project secure!