Security Policy

Supported Versions

We provide security updates for the following versions:

Version	Supported
2.x.x	:white_check_mark:
1.x.x	:x:

Reporting a Vulnerability

We take the security of AI RFP Risk Scanner seriously. If you discover a security vulnerability, please follow these steps:

How to Report

1. **DO NOT** create a public GitHub issue for security vulnerabilities
2. Email us at: security@yourdomain.com (replace with your actual email)
3. Include the following information:
   - Description of the vulnerability
   - Steps to reproduce the issue
   - Potential impact assessment
   - Any suggested fixes (if available)

What to Expect

- **Initial Response**: Within 24 hours
- **Status Updates**: Every 48-72 hours until resolution
- **Resolution Timeline**: We aim to resolve critical issues within 7 days

Security Measures

Our application implements several security measures:

- **Authentication**: Secure user authentication with NextAuth.js
- **Database Security**: Prepared statements via Prisma ORM
- **Input Validation**: Comprehensive input sanitization
- **File Upload Security**: Type validation and size limits
- **CSRF Protection**: Cross-site request forgery protection
- **XSS Protection**: Output encoding and CSP headers
- **Dependency Scanning**: Automated vulnerability scanning

Responsible Disclosure

We follow responsible disclosure practices:

1. We will acknowledge receipt of your vulnerability report

2. We will provide regular updates on our progress
3. We will notify you when the vulnerability is fixed
4. We will publicly credit you for the discovery (if desired)

Bug Bounty

We currently do not offer a bug bounty program, but we greatly appreciate security researchers who help us improve our security posture.

Security Best Practices for Users

- Use strong, unique passwords
- Keep your environment variables secure
- Regularly update dependencies
- Use HTTPS in production
- Configure proper database permissions
- Implement proper firewall rules

Contact Information

- Security Email: security@yourdomain.com
- GPG Key: Available on request
- Response Time: 24 hours maximum

Thank you for helping keep AI RFP Risk Scanner secure!