# Security Policy

## Supported Versions

We actively support the following versions with security updates:

| Version | Supported |
|---|---|
| 2.x.x | ✅ Yes |
| 1.x.x | ✅ Yes (LTS) |
| < 1.0 | ❌ No |

## Reporting a Vulnerability

We take security vulnerabilities seriously. If you discover a security vulnerability, please follow these steps:

### For Sensitive Security Issues

**Please DO NOT create a public GitHub issue for sensitive security vulnerabilities.**

Instead, use one of these secure reporting methods:

1. **GitHub Private Vulnerability Reporting** (Recommended)
   - Go to the Security tab in this repository
   - Click “Report a vulnerability”
   - Fill out the private vulnerability report form

2. **Email Reporting**
   - Send an email to: security@empire325marketing.com
   - Include “SECURITY VULNERABILITY” in the subject line
   - Encrypt your message using our PGP key (available on request)

3. **Security Contact Form**
   - Visit: https://empire325marketing.com/security-contact
   - Fill out the secure contact form

### For Non-Sensitive Security Issues

For general security improvements, configuration issues, or questions that don’t involve active vulnerabilities, you can:

- Create a public issue using the “Security Vulnerability” template
- Start a discussion in the Security category

# What to Include in Your Report

Please provide as much information as possible:

- **Vulnerability Type**: Authentication, XSS, SQL Injection, etc.
- **Affected Components**: Which parts of the system are affected
- **Severity Assessment**: Your assessment of the impact
- **Reproduction Steps**: How to reproduce the issue (if safe to share)
- **Potential Impact**: What an attacker could achieve
- **Suggested Fix**: If you have ideas for remediation
- **Environment Details**: Versions, configurations, etc.

# Our Security Response Process

1. **Acknowledgment**: We'll acknowledge receipt within 24-48 hours
2. **Initial Assessment**: We'll perform an initial assessment within 72 hours
3. **Investigation**: We'll investigate and validate the vulnerability
4. **Fix Development**: We'll develop and test a fix
5. **Disclosure**: We'll coordinate disclosure with you
6. **Release**: We'll release the fix and security advisory

# Security Response Timeline

- **Critical Vulnerabilities**: 24-48 hours for initial response, 7 days for fix
- **High Vulnerabilities**: 48-72 hours for initial response, 14 days for fix
- **Medium Vulnerabilities**: 3-5 days for initial response, 30 days for fix
- **Low Vulnerabilities**: 5-7 days for initial response, 60 days for fix

# Vulnerability Disclosure Policy

We follow a **coordinated disclosure** approach:

- We'll work with you to understand and validate the vulnerability
- We'll develop a fix and prepare a security advisory
- We'll coordinate the public disclosure timing with you
- We'll credit you in the security advisory (if desired)
- We'll notify affected users through appropriate channels

# Security Measures

## Code Security

- **Static Analysis**: All code goes through automated security scanning
- **Dependency Scanning**: Regular vulnerability scans of dependencies
- **Code Review**: Security-focused code reviews for all changes
- **Secrets Management**: No hardcoded secrets, proper secret rotation

### Infrastructure Security

- **Network Security**: Proper network segmentation and firewall rules
- **Access Control**: Principle of least privilege, MFA required
- **Monitoring**: Comprehensive security monitoring and alerting
- **Encryption**: Data encrypted in transit and at rest

### Operational Security

- **Incident Response**: Documented incident response procedures
- **Security Training**: Regular security training for team members
- **Compliance**: SOC2, ISO 27001, and GDPR compliance
- **Auditing**: Regular security audits and penetration testing

## Security Best Practices for Contributors

### Code Contributions

- Follow secure coding practices
- Validate all inputs
- Use parameterized queries
- Implement proper authentication and authorization
- Handle errors securely (don’t expose sensitive information)

### Dependencies

- Keep dependencies up to date
- Review security advisories for dependencies
- Use dependency scanning tools
- Avoid dependencies with known vulnerabilities

### Configuration

- Use secure defaults
- Don’t commit secrets or credentials
- Use environment variables for configuration
- Implement proper logging (but don’t log sensitive data)

## Security Tools and Automation

We use various tools to maintain security:

- **SAST**: Static Application Security Testing
- **DAST**: Dynamic Application Security Testing
- **SCA**: Software Composition Analysis
- **Container Scanning**: Docker image vulnerability scanning
- **Infrastructure Scanning**: Terraform and Kubernetes security scanning

## Compliance and Certifications

We maintain compliance with:

- **SOC 2 Type II**: Annual audits for security controls
- **ISO 27001**: Information security management system
- **GDPR**: Data protection and privacy compliance
- **CCPA**: California Consumer Privacy Act compliance

## Security Contact Information

- **Security Team**: security@empire325marketing.com
- **Emergency Contact**: +1-XXX-XXX-XXXX (24/7 for critical issues)
- **PGP Key**: Available on request for encrypted communications

## Hall of Fame

We recognize security researchers who help improve our security:

## Legal

This security policy is subject to our Terms of Service (./TERMS.md) and Privacy Policy (./PRIVACY.md).

We will not pursue legal action against security researchers who:
- Follow this responsible disclosure policy
- Act in good faith
- Don’t access or modify user data beyond what’s necessary to demonstrate the vulnerability
- Don’t perform testing that could harm our systems or users

---

**Last Updated**: September 29, 2025
**Next Review**: December 29, 2025