We Hack Purple

Secure Coding Guidelines

> Give your software development team a head start on creating secure software with these tips. Add more items that match your specific business requirements!

1. Validate every input to your application, including your database, URL parameters and the data on your backend.
2. Output Encoding is required for all output to the screen.
3. Parameterized Queries are mandatory, inline SQL is forbidden!
4. All third-party code and components must be verified not to contain known vulnerabilities
5. Every applicable security header should be used.
6. All errors should be caught, handled, logged and if appropriate, alerted upon. Never log sensitive or PII information!
7. Use the identity and session management features in your framework or from your network or cloud provider.
8. Take every possible precaution when performing file uploads, including scanning it for vulnerabilities
9. Sensitive or decision-making information should never be stored in URL parameters.
10. Do not cache sensitive page data.
11. Sensitive data should be stored in secure cookies and use all available security features such as "secure and "httponly" flags.
12. Use the Authorization, Authentication and other security features in your framework, don't write your own.
13. Use HTTPS only, never HTTP. Only use unbroken and industry standard protocols and algorithms.
14. Keep your programming frameworks and dependencies up to date.