PCI DSS 4.0 For Developers
IN PLAIN ENGLISH

6.2.1

The Dev Team *really* needs to **focus on how to keep PCI Data safe within the apps** they build *from the start*.

6.2.2

Developers need to **learn how to write secure code** and get familiar with tools to detect vulnerabilities to test it.

6.2.3

Before publishing apps or new updates, the **code must be reviewed by a pro or automated tool.** Issues found? Rinse & repeat.

6.2.4

Know what the most common types of attacks are and write code that defends against these specified attacks.

6.3.1

Not all vulns are created equal. **Identify which are high-risk and low-risk.** Create a process to handle them effectively.

6.3.2

3rd Party Libraries:

- **Keep track** of which libraries are in use
- **Stay informed** of any security issues for fast remediation

6.3.3

Prioritize patching for any high-risk vulns in 3rd party libraries within 1 month.

6.4.1

Website or SaaS apps:
Conduct in-depth checks annually and before major releases to prevent attacks detailed in 6.2.4.

6.4.2

Similar to 6.4.1, **ensure automatic tools are properly configured** and up-to-date with any alerts addressed ASAP.

6.4.3

Protect all web-based checkout pages/carts, etc to ensure attackers cannot manipulate these pages by including a malicious script.