

BUILD A PAYMENT-SECURITY PORTFOLIO WITHOUT TOUCHING REAL CARD DATA

A strong early-career portfolio shows reasoning, source discipline, communication, and safe boundaries-not unauthorized access to a real payment environment.

PRACTITIONER POSITION

Students can demonstrate relevant skill through fictional architecture narratives, responsibility maps, evidence models, test-method comparisons, operating calendars, provider reviews, and source-linked research. The artifact should disclose assumptions, avoid real account data and credentials, respect authorization, and make limitations obvious. Public work is strongest when another person can review how the conclusion was reached.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

A student wants experience and considers scanning a local business or copying screenshots from an internship. A safer portfolio uses a fictional campus bookstore, synthetic data, public product documentation, primary PCI SSC sources, declared assumptions, and a reproducible reasoning trail.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- Real customer, employer, or client information appears in a project.
- Testing occurs without explicit written authorization.
- The artifact claims certification or assessment authority the learner does not possess.
- Sources, assumptions, and limitations are missing.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Select a fictional scenario and define prohibited data and actions before beginning.

Choose one useful deliverable rather than imitating an entire assessment.

Cite primary sources and label every assumption, observation, inference, and practitioner recommendation.

Ask a reviewer to challenge both the reasoning and the safety boundary.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 Can this project be completed with synthetic data?
- 02 Is every test explicitly authorized?
- 03 Does the artifact overstate qualification?
- 04 Can a reviewer reproduce the reasoning without sensitive material?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Choose a fictional case and a bounded professional question.

02 / MAP

Connect sources, assumptions, methods, artifacts, limitations, and intended audience.

03 / EXPLAIN

State what the work demonstrates and what it does not authorize.

04 / REDUCE

Remove sensitive material, real identifiers, overclaiming, and decorative bulk.

05 / PROVE

Publish a reproducible artifact with citations, version history, and reviewer notes.

THE FIELD LAW

THE LINE WORTH REMEMBERING

YOUR PORTFOLIO SHOULD PROVE JUDGMENT WITHOUT CREATING A SECURITY, PRIVACY, OR CONFIDENTIALITY PROBLEM.

Download the Safe Portfolio Project Brief and build one reviewable artifact from a W/ Campus case.

TECHNICAL GROUNDING

START WITH THE SOURCE MATERIAL

These references ground the practitioner interpretation. They do not turn the metaphor or method into official PCI DSS terminology.

- WACK-SOURCE-0107 / NICE Framework Resource Center: Getting Started / National Institute of Standards and Technology / [Open source](#)
- WACK-SOURCE-0108 / Workforce Framework for Cybersecurity (NICE Framework), NIST SP 800-181 Rev. 1 / National Institute of Standards and Technology / [Open source](#)
- WACK-SOURCE-0109 / Cyber Career Pathways Tool / Cybersecurity and Infrastructure Security Agency / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-15 against canonical digest

534fb928cc2dc62bf42ba1d832f029c3afeb04deecc067bd55eec7e034c3bb28. Educational content, not a compliance determination.

Independent practitioner resource; not affiliated with or endorsed by PCI SSC. Authorship and authority classification do not determine legal intellectual-property ownership.