Midterm Project Demonstrations

CEN429 Secure Programming — Week 7

Asst. Prof. Dr. Uğur CORUH · 30.10.2026

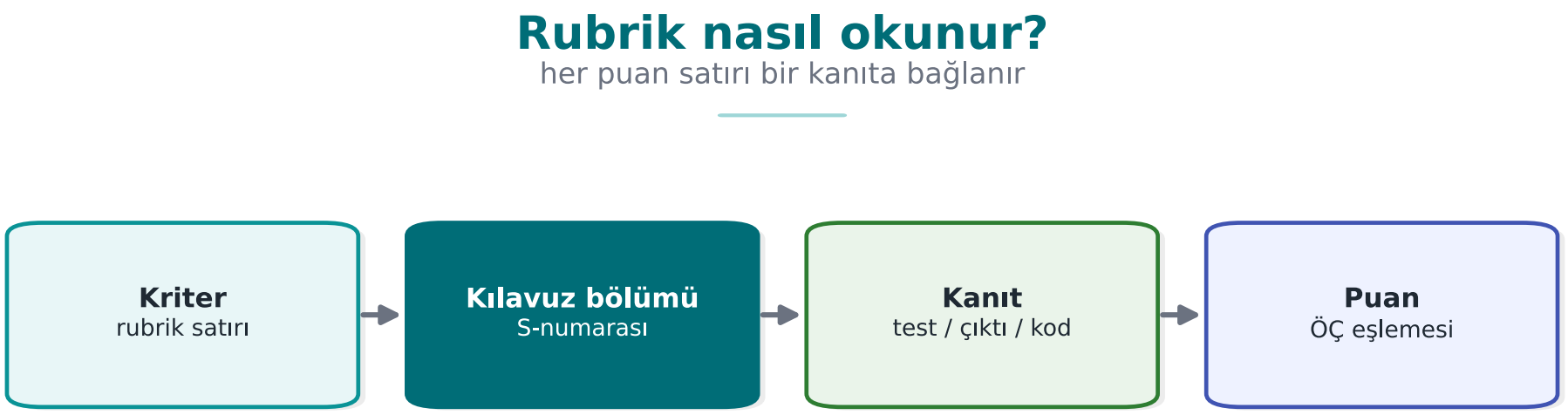
This Week: Midterm Project Demonstrations (RAP1)

- No lecture; each team **submits its interim report** and **demonstrates its application**
- RAP1 = **60%** of the midterm · Quiz-1 = **40%** → `Grade_Midterm = 0.6·RAP1 + 0.4·QUIZ1`
- Detailed rubric: project guide · order, timing, submission time: in class
- ⚠️ Late submissions are not accepted

Midterm Rubric: Five Criteria

Criterion	LO	Guide
Security analysis	1	S2 · S3 interface table · S4 threat/attacker model
Data security	2	S5 asset list · S7 shell matrix
C/C++ hardening and RASP	3	S9 (basic) · S10
Project management	5	S13 process, SBOM · GitHub repo and plan
Interim report	7	All midterm sections

How the Rubric Is Read — Diagram



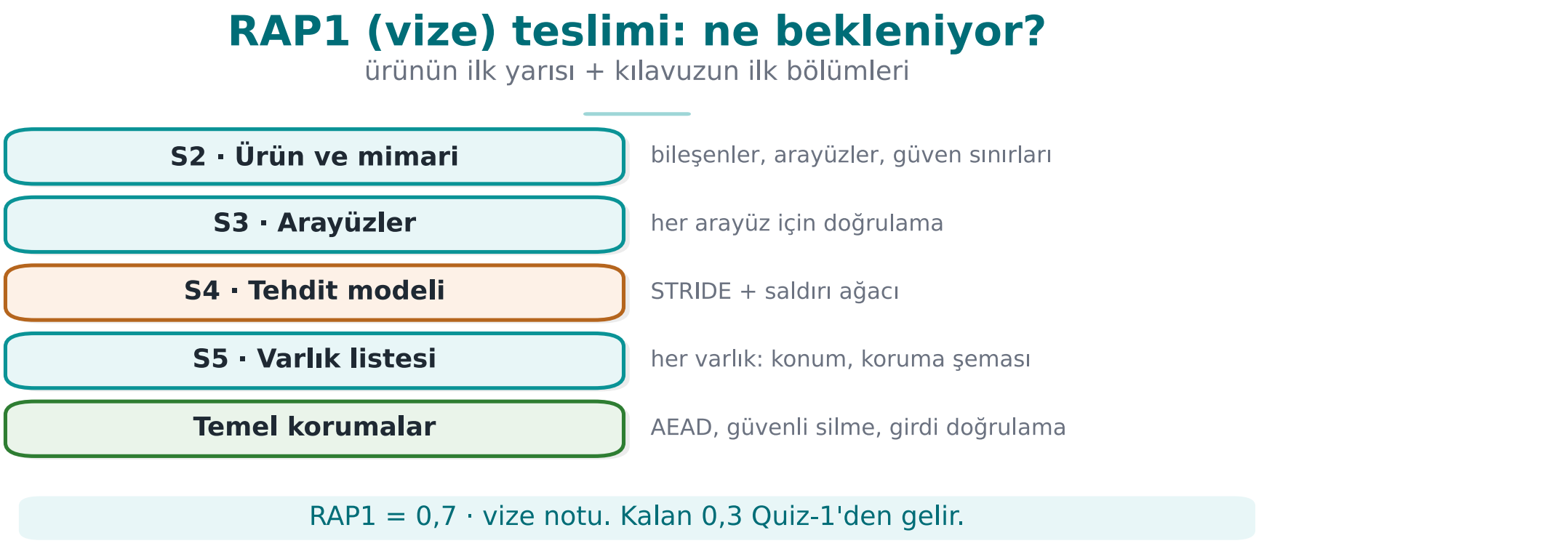
Kanıtı olmayan satır puanlanmaz — 13. haftanın uyum matrisi mantığı burada da geçerli.

Which Sections in the Interim Report?

Complete	Draft / brief / plan
S0 cover · S2 overview · S3 architecture · S4 threat model	S1 scope (draft) · S5 assets (draft)
S7 data security · S10 RASP · S13 process	S9 hardening (basic) · S12 reporting (brief)
	S16 testing (plan) · S17 compliance matrix (draft)

Left for the final: S6 · S8 · S11 · S14 · S15

RAP1 Submission — Diagram



Preparation Checklist

Week	What you should be able to show
1	Repo + plan · S2 · S3 interface table · S4 STRIDE + attack tree · S5 draft
2	Every threat → CWE + CVSS v3.1 vector
3	S7 algorithm/key/binding · shell matrix · CSPRNG · AEAD verification
4	S9 protection table · CERT findings · ASan+UBSan · fuzz result
5	SBOM + scan · input validation table
6	S10 RASP inventory · response policy · a bypass attempt

Suggested Demonstration Flow

1. **Product and architecture** (S2–S3): one diagram, trust boundaries
2. **Threats and assets** (S4–S5): the three most critical threats
3. **Live demonstration:** at least one control **working live**
4. **Evidence:** protection table, sanitizer/fuzz, SBOM — command + output
5. **Remaining risk and plan:** what remains before the final?

For every control: **What does it protect? · How was it built? · How was it proven?**

Demonstration Day Flow — Diagram

Yazdığınız her satırı açıklayabilmelisiniz; açıklayamadığınız kod puan getirmez.

Sample Questions

- Which flow crossing a trust boundary is the riskiest?
- How long does this asset stay unencrypted in memory, and where is it wiped?
- Where does the key come from, where does it live? Can the nonce repeat?
- Which compiler protection is turned off, and why?
- What happens when a RASP check fails?
- Does the SBOM contain a vulnerable component? Are you affected?

Common Mistakes

Mistake	Why is it a problem?
Guide and code are inconsistent	One of the most serious findings
"Secure" claimed without evidence	Not scored
Keys/logs/code missing from the asset list	What is not in the list is not protected
Threat table from general knowledge	Project-specific threats get missed
Unrehearsed demonstration	Time is wasted
Real password/key/personal data in the repo	A serious security mistake; values must be **synthetic**

Common Mistakes — Diagram

Academic Integrity and After

- Uncredited code/text, work from outside the team, fabricated results **are not acceptable**
- Every submitted line must be explainable
- Any team member may be asked a question

After the demonstration: write the feedback as a **finding list** (finding · severity · fix · date) → a small model of Week 12

Final sections: S6 · S8 · S11 · S14 · S15 · S16 results · S17

Next Week

Week 8 — Midterm Exam Week: Quiz-1

- Scope: weeks 1–6
- Study guide and sample questions: Week 8 page

Appendix · Rubric Item by Item

What Does the Rubric Measure?

The midterm demonstration measures the **first half** of your project:

- product, architecture, threat model
- asset management
- basic protections
- documentation and presentation

Item · Product and Architecture

- What does it do, which components?
- One diagram + the three most critical assets.
- **Evidence:** S2–S4 documentation.

Item · Threat Model

- STRIDE / attack tree.
- A control for every threat.
- **Evidence:** S4 threat table.

Item · Asset Management

- Asset list + C/I/I+.
- Lifecycle.
- **Evidence:** S5.

Item · Basic Protections

- Cryptography (S8, partial), secure code (S9, partial).
- **Evidence:** code + tests.

Item · Documentation and Presentation

- Consistency, version identity.
- Clear delivery.
- **Evidence:** the entire guide.

Appendix · Demonstration Flow

Flow · 1. Summary

- Product, architecture, the three most critical assets.
- One diagram, two minutes.

Flow · 2. Threat Model

- One example from STRIDE and the attack tree.
- "This threat, that control."

Flow · 3. Live Demonstration

- Show a control **working live**.
- E.g., encrypted data, a verified signature.

Flow · 4. Evidence

- Tests, protection table.
- "This command, this output."

Flow · 5. Remaining Risk

- What did you deliberately scope out?
- Honest analysis earns points.

Appendix · Preparation Checklist

Checklist · Documentation

- [ ] S0 version identity up to date
- [ ] S2–S5 complete
- [ ] Guide and code version consistent

Checklist · Demonstration

- [ ] Live demo works (backup video ready)
- [ ] Commands ready
- [ ] Every team member can present a section

Checklist · Security

- [ ] No real secret/personal data in the repo
- [ ] Values are synthetic
- [ ] Remaining risk is documented

Appendix · Sample Questions

Question 1

Your three most critical assets and their C/I/I+ labels?

Keep your answer ready; know the lifecycle of every asset.

Question 2

Which control against this threat, and how was it verified?

Show the threat → control → evidence chain.

Question 3

Where does this key come from, where does it live, when is it deleted?

Explain the key's lifecycle.

Question 4

What is your remaining risk? Why is it acceptable?

Answer honestly and with justification.

Appendix · Common Mistakes

Mistake List

- Guide and code version differ.
- "Done" without evidence.
- Live demo crashes (no backup).
- Remaining-risk section is empty.
- Real data in the repo.

Final Word (RAP1)

> A demonstration is a presentation of **evidence**: every claim should be backed by a document, a test, or live output.

Midterm feedback becomes a **finding–action** list at the final.