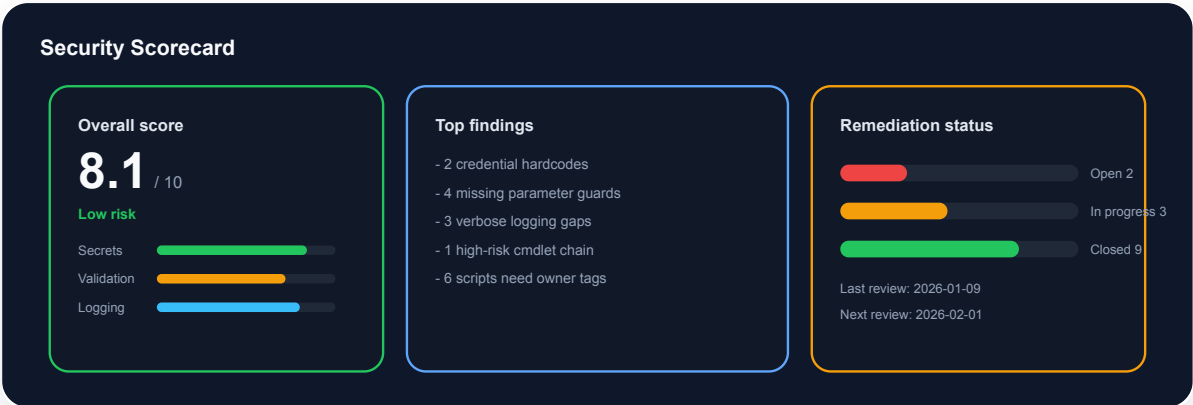# Module 03: AI Analysis and Security

Objectives

- Run an AI analysis on a script
- Interpret security and quality scores
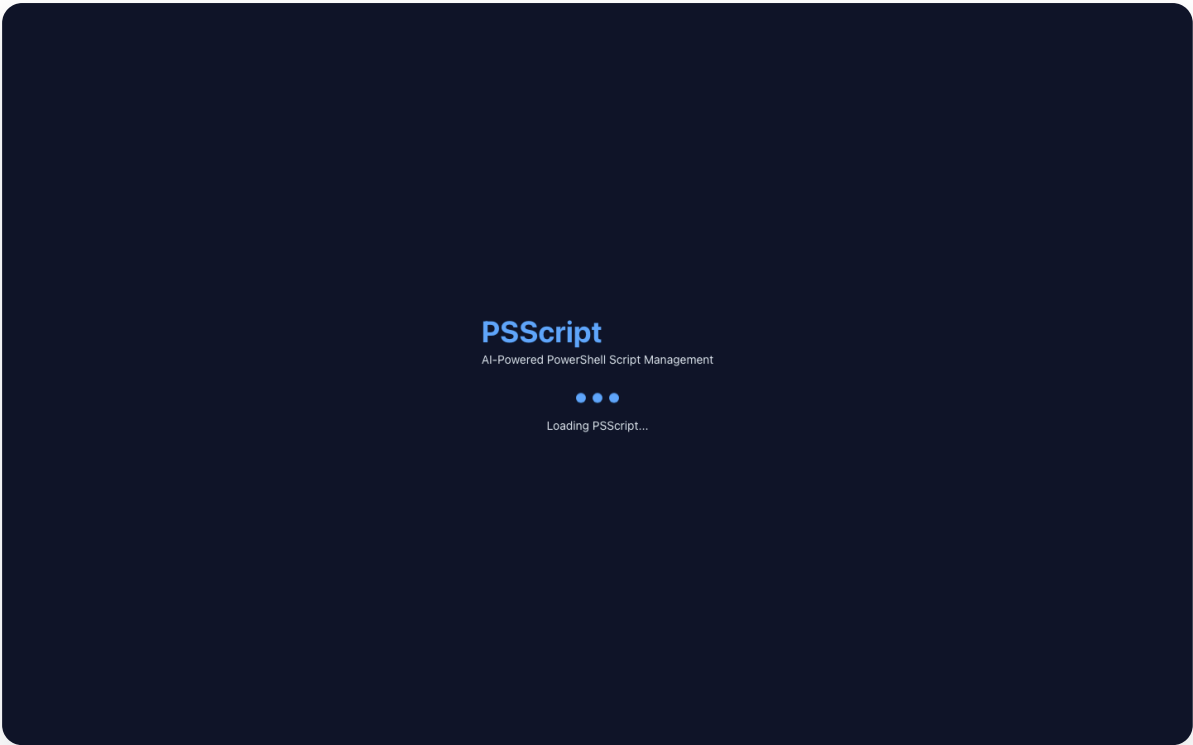- Track recommended improvements

Walkthrough

1. Open a script detail page.
2. Trigger analysis or open the analysis tab.
3. Review security findings and recommendations.
4. Capture a remediation note for the top issue.

Scorecard snapshot

Security Scorecard

Overall score

8.1 / 10

Low risk

Secrets
Validation
Logging

Top findings

- 2 credential hardcodes
- 4 missing parameter guards
- 3 verbose logging gaps
- 1 high-risk cmdlet chain
- 6 scripts need owner tags

Remediation status

Open 2
In progress 3
Closed 9

Last review: 2026-01-09
Next review: 2026-02-01

Screenshots

Score interpretation

Band	Meaning	Action
9.0 - 10	Low risk	Approve and monitor
7.0 - 8.9	Moderate risk	Plan fixes and re-run analysis
< 7.0	High risk	Remediate before execution

Sample analysis output

```json
{
  "security_score": 7.8,
  "quality_score": 8.3,
  "issues": [
    "Hardcoded credential found on line 42",
    "Missing input validation for parameters"
  ],
  "recommendations": [
    "Use Get-Credential or SecretStore",
    "Add ValidateSet or ValidatePattern"
  ]
}
```

What to look for

- Hardcoded credentials or unsafe commands
- Missing parameter validation
- Error handling and logging gaps

Verification checklist

- Analysis results display successfully
- At least one recommendation is recorded for follow up

Generated 2026-01-13 06:26 UTC