PEN-101 Anchor Reading Guide

3,677 words · ~17 min read

---

*VCA-PEN-101 cross-chapter reading-guide handout. Companion to the catalog page at `https://virtuscyberacademy.org/vca-pen-101`. Audience: Belt-3 pentest-track students arriving from the catalog's distilled "What Belt-3 PEN-Track Graduates Recognize" register. *

The catalog page tells you WHAT the course covers. This guide tells you HOW to read the canonical anchors that build the Belt-3: which courses, which books, which platforms, in which order, what to extract on each pass, and how the anchors compose into a coherent vocabulary that prepares you for ADV-101 CVE-to-tool work, the academy's OSCP-prep sequence, and the five-day simulated engagement capstone.

---

§0. What this guide is for

PEN-101 is the academy's pentest-track foundations course. Four anchors carry the Belt-3: Heath Adams's *Practical Ethical Hacking* (TCM Security) for the build-it-yourself methodology companion, OffSec's PEN-200 / OSCP+ for the institutional gold-standard credential pathway, Stuttard and Pinto's *The Web Application Hacker's Handbook* (2nd edition) for the practitioner-narrative reference on web pentest, and Seitz and Arnold's *Black Hat Python* (2nd edition) for the build-from-scratch offensive-Python scripting register. Two practitioner-training platforms (PortSwigger Web Security Academy; HackTheBox Academy and TryHackMe) are mentioned briefly in §0 framing as parallel companions but do not earn full per-anchor walks at the Belt-3.

The four primary anchors do not compose a textbook tour. Heath Adams plus OffSec PEN-200 compose the build-it-yourself plus credential pair the discipline trains itself through; Stuttard-Pinto plus Seitz-Arnold compose the practitioner-narrative pair the discipline reads itself through. By the end of PEN-101 a student should be able to (a) discuss the seven engagement phases (pre-engagement, reconnaissance, scanning, enumeration, exploitation, post-exploitation, reporting), the SOW-versus-ROE-versus-authorization-letter distinctions, and the named tool families (Nmap, Masscan, Burp Suite, Nessus, Nuclei, Metasploit, Hashcat, Impacket, LinPEAS, WinPEAS) in the same vocabulary the practitioner community uses, (b) execute the engagement methodology

against a five-day simulated target, (c) author client-style written reports with oral debriefs, and (d) move into ADV-101 with the practitioner-foundation literacy that the CVE-to-tool work assumes.

This guide is opinionated by design. It is not a comprehensive bibliography. Anchors that other peer programs lean on (Weidman's *Penetration Testing*; Kim's *The Hacker Playbook 3*; specific vendor-tool documentation read in isolation) are deliberately not the primary anchors at this level because they are dated, idiosyncratic, or vendor-shaped. PEN-101 graduates know the supplementary material exists; they were trained on the opinionated material that the academy's OSCP-prep sequence requires.

The guide reads Heath Adams first because the build-it-yourself methodology is the Belt-3 backbone; OffSec PEN-200 is named as the credential pathway PEN-101 prepares for, not as a Belt-3 reading. Stuttard-Pinto third because the web-app pentest narrative builds on the methodology Heath Adams installs. Seitz-Arnold fourth because the build-from-scratch scripting register is the academy's bridge to ADV-101 custom-tooling.

---

§1. The anchor reading register

Four anchors. Read in this order on first pass; revisit per the per-anchor walks below for capstone preparation.

Anchor 1: Heath Adams (TCM Security), *Practical Ethical Hacking*

Edition / pointer: Heath Adams, *Practical Ethical Hacking: The Complete Course*, TCM Security, ~$30 (frequently discounted to ~$15-25). Approximately 25-30 hours of video plus hands-on labs. Continuously updated; the TCM platform tracks current tooling. The canonical entry-tier methodology companion for the discipline; recommended by the OffSec community as a PEN-200 prerequisite.

Why this matters at Belt-3: Heath Adams's *Practical Ethical Hacking* is the academy's primary build-it-yourself anchor for the pentest methodology. The course walks the seven engagement phases against a series of academy-style lab targets; the student executes the methodology end-to-end against each target rather than reading about it. The course's structure maps almost directly onto PEN-101's week-by-week curriculum: reconnaissance, scanning, enumeration, exploitation, post-exploitation, reporting. A Belt-3 graduate who has worked through Heath Adams's course has the procedural fluency PEN-101's labs assume; the academy's labs reinforce and extend rather than introduce.

Suggested reading order: First. Walk Heath Adams's course in parallel with PEN-101 Labs 1-7 rather than reading it in advance; the course's lab progression maps onto the academy's lab progression and walking them together reinforces both. Students with prior pentest experience can skim the early modules and focus on the modules that map to PEN-101 Labs 8-10.

Cross-link to academy artifacts: PEN-101 Labs 1-7 (every primary lab has a named Heath Adams module companion); PEN-101 capstone (the five-day simulated engagement; Heath Adams's methodology is the procedural anchor); ADV-101 (the CVE-to-tool work assumes the engagement methodology Heath Adams teaches); the academy's OSCP-prep sequence (PEN-101 plus ADV-101 plus ADV-102 plus PEN-200; Heath Adams is the first build-it-yourself layer).

Anchor 2: OffSec, PEN-200 / OSCP+

Edition / pointer: OffSec, *PEN-200: Penetration Testing with Kali Linux* / OSCP+ certification, institutional pricing ~$1,749 (90-day lab access) to ~$2,599 (365-day lab access). The institutional gold-standard pentest credential since the early 2010s; the OSCP+ refresh in 2024 modernised the lab environment and the exam format. **PEN-101 plus ADV-101 is the academy's OSCP-prep sequence**; PEN-200 follows after the academy sequence completes. PEN-200 is named in this anchor list as the credential pathway, not as Belt-3 reading.

Why this matters at Belt-3: OffSec's PEN-200 is the canonical industry credential for the pentest discipline. The OSCP examination is a 24-hour-plus-24-hour hands-on practical: students attack a network of machines, achieve specific objectives, and write a client-style report. Employers in the pentest market treat the OSCP as the discipline's professional baseline; the academy's PEN-101 plus ADV-101 sequence is calibrated to bring graduates to a state where they can sit PEN-200 with confidence. A Belt-3 graduate should know that the OSCP exists, what it requires, and how the academy's sequence prepares them; they should not be expected to sit it during PEN-101.

Suggested reading order: Second. Read the OffSec course outline and the OSCP examination details after Heath Adams because the OffSec material is most legible when the methodology vocabulary is already installed. Students should treat the OffSec PEN-200 material as a future-state reference: this is what you are building toward, here is what it requires, here is when to register.

Cross-link to academy artifacts: The academy's OSCP-prep sequence (PEN-101 → ADV-101 → ADV-102 → PEN-200); ADV-101 (the CVE-to-tool work prepares students for OSCP-style exploit-and-pivot exercises); the academy's labs are calibrated to OSCP-style

targets (Active Directory misconfigurations, web-app vulnerabilities, privilege escalation, lateral movement). Students who complete the academy sequence are typically ready to register for PEN-200 within one to three months.

Anchor 3: Stuttard + Pinto, *The Web Application Hacker's Handbook*, 2nd edition

Edition / pointer: Dafydd Stuttard and Marcus Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, 2nd edition, Wiley, 2011 (ISBN 978-1-118-02647-2). The discipline's canonical web-app pentest reference; Stuttard is the creator of Burp Suite and the book's vocabulary is what Burp's UI assumes. No 3rd edition exists; the 2nd edition remains canonical. Library-acquire or paperback ~$50-60.

Why this matters at Belt-3: Stuttard and Pinto's *Web Application Hacker's Handbook* (commonly abbreviated "WAHH") is the practitioner-narrative reference for web-app pentest. The book walks every major web-app vulnerability class (injection, broken authentication, broken access control, XSS, CSRF, server-side request forgery) at the practitioner-foundation register: how the bug class works, how to find it, how to exploit it, how to report it. A Belt-3 graduate who has read WAHH Chapters 1-9 has the web-app vocabulary PEN-101 Lab 4 (web-recon) and Lab 8 (web-app exploitation) assume; the labs reinforce and extend rather than introduce.

Suggested reading order: Third. Read WAHH after Heath Adams because the methodology Heath Adams installs is what WAHH's vulnerability-class walks assume. Students should plan to read WAHH Chapters 1-9 over the first eight weeks of PEN-101; the later chapters belong at ADV-101 register.

Cross-link to academy artifacts: PEN-101 Lab 4 (web reconnaissance with Burp Suite; WAHH Chapter 4 is the textbook companion); PEN-101 Lab 8 (web-app exploitation; WAHH Chapters 7-9 compose the read); ADV-101 (CVE-to-tool work where the target is a web app; WAHH's vulnerability-class taxonomy is the methodology anchor); the academy's PortSwigger Web Security Academy companion (PortSwigger's labs walk WAHH's content at a hands-on register).

Anchor 4: Seitz + Arnold, *Black Hat Python*, 2nd edition

Edition / pointer: Justin Seitz and Tim Arnold, *Black Hat Python: Python Programming for Hackers and Pentesters*, 2nd edition, No Starch Press, 2021 (ISBN 978-1-7185-0112-6). The discipline's canonical build-from-scratch offensive-Python scripting reference. The 2nd edition modernised the Python and tooling examples (Python 3, modern library APIs); the 1st edition (2014) is dated and not recommended. Paperback ~$40-50.

Why this matters at Belt-3: Seitz and Arnold's *Black Hat Python* is the academy's primary build-from-scratch anchor for offensive-Python scripting. The book walks the construction of small offensive tools in Python: TCP server-and-client patterns, raw-socket sniffers, ARP-cache poisoner, Burp-extension authoring, custom credential-harvester. The build-from-scratch frame is what differentiates a Belt-3 graduate (who can write custom tools when commercial tools fall short) from a Belt-3 reader (who can only run the canonical tools). A Belt-3 graduate who has worked through *Black Hat Python* Chapters 2-7 has the offensive-Python fluency PEN-101 Lab 10 (custom-tooling exercise) assumes.

Suggested reading order: Fourth. Read *Black Hat Python* in parallel with PEN-101 Lab 10 rather than as front-loaded reading; the chapters' patterns map onto specific lab moments. Students with strong Python backgrounds can move quickly through the early chapters; students new to Python should plan to walk Chapters 2-3 carefully before attempting Lab 10.

Cross-link to academy artifacts: PEN-101 Lab 10 (custom-tooling exercise; *Black Hat Python* is the canonical companion); the academy's encouragement for students to author custom tools rather than over-rely on Metasploit; ADV-101 (CVE-to-tool work where the deliverable is a custom reproduction tool; *Black Hat Python*'s scripting register is the methodology anchor).

---

§2. Heath Adams *Practical Ethical Hacking* deep walk: methodology-first build-it-yourself

Heath Adams's course is the academy's primary build-it-yourself anchor for the pentest methodology. Walk for the seven-phase methodology as the course's central operational primitive.

What to extract

A Belt-3 graduate should carry the following five facts from the Heath Adams course:

1. **The seven engagement phases are pre-engagement, reconnaissance, scanning, enumeration, exploitation, post-exploitation, reporting.** Each phase has its own discipline, tools, and deliverables. Belt-3 graduates should be able to name all seven phases and articulate what each phase produces.

2. **Reconnaissance is OSINT-without-detection.** Passive reconnaissance (open-source intelligence; Shodan; Censys; certificate-transparency logs; LinkedIn scraping) gathers information about the target without touching the target. Belt-3 graduates should be able to articulate the active-versus-passive distinction and execute basic passive reconnaissance.
3. **Scanning is structured probing.** Nmap is the canonical scanner; Masscan is the canonical wide-scope scanner; both have specific syntax patterns the practitioner internalises. Belt-3 graduates should be able to run targeted Nmap scans and interpret the output.
4. **Enumeration extracts service-specific detail.** Service-by-service enumeration (SMB share enumeration; HTTP directory enumeration; LDAP query; SNMP walk) deepens the scanning output. Belt-3 graduates should know which enumeration tools belong to which services and execute the canonical patterns.
5. **Reporting is client-facing not just technical.** A pentest report has an executive summary (for the client's leadership), a technical summary (for the client's security team), and finding-by-finding detail (with severity, evidence, and remediation). Belt-3 graduates should be able to author all three sections at the practitioner-foundation tier.

What is out-of-scope at Belt-3

Heath Adams's later modules (Active Directory deep dive; advanced post-exploitation; advanced privilege escalation) belong at ADV-101 register. The course's specific tooling deep-dives (specific Burp Suite plugin development; specific BloodHound query authoring) are valuable as supplementary reading and out-of-scope at the Belt-3 first-walk tier.

Cross-anchor connections

Heath Adams's seven-phase methodology is the foundation OffSec PEN-200 assumes; reading Heath Adams first makes PEN-200 legible as a deeper application of the same methodology rather than as a separate course. Heath Adams's web-recon module lands directly on Stuttard-Pinto's web-app vulnerability classes; the student who has walked Heath Adams's recon module reaches WAHH with the right vocabulary already installed. Heath Adams's custom-tooling philosophy lands on Seitz-Arnold's *Black Hat Python*; the build-from-scratch register the course encourages is what *Black Hat Python* operationalises.

§3. OffSec PEN-200 / OSCP+ deep walk: the institutional credential pathway

OffSec PEN-200 is the discipline's institutional gold-standard credential. Read the course outline and examination format for the future-state credential pathway as the anchor's central operational primitive.

What to extract

A Belt-3 graduate should carry the following five facts from the OffSec PEN-200 / OSCP+ material:

1. **The OSCP examination is 24+24 hours hands-on.** Students attack a network of target machines, achieve specific objectives, and submit a client-style report. The first 24 hours are the practical examination; the second 24 hours are the report-writing window. Belt-3 graduates should know the format and the expectations.
2. **OSCP+ is the 2024 refresh.** The 2024 update modernised the lab environment (Active Directory machines; modern Windows server versions; current vulnerability classes), modernised the examination format (specific objective-completion patterns), and refreshed the course material. OSCP+ replaces OSCP for new candidates; older OSCP holders are encouraged to refresh.
3. **The lab environment is the canonical practice surface.** OffSec's labs include dozens to hundreds of target machines covering the discipline's full attack surface (web apps, AD misconfigurations, privilege escalation, lateral movement, pivoting). Belt-3 graduates should know that the labs are where most candidates spend the majority of their preparation time.
4. **The 90-day-versus-365-day-lab decision is a personal-pacing question.** OffSec offers 90-day and 365-day lab access at different price points; the right choice depends on the candidate's available study time per week. Belt-3 graduates should be able to articulate the trade-off when planning their post-academy credential timeline.
5. **The OSCP is the entry credential for many pentest roles.** Employers in the pentest market frequently list OSCP as a baseline requirement; some prefer it explicitly over alternative credentials. Belt-3 graduates should know the credential's market position when planning their career trajectory.

What is out-of-scope at Belt-3

The specific OffSec lab-machine walkthroughs (which targets to attempt first; which exploits to chain) belong at PEN-101 capstone register and beyond. The specific report-writing rubric OffSec uses is similar to but not identical to the academy's; differences belong at the academy's ADV-101 reporting module.

Cross-anchor connections

OffSec PEN-200 builds on Heath Adams's seven-phase methodology at deeper depth; the OSCP examination effectively tests whether the candidate can execute the methodology under time pressure against a multi-target network. The OSCP's web-app component aligns with Stuttard-Pinto's vocabulary; candidates with WAHH internalised approach the OSCP web-app challenges with the right register. The OSCP's custom-tooling expectations align with Seitz-Arnold's build-from-scratch frame; candidates who have walked *Black Hat Python* Chapters 2-7 can write the small scripts the OSCP examination occasionally requires.

---

§4. Stuttard + Pinto WAHH deep walk: web-app vulnerability practitioner narrative

Stuttard and Pinto's *Web Application Hacker's Handbook* (commonly abbreviated WAHH) is the canonical web-app pentest reference. Read for the vulnerability-class taxonomy as the book's central operational primitive.

What to extract

A Belt-3 graduate should carry the following five facts from WAHH Chapters 1-9:

1. **HTTP state management is the foundational web-app concept.** Cookies, sessions, tokens, and authentication state determine what a web app does and what a pentest can attack. Belt-3 graduates should be able to articulate the canonical state-management patterns and recognise them in any web app.
2. **Injection is the single largest web-app vulnerability class.** SQL injection, command injection, LDAP injection, XPath injection, server-side template injection (SSTI) all share the same root: untrusted input lands in a context where it is interpreted as code. Belt-3 graduates should be able to recognise injection vectors and execute basic SQL injection against an academy lab target.

3. **Broken access control is the vulnerability automated scanners miss.** IDOR (insecure direct object reference) and broken access control require human reasoning about what the application's authorization model should be; automated scanners cannot infer the model. Belt-3 graduates should be able to identify IDOR patterns by hand.
4. **XSS comes in three flavours.** Reflected (the input is echoed back in the response); stored (the input is saved and served to other users); DOM-based (the JavaScript itself processes attacker input). Belt-3 graduates should be able to distinguish the three and execute basic reflected and stored XSS against academy lab targets.
5. **CSRF and clickjacking are protocol-level web vulnerabilities.** CSRF (cross-site request forgery) exploits the browser's cookie-attaching behaviour; clickjacking exploits the browser's frame-rendering behaviour. Belt-3 graduates should know both classes and the canonical defenses (CSRF tokens; X-Frame-Options).

What is out-of-scope at Belt-3

WAHH's later chapters (advanced injection variations; specific framework vulnerabilities; advanced authentication attacks) belong at ADV-101 register. The book's specific case studies of historical vulnerabilities are valuable as practitioner-narrative entertainment and out-of-scope at the Belt-3 first-pass tier. The discipline's modern additions since the 2nd edition (server-side request forgery at depth; modern OAuth attacks; specific JWT vulnerabilities) live in companion academy material rather than in WAHH itself.

Cross-anchor connections

WAHH's vulnerability-class taxonomy lands directly on Heath Adams's web-recon and exploitation modules; the student who has walked both reaches PEN-101 Lab 8 with the right vocabulary already installed. WAHH's vulnerability-class taxonomy lands on the OWASP Top 10 cross-track register (which SEC-101 covers); the two are mutually reinforcing. WAHH's authentication-attack chapters land on the WPA-AKA-progression cross-chapter handout (which WIR-101's Week 4 sidebar walks); the parallel between web-app authentication and wireless authentication is a Belt-3 insight.

---

§5. Seitz + Arnold *Black Hat Python* deep walk: build-from-scratch offensive-Python

Seitz and Arnold's *Black Hat Python* (2nd edition) is the academy's primary build-from-scratch offensive-Python anchor. Walk for the small-tool-author register as the book's central operational primitive.

What to extract

A Belt-3 graduate should carry the following five facts from *Black Hat Python* Chapters 2-7:

1. **TCP server-and-client patterns in Python are short and clear.** Chapter 2 walks the canonical TCP server and client in Python. Belt-3 graduates should be able to write both from memory; the patterns are the foundation for every subsequent custom tool.
2. **Raw-socket sniffers expose layer-3 packets.** Chapter 3 walks raw-socket packet capture in Python; the sniffer reads link-layer frames directly without library abstraction. Belt-3 graduates should know that raw-socket access requires elevated privileges and that the packet-decoding work is hand-rolled.
3. **Scapy is the discipline's primary packet-construction library.** Chapter 4 introduces Scapy for constructing and sending custom packets; ARP-cache poisoning, custom DNS responses, and arbitrary protocol authoring all use Scapy. Belt-3 graduates should be able to construct a basic Scapy-based ARP-cache poisoner.
4. **Burp extension authoring is Python's web-app pentest contribution.** Chapter 6 walks Burp extension authoring in Python; the Burp Extender API is Java-shaped but the Jython runtime exposes it to Python. Belt-3 graduates should know that Burp extensions exist and what they enable.
5. **The build-from-scratch register matters in client engagements.** Commercial tools cover the common cases; custom tools cover the gaps. The discipline values practitioners who can author small custom tools to address specific engagement needs. Belt-3 graduates should approach Lab 10 (custom-tooling exercise) with the build-from-scratch register installed.

What is out-of-scope at Belt-3

Black Hat Python's later chapters (advanced exfiltration patterns; specific malware-development primitives; specific evasion techniques) belong at ADV-101 register or beyond. The book's chapters on automation against Active Directory deeper than entry-tier belong at ADV-101.

Cross-anchor connections

Seitz-Arnold's TCP server-and-client patterns instantiate Beej's *Guide to Network Programming* in Python rather than in C; the student who has walked Beej (per NET-101) recognises every line of *Black Hat Python*'s socket code. Seitz-Arnold's Burp extension chapter lands on Stuttard-Pinto's web-app vulnerability work; custom Burp extensions extend Burp's discovery capabilities for vulnerabilities WAHH walks. Seitz-Arnold's raw-socket sniffer lands on the Wireshark-and-tshark practitioner discipline (per Sanders, NET-101 anchor 4); the same packets Wireshark dissects can be hand-decoded in Python.

---

§6. Summary: how the anchors compose at Belt-3

Anchor	Role	Belt-3 deliverable it supports
Heath Adams Practical Ethical Hacking	Build-it-yourself methodology companion	Labs 1-7 walkthroughs; capstone procedural anchor; OSCP-prep first layer
OffSec PEN-200 / OSCP+	Institutional credential pathway	Future-state credential planning; capstone calibration; ADV-101 prerequisite
Stuttard + Pinto WAHH 2e	Web-app vulnerability practitioner narrative	Lab 4 web reconnaissance; Lab 8 web-app exploitation; ADV-101 web-app CVE work
Seitz + Arnold Black Hat Python 2e	Build-from-scratch offensive-Python	Lab 10 custom-tooling exercise; capstone custom-tool artifacts; ADV-101 reproduction-tool work

The composition is opinionated by design. Heath Adams gives the seven-phase methodology; OffSec PEN-200 names the credential the methodology prepares for; WAHH gives the web-app vocabulary; *Black Hat Python* gives the build-from-scratch scripting register. The four anchors do not reduce to one anchor; each earns its place because the others assume its content. The Belt-3 is what the composition produces.

---

§7. What's next at Belt-4 and Belt-5

PEN-101 graduates carry the four-anchor foundation into ADV-101 (Belt 4; CVE-to-tool work; the SB6141 CSRF reproduction is the canonical capstone) and into ADV-102 (Belt 4; LLM-CVE variant; CVE-2025-65106 LangChain Jinja2 SSTI). The pentest track does not currently have a Belt-5 terminal course; advanced pentest work is integrated into the academy's broader RE and AI capstone arcs.

Anchors that return at deeper register:

- **Heath Adams returns at ADV-101** as the methodology anchor for the CVE-to-tool engagement workflow.
- **OffSec PEN-200 is the credential pathway** that PEN-101 plus ADV-101 plus ADV-102 plus PEN-200 composes the academy's OSCP-prep sequence.
- **WAHH returns at ADV-101 and ADV-102** for the deeper web-app and LLM-web-app vulnerability classes.
- **Seitz-Arnold returns at ADV-101** for the custom-reproduction-tool authoring register.

The capstone work PEN-101 prepares for: a five-day simulated engagement against an academy-owned target with a client-style written report and oral debrief, graded on a two-tier rubric (five binary engagement-discipline gates plus a 40-30-30 technical-depth, report-craft, and engagement-discipline split). Students who carry the four-anchor foundation into the capstone produce stronger artifacts than students who learn the vocabulary during the capstone.

Practitioner-training platforms parallel: PortSwigger Web Security Academy (free at portswigger.net/web-security; the discipline's most-cited free hands-on web-pentest training); HackTheBox Academy and TryHackMe (subscription; broader pentest training across web, network, and Active Directory). PEN-101 graduates are encouraged to use these platforms as ongoing practice between courses.

Credential-prep parallel: the academy's full OSCP-prep sequence is PEN-101 → ADV-101 → ADV-102 → PEN-200. Students typically sit PEN-200 within three to six months of completing the academy sequence. Alternative credentials (CompTIA PenTest+; eLearnSecurity eJPT; SANS GPEN) are mentioned in the catalog page's Certification Alignment section and not detailed here.

---

§8. Cross-references

Artifact	Path	Relationship
Catalog page (the page you arrived from)	`/vca-pen-101`	Distilled register; this guide is its forward-pointer destination
Companion handout: WIR-101 anchor reading guide	`/handouts/cross-chapter-wir-101-anchor-reading-guide.md`	Companion Belt-3 handout; wireless-track foundations
Companion handout: HW-101 anchor reading guide	`/handouts/cross-chapter-hw-101-anchor-reading-guide.md`	Companion Belt-3 handout; hardware-track foundations
Companion handout: NET-101 anchor reading guide	`/handouts/cross-chapter-net-101-anchor-reading-guide.md`	Companion Belt-3 handout; networking-track foundations
ADV-101 catalog page	`/vca-adv-101`	Belt-4 PT/ADV-track; CVE-to-tool work; SB6141 CSRF reproduction capstone
ADV-102 catalog page	`/vca-adv-102`	Belt-4 PT/ADV-track; LLM-CVE variant; CVE-2025-65106