



GHOST
PROTOCOL

GL

THE FIELD LIBRARY

COMPANION

EVERY TERM, AND THE TRUTHS

The Glossary and the Ledger

The library's terms defined plainly, and the
ledger: the consolidated one-line truths of
the whole shelf.



Ghost Protocol (Pvt) Ltd · Colombo · ghosts.lk

Security internship training · The Field Library · Edition 1 · 2026

THE GHOST PROTOCOL FIELD LIBRARY · COMPANION

The Glossary and the Ledger

The library's terms defined plainly, and the ledger:
the consolidated one-line truths of the whole
shelf.

Ghost Protocol (Pvt) Ltd · Colombo

The Field Library, Edition 1 · 2026

Copyright 2026 Ghost Protocol (Private) Limited. All rights reserved.

Sold as a PDF for the buyer's own reading. Please do not share or resell the file.

The library

The Field Library is a whole shelf, not one book. The Core Path is the spine everyone reads. The rest is depth and breadth, taken on as the work calls for it. The shelf is complete now, and you are reading the one marked here.

A · THE CORE PATH

O The Oath BUILT

I Groundwork BUILT

II The Web BUILT

III The Wider Field BUILT

IV The Work BUILT

V The Craft BUILT

B · DEEP TRACKS

AI and Agents BUILT

Reading Code BUILT

Internal and Active Directory BUILT

The Web, Deeper BUILT

Cloud and Containers BUILT

Mobile and APIs BUILT

Reverse Engineering BUILT

Hardware and the Edges BUILT

C · THE OPERATIONS

Red and Purple Team BUILT

OSINT and Recon BUILT

Report Writing Mastery BUILT

The Consulting Craft BUILT

Bug Bounty BUILT

D · THE OTHER SIDE

Detection and Response BUILT

Threat Hunting and Forensics BUILT

Hardening and Architecture BUILT

E · THE GROUND RULES

The Law, Deeper BUILT

Standards and Compliance BUILT

Ethics and Disclosure BUILT

F · COMPANIONS

The Reference Pack BUILT

The Lab Workbook BUILT

Case Files BUILT

The Bestiary BUILT

The Glossary and the Ledger YOU ARE HERE

Contents

- Opening 5
- 1** Glossary, A to F 6
- 2** Glossary, G to M 11
- 3** Glossary, N to S 15
- 4** Glossary, T to Z 19
- 5** The Ledger 22
- Worked answers 28

The words, and the one-liners



You had read most of the shelf, and the words had piled up: acronyms, class names, the house's own phrases. Blink kept almost remembering what one of them meant.

BLINK "What was BOLA again? And IMDS? And was it fourteen tactics now, or fifteen?"

SOL "Fifteen, since April. This is the book you keep open when the word is on the tip of your tongue. A glossary, so you speak precisely and mean exactly what an auditor or a client means. And the ledger: the distilled truths of the whole shelf, every one-line thing worth carrying, on pages you can keep beside you."

Wurm, who is the ledger as much as anyone, opened the one green eye.

WYRM "the words. the truths."

So the book is the reference: the terms of the craft defined plainly, and the consolidated ledger of everything the library asked you to keep.

CHAPTER ONE

Glossary: A to F

The vocabulary the Library uses, from authorisation to fuzzing, each in one to three plain sentences, with the volume it comes from where that helps. A lookup, not a lesson: the lesson is in the volume named.

This volume is the Library's dictionary. The other volumes teach the ideas; this one fixes the words, so that a term you use in a report means exactly one thing and an auditor can file it without arguing. Where a word has a current fact that moved, the entry states the current fact and dates it. Nothing here is new material: a reader who learned a term in its own volume will find it here unchanged, only shorter.

**SOL SAYS**

Learn the words so you can stop thinking about them, and spend the thinking on the judgment. A term used exactly is a finding the reader can act on. A term used loosely is a claim you cannot defend when someone asks you to. The glossary is here so that precision costs you nothing, not so that you can sound senior. The difference shows the first time a client reads the word back to you.

TERM	MEANING
Access control (broken)	The server's enforcement of what each caller may do to each object. When it is missing or wrong, a caller reaches data or actions that are not theirs. It is the top web class (Broken Access Control, AO1 in the OWASP Top 10) and the one the source code makes look most normal. (Volume II; Reading Code)
Active Directory (AD)	Microsoft's identity service that a Windows network trusts to say who a user is and what they may reach. Nearly every internal attack is an abuse of one normal step in that machine, so learn the honest machine first. (Internal and Active Directory)
Active testing	Sending crafted traffic to a target rather than only observing it. It touches someone else's system, so it needs written authorisation. Contrast passive testing. (Volume O; Volume II)
Agent (AI agent)	A language model wired to tools and a loop, so it can take actions and not only produce text. The safe shape is that the model proposes and deterministic code disposes, keeping the trigger in code. (AI and Agents)
API (and API security)	An Application Programming Interface: the real system behind a thin client, answering anyone who speaks its language. Testing it is not testing a page, because identity is a token, the request is the tool, and old versions and forgotten verbs hide surface. (Mobile and APIs)
APT (Advanced Persistent Threat)	A well-resourced adversary that gets in and stays, operating quietly over a long period. The threat model red teams emulate and hunters assume. (Red and Purple Team; Threat Hunting and Forensics)
ASVS	OWASP's Application Security Verification Standard: a checklist of security requirements an application should meet, by level. A requirements standard, not a list of risks. (The Reference Pack)

TERM	MEANING
ATLAS	See MITRE ATLAS (Chapter Two).
ATT&CK	See MITRE ATT&CK (Chapter Two).
Attack surface	Every point where an attacker can try to interact with a system: inputs, endpoints, services, people. Recon maps it; the test spends its hours on it. (OSINT and Recon)
Authentication	The check of who a caller is: a login, a token, a certificate. It answers "who are you", and is distinct from authorisation, which answers "may you". (Volume II)
Authorisation	In the engagement sense, written permission from someone with the authority to grant it, to test named systems. It is what makes access lawful, and your protection is the signature, never your intent. In the access-control sense, the in-application check of whether an authenticated caller may perform this action on this object; broken access control is that check never being made. (Volume O; Volume II)
Beacon	The regular check-in from an implant to its command server. Its regularity, not its payload, is the tell a defender reads. (Red and Purple Team; Detection and Response)
BFLA	Broken Function Level Authorization: an API caller reaching a function, often an admin action, they are not entitled to call. The wrong function. API5 in the OWASP API Security Top 10 (2023), proven with two of your own accounts at different privilege levels. (Mobile and APIs)
Black-box testing	Testing with no inside knowledge, from the outside as an attacker sees it. Contrast white-box and grey-box. (Reading Code)
Blue team	The defenders: the people and systems that detect and respond to attacks. (Detection and Response)
BOLA	Broken Object Level Authorization: an API caller reaching another user's object by changing an identifier. The wrong object. API1, the top entry in the OWASP API Security Top 10 (2023), and the API-specific name for IDOR. (Mobile and APIs)
BOPLA	Broken Object Property Level Authorization: reading or writing object properties a caller should not touch (mass assignment and excessive data exposure combined). The wrong property. API3 in the 2023 API list. (Mobile and APIs)
Brute force	Trying many values (passwords, tokens, identifiers) until one works. Rate limits and lockouts are the defence.
Bug bounty	A written, public invitation to test named systems for pay. The invitation is only ever as wide as the policy page: two authorisations, not one. (Bug Bounty)
Business logic flaw	Abuse of an application's intended rules (price, quantity, workflow, sequence) rather than a technical defect. The class scanners miss, proven by the final state. (Volume II)
C2 (Command and Control)	The channel an attacker uses to control compromised hosts. Detected by the shape of its traffic, not the contents of its payload. (Red and Purple Team; Detection and Response)
Canary (token)	A benign marker planted to prove an action happened, such as a request to a domain you own or a unique string returned in a response, without causing harm. The clean way to prove a dangerous capability at its edge. (AI and Agents; Volume II)

TERM	MEANING
CIA triad	Confidentiality, Integrity, Availability: the three properties security protects. A quick lens for what a finding actually threatens.
Clean conduct	Ghost Protocol's doctrine and its strategy both: win on the merits only, never leverage what the access showed you, never manufacture fear. Reputation is the one asset that compounds and the one you cannot buy back. (Volume 0; Ethics and Disclosure)
Container	A fenced process sharing the host's kernel, not a virtual machine and not a wall. An escape crosses from the container to the host; prove the setting on the client, prove the escape at home. (Cloud and Containers)
CORS	Cross-Origin Resource Sharing: the browser rules that decide when a page may read a response from another origin. A policy left too open can hand data to a hostile site. (The Web, Deeper)
Credential stuffing	Replaying username and password pairs leaked elsewhere, betting on reuse across sites.
CSP	Content Security Policy: a response header that restricts what a page may load and run. Defence in depth against XSS, never a cure for it. (Hardening and Architecture)
CSRF	Cross-Site Request Forgery: tricking a logged-in user's browser into making a state-changing request they did not intend. The server trusting a cookie as proof of intent. CWE-352. (Volume II)
CVE	Common Vulnerabilities and Exposures: the scheme that gives a specific, known vulnerability in a specific product one public identifier, for example CVE-2024-3094. A CVE is one instance; a CWE is the weakness type behind it. (The Reference Pack)
CVSS	Common Vulnerability Scoring System: a shared, auditable way to score a vulnerability's severity, giving a number and a vector string. The current version is 4.0 (2023); 3.1 (2019) is still widely used, so name the version. The base score describes the vulnerability; the severity you report is risk in context, so start from CVSS and rate by context, and never reprint a scanner's number as your rating. (Report Writing Mastery; The Reference Pack)
CWE	Common Weakness Enumeration: MITRE's catalogue of weakness types, for example CWE-79 (cross-site scripting), CWE-89 (SQL injection), CWE-918 (SSRF). Keying a finding to a stable CWE outlasts a Top 10 rank that moves between editions. (The Reference Pack; Reading Code)
DAST	Dynamic Application Security Testing: testing a running application from the outside by sending it traffic. Contrast SAST. (Reading Code)
Defence in depth	Independent layers, so one control failing does not open the whole system. Trust no single control, including your own, and treat detection as a layer. (Hardening and Architecture)
Deny-by-default egress	Blocking all outbound traffic except an explicit allow-list, so a compromised component cannot phone out or send data away. A core containment for agent and SSRF risk. (AI and Agents; Hardening and Architecture)
Deserialization (insecure)	Turning attacker-supplied bytes back into an object, where the bytes choose the type and a native deserializer may run its own code while rebuilding them. CWE-502. Prove it with an out-of-band callback, not a shell. (The Web, Deeper)

TERM	MEANING
Detection engineering	Writing detections as versioned, reviewed code, each mapped to a technique and tested by firing the real attack. A rule you never fired is only a hypothesis. (Detection and Response; Threat Hunting and Forensics)
Disclosure (coordinated)	Reporting a flaw privately, giving a fair bounded time to fix, and coordinating the public release with the fix. Also called responsible disclosure. A finding is a gift to be given, never a lever to be pulled. (Ethics and Disclosure)
DNS exfiltration	Smuggling data out inside DNS queries, which often leave a network even when nothing else can.
DNS rebinding	Flipping a hostname's address after a page has loaded, to reach internal services a browser would otherwise block. A case an SSRF guard must defend against. (The Web, Deeper)
DoS / DDoS	Denial of Service: making a service unavailable by exhausting it, from one source or many. Usually out of scope, and never a demonstration you run against a live client.
EDR	Endpoint Detection and Response: agent software on hosts that records and flags suspicious behaviour and supports response. (Detection and Response)
Egress filtering	Controlling outbound traffic. See deny-by-default egress.
Engagement	A scoped, authorised, paid test that ends in a written report. (Volume IV; The Consulting Craft)
Enumeration	Asking a system the right questions to list its users, shares, endpoints, or objects, quietly first. Internal tests are won here: arrive at the loud tools already knowing where to point them. (Internal and Active Directory; OSINT and Recon)
Evidence	The exact request and response, or the artefact, that proves a finding's specific claim, and nothing more. (Volume II; Report Writing Mastery)
Exfiltration	Moving data off a target to somewhere the attacker controls. One leg of the lethal trifecta for agents. (AI and Agents)
Exploit	Code or a sequence of steps that turns a weakness into a working attack.
False negative	A real issue a tool missed. A clean scan is not a clean system.
False positive	A tool-flagged issue that proves not to be real once verified by hand. (Volume II)
Finding	One issue in a report, in a fixed order of seven parts: title, affected asset, severity (with the CVSS vector), steps to reproduce, evidence, impact, remediation. Each part answers the reader's next question, and does its own job and no other. (Report Writing Mastery)
Forensics	Reading a compromised system's artifacts to reconstruct what happened, preserving the chain of custody from the first byte. (Threat Hunting and Forensics)
Free scan	The passive, public-surface look Ghost Protocol leads with. Agreed and bounded, no active testing, and still a scoped, authorised action, never a surprise sprung on a prospect. (Volume 0)
Fuzzing	Feeding a target many malformed or unexpected inputs to find the one that breaks it.

	THE PART	THE READER ASKS	WHO
1	Title	What is wrong, where?	] triage routes it
2	Affected asset	Which exact thing?	
3	Severity + vector	How bad? Can I check it?	
4	Steps to reproduce	Can I make it happen?	] the sceptic checks it
5	Evidence	How do you know?	
6	Impact	Why should we care?	] decision-maker
7	Remediation	What do we change?	] developer

The seven parts of a finding.

■ ON YOUR FEET

Your scanner reports a SQL injection with a CVSS base score of 9.8, labelled Critical, on a client's internal reporting tool. You have not yet reproduced it. Using only the words in this chapter, what is CVSS actually telling you, what is it not telling you, and what has to happen before the word Critical, or any severity, goes into the report at all?



WHAT WYRM KEEPS

The vocabulary is for precision, not performance. A word used exactly is a finding the reader can file; a word used loosely is a claim you cannot defend.

- Authorisation is the signature, never the intent. Authentication asks who you are; authorisation asks whether you may.
- CVSS is a shared starting point (4.0 current, 3.1 still in use), not the rating. Key findings to a stable CWE, not to a Top 10 rank that moves.
- A scanner flag is a lead: a false positive until verified by hand. BOLA, BFLA and BOPLA are the API forms of broken access control.
- Clean conduct is the ethic and the strategy both. Reputation is the one asset you cannot buy back.