



GHOST  
PROTOCOL

RW

THE FIELD LIBRARY

OPERATIONS

THE PRODUCT IS THE PAPER

# Report Writing Mastery

Why the report is the product, the anatomy  
of a finding, severity done honestly, writing  
for the reader, and the deliverable.



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

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

THE GHOST PROTOCOL FIELD LIBRARY · OPERATIONS

# Report Writing Mastery

Why the report is the product, the anatomy of a finding, severity done honestly, writing for the reader, and the deliverable.

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 YOU ARE HERE

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 BUILT

# Contents

- Opening ..... 5
- 1** The Report Is the Product ..... 6
- 2** Anatomy of a Finding ..... 10
- 3** Severity and Risk ..... 15
- 4** Writing for the Reader ..... 20
- 5** The Deliverable ..... 24
- Worked answers ..... 29

# What they actually buy



The test was done, a good one, three real findings proven by hand. Blink was ready to call it finished and move on.

BLINK "We found the bugs. That is the job."

SOL "That is half the job, and the half the client never sees. They did not buy your testing. They bought a document they can act on: what you found, how bad it is, and exactly what to do about it. A brilliant test written up badly is a brilliant test nobody fixes. The report is the product, and it is the only part of you that stays in the room after you leave."

Worm's eye settled on a draft, on a line that said the impact "could be severe", and did not say for whom, or how.

WORM "say what's true."

That is the whole book. How to turn a finding into a fix, written so a developer can reproduce it, a manager can rank it, and nobody has to take your word for anything.

## CHAPTER ONE

# The Report Is the Product

The client never watched you work. They read a document and decide what to do about their business from it. This chapter is about treating that document as the thing you were paid to make, and about the habit that keeps it worth reading: every sentence is a claim you can back.

---

An engagement happens in two places that never meet. One is the test: your terminal, the proxy, the long hours reading responses until a pattern shows. The other is a PDF open on a director's screen for twenty minutes. The client paid for the second one. They will almost never see the first, and they will act on what the second one says. Get good at the testing and bad at the report, and you have done excellent work that no one can use. This volume is about the half the client actually receives.

## What the client is buying

---

Strip the engagement down and the client is buying a decision they can make with confidence: what to fix, in what order, and how. They are not buying your cleverness, your tooling, or the hours you spent. Those paid for the knowledge. The report is the only object that carries that knowledge from your side of the glass to theirs, and it is the only part of the work they can hold, forward, and come back to in a year. A chain you are proud of does not exist to the client until a sentence on the page carries it, in words a reader who was not there can follow.

This is why a report is not a record of what you did. A reader does not need your afternoon. They need the few things that change what they should do on Monday, said clearly enough that they do the right one. The test produces far more than belongs in the document. Choosing what to leave out, and saying what stays in so a non-specialist can act on it, is the craft this book teaches.

## The report outlives the test

---

The document you hand over has a longer life than the engagement that made it. It goes to a board that approves the budget to fix things. It goes to an auditor who files it against a control. It goes to a prospective customer running vendor due diligence, who may read it before signing a contract with your client. It goes to the development team a year from now, when the person who fixed the first finding has left and someone new is reading the retest. In some cases it reaches a regulator. Every one of those readers was absent from the test and cannot ask you what you meant. The report has to answer on its own, long after you have forgotten the target.

So write for the reader who has only the page. If a finding needs you standing next to it to make sense, it is not finished. If the executive summary only works for someone who already sat through the debrief, it does not work. The test of a sentence is whether it survives being read by a stranger, months later, with no one to interpret it.

## A report is a stack of claims

---

Read any report one line at a time and you will see it is made of assertions. This is here. It does this. It matters this much. Fix it this way. Each of those is a claim, and a claim is only worth the evidence standing behind it. A finding that says a logged-in customer can read another customer's records is a promise that you can produce the request that asked for the other customer's record and the response that returned it. If you can, the claim is a finding. If you cannot, it is a feeling, and a feeling in a client report is a liability with your name on it.

That habit, treating every sentence as a claim you must be able to prove, is the spine of the whole volume. Volume II drilled it as the rule you verify a finding before you believe it. Here it becomes the rule you verify a sentence before you write it. The two are the same discipline at different ends of the work, and the report is where it either holds or shows.

## The report is the house speaking

---

When a report leaves Ghost Protocol, it is the firm's word in the reader's hands, over a name that has to mean something to the next client too. A careful reader does not grade a report on its best page. They grade it on the first sentence they catch being wrong. One severity inflated to look impressive, one impact paragraph that is true of the class and of no particular target, one line a tool could have written about any system on earth, and the reader quietly stops trusting the rest, including the parts that were right. Credibility is the single asset the work cannot buy back once it is spent, and the report is where it is most easily spent by accident.

## What it is not

---

Because the report is the product, it is worth naming the things it is not, since each one is a draft that mistook itself for finished.

- It is not a scanner's output with a cover page. A tool's list is an input to your judgment. Rating and evidence are covered in Chapters Three and Two, and neither is something a tool finished for you.
- It is not a diary of your machine. The reader does not need your virtual machine, your wordlist, or the order you tried things. They need the test you ran and what it proved.
- It is not a place to be clever. The war story about how you chained three small things stays in your notes unless the chain is the finding. The reader's time is the budget.
- It is not a feelings document. "This looks dangerous" is not a severity, and "I think an attacker could" is not evidence.

The rest of this volume takes the report apart and rebuilds it to this standard: the anatomy of a single finding (Chapter Two), severity rated honestly (Chapter Three), writing for the two readers who will actually read it (Chapter Four), and assembling, checking, and delivering the whole with nothing untrue in it (Chapter Five). Where the report sits inside the engagement, how the work was won and scoped, is Volume IV, The Work. The fill-in templates, the report shape and the before-you-send checklist, live in the Reference Pack companion. This volume is the craft those forms assume.



## SOL SAYS

The work is for you. The report is for them. On the page your job is to disappear, so that what is left is the reader and a decision they can make without you in the room. The intern who writes to show how hard the test was writes a report about themselves. The professional writes one the reader forgets they are reading, because it is only ever about the reader's own systems and what to do about them. Aim to be forgotten. It means the page did its job.

## ■ EXERCISE

Take a report you have written, or if you have none yet, take a lab you have solved (a DVWA level, a PortSwigger Web Security Academy lab) and write it up as one finding plus a half-page executive summary. Now hand only the summary to someone who is not technical and does not know the target. Ask them to tell you, from that half-page alone, what they would fix first and why it matters. If they cannot answer, the product failed, however good the test behind it was. Rewrite the summary until a stranger can make the decision from it, then check that the finding underneath still proves every claim the summary makes.

## ■ VERIFY IT

Read a finding of yours sentence by sentence, and against each one ask the plain question: which exact request and which exact response proves this? If you can put a finger on both, the sentence is a finding. If you have to reconstruct it from memory or hope it reproduces, it is a draft, and it does not go to a client until it is more than that. A belief you have reproduced is worth writing down. A belief you have not is a note to yourself, not a line in someone's security report.

## ■ THE LINE

A report only covers what you were authorised, in writing, to test. The law and the authorisation are Volume 0, read before any technique and not re-argued here. In the document it shows as the scope and authorisation section, and that section is not throat-clearing to get past. It is the true boundary of the work, stated as fact: these systems, this window, this signed grant. Nothing you tested outside that boundary belongs in the report, because it should not have been tested at all. An out-of-scope asset you noticed and did not touch is different: it goes in as an observation, flagged for the client to scope.

## ■ ON YOUR FEET

Near the end of the window you see something that looks real and serious, but you did not have time to reproduce it cleanly, and the report is due first thing tomorrow. Do you write it up as a finding with a severity and an impact, leave it out entirely, or something else? What, exactly, do you put on the page, and where?



## WHAT WYRM KEEPS

The client buys the report, not the test. It is the only artefact that crosses into their world, it outlives the engagement, and it is the house's word. Every sentence is a claim you can back, or it does not go in.

- The test produces the knowledge. The report is the product. Work done but not carried onto the page cannot be acted on by anyone.
- The document is read by people who were never in the room and cannot ask what you meant, so it has to stand alone, months later, without you.
- A report is a stack of claims. A claim you cannot prove with the exact request and response is a liability, not a finding.
- A reader grades the whole report on the first sentence they catch being wrong. One untrue line spends the credibility the next client was relying on.

## CHAPTER TWO

# Anatomy of a Finding

A finding has seven parts, and each one answers a question the reader is about to ask. This chapter builds one finding from title to remediation, so you can write any finding to a shape a developer can act on and a reviewer can check.

A finding is the unit the whole report is made of, and it has a fixed shape for a reason: a reader works through it in the same order every time, and each part answers the next question they have. What is wrong, and where. How bad. How you know. What it means for us. What we change. Write the parts out of order or leave one weak and the reader stalls on the question you skipped. We will build a single finding across this chapter, one part at a time, and by the end you will have a template you carry in your head.

|   | 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             |

Seven parts, always in this order. Each answers the question its reader is about to ask.

## The seven parts

Every Ghost Protocol finding carries these seven, in this order, in every report and in every volume of this Library:

1. **Title:** what is wrong, and where, in one line.
2. **Affected asset:** the exact thing it is wrong in.
3. **Severity,** with the CVSS vector: how much it matters, with the rating made auditable.
4. **Steps to reproduce:** how someone else repeats it.
5. **Evidence:** the proof that this exact thing happens.
6. **Impact:** what it means for this client.
7. **Remediation:** the specific change that closes it.