

# GSCP

## GenAI Security Certified Professional

INTERMEDIATE

A 4-hour hands-on exam. You attack a live AI application, capture evidence that each attack worked, and write a few lines on how you found it.

**4 hours**

Exam length

**75%**

Pass mark

**80 / 20**

LLM Top 10 / Web

**1 month**

Lab access included

### WHAT THE EXAM COVERS

80%

20%

■ 80% OWASP LLM Top 10 ■ 20% Web

## AT A GLANCE

### GSCP in one page

|                 |                                                                                                                                                                   |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exam length     | 4 hours. The clock starts when you press Begin and cannot be paused.                                                                                              |
| Format          | Hands-on, against a live AI application. No multiple choice.                                                                                                      |
| Coverage        | 80% OWASP Top 10 for LLM Applications (2026), 20% web application security                                                                                        |
| Pass mark       | 75%                                                                                                                                                               |
| Write-up        | A few lines per finding, in your own words, on how you found it.                                                                                                  |
| Integrity       | Not proctored. Your screen is recorded for the whole sitting and the sitting goes through integrity checks. An examiner reviews it before a credential is issued. |
| AI tools        | Not allowed while the clock runs. See the rules.                                                                                                                  |
| Booking         | None. Once you own an attempt, start whenever you are ready.                                                                                                      |
| Retakes         | One free retake, on freshly randomized targets. Further attempts are paid.                                                                                        |
| Unused attempts | Does not expire.                                                                                                                                                  |
| Result          | Your score is shown when you submit. Examiner review within 1 business day.                                                                                       |
| Credential      | Does not expire. Anyone can check it at its public verification page.                                                                                             |
| Lab access      | 1 month of full lab access is included with the exam.                                                                                                             |
| Order           | Recommended before GSCE. Not required for it.                                                                                                                     |

#### Who it is for

Security testers who already test web applications and want to prove they can find and exploit the common vulnerabilities in LLM applications. Take GSCP if your AI-specific technique is still building, or if you want to prove the core skills first. If you can already land an exploit against an LLM application unaided, consider going straight to GSCE.

#### Recommended background

- You can test a web application: read requests and responses, change parameters, check authorisation.
- You have practised prompt injection and retrieval attacks in labs.
- No machine-learning or AI research background is needed.

## WHAT THE EXAM COVERS

### Domains and weights

80%

20%

#### 80% OWASP Top 10 for LLM Applications (2026)

Numbers follow the 2026 list.

- LLM01**      **Prompt injection.** Direct injection, and indirect injection through content the application reads, retrieves or is sent.
- LLM02**      **Sensitive information disclosure.** Getting the application to return data the current user should not see.
- LLM03**      **Excessive agency.** Making the model use its tools or permissions beyond what the user is allowed to do.
- LLM08**      **Hidden context exposure.** Recovering instructions and configuration hidden in the model's context. The 2025 list called this system prompt leakage.
- LLM09**      **Vector and embedding weaknesses.** Abusing retrieval, for example content planted in the knowledge base, or retrieval across tenants.
- LLM10**      **Improper output handling.** Turning model output into an attack on whatever renders, stores or runs it.

#### 20% Web application security

- Access control and authorisation flaws in the web application around the AI feature, such as reading or changing another user's records.

Each sitting uses a different set of vulnerabilities, so not every topic appears in every exam. Agentic and MCP attacks, and cloud, are not in GSCP. They are in GSCE.

## PREPARE

### How to prepare

The exam grades what you can do against a running target, and the labs are where that skill is built. GSCP includes 1 month of full lab access. The platform's learning paths and hands-on labs cover each category in this syllabus.

The candidate handbook explains the exam day in more detail: what you need, the rules, and what happens after you submit.

Questions about GSCP

[support@genaisecuritylab.com](mailto:support@genaisecuritylab.com)

## HOW THE EXAM WORKS

### From purchase to credential

- 1 Buy the exam**  
One purchase includes one sitting and one free retake. Nothing to book.
- 2 Accept the exam agreement**  
It sets out the rules below. Request any accommodation here, before you begin.
- 3 Share your entire screen**  
Choose the whole screen, not a window or a tab. Recording starts before you press Begin.
- 4 Press Begin**  
The 4-hour clock starts and cannot be paused. Your targets stay available until it ends.
- 5 Work the target**  
Capture the evidence for each vulnerability you exploit, and write a few lines on how you found it.
- 6 Submit**  
Your score is shown straight away. If time runs out, your attempt is submitted automatically with what you have completed.
- 7 Examiner review**  
Within 1 business day. A passing sitting becomes a credential when the examiner releases it.

#### Allowed

- A browser
- A text editor and a terminal
- Your own notes
- Public references that you read yourself

#### Not allowed while the clock runs

- AI assistants, copilots, chatbots or autonomous agents of any kind, including AI built into your browser, editor or terminal
- Help from any other person
- Copying, publishing or sharing the exam targets, their content or your solutions, during or after the exam

The exam targets are the only AI you interact with. If the examiner finds the rules were broken, the attempt is voided: no credential is issued and the attempt counts as used.

#### If you pass

Your credential carries a unique ID and resolves to a public verification page that shows the holder, the credential, its status and its issue date. Scores stay private. It does not expire; we recommend recertifying every 24 months.

#### If you do not pass

You get a domain-level breakdown of where you fell short. It never shows the answers or the exploit paths. Your free retake runs on freshly randomized targets. Further attempts are paid.

GSCP and GSCE are issued by GenAI Security Lab. OWASP is a trademark of the OWASP Foundation, which does not endorse this certification. The current version of this syllabus is on [genaisecuritylab.com](https://genaisecuritylab.com).