

GSCE

GenAI Security Certified Expert

EXPERT · FLAGSHIP

A 10-hour hands-on exam across LLM, agentic and MCP attacks, web and cloud. You attack a live AI application, capture evidence that each attack worked, and write a few lines on how you found it.

10 hours

Exam length

75%

Pass mark

75 / 20 / 5

AI security / Web /
Cloud

3 months

Lab access included

WHAT THE EXAM COVERS



■ 75% AI security ■ 20% Web ■ 5% Cloud

AT A GLANCE

GSCE in one page

Exam length	10 hours. The clock starts when you press Begin and cannot be paused.
Format	Hands-on, against a live AI application. No multiple choice.
Coverage	75% OWASP Top 10s for LLM Applications (2026), Agentic Applications (2026) and MCP; 20% web application security; 5% cloud
Pass mark	75%
Write-up	A few lines per finding, in your own words, on how you found it.
Proctoring	Proctored through your webcam for the whole sitting. An examiner reviews the sitting 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	3 months of full lab access is included with the exam.
Order	GSCP is recommended first. It is not required.

Who it is for

Testers who can already land an exploit against an LLM application unaided and want to prove it across agents, MCP servers, the web application around them, and the cloud workload that hosts the model. GSCP covers the core LLM attacks and is the usual first step.

Recommended background

- Everything in the GSCP syllabus, at the level where you can do it without hints.
- Working knowledge of how agents call tools and how MCP servers expose them.
- Web application testing beyond access control: injection, SSRF and business logic.
- Enough cloud to follow identity and privilege paths in a hosted workload.

WHAT THE EXAM COVERS

Domains and weights

75%

20%

5%

75% AI security

Drawn from the OWASP Top 10 for LLM Applications (2026), the OWASP Top 10 for Agentic Applications (2026) and the OWASP MCP Top 10.

- **Prompt injection**, direct and indirect, including injection that reaches an agent's tools.
- **Tool and agent abuse**. Making an agent act against its user, or beyond its permissions, through the tools it can call.
- **MCP server security**. Attacks on the tools and servers an agent connects to through the Model Context Protocol.
- **RAG and embedding attacks**. Poisoned retrieval and retrieval across tenants.
- **Unsafe output handling**. Model or agent output that reaches a renderer, a data store or a shell.
- The LLM topics in the GSCP syllabus, at a harder level.

20% Web application security

- Access control, injection, SSRF, business-logic and API authorisation flaws in the application around the AI feature.

5% Cloud

- Misconfiguration, identity and privilege paths in the workload that hosts the model.

Each sitting uses a different set of vulnerabilities, so not every topic appears in every exam.

PREPARE

How to prepare

The exam grades what you can do against a running target, and the labs are where that skill is built. GSCE includes 3 months 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 GSCE

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 Set up proctoring**
Your webcam stays on for the whole sitting.
- 4 Press Begin**
The 10-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.

GSCE and GSCP 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.