

Web Application Security Assessment – Engagement Terms

Lachlan Harris • {date} • {client}

Section 1: Definitions

- “Assessment” refers to the web application penetration test to be conducted by the Security Consultant.
- “Client” refers to the organisation or individual authorising and requesting the Assessment.
- “Consultant” refers to Lachlan Harris, the individual conducting the assessment
- “Target System(s)” refers to the website(s), web application(s), or digital service(s) explicitly included in the Scope of Assessment
- “Findings” refers to the vulnerabilities, security weaknesses, or issues identified during the Assessment
- “Report” refers to the final written deliverable containing the Findings and recommended mitigations

Section 2: Purpose

The Consultant has been authorised by the Client to perform a professional security Assessment of the Client's digital assets. The purpose of this engagement is to identify technical vulnerabilities and provide remediation advice to enhance the Client's cyber resilience.

This engagement is provided in exchange for a charitable donation made directly by the Client to a humanitarian program in Cambodia, facilitated by the Consultant's school.

Section 3: Scope

The following systems and services are explicitly in scope:

- {domains, applications, IP ranges}

The following systems are explicitly out of scope, unless amended in writing:

- Internal networks or systems not publicly accessible
- Client-owned infrastructure not explicitly listed above
- Denial of Service (DoS) attacks
- Phishing, vishing or any form of social engineering
- Physical intrusion attempts
- Malware deployment or exploitation of third-party software beyond demonstration
- Any actions that may compromise client data integrity, availability or confidentiality

If any ambiguity arises regarding scope, the Consultant will pause activity and request clarification from the client.

Section 4: Rules of Engagement

The Consultant agrees to:

- Conduct all testing in a non-disruptive manner
- Avoid intentional modification or deletion of any data
- Cease testing immediately if a critical flaw is discovered that could affect availability
- Only access data and systems reasonably necessary to complete the Assessment and that are explicitly defined in the scope
- Maintain strict confidentiality around all findings and client information
- Provide a report within 14 calendar days of testing completion

The Client agrees to:

- Provide written authorisation for this Assessment prior to commencement
- Ensure all system owners and relevant stakeholders are informed of this engagement
- Not hold the Consultant liable for impacts reasonably related to vulnerabilities already present in the system
- Donate the agreed amount directly to the nominated humanitarian program and confirm donation upon request

Section 5: Deliverables

The Consultant will provide the Client with:

- A written technical report detailing discovered vulnerabilities
- Technical recommendations for remediation
- A summary of the tools and techniques used (excluding sensitive exploit methods)

The report will be delivered in DOCX (Microsoft Word) format, digitally signed and marked confidential.

Section 6: Confidentiality

All information shared during the engagement will be treated as confidential, including but not limited to system configurations, the Client’s data, assessment results, and business practices.

The Consultant agrees to:

- Not disclose or publish any findings, system details, client identifiers or any information explicitly deemed “confidential” without written consent
- Use any collected information solely for the purposes of this engagement

The Client may request anonymised redaction or deletion of records following report delivery. Unless otherwise requested, all client-related data will be securely deleted within 30 days of report delivery.

Section 7: Termination

Either party may terminate this agreement in writing at any time prior to testing. Upon termination:

- The Consultant shall destroy all collected data
- No report will be produced
- The Client is not obligated to complete the donation

If termination occurs after testing begins, the Consultant reserves the right to complete or withhold deliverables at their discretion.

Section 8: Liability

This assessment is performed in good faith, using industry-standard techniques and methodologies. However:

- The Consultant makes no guarantees regarding the completeness of the Assessment
- The Consultant is not liable for any direct or indirect damages, outages, financial loss or business interruption resulting from previously existing vulnerabilities
- The Consultant does not act as a legal or compliance advisor

The Client assumes all responsibility for interpreting and acting upon the report

Section 9: Acknowledgement & Authorisation

The undersigned confirm that they are authorised to enter into this Agreement, and grant explicit permission for the Consultant to conduct the specified Assessment within the described scope.

X

Client

X

Lachlan Harris
Consultant