

PENETRATION TESTING AGREEMENT

Agreement No. ____ | Date: «__» _____ 202__

This Agreement incorporates by reference the Non-Disclosure Agreement between the same parties of even date.

1. PARTIES

Client:

Company Name: [_____]

Incorporated in: England and
Wales

Company No.: [_____]

Registered Address:
[_____]

Represented by: *[Name, Title]*

Provider:

Company Name: Curly's
Technology Tmi

Incorporated in: Finland

Business ID: FI31760109

Registered Address:
Topeliuksenkatu 19 A35, 00250

Helsinki, Finland

Phone: +358 040 626 4009

Represented by: Artem
Naumenko, CEO

2. SUBJECT MATTER AND AUTHORISATION

2.1. The Provider agrees to perform penetration testing services ("Pentest") against the Client's systems listed in **Schedule A**, for the purpose of identifying security vulnerabilities.

2.2. The Client hereby grants **explicit written authorisation** to the Provider to perform scanning, testing and analysis solely against the assets listed in Schedule A. This authorisation is given for the purposes of the **Computer Misuse Act 1990** (UK) and the Client warrants it has the legal right to authorise testing of all listed assets.

2.3. If any assets are hosted on shared or third-party infrastructure, the Client warrants it has obtained the hosting provider's permission prior to the commencement of testing.

3. SCOPE OF TESTING — SCHEDULE A

To be completed and initialled by both parties for each engagement:

In-Scope Targets:

Domains: [example.co.uk, *.example.co.uk]

IP Addresses: [1.2.3.4, 1.2.3.5]

Technology: [WordPress CMS vX.X]

Explicitly Out of Scope:

- DoS / DDoS attacks of any kind
- Social engineering of Client's staff
- Physical access attempts
- Third-party infrastructure not owned by Client
- Any assets not listed above

Client initials: _____ Provider initials: _____

4. TIMELINE

Parameter	Value
Start date	«__» _____ 202__
End date	«__» _____ 202__
Permitted testing window	01:00–05:00 UTC daily
Report delivery deadline	5 business days after end date

4.1. The Client may suspend or terminate testing at any time by written notice (email sufficient). The Provider must cease all activities within **15 minutes** of receipt.

4.2. The Provider must immediately notify the Client upon discovery of any Critical severity vulnerability, without waiting for end of engagement.

5. FEES AND PAYMENT

5.1. **No-find, no-fee:** If no vulnerabilities are identified within scope, no payment is due and the Provider waives any claim for compensation.

5.2. Upon identification of confirmed vulnerabilities, the following fees apply:

Vulnerability Type	Fee
Remote Code Execution (RCE)	USD 1,000

Exposure of client personal data records	USD 5 per unique record confirmed
Website defacement (demonstrated capability)	USD 500
Other critical findings	To be agreed in writing

5.3. **Maximum aggregate payment** under this Agreement shall not exceed **USD 3,000**, regardless of the number or severity of findings.

5.4. Payment is due within **14 calendar days** of the Client's written confirmation of a validated finding. Payment details shall be specified in the invoice issued by the Provider.

5.5. All fees are exclusive of VAT. As the Client is UK-based and the Provider is EU-based (Finland), the **reverse charge mechanism** applies; the Client is responsible for accounting for any VAT due in the UK.

6. PROVIDER OBLIGATIONS

1. Limit exploitation strictly to what is necessary to demonstrate existence of a vulnerability (Proof of Concept only);
2. Not access, copy, download or retain any real personal data belonging to Client's end users;
3. Maintain confidentiality per the NDA of even date;
4. Deliver a written report including: vulnerability description, reproduction steps, CVSS severity rating, and remediation recommendations;
5. Not disclose the existence of this engagement or findings to third parties without Client's prior written consent.

7. CLIENT OBLIGATIONS

1. Warrant ownership or explicit authorisation over all assets in Schedule A;
2. Notify internal security / NOC / hosting provider of testing schedule;
3. Respond to Provider's confirmation requests within 3 business days;
4. Not use the Provider's authorised activities as grounds for any legal claim against the Provider.

8. LIABILITY AND INDEMNITY

8.1. The Provider shall not be liable for any disruption or data loss arising from authorised testing within agreed scope and testing window.

8.2. The Provider's total aggregate liability shall not exceed the total fees paid or payable hereunder.

8.3. Neither party shall be liable for indirect, consequential or punitive damages.

8.4. The Client shall indemnify the Provider against any third-party claims arising from Client's failure to obtain proper authorisation from hosting providers or other third parties.

9. RELATIONSHIP WITH NDA

9.1. This Agreement is to be read together with the Non-Disclosure Agreement between the same parties of even date. In the event of conflict, the NDA shall prevail with respect to confidentiality obligations.

10. GOVERNING LAW AND DISPUTES

10.1. This Agreement shall be governed by the **laws of England and Wales**.

10.2. Disputes shall first be subject to good-faith negotiation for 30 days. If unresolved, they shall be submitted to the exclusive jurisdiction of the **courts of England and Wales**.

11. GENERAL

11.1. This Agreement constitutes the entire agreement on its subject matter and supersedes all prior discussions.

11.2. Changes to scope, timeline or fees require a written amendment signed by both parties.

11.3. This Agreement may be executed electronically with full legal effect under the Electronic Communications Act 2000 (UK).

SIGNATURES

Client

Name:

Provider

Name: Artem Naumenko

Title:

Date:

Signature:

Title: CEO, Curly's Technology
Tmi
Date:

Signature:
