



TRESPASS
SECURITY

2026

Penetration Test Report

External Network Assessment

PREPARED FOR

Fishing Rods LLC

fishingrods.example

ISSUED

10 September 2026

VERSION

1.0

Business Relationship

CLIENT

Fishing Rods LLC

Fishing Rods LLC designs bass fishing rods around a six-rod system covering a range of lures and techniques.

The company sells individual rods and bundles through its online store, with product guidance, instructional content, and customer support. Its rods are also available through Tackle Warehouse.

REQUESTING PARTY

Tackle Warehouse

Tackle Warehouse specializes in fishing tackle for recreational and professional bass anglers. Its range includes rods, reels, lures, and accessories.

Alongside its product selection, Tackle Warehouse publishes instructional articles and videos to help anglers choose equipment and develop their techniques. It is an authorized seller of rods made by Fishing Rods LLC.

Reason for the assessment

Tackle Warehouse requested an independent penetration test as part of its review of the business relationship.

Fishing Rods LLC engaged Trespass Security to assess the external network services defined in the agreed scope. The work examined those services and their security controls during the assessment period.

This report records the scope, work performed, and final results for both companies to review together.

Proof of Engagement

Penetration Testing

31 August 2026

Reference: TS-JOB-2026-001

TO

Tackle Warehouse

Re: Fishing Rods LLC

Dear Tackle Warehouse Team,

Fishing Rods LLC has entered into an agreement with Trespass Security LLC for an independent penetration test. At the client's request, we are providing this letter to confirm the engagement in support of your review.

Our team will test the client's security protections and investigate any areas that need attention. We will explain the results and provide practical guidance on any changes we recommend.

Once testing is complete, we will provide the client with a written report explaining what we tested and what we found. The client can share that report with you. Please contact us using the details below if you would like to verify this engagement.

Sincerely,

Daniel Brooks

Daniel Brooks

Authorized Representative

Trespass Security LLC

TRESPASS SECURITY LLC

304 S. Jones Blvd, Suite 1254
Las Vegas, NV 89107

trespasssec.com

hello@trespasssec.com
(775) 278-2244

Executive Summary

Fishing Rods LLC engaged Trespass Security to independently evaluate the protections supporting its operations and information. The purpose was to provide a clear view of the security measures in place and identify where further attention would strengthen them.

Together, the client and Trespass Security identified the systems and services relevant to the business relationship and agreed on the testing scope. The client's knowledge of its operations helped focus the work on the areas that mattered to the request.

Within that scope, Trespass Security combined automated testing with hands-on investigation to examine potential routes to unauthorized access. Potential issues were investigated and validated before being presented to the client, with supporting detail to guide its response.

The client used the results to make security improvements. Trespass Security then retested the affected services to verify the changes and confirm closure of the reported findings.

Taken together, the testing and verified improvements provide a basis for confidence in the protections examined. This conclusion relates to the assessed systems and their role in the business relationship at the completion of the engagement.

ASSESSMENT CONCLUSION

No significant security issues identified in the final assessment.

Evan Reed

Evan Reed

Security Assessor

Trespass Security

Assessment Scope

Testing examined the target below from outside the client's network. The assessment covered TCP ports 1–65,535 and the services discovered on those ports.

ASSESSMENT PERIOD**1–9 September 2026****ACCESS PROVIDED****No credentials or internal access**

Systems Included

HOSTNAME	IP ADDRESS	TCP PORTS
www.fishingrods.example	23.227.38.74	1–65,535

Testing Coverage

Discovery checked the full TCP port range for exposed services. Follow-up testing examined service configuration, encrypted connections, and network access controls where applicable.

Scope Boundaries

Coverage was limited to the listed target. Other hosts and IP addresses, UDP services, application functionality, internal systems, and source code were excluded. Shared hosting did not extend the scope to other customers or provider infrastructure.

Results describe the assessed target during the testing period.

Testing Approach

The work progressed from service discovery to hands-on examination and follow-up testing. Automated results were reviewed before being used to support a finding.

01 Service Discovery

The team checked TCP ports 1–65,535 on the scoped target and identified the services reachable from the testing location. These services formed the basis for further examination.

02 Hands-on Examination

The team checked service configurations, encrypted connections, and access restrictions. Potential issues were examined directly to establish what they meant for the client.

03 Follow-up Verification

After the client made changes, the affected services were tested again. The final assessment reflects those checks and the status of the items reviewed.

METHODOLOGY REFERENCE

The approach was informed by NIST SP 800–115, Technical Guide to Information Security Testing and Assessment. Procedures were selected to suit the external network scope.

Findings Summary

Testing identified one low-severity configuration finding. The client addressed it, and Trespass Security confirmed the change through follow-up testing.

Final Status

FINDING	IDENTIFIED	CLOSED	OPEN
NET-01 · Version disclosure	1	1	0

Follow-up Verification

The HTTPS responses were checked again after the configuration change. The version details were no longer present. The following page records the observation and verification.

ASSESSMENT CONCLUSION

All identified findings were resolved and their closure verified.

Finding status reflects the assessed target at the completion of follow-up testing.

Finding Detail

NET-01

Service Version Disclosure

SEVERITY	FINAL STATUS	AFFECTED SERVICE
Low	Closed	www.fishingrods.example · HTTPS

Observation

The HTTPS service returned software version information in its response headers. This information was not needed to deliver the site and could be read without signing in.

Practical Significance

Version details can help an external observer identify the software in use. The disclosure alone did not demonstrate unauthorized access or an exploitable condition.

Change Made

The service configuration was updated to omit unnecessary version details from public responses.

Verification

Trespass Security repeated the response-header checks after the change. The previously observed version information was no longer present in the responses examined, and the finding was closed.

Verify This Report

To confirm that this report was issued by Trespass Security, or to ask a question about the assessment, contact us using the details below.

EMAIL

hello@trespasssec.com

PHONE

(775) 278-2244

Please quote the job reference when contacting us.

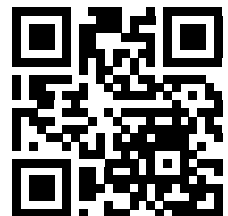
JOB REFERENCE

TS-JOB-2026-001

PREPARED FOR

Fishing Rods LLC

Trespass Security LLC

trespasssec.com[Visit our website](https://trespasssec.com)