



CASE STUDY

The Penetration Test That Paid for Itself within Three Weeks

A proactive web server assessment, a real attack, and a fast recovery.

CLIENT	Tech and Mech
INDUSTRY	IT development and support (web and cloud)
ENGAGEMENT	Web server penetration test and hardening
PROVIDER	Berkner Tech
OUTCOME	Recovered from a live denial-of-service attack with minimal downtime

PENETRATION TEST FINDINGS: 11 TOTAL



Context

Tech and Mech is an IT development and support firm that specializes in web and cloud architecture. Their work includes web development, technology audits, and SEO optimization. The business is growing quickly as they expand to larger enterprise clients.

Challenge

Tech and Mech understood that larger clients draw more attention from attackers, and that automation and AI have made it cheap to run attacks at scale. They wanted defenses in place early rather than after a problem.

Security testing is a specialized field of its own, separate from the development and cloud work the team does every day. Recognizing that, Tech and Mech made the proactive call to bring in a dedicated specialist. They engaged Berkner Tech to assess and harden their web server defenses as the business grew.

What Actually Happened

Berkner Tech delivered a complete penetration test of Tech and Mech's WordPress web server. The report documented 11 findings: 3 Critical, 4 High, 3 Medium, and 1 Low. Each finding included proof of the vulnerability, step-by-step instructions to reproduce it, and the exact commands to fix it.

Three weeks later, Tech and Mech was hit with a denial-of-service attack. One of the sites covered in the test was knocked offline and could not be restarted.

The team already had the report, so they knew what to do. They applied the firewall configuration from Berkner Tech's findings, brought the site back online, and closed the gaps the attack had targeted. The site recovered with minimal downtime and no visible impact on their customers.

The test had paid for itself within three weeks of delivery.

Why This Matters

Most teams commission a penetration test after an incident. Tech and Mech did it first, and the report was already in hand when the attack came. That is the difference between a fast recovery and an open-ended outage.

If you are deciding whether a penetration test is worth it, ask a simpler question: how much is a fast recovery worth the next time you are attacked?

Talk to Berkner Tech

Berkner Tech performs web server and cloud penetration testing with clear, reproducible findings and exact remediation steps.

Learn more: berkner.tech

[Schedule a call](#)