SysGroup

CASE STUDY

UK-based Charity Customer

Introduction

01

Company Overview

SysGroup is a trusted provider of penetration testing, cyber maturity assessments, and compliance solutions. We empower organizations to secure their infrastructure, reduce risk exposure, and build long-term cyber resilience.

Client Background

Our client, a UK-based charity, supports critical services for communities across the country. With an increasing reliance on digital infrastructure and websites to deliver services, the charity recognized the importance of proactively testing its security posture to protect sensitive data and maintain stakeholder confidence.

Challenges

02

Initial Situation

The charity required an independent review of its **external infrastructure and public-facing websites** to identify vulnerabilities that could be exploited by malicious actors. No prior penetration testing had been conducted recently, meaning potential risks could have remained undetected.

Objectives

- Simulate the perspective of an external attacker using black-box testing.
- Identify exploitable vulnerabilities across servers, websites, and services.
- Provide clear remediation recommendations to strengthen defenses.

Solution

03

Approach

SysGroup performed a **three-day black-box penetration test** of the charity's external IP addresses and websites. The test mimicked real-world attack scenarios, combining automated and manual techniques aligned to OWASP standards and industry best practices.

Implementation

- Conducted reconnaissance, port scanning, and vulnerability analysis across 7 IPs and multiple web applications.
- Verified findings to eliminate false positives, focusing on vulnerabilities with real-world exploit potential.
- Delivered a **comprehensive technical report** outlining each vulnerability, its risk rating, evidence, and prioritized remediation recommendations.

Results

04

Outcomes

- Identified one **medium-risk issue:** an outdated version of OpenSSH on one host, requiring verification of patch backporting or upgrade.
- Exposed **low-risk findings** including accessible administrative interfaces, third-party hosted scripts without integrity checks, misconfigured HTTP headers, and weak cipher suites.
- Highlighted a **best practice gap** where website CMS versions were visible, increasing the risk of targeted exploits.

Benefits

- Enabled the charity to **understand its external attack surface** and address vulnerabilities before they could be exploited.
- Delivered **actionable recommendations,** such as restricting admin panel access, disabling CBC ciphers, and enforcing HSTS headers.
- Increased awareness of the need for **ongoing penetration testing and proactive patch management.**
- Provided assurance to trustees, partners, and donors that the charity is committed to safeguarding sensitive systems and data.

Conclusion

05

Summary

SysGroup successfully conducted an external penetration test for the charity, simulating real-world attacker behavior to uncover vulnerabilities. The engagement delivered clear, prioritized remediation guidance that significantly improved the charity's cyber resilience.

Future Plans

To maintain robust security, the charity plans to conduct r**egular penetration tests,** implement **continuous patching and monitoring processes,** and adopt **security best practices** across its digital infrastructure. SysGroup will continue to support with proactive testing, advisory services, and compliance guidance.