PENETRATION TESTING SERVICES BRIEF

Real Threats. Real Testing. Real Results.

SPECIALIZED S|3 SECURITY SERVICES

PENETRATION TESTING SERVICES

Test Like an Attacker. Defend Like a Leader.

Cyber threats don't wait—and neither should your defenses. Penetration testing helps validate your ability to withstand real-world attacks before they impact operations, reputation, or revenue. At Specialized Security Services, Inc. (S3 Security), we simulate adversary behavior to expose exploitable gaps across networks, applications, and cloud environments, delivering clarity and control in the face of uncertainty.

Whether you're working toward compliance, validating controls, or proactively strengthening defenses, our penetration testing delivers results that are accurate, actionable, and defensible.

EXPERTISE YOU CAN TRUST

With over 25 years of experience, our team of certified ethical hackers and seasoned engineers has led thousands of successful engagements across regulated and high-risk industries. We follow proven methodologies from NIST, OWASP, PTES, and PCI guidance to deliver reliable, repeatable results. Our goal isn't just to identify vulnerabilities, but to help you understand and address them.

TAILORED TO YOUR BUSINESS

No two environments are the same. Our penetration testing approach is designed around your infrastructure, goals, and compliance needs. Whether you operate on-premises, in the cloud, or across hybrid systems, we work closely with your team to deliver insights that are relevant, practical, and prioritized to your specific threat landscape.

SIMULATING THE ADVISARY

S3 Security's penetration testing goes far beyond scanning tools. We use a blend of manual and automated techniques to replicate how real attackers operate, revealing the risks that matter most. Our team models attacker behavior to test your organization's ability to detect, respond to, and recover from an intrusion.

Visibility leads to action. Action strengthens resilience.

CERTIFIED EXPERTS & PROVEN TOOLS

Leading organizations choose S3 Security for our real-world experience and advanced offensive security expertise. We don't just run tools. We apply them with strategic intent to uncover critical risks before they disrupt operations or reputation.

- **Offensive Security:** OSCP, OSWP, OSEP, OSWE, OSEE, AWAE
- **GIAC Certifications:** GPEN, GWAPT, GSEC, GCIH, GXPN
- **Other Industry Certifications:** CEH, CISSP, CompTIA, SANS Mobile Security, SANS Advanced Web Application Security, SANS HACKFEST

To deliver thorough and accurate assessments, we use a combination of industry-recognized frameworks and advanced toolsets.

FRAMEWORKS & METHODOLOGIES

We align our testing to standards appropriate for your environment:

- **Web & Mobile:** OWASP Top 10, OWASP WSTG, OWASP MASVS
- **Network:** PTES, MITRE ATT&CK, NIST SP 800-115
- **Compliance-Driven:** PCI DSS, ISO 27001, NIST CSF
- **Threat Modeling:** STRIDE, PASTA, CWE Analysis

TOOLS & PLATFORMS

- **Kali Linux Tools** – Full suite of penetration testing capabilities
- **Metasploit Framework** – Exploitation and post-exploitation testing
- **Burp Suite** – Web vulnerability scanning and interception proxy
- **Rapid7 Nexpose** – Vulnerability scanning and asset discovery
- **Tenable Nessus** – Comprehensive vulnerability assessment
- **Invicti** – Web application and vulnerability scanning
- **Qualys** – Vulnerability management
- **OWASP ZAP** – Open-source web application security scanner
- **Nuclei** – Fast and customizable vulnerability scanner
- **Custom Tools** – Internal debuggers, WebRTC fuzzers, CI/CD taint injection scripts

Attackers don't follow scripts and neither do we. Our hands-on testing approach reveals what automated scans miss so you can act on what matters most.

TECHNICAL CAPABILITIES

S3 Security delivers deep, real-world expertise across a wide range of offensive security disciplines. Our team blends manual and automated techniques to uncover complex vulnerabilities that impact operations, compliance, and reputation. Below are key areas of focus:

Application Security Testing

We assess web, desktop, and embedded applications using white-box and black-box methods. Our engineers have uncovered zero-day vulnerabilities in enterprise software, medical devices, and EDR/AV platforms, often developing proof-of-concept exploits to validate real-world impact. Areas of expertise include reverse engineering, source code review, and post-exploitation in environments built on Java, Go, Ruby, and Python.

Web Application Testing

We test complex web applications and APIs using OWASP WSTG and custom methodologies. Our testers have identified critical vulnerabilities including chained CSRF/XSS, unauthenticated SQL injection, and WAF bypasses. We combine automation with deep manual testing to uncover risks scanners miss.

Network Penetration Testing

Our team has achieved complete domain compromise in the majority of Active Directory engagements. We simulate real-world attacker behavior across internal and external networks, often pivoting from developer endpoints to cloud infrastructure. Focus areas include credential abuse, ADCS exploitation, and lateral movement using tools like Responder and CrackMapExec.

Mobile Application Testing

We test Android and iOS apps using both static and dynamic analysis. Findings have included insecure credential storage, obfuscation bypass, and critical backend API flaws. Tools include Frida, MobSF, and rooted devices to mirror adversary techniques.

Large Language Model (LLM) Security

S3 Security has tested proprietary and public LLMs for prompt injection and misconfiguration issues. We've contributed to client LLM security initiatives and successfully bypassed controls in ChatGPT-backed and custom-engineered models.

Advanced testing. Actionable outcomes.

OUR PENETRATION TESTING METHODOLOGY

Our penetration testing methodology mirrors the behavior of real-world attackers to expose hidden weaknesses before they're exploited. Every step is built for accuracy, control, and business impact so your organization can identify risk and respond with confidence.

1

Planning

We begin by defining your organization's goals, scope, systems in scope, and testing constraints. Rules of engagement are established, and open-source intelligence is gathered to identify potential entry points across your internal and external environments.

2

Discovery (Reconnaissance)

Our team conducts detailed enumeration across applications, APIs, wireless signals, and network infrastructure. We perform both automated and manual scanning to uncover misconfigurations, vulnerabilities, and potential points of exploitation.

3

Attack

We validate findings by attempting safe, controlled exploitation using methods such as SQL injection, cross-site scripting (XSS), credential attacks, and privilege escalation. Where possible, we simulate attacker movement and data exfiltration to measure true impact.

4

Persistence & Lateral Movement

After initial compromise, we test how well your environment resists deeper access. This includes modeling Advanced Persistent Threat (APT) behavior to assess lateral movement and long-term access risks. At the end of this phase, we remove all artifacts and restore the environment.

5

Analysis & Reporting

We provide a comprehensive report detailing confirmed vulnerabilities, exploit paths, and areas of strength. Our recommendations are prioritized by business impact and mapped to your risk landscape, enabling informed decision-making and targeted remediation.

Test with purpose. Defend with confidence.

MEASURING WHAT MATTERS

What Constitutes a Compromise?

A compromise is more than a technical issue. It is a threat to your operations, data, and reputation. At S3 Security, we define compromise as either gaining unauthorized access to a system or successfully extracting sensitive data. Our testing reveals how those breaches could occur so your team can prevent them.

Risk Severity Ratings

We rank all findings by severity so your team can prioritize what to fix first. Our scoring aligns with industry standards and combines CVSS and OWASP models to give you a consistent, defensible view of risk.

Risk Level	NVD CVSS v3	OWASP Score	Definition
Critical	9.0–10.0	9.0–10.0	Immediate, system-wide risk with potential for full compromise and data loss. Often systemic in nature.
High	7.0–8.9	6.0–8.9	Serious vulnerabilities that may lead to sensitive data exposure or administrative access.
Medium	4.0–6.9	3.0–5.9	Issues that require chaining or elevated privileges to exploit, with moderate business impact.
Low	0.1–3.9	0.1–2.9	Minimal impact vulnerabilities unlikely to result in significant harm.
Informational	0.0	0.0	No direct risk, but useful for awareness and best practices.

Know the impact. Prioritize what matters.

Our reports prioritize what matters most. Each finding includes context, impact, and clear remediation guidance so your team can act quickly and effectively.

A BETTER TESTING EXPERIENCE

At S3 Security, we understand that how testing is managed impacts everything from clarity to confidence. That's why we provide a dedicated engagement team focused on keeping your project on track and your leadership informed at every step.

What You Can Expect:

- A dedicated Client Administrator (CA) to oversee the engagement
- Clear communication & scheduling from kickoff to closeout
- Defined timelines & deliverables
- Guidance on data collection & pre-engagement requirements
- Proactive status updates & milestone tracking

From agenda calls to report delivery, every step is designed to ensure a smooth, transparent, and high-quality experience.

BUILT-IN QUALITY ASSURANCE

Our quality process ensures every report is not just technically accurate, but also clear, defensible, and ready for executive audiences and auditors alike.

S3 Security QA Process:

- **Engineering QA** – Validation by Engineering Principal
- **VP Review** – Review for completeness and content structure
- **Executive Review** – Final approval by EVP/CTO
- **Delivery QA** – Final check by Business Operations prior to presentation

Every report we deliver is designed to meet the highest standard: it must be accurate, defensible, and actionable.

WHAT TO EXPECT DURING YOUR PENETRATION TESTING ENGAGEMENT

Successful testing depends on more than technical skill. It requires a structured process that delivers clarity, consistency, and accountability. Each phase of our engagement is led by a specialized role to keep your project on track and your team aligned.

Pre-Engagement
Lead by the Client Administrator

- Identify key stakeholders and confirm business objectives
- Schedule agenda and recurring status calls
- Distribute and collect required documentation, including pre-engagement questionnaires and network diagrams
- Confirm technical scope and communication preferences
- Validate testing rules of engagement and logistics

Service Execution
Lead by Cybersecurity Engineers

- Perform reconnaissance and map attack paths
- Execute manual and automated testing based on defined scope
- Attempt exploitation using approved techniques and adhere to agreed-upon rules of engagement

Reporting
Lead by Engineering Team & Executive Leadership

- Draft detailed findings, screenshots, and remediation guidance
- Identify PCI-impacted findings if applicable
- Undergo multi-step internal QA review
- Present final report and recommendations to stakeholders alongside S3 Security Executive Leadership

Project Management & Strategic Oversight

Every step in our process is built to reduce disruption, increase visibility, and ensure clear next steps. You'll always know what's happening, who's accountable, and what's coming next.

Clear roles. Smooth execution. Strong results.

PENETRATION TESTING REPORT SAMPLES

Summary of Findings

Specialized Security Services, Inc. has determined that [redacted] has received a **Compromised** rating for this penetration testing engagement.

Scoped Environment	Compromised Status	Notable Vulnerabilities
External	COMPROMISED	YES
Internal	COMPROMISED	YES

As a result of the testing, Specialized Security Services, Inc. discovered critical vulnerabilities on external and internal assets, compromised an external webserver and numerous hosts in the internal environment and obtained administrative credentials to [redacted] Active Directory (AD) environment during [redacted] penetration testing engagement.

The following compromises consisted of the listed types of exploits:

- SQL Injection
- Running commands on a target system
- Default Credentials on Exposed Internet Applications
- Credential Theft
- Escalation of privileges
- Account Takeover
- Remote Code Execution
- Sensitive Data Exposure
- Lack of MFA Enforcement

Compromised Findings

The following table outlines the compromised exploits and vulnerabilities with exploitable modules identified during this penetration testing engagement.

Scoped Environment	Critical	High	Medium	Low
External	**1**	**0**	**0**	**0**
Internal	**6**	**10**	**1**	**0**

The following table provides a summary of the identified compromised exploits and vulnerabilities with exploitable modules. Full details for each can be found in the scope-specific breakdown of findings.

Severity	Environment	Finding Title
CRITICAL	EXTERNAL	Blind & Union-Based SQL Injection
CRITICAL	INTERNAL	Active Directory Certificate Services (ADCS) Certificate Authority Vulnerable to ESC8
CRITICAL	INTERNAL	Systems Vulnerable to MS17-010 (ETERNALBLUE)
CRITICAL	INTERNAL	Systems Vulnerable to Microsoft RDP Remote Code Execution (CVE-2019-0708) (BlueKeep)
CRITICAL	INTERNAL	Systems Vulnerable to SMBv2 Negotiation Remote Code Execution (CVE-2009-3103)
CRITICAL	INTERNAL	Apache Tomcat Using Default Credentials

PENETRATION TESTING REPORT SAMPLES

Notable Vulnerabilities

Specialized Security Services, Inc. has identified the following Notable Vulnerabilities. Significant critical and high vulnerabilities discovered and not compromised during testing are summarized below for this penetration testing engagement.

The following Notable Vulnerabilities consisted of the listed types of vulnerabilities:

- Management Protocols and Administrative Interface Exposed to the Internet
- Out of Date Software
- Misconfigured User and Admin User Accounts
- Unsupported Operating Systems
- SMB Misconfigurations

The following table outlines the identified Notable Vulnerabilities.

Scoped Environment	Critical	High	Medium	Low
External	**0**	**3**	**3**	**1**
Internal	**0**	**2**	**3**	**0**

The following table provides a summary of the identified Notable Vulnerabilities. Full details for each can be found in the scope-specific breakdown of findings.

Severity	Environment	Finding Title
HIGH	EXTERNAL	PhpMyAdmin Panel Exposed to the Internet
HIGH	EXTERNAL	Management Protocols Exposed to the Internet
HIGH	EXTERNAL	Out of Date Software

PENETRATION TESTING REPORT SAMPLES

The following table describes how S3 Security targeted assets in scope, step by step:

Step	Action	Recommendation
1	Performed TCP and UDP scans of in-scope external targets.	[redacted] should review log sources to identify this enumeration activity.
2	Identified SQL injection and XSS vulnerabilities on in scope external targets. S3 Security exploited the SQL injection vulnerability to dump data from the database.	[redacted] should ensure that all user input is being sanitized by the applications to ensure that malicious input is not being processed by the application.
3	Performed automated vulnerability scanning of in-scope external assets to identify known vulnerabilities and HTTP misconfigurations.	[redacted] should review log sources to identify this enumeration activity.
4	Reconnaissance tasks were performed using automated tools and manual validation checks within the [redacted] environments to gain an understanding of potential weaknesses and vulnerabilities. During the engagement, the engineer assessed in-scope systems using various scanning tools, such as Nexpose, NMAP, Burp Suite Pro and manual exploitation tools and scripts. The engineer also validated crafted usernames against the Domain Controller to identify valid users.	[redacted] should review log sources to identify this enumeration activity.
5	Performed a kerberoasting attack and obtained the hashes for 4 user accounts. The engineer cracked two of the hashes and obtained plaintext credentials for those accounts.	Remove SPNs from users if they are unnecessary and consider using group managed service accounts and complex passwords if SPNs are required. Additionally, users with SPNs should have limited domain privileges to prevent abuse if compromised.
6	Executed BloodHound to obtain AD information including users, groups, GPOs, computers, and ACLs to search for misconfigurations. Identified that the [redacted]com\[redacted] account had local administrator rights to 15 servers.	[redacted] should review log sources to identify this enumeration activity.
7	Enumerated ADCS systems for misconfigurations that could be abused to elevate privileges in the domain using certipy. The engineer did not identify any enabled Certificate Authorities in the [redacted] environment.	[redacted] should review log sources to identify this enumeration activity.
8	Dumped the SAM registry hive on multiple SQL servers that [redacted]com\[redacted] had local administrator rights over.	[redacted] should review security alerts and log sources to identify credential dumping activity on systems in the environment.
9	Performed a password spray using the local Administrator credentials against the [redacted] and [redacted] networks to identify reused local Administrator credentials.	[redacted] should review security alerts and log sources to identify password spray activity as this could be a precursor to follow on attacks.

PENETRATION TESTING REPORT SAMPLES

External Penetration Test Findings

Blind & Union-Based SQL Injection – CRITICAL

Classification Type:	**COMPROMISE**
Description:	S3 Security discovered a Blind and Union-based SQL Injection vulnerability on the 'City' parameter in the [redacted] request for [redacted]com.
Severity:	Critical
System(s):	• [redacted]com[redacted]
Recommendations:	[redacted] should ensure that user input is sanitized prior to processing it in backend database queries. [redacted] should consider using prepared statements in addition to sanitizing user input to prevent SQL injection vulnerabilities.
References:	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
Exploitation Proof of Concept:	

Figure 13 shows the backend database's version number in the response to a malicious request containing a union-based SQL injection query, Figure 14 shows the current database user, and Figure 15 shows an external DNS interaction.

[redacted]

Figure 13: SQL injection vul

PHPMyAdmin Exposed to the Internet – HIGH

Classification Type:	**NOTABLE FINDING**
Description:	S3 Security discovered that the PHPMyAdmin service was exposed to the Internet and did not restrict access to authorized parties only. S3 Security performed a default credential check to determine if default credentials were used by the application but was unsuccessful. However, an attacker with enough time can perform a brute force attack against the service to discover the root credentials and authenticate to the application.
Severity:	High
System(s):	[redacted]
Recommendations:	[redacted] should ensure that sensitive applications like PHPMyAdmin use a firewall to control access to the panel to prevent unauthorized access and possible compromise of the system.
References:	
Exploitation Proof of Concept:	

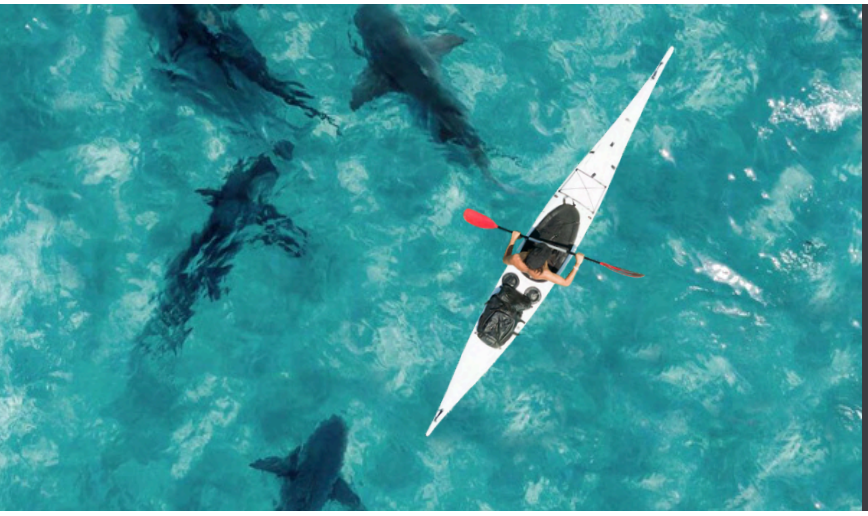
S3 Security engineers discovered that [redacted] exposed the PHPMyAdmin panel to the Internet as shown in Figure 41 below.

[redacted]

Figure 41: PHPMyAdmin panel exposed to the Internet

The panel was not using default credentials, however the password chosen could be determined via a brute force attack against the panel. S3 Security engineers identified the plaintext password using the SQL injection vulnerability and authenticated to PHPMyAdmin as shown in Figure 42 below.

YOUR CYBERSECURITY PARTNER



S|3 SPECIALIZED SECURITY SERVICES

FLOAT ON

Cybersecurity and compliance to ward off any threat.

Wherever You Are in Your Cybersecurity Journey—We're With You

Whether you're preparing for your first penetration test or optimizing a mature security program, S3 Security is here to help. We bring clarity to complexity, and peace of mind to decision-makers.

Our mission is to strengthen your resilience, protect your reputation, and drive long-term success through security strategies aligned with your business goals.

With over 25 years of experience helping clients stay secure amid evolving threats and regulatory demands, S3 Security is your trusted partner for offensive testing, risk visibility, and strategic guidance.

CONTACT US

SPECIALIZED SECURITY SERVICES, INC.
4975 Preston Park Blvd., Suite 510
Plano, TX 75093
972-378-5554 | info@s3security.com
www.s3security.com