ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

External Audit Services and **Web Application Audit** Services *(Hacking Ético)*

OVERVIEW

SMEs face a series of complex challenges, spurred by a tremendously agile and constantly evolving market. From economic uncertainty to fierce competition, SMEs must adapt to changing trends and the rapid evolution of technology, staying updated and flexible to ensure the relevance of their products and services. Digitalization is also highlighting the growth of the attack surface, thereby increasing the likelihood of experiencing a cyber incident and the potential consequences it can have for their survival.

KEY FIGURES

- **83% of SMEs** are **not prepared** to respond to a cyber attack.
- **30% of SMEs** fear **phishing** as one of their main cyber threats.
- **91% of SMEs** still do **not** have **cyber liability insurance.**

SOLUTIONS

We deeply understand the needs of SMEs and strive to meet them by designing, implementing, maintaining, and operating comprehensive security plans based on the six functions of NIST (Governance, Identification, Protection, Detection, Response, and Recovery). Within them, our External Audit service will allow you to understand your exposure perimeter, acquiring a clear picture of your exposed vulnerabilities and how to address them.

Phase 1: Footprint (OSINT)

During the first phase of the service, the Zerolynx team will map the attack surface exposed to the Internet. For this task, open and private sources will be consulted with the aim of conducting Footprinting processes to search for all kinds of sensitive information that currently exists or may have been published in the past on the Internet. For this task, different techniques based on OSINT methodologies will be used, with special emphasis on:

- Hacking with search engines (Google, Bing, Yandex, Exalead, Duckduckgo, and Baidu).
- Asset search services (Shodan, Censys, Greynoise, Zoomeye, Fofa, Onyphe, Binayedge, Wigle, and Oshadan).
- Threat Intelligence search services (RiskIQ, Cisco Talos Intelligence, ThreatExchange, VirusTotal).
- Asset enumeration on paste websites (Pastebin, Pasteguru, TextSnip, Snip.Net, Hastebin, Anonpaste, etc.).
- Crawling tools and massive content analysis on the Internet.
- Whois records lookup.
- Mobile app stores (AppStore, PlayStore, etc.).
- Analysis of IP addresses and domains (Robtex, Ipv4info, ThreatCrowd, MxToolBox, IPStack, DB-IP, Ultratools).
- Public code repositories (github, gitlab, bitbucket, etc.).
- Password leaks published on the Internet and the Dark Web.
- Study of visually similar possible domains (Typosquatting), using custom scripts and online technologies.
- Analysis of old websites published on Archive.org.
- Tracking of applications on social networks (Twitter, Facebook, Instagram, and LinkedIn, among others).
- Analysis of possible sites that, while potentially legitimate, have been classified as phishing on platforms like OpenPhish, PhisTank, or PhisStats.
- Location of data sold in underground Internet markets.

ABOUT ZEROLYNX

European Cybersecurity and Intelligence Provider.
Global Top 100 Providers ranked 2023.

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY™ MADE IN EUROPE

Phase 2: Fingerprinting

Once the initial information for each application/service has been gathered, the Fingerprinting process will begin, involving an in-depth analysis of assets for subsequent exploitation. To create a comprehensive map of the attack surface, all exposed ports and services will be enumerated, with a focus on identifying the following elements:

- Ports and services accessible from the Internet.
- Software and version used in each service.
- Technologies used, especially those outdated or with known vulnerabilities.
- External libraries used and other relationships between different assets.

Simultaneously, an active search for potential exploitation vectors valid for subsequent stages of the process will be executed. Special emphasis will be placed on detecting functionalities that typically pose a higher risk of being exploited to compromise the perimeter, whether through vulnerabilities, code injections, uploading of malicious files, or even brute force attacks or previously leaked credentials. Some of the functionalities that will receive special attention include:

- Web authentication panels.
- File upload forms.
- File exchange services.
- Remote access technologies for administration.
- Remote desktop technologies.
- VPN connections.

Therefore, for the MITRE ATT&CK attack matrix purposes, the search for elements facilitating access through the following Initial Access techniques is considered:

- Exploit Public-Facing Application (T1190).
- External Remote Services (T1133).
- Valid Accounts (T1078.001, T1078.002, T1078.003, T1078.003).

The rest of the attack vectors, including compromise of third parties or physical access, would initially be beyond the scope of the project.

Phase 3: Vulnerability Analysis

The following phase utilizes all the previously gathered information as a foundation for detecting potential attack vectors. These will be prioritized based on exploitability and potential impact, aiming to maximize focus on finding the most critical vulnerabilities, such as data exfiltration or remote code execution.

This phase, in any case, covers the majority of the security audit and allows for the identification of vulnerabilities related to identity management, authentication, authorization, or session management. Special attention is also given to injections through input validation tests. Finally, it enables the discovery of error management flaws, incorrectly implemented cryptographic methods, and vulnerabilities in business logic. Broadly speaking, the active OWASP testing categories at the time of the review will also be covered.

- Information Gathering
- Configuration and Deployment Management
- Identity Management and Session Management
- Authentication and Authorization
- Input Validation and Error Handling
- Weak Cryptography
- Business Logic and Client-Side

In the event that the discovered vulnerabilities allow for particularly harmful scenarios, such as remote code execution or privilege escalation, prior communication will be conducted with the security audit management stakeholders to decide whether to proceed with proof-of-concept testing or halt the tests without exploitation. In either case, vulnerabilities of critical impact will be immediately reported to the client to minimize the time during which such a potential breach remains active.

Phase 4: Results Analysis

In the event of detecting high-impact vulnerabilities reported during the service, the client may raise questions or request additional tests to clarify such weaknesses, for example, if a countermeasure or solution is deployed during the project timeline. However, it's important to understand that under no circumstances can the conduct of additional tests impact the project planning, consuming the days dedicated to the completion of the final report, unless both Zerolynx and the client agree to such a situation beforehand. In any case, Zerolynx offers the client the possibility to contract additional days for vulnerability analysis and retesting if necessary.

External Audit Services and **Web Application Audit** Services *(Hacking Ético)*

Final Report

By consolidating all the evidence obtained, a comprehensive technical and executive report will be constructed according to the Zerolynx model, and it will include, at a minimum, the following points:

- Audit Object and Scope
- Audited Systems
- Audit Team
- Interlocutors involved in the audit
- Dates of testing
- Reference documentation
- Confidentiality clause
- Detected vulnerabilities, classified according to their importance
- Recommended solutions for vulnerabilities
- Vulnerabilities addressed during the audit
- Observations
- Strengths and areas for improvement
- Conclusions reached

The report will feature an Executive Summary, highlighting the main risks detected and prioritized recommendations for potential resolution. Below are examples of an executive summary and vulnerability cards used by Zerolynx. However, the information in the report and vulnerabilities can be tailored to the needs and requirements of the client if necessary.

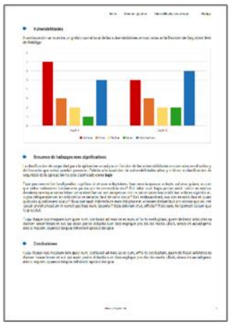
Título del Documento

Subtítulo del Documento

Cliente

XX/XX/2021

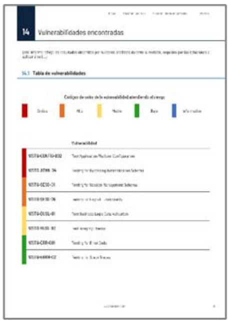
ZEROLYNX



Vulnerabilidades

Resumen de hallazgos más significativos

Conclusiones



14 Vulnerabilidades encontradas

14.1 Tabla de vulnerabilidades

Código de colores de la vulnerabilidad atendiendo al riesgo

Vulnerabilidad

Nombre de la vulnerabilidad

Estado actual

Controles

Activos Afectados

Descripción

Additionally, Zerolynx provides the client with a high-level presentation at the end of the project documenting the main findings and remediations.