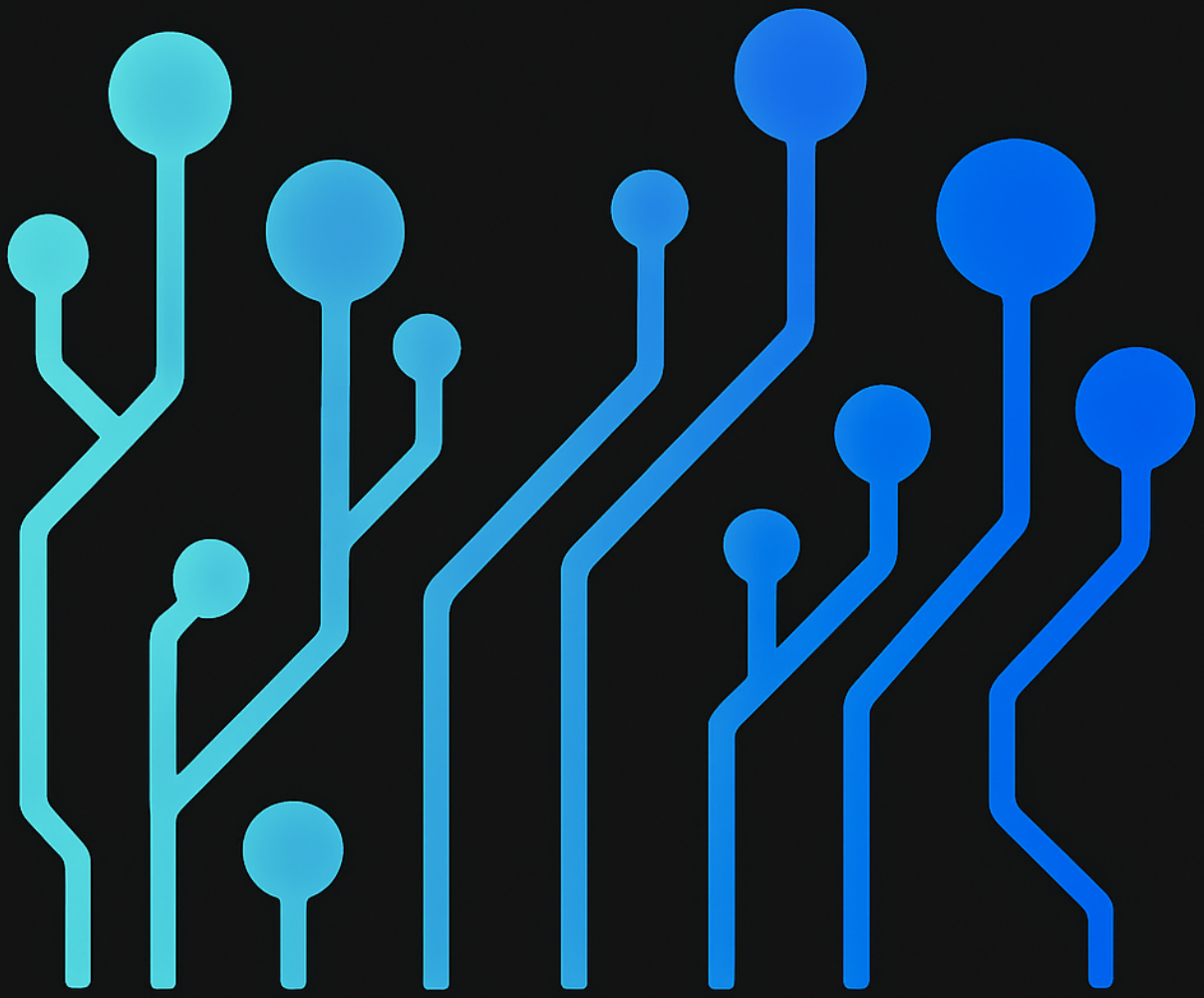
Vulnerability Test Report

InLighn Tech
Experience, Learn, Thrive



- **Test Report : -**

Unified Security Report

Trivy Findings:

ID/Package	Severity	Description/Title
CVE-2024-28085	MEDIUM	util-linux: CVE-2024-28085: wall: escape sequence injection
CVE-2023-4039	LOW	gcc: -fstack-protector fails to guard dynamic stack allocations on ARM64
CVE-2024-28085	MEDIUM	util-linux: CVE-2024-28085: wall: escape sequence injection
CVE-2023-4911	HIGH	glibc: buffer overflow in ld.so leading to privilege escalation
CVE-2023-6246	HIGH	glibc: heap-based buffer overflow in __vsyslog_internal()
CVE-2023-6779	HIGH	glibc: off-by-one heap-based buffer overflow in __vsyslog_internal()
CVE-2024-2961	HIGH	glibc: Out of bounds write in iconv may lead to remote code execution
CVE-2024-33599	HIGH	glibc: stack-based buffer overflow in netgroup cache
CVE-2023-4527	MEDIUM	glibc: Stack read overflow in getaddrinfo in no-aaaa mode
CVE-2023-4806	MEDIUM	glibc: potential use-after-free in getaddrinfo()
CVE-2023-6780	MEDIUM	glibc: integer overflow in __vsyslog_internal()
CVE-2024-33600	MEDIUM	glibc: null pointer dereferences after failed netgroup cache insertion
CVE-2024-33601	MEDIUM	glibc: netgroup cache may terminate daemon on memory allocation failure
CVE-2024-33602	MEDIUM	glibc: netgroup cache assumes NSS callback uses in-buffer strings
CVE-2025-0395	MEDIUM	glibc: buffer overflow in the GNU C Library's assert()
CVE-2023-4911	HIGH	glibc: buffer overflow in ld.so leading to privilege escalation
CVE-2023-6246	HIGH	glibc: heap-based buffer overflow in __vsyslog_internal()
CVE-2023-6779	HIGH	glibc: off-by-one heap-based buffer overflow in __vsyslog_internal()
CVE-2024-2961	HIGH	glibc: Out of bounds write in iconv may lead to remote code execution
CVE-2024-33599	HIGH	glibc: stack-based buffer overflow in netgroup cache
CVE-2023-4527	MEDIUM	glibc: Stack read overflow in getaddrinfo in no-aaaa mode
CVE-2023-4806	MEDIUM	glibc: potential use-after-free in getaddrinfo()
CVE-2023-6780	MEDIUM	glibc: integer overflow in __vsyslog_internal()
CVE-2024-33600	MEDIUM	glibc: null pointer dereferences after failed netgroup cache insertion
CVE-2024-33601	MEDIUM	glibc: netgroup cache may terminate daemon on memory allocation failure
CVE-2024-33602	MEDIUM	glibc: netgroup cache assumes NSS callback uses in-buffer strings
CVE-2025-0395	MEDIUM	glibc: buffer overflow in the GNU C Library's assert()
CVE-2025-1390	MEDIUM	libcap: pam_cap: Fix potential configuration parsing error
CVE-2024-45491	CRITICAL	libexpat: Integer Overflow or Wraparound
CVE-2024-45492	CRITICAL	libexpat: integer overflow
CVE-2024-45490	HIGH	libexpat: Negative Length Parsing Vulnerability in libexpat
CVE-2023-4039	LOW	gcc: -fstack-protector fails to guard dynamic stack allocations on ARM64

CVE-2024-0553	HIGH	gnutls: incomplete fix for CVE-2023-5981
CVE-2024-0567	HIGH	gnutls: rejects certificate chain with distributed trust
CVE-2025-32988	HIGH	gnutls: Vulnerability in GnuTLS otherName SAN export
CVE-2025-32990	HIGH	gnutls: Vulnerability in GnuTLS certtool template parsing
CVE-2023-5981	MEDIUM	gnutls: timing side-channel in the RSA-PSK authentication
CVE-2024-12243	MEDIUM	gnutls: GnuTLS Impacted by Inefficient DER Decoding in libtasn1 Leading to Remote DoS
CVE-2024-28834	MEDIUM	gnutls: vulnerable to Minerva side-channel information leak
CVE-2024-28835	MEDIUM	gnutls: potential crash during chain building/verification
CVE-2025-32989	MEDIUM	gnutls: Vulnerability in GnuTLS SCT extension parsing
CVE-2025-6395	MEDIUM	gnutls: NULL pointer dereference in _gnutls_figure_common_ciphersuite()
CVE-2024-37371	CRITICAL	krb5: GSS message token handling
CVE-2024-37370	HIGH	krb5: GSS message token handling
CVE-2023-36054	MEDIUM	krb5: Denial of service through freeing uninitialized pointer
CVE-2024-26462	MEDIUM	krb5: Memory leak at /krb5/src/kdc/ndr.c
CVE-2025-24528	MEDIUM	krb5: overflow when calculating ulog block size
CVE-2024-37371	CRITICAL	krb5: GSS message token handling
CVE-2024-37370	HIGH	krb5: GSS message token handling
CVE-2023-36054	MEDIUM	krb5: Denial of service through freeing uninitialized pointer
CVE-2024-26462	MEDIUM	krb5: Memory leak at /krb5/src/kdc/ndr.c
CVE-2025-24528	MEDIUM	krb5: overflow when calculating ulog block size
CVE-2024-37371	CRITICAL	krb5: GSS message token handling
CVE-2024-37370	HIGH	krb5: GSS message token handling
CVE-2023-36054	MEDIUM	krb5: Denial of service through freeing uninitialized pointer
CVE-2024-26462	MEDIUM	krb5: Memory leak at /krb5/src/kdc/ndr.c
CVE-2025-24528	MEDIUM	krb5: overflow when calculating ulog block size
CVE-2024-37371	CRITICAL	krb5: GSS message token handling
CVE-2024-37370	HIGH	krb5: GSS message token handling
CVE-2023-36054	MEDIUM	krb5: Denial of service through freeing uninitialized pointer
CVE-2024-26462	MEDIUM	krb5: Memory leak at /krb5/src/kdc/ndr.c
CVE-2025-24528	MEDIUM	krb5: overflow when calculating ulog block size
CVE-2025-31115	HIGH	xz: XZ has a heap-use-after-free bug in threaded .xz decoder
CVE-2024-28085	MEDIUM	util-linux: CVE-2024-28085: wall: escape sequence injection
CVE-2024-28085	MEDIUM	util-linux: CVE-2024-28085: wall: escape sequence injection
CVE-2023-7104	HIGH	sqlite: heap-buffer-overflow at sessionfuzz
CVE-2023-5363	HIGH	openssl: Incorrect cipher key and IV length processing
CVE-2024-6119	HIGH	openssl: Possible denial of service in X.509 name checks
CVE-2023-2975	MEDIUM	openssl: AES-SIV cipher implementation contains a bug that causes it to ignore empty associate
CVE-2023-3446	MEDIUM	openssl: Excessive time spent checking DH keys and parameters

CVE-2023-3817	MEDIUM	OpenSSL: Excessive time spent checking DH q parameter value
CVE-2023-5678	MEDIUM	openssl: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH key
CVE-2023-6129	MEDIUM	openssl: POLY1305 MAC implementation corrupts vector registers on PowerPC
CVE-2023-6237	MEDIUM	openssl: Excessive time spent checking invalid RSA public keys
CVE-2024-0727	MEDIUM	openssl: denial of service via null dereference
CVE-2024-13176	MEDIUM	openssl: Timing side-channel in ECDSA signature computation
CVE-2024-4603	MEDIUM	openssl: Excessive time spent checking DSA keys and parameters
CVE-2024-4741	MEDIUM	openssl: Use After Free with SSL_free_buffers
CVE-2024-5535	MEDIUM	openssl: SSL_select_next_proto buffer overread
CVE-2024-2511	LOW	openssl: Unbounded memory growth with session handling in TLSv1.3
CVE-2024-9143	LOW	openssl: Low-level invalid GF(2^m) parameters lead to OOB memory access
CVE-2023-4039	LOW	gcc: -fstack-protector fails to guard dynamic stack allocations on ARM64
CVE-2023-50387	HIGH	bind9: KeyTrap - Extreme CPU consumption in DNSSEC validator
CVE-2023-50868	HIGH	bind9: Preparing an NSEC3 closest encloser proof can exhaust CPU resources
CVE-2023-7008	MEDIUM	systemd-resolved: Unsigned name response in signed zone is not refused when DNSSEC=yes
CVE-2025-4598	MEDIUM	systemd-coredump: race condition that allows a local attacker to crash a SUID program and gain
CVE-2024-12133	MEDIUM	libtasn1: Inefficient DER Decoding in libtasn1 Leading to Potential Remote DoS
CVE-2023-50387	HIGH	bind9: KeyTrap - Extreme CPU consumption in DNSSEC validator
CVE-2023-50868	HIGH	bind9: Preparing an NSEC3 closest encloser proof can exhaust CPU resources
CVE-2023-7008	MEDIUM	systemd-resolved: Unsigned name response in signed zone is not refused when DNSSEC=yes
CVE-2025-4598	MEDIUM	systemd-coredump: race condition that allows a local attacker to crash a SUID program and gain
CVE-2024-28085	MEDIUM	util-linux: CVE-2024-28085: wall: escape sequence injection
CVE-2023-4641	MEDIUM	shadow-utils: possible password leak during passwd(1) change
CVE-2023-29383	LOW	shadow: Improper input validation in shadow-utils package utility chfn
CVE-2024-28085	MEDIUM	util-linux: CVE-2024-28085: wall: escape sequence injection
CVE-2023-5363	HIGH	openssl: Incorrect cipher key and IV length processing
CVE-2024-6119	HIGH	openssl: Possible denial of service in X.509 name checks
CVE-2023-2975	MEDIUM	openssl: AES-SIV cipher implementation contains a bug that causes it to ignore empty associate
CVE-2023-3446	MEDIUM	openssl: Excessive time spent checking DH keys and parameters
CVE-2023-3817	MEDIUM	OpenSSL: Excessive time spent checking DH q parameter value
CVE-2023-5678	MEDIUM	openssl: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH key
CVE-2023-6129	MEDIUM	openssl: POLY1305 MAC implementation corrupts vector registers on PowerPC
CVE-2023-6237	MEDIUM	openssl: Excessive time spent checking invalid RSA public keys
CVE-2024-0727	MEDIUM	openssl: denial of service via null dereference
CVE-2024-13176	MEDIUM	openssl: Timing side-channel in ECDSA signature computation
CVE-2024-4603	MEDIUM	openssl: Excessive time spent checking DSA keys and parameters
CVE-2024-4741	MEDIUM	openssl: Use After Free with SSL_free_buffers
CVE-2024-5535	MEDIUM	openssl: SSL_select_next_proto buffer overread

CVE-2024-2511	LOW	openssl: Unbounded memory growth with session handling in TLSv1.3
CVE-2024-9143	LOW	openssl: Low-level invalid GF(2^m) parameters lead to OOB memory access
CVE-2023-4641	MEDIUM	shadow-utils: possible password leak during passwd(1) change
CVE-2023-29383	LOW	shadow: Improper input validation in shadow-utils package utility chfn
CVE-2023-47038	HIGH	perl: Write past buffer end via illegal user-defined Unicode property
CVE-2024-56406	HIGH	perl: Perl 5.34, 5.36, 5.38 and 5.40 are vulnerable to a heap buffer overflow when transliterating
CVE-2022-48303	LOW	tar: heap buffer overflow at from_header() in list.c via specially crafted checksum
CVE-2023-39804	LOW	tar: Incorrectly handled extension attributes in PAX archives can lead to a crash
CVE-2024-28085	MEDIUM	util-linux: CVE-2024-28085: wall: escape sequence injection
CVE-2024-28085	MEDIUM	util-linux: CVE-2024-28085: wall: escape sequence injection
CVE-2023-30861	HIGH	flask: Possible disclosure of permanent session cookie due to missing Vary: Cookie header
CVE-2024-34069	HIGH	python-werkzeug: user may execute code on a developer's machine
CVE-2023-46136	MEDIUM	python-werkzeug: high resource consumption leading to denial of service
CVE-2024-49766	MEDIUM	werkzeug: python-werkzeug: Werkzeug safe_join not safe on Windows
CVE-2024-49767	MEDIUM	werkzeug: python-werkzeug: Werkzeug possible resource exhaustion when parsing file data in fo
CVE-2024-3651	MEDIUM	python-idna: potential DoS via resource consumption via specially crafted inputs to idna.encode()
CVE-2023-5752	MEDIUM	pip: Mercurial configuration injectable in repo revision when installing via pip
CVE-2018-18074	HIGH	python-requests: Redirect from HTTPS to HTTP does not remove Authorization header
CVE-2023-32681	MEDIUM	python-requests: Unintended leak of Proxy-Authorization header
CVE-2024-35195	MEDIUM	requests: subsequent requests to the same host ignore cert verification
CVE-2024-47081	MEDIUM	requests: Requests vulnerable to .netrc credentials leak via malicious URLs
CVE-2022-40897	HIGH	pypa-setuptools: Regular Expression Denial of Service (ReDoS) in package_index.py
CVE-2024-6345	HIGH	pypa/setuptools: Remote code execution via download functions in the package_index module in
CVE-2025-47273	HIGH	setuptools: Path Traversal Vulnerability in setuptools PackageIndex
CVE-2019-11324	HIGH	python-urllib3: Certification mishandle when error should be thrown
CVE-2023-43804	HIGH	python-urllib3: Cookie request header isn't stripped during cross-origin redirects
CVE-2018-25091	MEDIUM	urllib3: urllib3 does not remove the authorization HTTP header when following a cross-origin redi
CVE-2019-11236	MEDIUM	python-urllib3: CRLF injection due to not encoding the '\r\n' sequence leading to possible attack o
CVE-2020-26137	MEDIUM	python-urllib3: CRLF injection via HTTP request method
CVE-2023-45803	MEDIUM	urllib3: Request body not stripped after redirect from 303 status changes request method to GET
CVE-2024-37891	MEDIUM	urllib3: proxy-authorization request header is not stripped during cross-origin redirects
CVE-2025-50181	MEDIUM	urllib3: urllib3 redirects are not disabled when retries are disabled on PoolManager instantiation
CVE-2024-5569	MEDIUM	github.com/jaraco/zipp: Denial of Service (infinite loop) via crafted zip file in jaraco/zipp

Bandit Findings:

ID/Package	Severity	Description/Title

B104	MEDIUM	Possible binding to all interfaces.