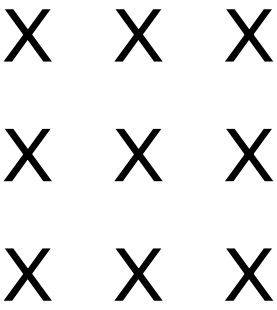

CSF.AE

REPORT

RESULTS OF PENETRATION TESTING
"SLEX.IO"

Contents

csf.ae
+97148826251
info@csf.ae

1. Penetration testing

1.1. Penetration testing of the outer network perimeter

1.1.1. Penetration testing of the node with 65.109.70.31 IP address

As a result of scanning network node with 65.109.70.31 IP-address a list of network services was identified, listed in Table 1.

Table 1 – List of network services on the node with 65.109.70.31 IP address

TCP-port	Status	Protocol	Product, version
80	Open	HTTP	Ngnix, version unidentified
443	Open	SSL/HTTP	Ngnix, version unidentified

During the process of identification and analysis of network services infrastructure done with special assessment tools, no vulnerabilities were found

1.2. Penetration testing of web resources

1.2.1. Penetration testing of “slex.io”

Information about OS, Web-server, software tools and frameworks, used in “slex.io” web-resource structure, is presented in table 2.

Table 2 – “slex.io” web-resource structure

Components	Information received during the analysis
Operating System	– OS version unidentified.
Web-server (HTTP-server)	– Nginx, version unidentified.
Other utilized software tools and frameworks on the web-resource	– Web Framework Next.js 14.4.9;

List of vulnerabilities found during automatic analysis of “slex.io” components are listed in table 2.

During manual analysis of “slex.io”, vulnerabilities found during automatic analysis were confirmed.

Table 3 – “slex.io” vulnerability list

Vulnerability name	Description
Lack of HTTP-header Strict-Transport-Security, required for HSTS.	Server’s response to HTTP-query does not contain HTTP-header Strict-Transport-Security, responsible for HSTS standard. HSTS (HTTP Strict Transport Security) — Security policy mechanism forcing secure connection via HTTPS protocol.
Lack of frame-ancestors pragma in HTTP-header Content-Security-Policy, meant for protection against Clickjacking-attacks	Clickjacking – attack with alteration of user interface by implementing website’s content in other sites. The server did not return frame-ancestors pragma in HTTP-header Content-Security-Policy, which guarantees protection from implementing website’s content in other sites.
Disclosure of Software version and frameworks by headers in web-server responses.	HTTP-responses, returned by this web application, includes the following headers: – Server, disclosing usage of nginx; – X-Powered-By, disclosing usage of Next.js framework. Information about used software and frameworks can be used by a potential intruder to prepare a more targeted attack.

Vulnerability name	Description
Using outdated Next.js version (14.4.9.)	Next.js 14.4.9 is outdated and is susceptible to multiple vulnerabilities, such as: Denial of Service (CVE-2022-21721, CVE-2021-43803) and Cross-Site Scripting (CVE-2021-39178, CVE-2018-18282)

Vulnerabilities found during penetration testing of “slex.io” website were scored and assessed in accordance with base metrics, CVSS 3.1, shown in table 3.

Table 4 – “slex.io” Vulnerability scoring

Vulnerability Name	ID and CWE name	Base metrics CVSS 3.1	CVSS 3.1 Score
Lack of HTTP-header Strict-Transport-Security, required for HSTS.	CWE-523: Unprotected Transport of Credentials	/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	Medium (6.5)
Lack of frame-ancestors pragma in HTTP-header Content-Security-Policy, meant for protection against Clickjacking-attacks	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	Medium (5.3)
Disclosure of Software version and frameworks by headers in web-server responses.	CWE-1021: Improper Restriction of Rendered UI Layers or Frames	/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N	Medium (4.3)

1.3. DoS-attack rigidity testing

DoS-attack was done to “slex.io” using “Apache Benchmark” utility.

DoS-attack was done in two stages: standard testing and direct test of the API used by the resource.

Despite the successful recovery of the resource after the attack, as a result of the test a DoS vulnerability was defined, making further testing by DDoS-attack unnecessary.

1.3.1. DoS-attack rigidity testing of the API

As a result of conducted testing the following was found: at 500 concurrent queries from two APMs Denial of Service occurs, resulting in error code 500 by the API. API malfunction is defined by displaying incorrect plot of “BTC” to “USD” price ratio at web-interface. The test was conducted the following way:

1) 500 sent queries, concurrent threads: 5. Stress-test passed successfully.
2) 2500 sent queries, Concurrent threads: 10. Stress-test passed successfully.

csf.ae
+97148826251
info@csf.ae

3) 10000 sent queries, Concurrent threads: 500. API responded with code 500 “Internal Server error”. Denial of Service occurs, evident by incorrect display of “BTC” to “USD” ratio plot.

1.1.1. DoS-attack rigidity testing of “slex.io” web resource

The rigidity test way conducted the following way:

1) 500 sent queries, concurrent threads: 5. Stress-test passed successfully.
2) 2500 sent queries, Concurrent threads: 10. Stress-test passed successfully.
3) 10000 sent queries, Concurrent threads: 500. Server responds with 24000 ms delay.

As a result of the test DoS-vulnerability of the resource was found.

csf.ae
+97148826251
info@csf.ae

2. Recommendations after test conclusion

2.1. Patching vulnerabilities at outer network perimeter

No patching is required at a network node with 65.109.70.31 IP address, since no vulnerabilities were found.

2.2. Patching vulnerabilities on web-resources

Recommendations for patching vulnerabilities on “slex.io” website are listed in table 4.

Table 5 – Recommendations for patching vulnerabilities on “slex.io” website

Vulnerability Name	Recommendations to patch the vulnerability
Lack of HTTP-header Strict-Transport-Security, required for HSTS.	Include Strict-Transport-Security HTTP-header to web-server configuration.
Lack of frame-ancestors pragma in HTTP-header Content-Security-Policy, meant for protection against Clickjacking-attacks	Include Content-Security-Policy HTTP-header with frame-ancestors pragma to web-server configuration.
Disclosure of Software version and frameworks by headers in web-server responses.	Exclude optional Server и X-Powered-By from server response.

2.3. Recommendations after results of DoS-attack rigidity

As a result of conducting the test of “slex.io” with the purpose to protect the system from DoS and DDoS attacks it is recommended to use traffic filters and IP-blockers: firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

2.4. General recommendations

Patch the vulnerabilities found during the penetration testing.

Keep all used software versions up to date.

Periodically conduct IT Infrastructure security audit to preliminary identify and patch vulnerabilities, keeping high security level.