Appendix

Vulnerabilities

List vulnerabilities frontend:

next	16.0.0-canary.0 - 16.0.6	Critical	RCE in React Flight Protocol	Upgrade 16.0.7

List vulnerabilities backend:

@babel/helpers	<7.26.10	Moderate	Inefficient RegExp complexity in transpiled code	npm audit fix
@babel/runtime	<7.26.10	Moderate	Inefficient RegExp complexity in transpiled code	npm audit fix
@babel/traverse	<7.23.2	Critical	Arbitrary code execution when compiling malicious code	npm audit fix
body-parser	<1.20.3	High	Denial of Service when URL encoding is enabled	npm audit fix
brace-expansion	1.0.0 - 1.1.11	High	Regular Expression Denial of Service (ReDoS)	npm audit fix
braces	<3.0.3	High	Uncontrolled resource consumption	npm audit fix
cookie	<0.7.0	High	Accepts cookie name, path, domain with out-of-bounds characters	npm audit fix
cross-spawn	7.0.0 - 7.0.4	High	ReDoS	npm audit fix
js-yaml	<3.14.2 or >=4.0.0 <4.1.1	Moderate	Prototype pollution in merge (<<)	npm audit fix
micromatch	<4.0.8	Moderate	ReDoS	npm audit fix
nodemailer	<=7.0.10	Moderate/High	DoS in addressparser via recursive calls	npm audit fix
path-to-regexp	<=0.1.11	High	ReDoS via backtracking regex	npm audit fix
semver	7.0.0 - 7.5.1	High	ReDoS	npm audit fix

simple-update-notifier	1.0.7 - 1.1.0	High	Depends on vulnerable semver	npm audit fix
nodemon	2.0.19 - 2.0.22	High	Depends on vulnerable simple-update-notifier	npm audit fix
send	<0.19.0	High	Template injection leading to XSS	npm audit fix
serve-static	<=1.16.0	High	Depends on vulnerable send	npm audit fix
tar	<6.2.1	Moderate	DoS when parsing tar files	npm audit fix
validator	<=13.15.20	High	URL validation bypass	npm audit fix
express	<=4.21.0 / 5.0.0-alpha.1 - 5.0.0	High	Depends on multiple vulnerable packages (body-parser, cookie, path-to-regexp, send, serve-static)	npm audit fix

Logging

Example of logging:

{"event":"LOGIN_ATTEMPT","ip":"::ffff:127.0.0.1","level":"info","message":"Login attempt for user Lukas","status":"attempt","timestamp":"2025-12-11T19:24:07.248Z","url":"/users/login","user":"Lukas"}

{"event":"FAIL_LOGIN","level":"info","message":"Failed login by Lukas - password incorrect","status":"request","timestamp":"2025-12-11T19:24:07.482Z","user":"Lukas"}

{"event":"FAIL_LOGIN","ip":"::ffff:127.0.0.1","level":"info","message":"Failed login for Lukas: Incorrect password.","status":"failure","timestamp":"2025-12-11T19:24:07.483Z","url":"/users/login","user":"Lukas"}

{"level":"error","message":"Error: Incorrect password. | URL: /users/login","timestamp":"2025-12-11T19:24:07.484Z"}

{"event":"LOGIN_ATTEMPT","ip":"::ffff:127.0.0.1","level":"info","message":"Login attempt for user Lukas","status":"attempt","timestamp":"2025-12-11T19:34:53.834Z","url":"/users/login","user":"Lukas"}

{"event":"REQUIRED_MFAA","ip":"::ffff:127.0.0.1","level":"info","message":"MFA required for Lukas","status":"pending","timestamp":"2025-12-11T19:34:56.520Z","url":"/users/login","user":"Lukas"}

{"event":"SUCCESS_LOGIN","level":"info","message":"Successful login by Lukas","status":"request","timestamp":"2025-12-11T19:35:26.857Z","user":"Lukas"}

SSRF – login :

POST /users/login HTTP/1.1
Host: localhost:3000
Content-Length: 45
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: nl-NL,nl;q=0.9
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: */*
Origin: https://localhost:4000
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://localhost:4000/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
{"username":"Lukas","password":"Lukas12345!"}

HTTP/1.1 200 OK (response)
Content-Security-Policy: default-src 'self';script-src 'self' https://localhost:4000;style-src 'self' 'unsafe-inline' https://fonts.googleapis.com;font-src 'self' https://fonts.gstatic.com;img-src 'self' https://localhost:4000;connect-src 'self' https://localhost:4000;base-uri 'self';form-action 'self';frame-ancestors 'self';object-src 'none';script-src-attr 'none';upgrade-insecure-requests
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-Content-Type-Options: nosniff
X-DNS-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 0
Access-Control-Allow-Origin: https://localhost:4000
Vary: Origin
Access-Control-Allow-Credentials: true
X-RateLimit-Limit: 5
X-RateLimit-Remaining: 3
Date: Sun, 14 Dec 2025 18:52:57 GMT
X-RateLimit-Reset: 1765739278
Content-Type: application/json; charset=utf-8
Content-Length: 55
ETag: W/"37-zsFjv7pbwIbF/U5Muk3VNNT8FQc"
Connection: keep-alive
Keep-Alive: timeout=5{"message":"MFA code sent to email","requiresMfa":true}

POST /users/login-verify HTTP/1.1
Host: localhost:3000
Content-Length: 55
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: nl-NL,nl;q=0.9
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/143.0.0.0 Safari/537.36
Accept: */*
Origin: https://localhost:4000
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://localhost:4000/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
{"username":"Lukas","code":"970968","rememberMe":false}

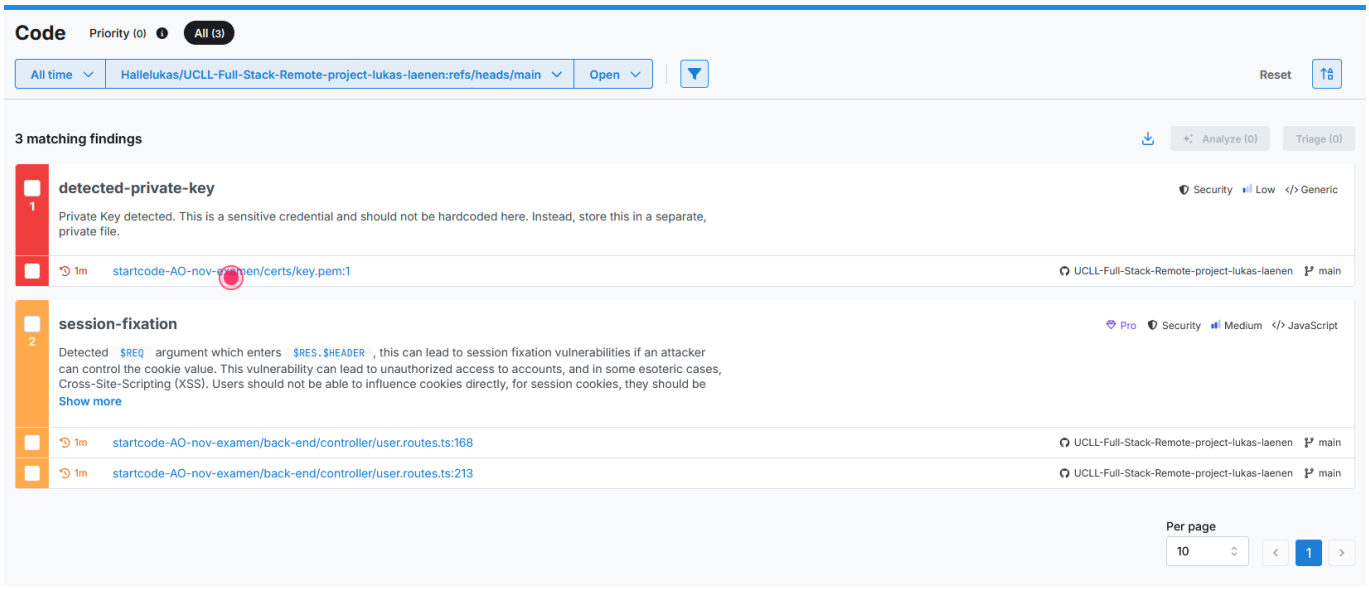
HTTP/1.1 200 OK (response)
Content-Security-Policy: default-src 'self';script-src 'self' https://localhost:4000;style-src 'self'
'unsafe-inline' https://fonts.googleapis.com;font-src 'self' https://fonts.gstatic.com;img-src 'self'
https://localhost:4000;connect-src 'self' https://localhost:4000;base-uri 'self';form-action
'self';frame-ancestors 'self';object-src 'none';script-src-attr 'none';upgrade-insecure-requests
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-Content-Type-Options: nosniff
X-DNS-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 0
Access-Control-Allow-Origin: https://localhost:4000
Vary: Origin
Access-Control-Allow-Credentials: true
X-RateLimit-Limit: 5
X-RateLimit-Remaining: 2
Date: Sun, 14 Dec 2025 18:53:22 GMT
X-RateLimit-Reset: 1765739278
Set-Cookie:
auth_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Ikx1a2FzIiwicm9sZSI6InN0
dWRlbnQiLCJpYXQiOjE3NjU3Mzg0MDMsImV4cCI6MTc2NTc0NTYwMywiaXNzIjoidGVhbV9hcHAifQ.
PSvVDE1x5VshZUpIJDsNbOkXplbRxNSGFcehwMyzWNs; Max-Age=7200; Path=/; Expires=Sun, 14
Dec 2025 20:53:23 GMT; HttpOnly; Secure; SameSite=Lax
Content-Type: application/json; charset=utf-8
Content-Length: 50

ETag: W/"32-aIDI34o+zQRVKhF+noxI9UzwT9U"
Connection: keep-alive
Keep-Alive: timeout=5

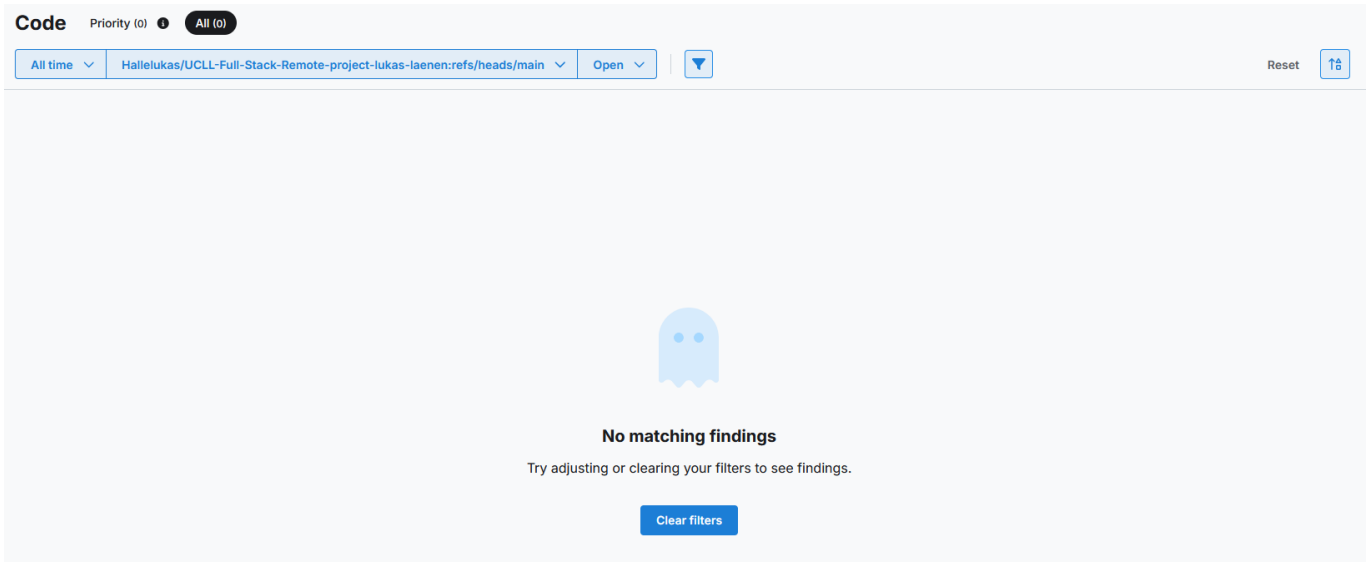
{"requiresMfa":false,"message":"Login successful"}

Security Testing

- **SAST V1**



- **SAST V2**



Debugging Info

SCAN ENVIRONMENT
versions - semgrep 1.144.1 on python 3.12.12
environment - running in environment semgrep-managed-scan, triggering event is unknown

CONNECTION
Initializing scan (deployment=lukas-laenen-student-ucll-be, scan_id=118413404)
Enabled products: Code, Supply Chain

ENGINE
Using Semgrep Pro Version: 1.144.1
Installed at /usr/lib/python3.12/site-packages/semgrep/bin/semgrep-core-proprietary
no version for dependency: node_modules/exam_api
no version for dependency:

Scan Status

Scanning 86 files tracked by git with 2454 Code rules, 4809 Supply Chain rules:

CODE RULES

Language	Rules	Files
<multilang>	61	86
ts	334	47
json	4	9
js	324	7
yaml	31	1
html	1	1

Origin	Rules
Pro rules	1390
Community	1064

SUPPLY CHAIN RULES

Dependency Sources	Resolution Method	Ecosystem	Dependencies	Rules
startcode-AO-nov-examen/back-end/package-lock.json	Lockfile	Npm	522	4809
startcode-AO-nov-examen/front-end/package-lock.json	Lockfile	Npm	180	4809

Analysis	Rules
Basic	3612
Reachability	1197

no files modified.
Uploading scan results
Finalizing scan

Scan Summary

✅ CI scan completed successfully.
- Findings: 0 (0 blocking)
- Rules run: 28167
- Targets scanned: 86
- Parsed lines: ~100.0%
- Scan skipped:
  - Files larger than files 1.0 MB: 2
- Scan was limited to files tracked by git
- For a detailed list of skipped files and lines, run semgrep with the --verbose flag

CI scan completed successfully.
View results in Semgrep Cloud Platform:
https://semgrep.dev/orgs/lukas-laenen-student-ucll-be/findings?repo=Hallelukas/UCLL-Full-Stack-Remote-project-lukas-laenen&ref=main
https://semgrep.dev/orgs/lukas-laenen-student-ucll-be/supply-chain/vulnerabilities?repo=Hallelukas/UCLL-Full-Stack-Remote-project-lukas-laenen&ref=main
No blocking findings so exiting with code 0