Gitleaks Scan Report

Generated from: app/repositories/juice-shop/gitleaks-report.json

Detected Secrets:

File: test/api/web3Spec.ts
Line: 36
Commit: 4e1b04d8043428b71cab5ad020c18b3db42b4361
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/web3Spec.ts
Line: 48
Commit: 4e1b04d8043428b71cab5ad020c18b3db42b4361
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/web3Spec.ts
Line: 60
Commit: 4e1b04d8043428b71cab5ad020c18b3db42b4361
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/erasureRequestApiSpec.ts
Line: 99
Commit: de491d5f28274b26efdb03e6fadf84531496326c
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/erasureRequestApiSpec.ts
Line: 119
Commit: de491d5f28274b26efdb03e6fadf84531496326c
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/erasureRequestApiSpec.ts
Line: 139
Commit: de491d5f28274b26efdb03e6fadf84531496326c
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: frontend/src/app/faucet/faucet.component.ts
Line: 828
Commit: c800f7092d8bc08e36da46b8f460b0bb576e832d
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: cypress/integration/e2e/forgedJwt.spec.ts
Line: 7
Commit: 1d1571854621f9fa4150e6fae93b24504d4e5a11
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: cypress/integration/e2e/forgedJwt.spec.ts
Line: 22
Commit: 1d1571854621f9fa4150e6fae93b24504d4e5a11
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit

File: cypress/integration/e2e/totpSetup.spec.ts
Line: 7
Commit: 1d1571854621f9fa4150e6fae93b24504d4e5a11
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: frontend/src/app/last-login-ip/last-login-ip.component.spec.ts
Line: 50
Commit: 1bb101b122c95236faace995a89a2bc5df92b0c3
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/api/erasureRequestApiSpec.ts
Line: 37
Commit: a03905e4add2087df38d8b193194418ecae87258
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: cypress/integration/e2e/totpSetup.spec.ts
Line: 7
Commit: b19993bcee5587459474fc495f35977f542d26e8
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: cypress/integration/e2e/forgedJwt.spec.ts
Line: 7
Commit: 9aafdbae600a9e334b33fcb2faca854a87de1ef8
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: cypress/integration/e2e/forgedJwt.spec.ts
Line: 22
Commit: 9aafdbae600a9e334b33fcb2faca854a87de1ef8
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: routes/login.ts
Line: 66
Commit: b27b94f056409bbdfaf8ddd9df60f84776b6b476
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/productReviewApiSpec.ts
Line: 106
Commit: 279961895c88eae489dae71373e216755bea6ab7
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/e2e/forgedJwtSpec.ts
Line: 11
Commit: fcf8c104c4c23d9d1d5c93ac253a83d6108cda8d
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/e2e/forgedJwtSpec.ts
Line: 21
Commit: fcf8c104c4c23d9d1d5c93ac253a83d6108cda8d
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/currentUserSpec.ts
Line: 31
Commit: 3ad2c3f7463662399849d34d3fac098e14e7b22c
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.ts
Line: 262
Commit: 3ad2c3f7463662399849d34d3fac098e14e7b22c
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.ts
Line: 274
Commit: 3ad2c3f7463662399849d34d3fac098e14e7b22c
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.ts
Line: 296
Commit: 3ad2c3f7463662399849d34d3fac098e14e7b22c
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.ts
Line: 308
Commit: 3ad2c3f7463662399849d34d3fac098e14e7b22c
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/api/userApiSpec.ts
Line: 262
Commit: 660f3abd11dea0019526c6b328dc7907813a9cab
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/api/chatBotSpec.js
Line: 161
Commit: ecbd8903801fd86afcd8a2e3b92221175857b1fb
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: frontend/src/app/app.guard.spec.ts
Line: 40
Commit: 6f79b44421dc8e79ed8a61450d58a5c66d14b61f
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/api/chatBotSpec.js
Line: 99
Commit: ca61daf7a96c585a509616f183afa8f8884fcab8
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/chatBotSpec.js
Line: 127
Commit: ca61daf7a96c585a509616f183afa8f8884fcab8
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/chatBotSpec.js
Line: 180
Commit: ca61daf7a96c585a509616f183afa8f8884fcab8
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: frontend/src/app/oauth/oauth.component.spec.ts
Line: 83
Commit: d73a4d4231f5ee97a2f92efd99893d0158fa4f33
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: frontend/src/app/oauth/oauth.component.spec.ts
Line: 83
Commit: d73a4d4231f5ee97a2f92efd99893d0158fa4f33
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: frontend/src/app/oauth/oauth.component.spec.ts
Line: 90
Commit: d73a4d4231f5ee97a2f92efd99893d0158fa4f33
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/chatBotSpec.js
Line: 153
Commit: eadb44a8106fb2feed3cfb5825fb33a86280bcd5
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/chatBotSpec.js
Line: 154
Commit: e6137d76bb18c55875b4284761e8939635f127af
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/chatBotSpec.js
Line: 150
Commit: cda3cbc2aa8c5a61782bbc679cbb1ccb269b43cc
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/chatBotSpec.js
Line: 72
Commit: f672660b96a48d8bbd2d6382321a0c0c1628cb25
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/chatBotSpec.js
Line: 106
Commit: f672660b96a48d8bbd2d6382321a0c0c1628cb25
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/e2e/forgedJwtSpec.js
Line: 20
Commit: c1ccf7243a6fa7a44a84cd5a4b2f1e5497d055fe
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.js
Line: 291
Commit: c1ccf7243a6fa7a44a84cd5a4b2f1e5497d055fe
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.js
Line: 303
Commit: c1ccf7243a6fa7a44a84cd5a4b2f1e5497d055fe
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/currentUserSpec.js
Line: 31
Commit: 57a9bf5559105d8e5810bcef216c85601cf663b1
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/e2e/forgedJwtSpec.js
Line: 18
Commit: 531e32d9d84bb76b16c51b4dffbed1ce5a26f781
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/currentUserSpec.js
Line: 29
Commit: 128e3a3a9b1b13d44fef28360976531a5ce0a5fa
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/currentUserSpec.js
Line: 31
Commit: 128e3a3a9b1b13d44fef28360976531a5ce0a5fa
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.js
Line: 289
Commit: 128e3a3a9b1b13d44fef28360976531a5ce0a5fa
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.js
Line: 301
Commit: 128e3a3a9b1b13d44fef28360976531a5ce0a5fa
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/currentUserSpec.js
Line: 31
Commit: 9b6b0b5e49ca4122f0d6daa7433d3d2c1833ce38
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: routes/login.js
Line: 65
Commit: b8fee634c2762e6df287ccd988129c5bb557efb5
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/server/currentUserSpec.js
Line: 24
Commit: 6dcd8f5446be322bd58df2a750a0d9bbb8d853d8
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/currentUserSpec.js
Line: 26
Commit: 6dcd8f5446be322bd58df2a750a0d9bbb8d853d8
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/api/userApiSpec.js
Line: 254
Commit: 1a5ce906c84c4d7cfbb994910b4e23742fa42bae
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: data/static/users.yml
Line: 37
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/userApiSpec.js
Line: 146
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/feedbackApiSpec.js
Line: 110
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/feedbackApiSpec.js
Line: 143
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/dataExportApiSpec.js
Line: 13
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/dataExportApiSpec.js
Line: 40
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/dataExportApiSpec.js
Line: 69
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: routes/login.js
Line: 72
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/basketApiSpec.js
Line: 81
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/erasureRequestApiSpec.js
Line: 12
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/erasureRequestApiSpec.js
Line: 26
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/loginApiSpec.js
Line: 143
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/loginApiSpec.js
Line: 245
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/loginApiSpec.js
Line: 266
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/productReviewApiSpec.js
Line: 99
Commit: 206336a5e5db795e387fd0405365795fdf25c7b6
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/loginApiSpec.js
Line: 245
Commit: 2a8f815583bf5e91e655b0ea5d38529c89e64b20
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/loginApiSpec.js
Line: 266
Commit: 2a8f815583bf5e91e655b0ea5d38529c89e64b20
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/productReviewApiSpec.js
Line: 99
Commit: 994b994503142849b62d543e54e66d92ca83c34e
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: routes/login.js
Line: 72
Commit: f121dcfc0b8a7970c50153490321943d03ce74ba
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/dataSubjectApiSpec.js
Line: 13
Commit: 91a7cac7465461d6dc1a2c52d6543e23d19994bf
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/dataSubjectApiSpec.js
Line: 27
Commit: 91a7cac7465461d6dc1a2c52d6543e23d19994bf
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/2faSpec.js
Line: 345
Commit: 87e328633380e3aff53339b9416ce05e9182b80e
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/e2e/2faSetupSpec.js
Line: 25
Commit: 48b05c876a345f6369c6eeadcb6ca04d14c82ab9
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/2faSpec.js
Line: 110
Commit: f01c45062da3b3e1f5be2e5b679bc84acf5e7d43
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/2faSpec.js
Line: 111
Commit: 99e1d29e3fe596f7a5374e7f5f3a132f68bd86c1
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/dataExportApiSpec.js
Line: 12
Commit: c98a53f3effa49653c2ac1baf4d41b42c018000b
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/dataExportApiSpec.js
Line: 36
Commit: c98a53f3effa49653c2ac1baf4d41b42c018000b
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/dataExportApiSpec.js
Line: 65
Commit: c98a53f3effa49653c2ac1baf4d41b42c018000b
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: data/static/users.yml
Line: 84
Commit: 06e3afc010bcc9fab17b7c88a3c8aa42356897f8
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: data/static/users.yml
Line: 75
Commit: b751705ebff0d6fd03331a2a8e64f1c5816badd7
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: data/static/users.yml
Line: 45
Commit: d5568f5c196d5a5f983b33898f91cb1ec808860a
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: routes/login.js
Line: 41
Commit: 434a1428f16a38abf9185111f7c57379f8c349f3
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/basketApiSpec.js
Line: 81
Commit: 434a1428f16a38abf9185111f7c57379f8c349f3
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/feedbackApiSpec.js
Line: 110
Commit: 434a1428f16a38abf9185111f7c57379f8c349f3
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/feedbackApiSpec.js
Line: 143
Commit: 434a1428f16a38abf9185111f7c57379f8c349f3
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/passwordApiSpec.js
Line: 42
Commit: 434a1428f16a38abf9185111f7c57379f8c349f3
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/userApiSpec.js
Line: 118
Commit: 434a1428f16a38abf9185111f7c57379f8c349f3
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: data/static/users.yml
Line: 18
Commit: e4886a82bccc81f178b7e843eded90cb7b97c33e
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/loginApiSpec.js
Line: 125
Commit: e4886a82bccc81f178b7e843eded90cb7b97c33e
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/e2e/forgedJwtSpec.js
Line: 4
Commit: eb864dd8a6842b4de68c199c706bd2626be6cc5d
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/e2e/forgedJwtSpec.js
Line: 5
Commit: eb864dd8a6842b4de68c199c706bd2626be6cc5d
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/e2e/forgedJwtSpec.js
Line: 14
Commit: eb864dd8a6842b4de68c199c706bd2626be6cc5d
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/e2e/forgedJwtSpec.js
Line: 15
Commit: eb864dd8a6842b4de68c199c706bd2626be6cc5d
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: data/static/users.yml
Line: 18
Commit: 114803a321f29442ed8588154e27c103702c5f83
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: data/static/users.yml
Line: 15
Commit: 4c4fe4a1ed5748f281afc9329feb457b1c028cee
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: data/data/users.json
Line: 22
Commit: a9139a134eefb60a7441b7619b991e62d5faf8d9
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/server/verifySpec.js
Line: 225
Commit: f3f7a81f316ada34609e1220fb0be4f602b49b82
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.js
Line: 237
Commit: f3f7a81f316ada34609e1220fb0be4f602b49b82
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.js
Line: 258
Commit: f3f7a81f316ada34609e1220fb0be4f602b49b82
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.js
Line: 270
Commit: f3f7a81f316ada34609e1220fb0be4f602b49b82
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/api/passwordApiSpec.js
Line: 63
Commit: 4e91654448ba527161dbab0a9ce975ecd1b3fcee
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/loginApiSpec.js
Line: 94
Commit: 4e91654448ba527161dbab0a9ce975ecd1b3fcee
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/server/verifySpec.js
Line: 239
Commit: 318ba467ea39276f0467cf3bf0664153a696cc58
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.js
Line: 272
Commit: 318ba467ea39276f0467cf3bf0664153a696cc58
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/e2e/forgedJwtSpec.js
Line: 4
Commit: 7fa085f79ac217ec0ab8e7d402598c781e07215e
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/e2e/forgedJwtSpec.js
Line: 13
Commit: 7fa085f79ac217ec0ab8e7d402598c781e07215e
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.js
Line: 227
Commit: 0ac15ff7f7ea26b7a1c4d240441de6d348b11a5b
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: test/server/verifySpec.js
Line: 248
Commit: 0ac15ff7f7ea26b7a1c4d240441de6d348b11a5b
Description: Uncovered a JSON Web Token, which may lead to unauthorized access to web applications and sensit
Rule ID: jwt

File: lib/insecurity.js
Line: 10
Commit: 2adcd7231f30e12601c8e80a3b49b3420418debe
Description: Identified a Private Key, which may compromise cryptographic security and sensitive data encryption.
Rule ID: private-key

File: lib/insecurity.js
Line: 12
Commit: 08af603f65bee78c1370f4ecb8f0739c3718e3b0
Description: Identified a Private Key, which may compromise cryptographic security and sensitive data encryption.
Rule ID: private-key

File: test/api/feedbackApiSpec.js
Line: 85
Commit: e970d58af6627e2a7ddad0d7cc8c01c3192b13c8
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/feedbackApiSpec.js
Line: 112
Commit: e970d58af6627e2a7ddad0d7cc8c01c3192b13c8
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/basketApiSpec.js
Line: 94
Commit: e970d58af6627e2a7ddad0d7cc8c01c3192b13c8
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/userApiSpec.js
Line: 122
Commit: e970d58af6627e2a7ddad0d7cc8c01c3192b13c8
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/userApiSpec.js
Line: 249
Commit: e970d58af6627e2a7ddad0d7cc8c01c3192b13c8
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/basketApiSpec.js
Line: 94
Commit: 03f756d221a0d6473a0174a55fefe189ee7ecd85
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/userApiSpec.js
Line: 414
Commit: e970d58af6627e2a7ddad0d7cc8c01c3192b13c8
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/feedbackApiSpec.js
Line: 85
Commit: 03f756d221a0d6473a0174a55fefe189ee7ecd85
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/feedbackApiSpec.js
Line: 112
Commit: 03f756d221a0d6473a0174a55fefe189ee7ecd85
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/userApiSpec.js
Line: 122
Commit: 03f756d221a0d6473a0174a55fefe189ee7ecd85
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/userApiSpec.js
Line: 249
Commit: 03f756d221a0d6473a0174a55fefe189ee7ecd85
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: test/api/userApiSpec.js
Line: 414
Commit: 03f756d221a0d6473a0174a55fefe189ee7ecd85
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: data/datacreator.js
Line: 510
Commit: af5dfc11265014f780ba31b7b696f55be3d9ea67
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: vagrant/.vagrant/machines/default/virtualbox/private_key
Line: 1
Commit: 48174b3e4188811db7b6f128cbf11da7fd9cde82
Description: Identified a Private Key, which may compromise cryptographic security and sensitive data encryption.
Rule ID: private-key

File: test/server/userApiSpec.js
Line: 190
Commit: 03d0e94f33e747ccb8a2e4cce45882ea76858464
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: routes/login.js
Line: 13
Commit: 3df64d5cc9ed0ed0f429eb537973430c66280cfe
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: data/datacreator.js
Line: 317
Commit: 3df64d5cc9ed0ed0f429eb537973430c66280cfe
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: server.js
Line: 24
Commit: ac11dd38cf84483608c03504a9f353fe2f4ed76f
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key

File: .travis.yml
Line: 8
Commit: 8a474274d6fa9335c23fe1ca2dc19688e7dffac5
Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.
Rule ID: generic-api-key