

drupal

github.com/drupal/drupal

Scanned 24 September 2026 at 07:36 · Report generated 29 October 2026 · PHP · 4,290 stars

OVERALL ASSESSMENT

High

Combined score 138 · 94 findings after filtering

Summary

28 findings likely need attention, 16 look like noise. Most notable: The 'phpinfo' function may reveal sensitive information about your environment. (50% confidence).

Generated from finding counts. A plain-English summary was not available for this scan.

Risk, by type

MalDet scores two different questions separately, because they call for different responses: code can be badly written without being hostile, and hostile code is not always badly written.

VULNERABILITY

High (133)

Insecure coding an attacker could exploit. Usually mistakes, and usually fixable in place.

MALICIOUS PATTERN

Low (5)

Signs the code may be trying to do harm: hidden payloads, credential access, persistence, exfiltration.

What each detector found

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
semgrep	Insecure coding patterns across many languages	3	79	1	83
yara	Signatures of malicious behaviour in source files	8	0	1	9
guarddog	Malicious package and install-time behaviour	0	1	1	2

28 of 94 findings were rated more likely genuine than noise by the classifier.

Evidence

Identical findings are grouped, so a single rule firing many times takes one row. Ordered worst first. “Seen” is how many times that finding occurred.

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	semgrep	The 'phpinfo' function may reveal sensitive information about your environment.	1	/core/modules/system/src/Controller/SystemInfoController.php:83
HIGH	semgrep	Executing non-constant commands. This can lead to command injection.	2	/core/lib/Drupal/Core/Command/ServerCommand.php:237
HIGH	yara	YARA rule matched: detect_base64_exec — Encoded payload decoded and then executed	2	/core/assets/vendor/ckeditor5/ckeditor5.md.js.map
HIGH	yara	YARA rule matched: detect_obfuscated_string_execution — Reconstructs a string character-by-character or from hex escapes, then immediately executes it - fromCharCode/chr() alone are common in ordinary text-processing code, so this requires both the reconstruction and an execution call together	6	/core/assets/vendor/ckeditor5/ckeditor5.md.js.map
MEDIUM	semgrep	RegExp() called with a `config` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controll	1	/core/modules/ckeditor5/js/ckeditor5.js:89
MEDIUM	semgrep	RegExp() called with a `event` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlle	1	/core/modules/file/js/file.js:161

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	RegExp() called with a `response` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-control	1	/core/modules/views_ui/js/ajax.js:142
MEDIUM	semgrep	RegExp() called with a `settings` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-control	1	/core/misc/machine-name.js:45
MEDIUM	semgrep	This code contains bidirectional (bidi) characters. While this is useful for support of right-to-left languages such as Arabic or Hebrew, it can also be used to trick language parsers into executing code in a manner that is different from how it is displayed in code editing and review tools. If this	8	/core/lib/Drupal/Core/Language/LanguageManager.php:339
MEDIUM	semgrep	It looks like MD5 is used as a password hash. MD5 is not considered a secure password hash because it can be cracked by an attacker in a short amount of time. Use a suitable password hashing function such as bcrypt. You can use `password_hash(\$PASSWORD, PASSWORD_BCRYPT, \$OPTIONS);`.	1	/core/lib/Drupal/Core/Password/PhpPassHashedPasswordBase.php:224
MEDIUM	guarddog	Detects unicode homoglyphs and uncommon characters used for obfuscation [threat-runtime-obfuscation-unicode]	1	/core/assets/vendor/ckeditor5/translations/bg.umd.js:7

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	This .yarnrc.yml does not set a minimal age gate or sets it too low. Newly published packages can be malicious or unstable. Add `npmMinimalAgeGate: "7d"` to wait 7 days before resolving newly published package versions. Added in: 4.10 Reference: https://yarnpkg.com/configuration/yarnrc#npmMinimalAge	1	/core/.yarnrc.yml:8
MEDIUM	semgrep	File name based on user input risks server-side request forgery.	9	/.gitlab-ci/scripts/component-coverage-metrics.php:45
MEDIUM	semgrep	Make sure comparisons involving md5 values are strict (use `===` not `==`) to avoid type juggling issues	1	/core/lib/Drupal/Component/Transliteration/PhpTransliteration.php:158
MEDIUM	semgrep	The `redirect()` method does not check its destination in any way. If you redirect to a URL provided by end-users, your application may be open to the unvalidated redirects security vulnerability. Consider using literal values or an allowlist to validate URLs.	9	/core/modules/comment/src/Controller/CommentController.php:179
MEDIUM	semgrep	Detection of insertAdjacentHTML from non-constant definition. This can inadvertently expose users to cross-site scripting (XSS) attacks if this comes from user-provided input. If you have to use insertAdjacentHTML, consider using a sanitization library such as DOMPurify to sanitize your HTML.	1	/core/modules/navigation/js/tooltip.js:51
MEDIUM	semgrep	Possibility of prototype polluting function detected. By adding or modifying attributes of an object prototype, it is possible to create attributes that exist on every object, or replace critical attributes with malicious ones. This can be problematic if the software depends on existence or non-exis	1	/core/misc/tableselect.js:154

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	RegExp() called with a `e` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled in	2	/core/modules/user/js/user.permissions.js:155
MEDIUM	semgrep	Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution. Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).	35	/core/lib/Drupal/Component/Plugin/Discovery/AttributeClassDiscovery.php:91
MEDIUM	semgrep	Using user input when deleting files with `unlink()` is potentially dangerous. A malicious actor could use this to modify or access files they have no right to.	7	/core/lib/Drupal/Component/PhpStorage/MTimeProtectedFastFileStorage.php:173
LOW	semgrep	Translated strings will not be escaped when rendered in a template. This leads to a vulnerability where translators could include malicious script tags in their translations. Consider using `force_escape` to explicitly escape a translated text.	1	/core/modules/workflows/help_topics/workflows overview.html.twig:10
LOW	guarddog	Detects heavy obfuscation techniques commonly used by malware [threat-runtime-obfuscation]	1	/core/assets/vendor/transliteration/bundle.umd.min.js:1
LOW	yara	YARA rule matched: detect_downloader — Downloads a remote resource - common and low-signal alone; see detect_download_and_execute for the composite version	1	/core/INSTALL.txt

How to read this report

- **This is a static scan.** The code was read, never executed. Behaviour that only appears at runtime is outside what any of these detectors can see.
- **Findings are not all equally real.** A classifier rates each finding on how likely it is to be genuine rather than noise, and that rating weights the scores. Measured against a hand-reviewed sample it reached precision 0.52 and recall 0.62 — useful for ranking, not a verdict on any single finding.
- **A high score is not proof of malice.** Security tools, penetration-testing frameworks and malware research repositories contain the same patterns as real malware by design. The two risk types above exist to keep that distinction visible.
- **Absence of findings is not proof of safety.** A detector that is not installed, or a language none of them parse, produces silence rather than a warning.
- **This scan is a snapshot.** The repository may have changed since 24 September 2026.