

Rails application audit

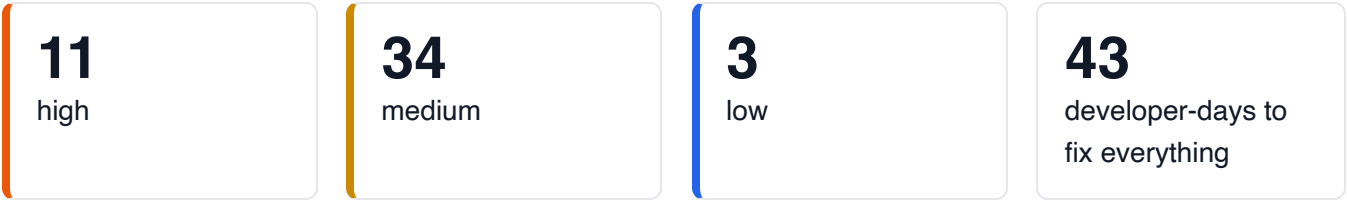
forem

Published as	A sample report, not a client engagement
Application	forem/forem (public, open source)
Revision examined	ea1291b
Code examined on	October 1, 2026
Prepared by	The Still River Software Company, LLC
Report version	1.0

Sample report. This is an audit of the public open-source codebase forem/forem as it was at the revision and on the date above, published to show what a client receives. Its maintainers did not commission it and are not a client. The findings come from the published code alone: how the project's own servers are configured is not visible from it. No client's report is published, in any form, without their written permission.

Where you stand

No critical issues were found, but 11 high issues should be scheduled soon.



What matters most

- 1. A third-party component the application depends on has a published security flaw. **HIGH**
- 2. The framework version is in its final support phase and will stop receiving security fixes. **MEDIUM**
- 3. Whether the application insists on an encrypted connection depends on a setting that could not be confirmed from the code. **MEDIUM**

If nothing is done

If nothing is done, expect the high-severity items to become urgent within the next 6 to 12 months, as support periods end and the distance to a supported setup grows.

What we examined

24 conditions examined across 4 areas. **14 passed.**

A passed condition is a place you do not need to spend money.

AREA	EXAMINED	PASSED	FAILED	NOT ASSESSABLE
Known vulnerabilities in Ruby dependencies	1	0	1	0
Security configuration	15	12	3	0
Rails and Ruby versions	6	2	4	0
Rails upgrade path	2	0	2	0

Also reviewed

These areas were reviewed as a whole rather than condition by condition.

AREA	RESULT
Known vulnerabilities in JavaScript dependencies	Needs work
Automated tests	No concerns
Continuous integration	Needs attention
Deployment	No concerns
Monitoring and error tracking	No concerns
Dependency freshness	Needs work
Database schema	Needs work
Code quality tooling	No concerns

The work

Each block below is a piece of work that can be approved or declined on its own. Together they come to **43 developer-days**.

1. Immediate security remediation

8 developer-days

Closes the known, publicly documented ways into the application before anything else is built on top of it.

Closes 11 findings, the most serious rated **HIGH**

2. Framework currency

15 developer-days

Returns the application to versions that still receive security fixes, which every later improvement depends on.

Closes 6 findings, the most serious rated **MEDIUM**

3. Engineering foundation

20 developer-days

Puts in place the automated checks that stop these problems from coming back once they are fixed.

Closes 31 findings, the most serious rated **MEDIUM**

Order and dependencies

None of these blocks depends on another, so they can be done in any order or in parallel. This is the order we recommend.

1. **Immediate security remediation** (8 developer-days)
2. **Framework currency** (15 developer-days)
3. **Engineering foundation** (20 developer-days)

Findings register

Every finding, grouped by the block of work that closes it, in the order we would fix them: most risk removed per hour first.

Immediate security remediation

HIGH	Known vulnerability in faraday
Evidence	Gemfile.lock pins faraday 2.14.2, which is affected by CVE-2026-54297: Faraday - Uncontrolled recursion in NestedParamsEncoder allows stack exhaustion DoS via deeply nested query parameters.
Where	Gemfile.lock : faraday (2.14.2)
Impact	The application runs faraday 2.14.2, which has a published vulnerability rated high (CVE-2026-54297). Flaws at this rating typically let an attacker read or change data, or take the application down, under conditions that are realistic for an internet-facing app. The details are public.
Remediation	Upgrade faraday to a patched release (~> 1.10.6, >= 2.14.3) with bundle update faraday , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54297
Estimate	4 hours

HIGH	Known vulnerability in faraday-http-cache
Evidence	Gemfile.lock pins faraday-http-cache 2.7.0, which is affected by GHSA-p8jg-8p9f-pgmr: Cache entries deserialized with JSON.load can instantiate arbitrary classes named by an origin server.
Where	Gemfile.lock : faraday-http-cache (2.7.0)
Impact	The application runs faraday-http-cache 2.7.0, which has a published vulnerability rated high (GHSA-p8jg-8p9f-pgmr). Flaws at this rating typically let an attacker read or change data, or take the application down, under conditions that are realistic for an internet-facing app. The details are public.
Remediation	Upgrade faraday-http-cache to a patched release (>= 2.8.0) with bundle update faraday-http-cache , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/sourcelevel/faraday-http-cache/security/advisories/GHSA-p8jg-8p9f-pgmr
Estimate	4 hours

HIGH Known vulnerability in httparty

Evidence	Gemfile.lock pins httparty 0.21.0, which is affected by CVE-2025-68696: httparty Has Potential SSRF Vulnerability That Leads to API Key Leakage.
Where	<code>Gemfile.lock</code> : httparty (0.21.0)
Impact	The application runs httparty 0.21.0, which has a published vulnerability rated high (CVE-2025-68696). Flaws at this rating typically let an attacker read or change data, or take the application down, under conditions that are realistic for an internet-facing app. The details are public.
Remediation	Upgrade httparty to a patched release ($\geq 0.24.0$) with <code>bundle update httparty</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/jnunemaker/httparty/security/advisories/GHSA-hm5p-x4rq-38w4
Estimate	4 hours

HIGH Known vulnerability in oauth

Evidence	Gemfile.lock pins oauth 0.5.10, which is affected by CVE-2026-54605: Cross-origin OAuth token-request redirects can expose signed request metadata.
Where	<code>Gemfile.lock</code> : oauth (0.5.10)
Impact	The application runs oauth 0.5.10, which has a published vulnerability rated high (CVE-2026-54605). Flaws at this rating typically let an attacker read or change data, or take the application down, under conditions that are realistic for an internet-facing app. The details are public.
Remediation	Upgrade oauth to a patched release ($\geq 1.1.6$) with <code>bundle update oauth</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://nvd.nist.gov/vuln/detail/CVE-2026-54605
Estimate	4 hours

HIGH Known vulnerability in oauth2

Evidence	Gemfile.lock pins oauth2 2.0.9, which is affected by CVE-2026-54603: OAuth2::Client#request: Protocol-relative redirect Location overrides authority, leaking bearer Authorization to attacker host.
Where	<code>Gemfile.lock</code> : oauth2 (2.0.9)
Impact	The application runs oauth2 2.0.9, which has a published vulnerability rated high (CVE-2026-54603). Flaws at this rating typically let an attacker read or change data, or take the application down, under conditions that are realistic for an internet-facing app. The details are public.
Remediation	Upgrade oauth2 to a patched release ($\geq 2.0.22$) with <code>bundle update oauth2</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://nvd.nist.gov/vuln/detail/CVE-2026-54603
Estimate	4 hours

HIGH Known vulnerability in oj

Evidence	Gemfile.lock pins oj 3.16.3, which is affected by CVE-2026-54592: Oj - Stack Buffer Overflow in Oj::Doc#each_child via Deeply Nested Input.
Where	<code>Gemfile.lock</code> : oj (3.16.3)
Impact	The application runs oj 3.16.3, which has a published vulnerability rated high (CVE-2026-54592). Flaws at this rating typically let an attacker read or change data, or take the application down, under conditions that are realistic for an internet-facing app. The details are public.
Remediation	Upgrade oj to a patched release ($\geq 3.17.3$) with <code>bundle update oj</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54592
Estimate	4 hours

HIGH Known vulnerability in puma

Evidence	Gemfile.lock pins puma 5.6.9, which is affected by CVE-2026-47736: Puma PROXY Protocol v1 Parser Allows Remote Memory Exhaustion.
Where	<code>Gemfile.lock</code> : puma (5.6.9)
Impact	The application runs puma 5.6.9, which has a published vulnerability rated high (CVE-2026-47736). Flaws at this rating typically let an attacker read or change data, or take the application down, under conditions that are realistic for an internet-facing app. The details are public.
Remediation	Upgrade puma to a patched release ($\sim 7.2.1$, $\geq 8.0.2$) with <code>bundle update puma</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord?id=CVE-2026-47736
Estimate	4 hours

HIGH Known vulnerability in puma

Evidence	Gemfile.lock pins puma 5.6.9, which is affected by CVE-2026-47737: Puma PROXY Protocol v1 Accepts Repeated Protocol Headers on Persistent Connections.
Where	<code>Gemfile.lock</code> : puma (5.6.9)
Impact	The application runs puma 5.6.9, which has a published vulnerability rated high (CVE-2026-47737). Flaws at this rating typically let an attacker read or change data, or take the application down, under conditions that are realistic for an internet-facing app. The details are public.
Remediation	Upgrade puma to a patched release ($\sim 7.2.1$, $\geq 8.0.2$) with <code>bundle update puma</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-47737
Estimate	4 hours

HIGH Known vulnerability in rubyzip

Evidence	Gemfile.lock pins rubyzip 2.4.1, which is affected by CVE-2026-85396: path traversal vulnerability in pre-3.4.0 rubyzip gem.
Where	<code>Gemfile.lock</code> : rubyzip (2.4.1)
Impact	The application runs rubyzip 2.4.1, which has a published vulnerability rated high (CVE-2026-85396). Flaws at this rating typically let an attacker read or change data, or take the application down, under conditions that are realistic for an internet-facing app. The details are public.
Remediation	Upgrade rubyzip to a patched release ($\geq 3.4.0$) with <code>bundle update rubyzip</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://nvd.nist.gov/vuln/detail/CVE-2026-85396
Estimate	4 hours

HIGH Known vulnerability in websocket-driver

Evidence	Gemfile.lock pins websocket-driver 0.7.7, which is affected by CVE-2026-61666: Denial of service via malformed Host header.
Where	<code>Gemfile.lock</code> : websocket-driver (0.7.7)
Impact	The application runs websocket-driver 0.7.7, which has a published vulnerability rated high (CVE-2026-61666). Flaws at this rating typically let an attacker read or change data, or take the application down, under conditions that are realistic for an internet-facing app. The details are public.
Remediation	Upgrade websocket-driver to a patched release ($\geq 0.8.2$) with <code>bundle update websocket-driver</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord?id=CVE-2026-61666
Estimate	4 hours

HIGH Known vulnerability in yard

Evidence	Gemfile.lock pins yard 0.9.36, which is affected by CVE-2026-41493: Possible arbitrary path traversal and file access via yard server.
Where	<code>Gemfile.lock</code> : yard (0.9.36)
Impact	The application runs yard 0.9.36, which has a published vulnerability rated high (CVE-2026-41493). Flaws at this rating typically let an attacker read or change data, or take the application down, under conditions that are realistic for an internet-facing app. The details are public.
Remediation	Upgrade yard to a patched release ($\geq 0.9.42$) with <code>bundle update yard</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://nvd.nist.gov/vuln/detail/CVE-2026-41493
Estimate	4 hours

Framework currency

MEDIUM Rails 8.0.5 receives security fixes only

Evidence	Gemfile.lock pins rails 8.0.5. The 8.0 series is in security-only maintenance.
Where	<code>Gemfile.lock</code>
Impact	The application runs Rails 8.0.5. The 8.0 series still gets security patches but no bug fixes, and it is the next series to reach end of life. Nothing is exposed today.
Remediation	Schedule the upgrade to the next Rails series now, while it is one version away (the current release is 8.1.4). Clear the deprecation warnings on the current version first; they are the upgrade's to-do list.
Estimate	Counted in the upgrade steps

LOW Rails 8.0.5 is behind the latest 8.0 patch release

Evidence	Gemfile.lock pins rails 8.0.5. The latest 8.0 release is 8.0.5.1.
Where	<code>Gemfile.lock</code>
Impact	The application runs Rails 8.0.5 and the latest release in the same series is 8.0.5.1. Patch releases carry bug fixes and security fixes and are designed to be drop-in.
Remediation	Run <code>bundle update rails --conservative</code> to move to 8.0.5.1, run the test suite, and deploy.
Estimate	1 hour

LOW Ruby 3.3.0 is behind the latest 3.3 patch release

Evidence	The repository pins Ruby 3.3.0. The latest 3.3 release is 3.3.12.
Where	<code>.ruby-version</code>
Impact	The application runs on Ruby 3.3.0 and the latest release in the same series is 3.3.12. Ruby patch releases carry bug fixes and security fixes and do not change behaviour.
Remediation	Update <code>.ruby-version</code> (and the Dockerfile, if there is one) to 3.3.12, run <code>bundle install</code> , run the test suite, and deploy.
Estimate	1 hour

MEDIUM Upgrade Rails 8.0 to 8.1

Evidence	The next Rails series after 8.0 is 8.1 (latest 8.1.4). Rails 8.1 needs Ruby 3.2.0 or newer, which the application already meets. No gem in the Gemfile blocks this step.
Where	<code>Gemfile.lock</code>
Impact	This step is part of the route from a series that gets security fixes only to one that is fully maintained. Rails upgrades go one minor release at a time, and each has to be deployed and stable before the next begins.
Why medium	Rails 8.0 receives security fixes only
Remediation	Clear the deprecation warnings Rails 8.0 prints, upgrade or replace the blocking gems listed in the evidence, then move to 8.1.4 with <code>bundle update rails</code> and <code>bin/rails app:update</code> , reviewing each changed file. Run on the old framework defaults first (<code>config.load_defaults "8.0"</code>), deploy, and switch the defaults over once it is stable. Do not start the next step until this one is in production.
Estimate	16 hours

MEDIUM 39 gems look abandoned

Evidence	No release in over two years, or the repository is archived: <code>better_errors</code> (last release 2023-06-14), <code>capypara</code> (last release 2024-01-27), <code>carrierwave-bombshelter</code> (repository archived), <code>cld3</code> (repository archived), <code>ddtrace</code> (last release 2024-07-01), <code>email_validator</code> (last release 2022-11-09), <code>emoji_regex</code> (last release 2023-04-05), <code>fakereidis</code> (last release 2023-05-04), <code>front_matter_parser</code> (last release 2021-07-20), <code>gemoji</code> (last release 2023-03-29), <code>guard-rspec</code> (last release 2016-07-29), <code>honeycomb-beeline</code> (repository archived), <code>html_truncator</code> (last release 2017-11-30), <code>imgproxy</code> (last release 2023-12-28), <code>inline_svg</code> (last release 2024-09-03), <code>jsbundling-rails</code> (last release 2024-07-29), <code>jsonapi-serializer</code> (last release 2021-03-11), <code>kaminari</code> (last release 2021-12-25), <code>memory_profiler</code> (last release 2024-09-17), <code>nakayoshi_fork</code> (last release 2018-04-13), <code>omniauth-github</code> (last release 2022-09-23), <code>pry-rails</code> (last release 2024-06-20), <code>rack-host-redirect</code> (last release 2017-04-04), <code>rack-timeout</code> (last release 2024-05-20), <code>rails-controller-testing</code> (last release 2020-06-23), <code>request_store</code> (last release 2024-05-01), <code>rolify</code> (last release 2023-02-02), <code>rpush-redis</code> (last release 2021-04-29), <code>rspec-retry</code> (repository archived), <code>rspec_junit_formatter</code> (last release 2022-09-29), <code>s3_direct_upload</code> (last release 2014-03-13), <code>sassc-rails</code> (repository archived), <code>slack-notifier</code> (last release 2021-05-07), <code>sprockets-rails</code> (last release 2024-07-31), <code>sterile</code> (last release 2024-02-20), <code>validate_url</code> (last release 2022-05-13), <code>wcag_color_contrast</code> (last release 2017-11-13), <code>yard-activesupport-concern</code> (last release 2015-06-02), and <code>zonebie</code> (last release 2016-04-13).
Where	<code>Gemfile.lock</code>
Impact	An archived repository means the author has stopped: there will be no fix for the next security flaw found in it, and no release that supports a newer Rails or Ruby. Gems like this are what turn a routine framework upgrade into a rewrite of whatever they did.
Why medium	5 of these have an archived repository, so no fix will ever be released
Remediation	For each gem, check whether it still works on current Rails and Ruby and whether anyone is maintaining a fork. Keep the ones that are simply finished. Replace the archived ones, and any that block an upgrade step, with a maintained alternative or a small amount of in-house code.
Estimate	54 hours

LOW Ruby 3.3.0 receives security fixes only

Evidence	The repository pins Ruby 3.3.0. The 3.3 series is in security-only maintenance.
Where	<code>.ruby-version</code>
Impact	The application runs on Ruby 3.3.0. The 3.3 series gets security patches but no bug fixes, and it is the next to reach end of life. Nothing is exposed today.
Remediation	Schedule the upgrade to the next Ruby series (the current release is 4.0.7). For most applications this is a small, well-understood change when done one version at a time.
Estimate	16 hours

Engineering foundation

MEDIUM HTTPS enforcement could not be confirmed from the code

Where	<code>config/environments/production.rb</code>
Impact	The code does not itself require an encrypted connection; that is left to the deployment. If it is not enforced there either, anyone positioned on the network between a user and the server can read session cookies and submitted form data, including passwords.
Why medium	<code>config.force_ssl</code> is set from <code>ENV["FORCE_SSL_IN_RAILS"] == "true"</code> , not to <code>true</code> , so whether HTTPS is enforced depends on how the application is deployed. Confirm it is on in production.
Remediation	Confirm how production is configured. If HTTPS is enforced there, record where; otherwise set <code>config.force_ssl = true</code> in <code>config/environments/production.rb</code> , after confirming the load balancer forwards X-Forwarded-Proto, or every request will redirect in a loop.
Estimate	1 hour

MEDIUM Sensitive parameters may be written to the logs

Where	<code>config/initializers/filter_parameter_logging.rb</code>
Impact	The log filter list is missing or minimal, so submitted values such as tokens, secrets and card details can be written to the production log in plain text. Logs are usually readable by more people and kept for longer than the database, and are often shipped to a third party.
Remediation	Extend <code>config.filter_parameters</code> in <code>config/initializers/filter_parameter_logging.rb</code> to cover passwords, tokens, secrets, keys and payment fields.
Estimate	1 hour

MEDIUM Secret files are not excluded from version control

Evidence	<code>.gitignore</code> does not exclude: <code>master.key</code> .
Where	<code>.gitignore</code>
Impact	<code>.gitignore</code> does not exclude <code>master.key</code> . Those files hold secrets, and nothing stops them being committed alongside the code.
Remediation	Add <code>master.key</code> to <code>.gitignore</code> , then check that none of them is already tracked with <code>git ls-files</code> .
Estimate	1 hour

MEDIUM Known vulnerability in `activestorage`

Evidence	<code>Gemfile.lock</code> pins <code>activestorage</code> 8.0.5, which is affected by CVE-2026-66066: Possible arbitrary file read and remote code execution in Active Storage variant processing.
Where	<code>Gemfile.lock</code> : <code>activestorage</code> (8.0.5)
Impact	The application runs <code>activestorage</code> 8.0.5, which has a published vulnerability (CVE-2026-66066). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade <code>activestorage</code> to a patched release (<code>~> 7.2.3, >= 7.2.3.2, ~> 8.0.5, >= 8.0.5.1, >= 8.1.3.1</code>) with <code>bundle update activestorage</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-66066
Estimate	4 hours

MEDIUM Known vulnerability in `bcrypt`

Evidence	<code>Gemfile.lock</code> pins <code>bcrypt</code> 3.1.20, which is affected by CVE-2026-33306: <code>bcrypt-ruby</code> has an Integer Overflow that Causes Zero Key-Strengthening Iterations at Cost=31 on JRuby.
Where	<code>Gemfile.lock</code> : <code>bcrypt</code> (3.1.20)
Impact	The application runs <code>bcrypt</code> 3.1.20, which has a published vulnerability (CVE-2026-33306). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade <code>bcrypt</code> to a patched release (<code>>= 3.1.22</code>) with <code>bundle update bcrypt</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/advisories/GHSA-f27w-vcwj-c954
Estimate	4 hours

MEDIUM Known vulnerability in blazer

Evidence	Gemfile.lock pins blazer 2.6.5, which is affected by GHSA-m5f6-4589-m89f: Stored XSS vulnerability.
Where	<code>Gemfile.lock</code> : blazer (2.6.5)
Impact	The application runs blazer 2.6.5, which has a published vulnerability (GHSA-m5f6-4589-m89f). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade blazer to a patched release ($\geq 3.5.0$) with <code>bundle update blazer</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/ankane/blazer/security/advisories/GHSA-m5f6-4589-m89f
Estimate	4 hours

MEDIUM Known vulnerability in devise

Evidence	Gemfile.lock pins devise 4.9.4, which is affected by CVE-2026-32700: Confirmable "change email" race condition permits user to confirm email they have no access to.
Where	<code>Gemfile.lock</code> : devise (4.9.4)
Impact	The application runs devise 4.9.4, which has a published vulnerability (CVE-2026-32700). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade devise to a patched release ($\geq 5.0.3$) with <code>bundle update devise</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/heartcombo/devise/security/advisories/GHSA-57hq-95w6-v4fc
Estimate	4 hours

MEDIUM Known vulnerability in devise

Evidence	Gemfile.lock pins devise 4.9.4, which is affected by CVE-2026-40295: Devise has an Open Redirect via Unvalidated <code>request.referrer</code> in Timeoutable Session Timeout Handler.
Where	<code>Gemfile.lock</code> : devise (4.9.4)
Impact	The application runs devise 4.9.4, which has a published vulnerability (CVE-2026-40295). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade devise to a patched release ($\geq 5.0.4$) with <code>bundle update devise</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/heartcombo/devise/security/advisories/GHSA-jp94-3292-c3xv
Estimate	4 hours

MEDIUM Known vulnerability in excon

Evidence	Gemfile.lock pins excon 0.104.0, which is affected by CVE-2026-54171: redact additional sensitive/risky headers when following redirects.
Where	<code>Gemfile.lock</code> : excon (0.104.0)
Impact	The application runs excon 0.104.0, which has a published vulnerability (CVE-2026-54171). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade excon to a patched release ($\geq 1.5.0$) with <code>bundle update excon</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord?id=CVE-2026-54171
Estimate	4 hours

MEDIUM Known vulnerability in faraday-http-cache

Evidence	Gemfile.lock pins faraday-http-cache 2.7.0, which is affected by GHSA-c33f-42f2-gwcc: Shared cache serves responses to authenticated requests to other callers.
Where	<code>Gemfile.lock</code> : faraday-http-cache (2.7.0)
Impact	The application runs faraday-http-cache 2.7.0, which has a published vulnerability (GHSA-c33f-42f2-gwcc). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade faraday-http-cache to a patched release ($\geq 2.8.0$) with <code>bundle update faraday-http-cache</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/sourcelevel/faraday-http-cache/security/advisories/GHSA-c33f-42f2-gwcc
Estimate	4 hours

MEDIUM Known vulnerability in loofah

Evidence	Gemfile.lock pins loofah 2.25.1, which is affected by GHSA-5qhf-9phg-95m2: Loofah <code>allowed_uri?</code> does not detect <code>javascript:</code> URIs split by numeric character references without semicolons.
Where	<code>Gemfile.lock</code> : loofah (2.25.1)
Impact	The application runs loofah 2.25.1, which has a published vulnerability (GHSA-5qhf-9phg-95m2). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade loofah to a patched release ($\geq 2.25.2$) with <code>bundle update loofah</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/flavorjones/loofah/security/advisories/GHSA-5qhf-9phg-95m2
Estimate	4 hours

MEDIUM Known vulnerability in loofah

Evidence	Gemfile.lock pins loofah 2.25.1, which is affected by GHSA-8whx-365g-h9vv: Loofah <code>allowed_uri?</code> does not detect <code>javascript:</code> URIs split by named whitespace character references.
Where	<code>Gemfile.lock</code> : loofah (2.25.1)
Impact	The application runs loofah 2.25.1, which has a published vulnerability (GHSA-8whx-365g-h9vv). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade loofah to a patched release ($\geq 2.25.2$) with <code>bundle update loofah</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/flavorjones/loofah/security/advisories/GHSA-8whx-365g-h9vv
Estimate	4 hours

MEDIUM Known vulnerability in loofah

Evidence	Gemfile.lock pins loofah 2.25.1, which is affected by GHSA-9wjq-cp2p-hrgf: SVG <code>href</code> attribute bypasses local-reference restriction in Loofah.
Where	<code>Gemfile.lock</code> : loofah (2.25.1)
Impact	The application runs loofah 2.25.1, which has a published vulnerability (GHSA-9wjq-cp2p-hrgf). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade loofah to a patched release ($\geq 2.25.2$) with <code>bundle update loofah</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/flavorjones/loofah/security/advisories/GHSA-9wjq-cp2p-hrgf
Estimate	4 hours

MEDIUM Known vulnerability in mail

Evidence	Gemfile.lock pins mail 2.9.0, which is affected by GHSA-mvxx-6m87-mv2q: Email address spoofing via malformed RFC 2047 encoded-words in mail.
Where	<code>Gemfile.lock</code> : mail (2.9.0)
Impact	The application runs mail 2.9.0, which has a published vulnerability (GHSA-mvxx-6m87-mv2q). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade mail to a patched release ($\geq 2.9.1$) with <code>bundle update mail</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/mikel/mail/security/advisories/GHSA-mvxx-6m87-mv2q
Estimate	4 hours

MEDIUM	Known vulnerability in oj
Evidence	Gemfile.lock pins oj 3.16.3, which is affected by CVE-2026-54500: Oj - intern.c form_attr (uninitialized stack read).
Where	Gemfile.lock : oj (3.16.3)
Impact	The application runs oj 3.16.3, which has a published vulnerability (CVE-2026-54500). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade oj to a patched release ($\geq$ 3.17.3) with <code>bundle update oj</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54500
Estimate	4 hours

MEDIUM	Known vulnerability in oj
Evidence	Gemfile.lock pins oj 3.16.3, which is affected by CVE-2026-54502: Oj - Stack Buffer Overflow in Oj.dump via Large Indent.
Where	Gemfile.lock : oj (3.16.3)
Impact	The application runs oj 3.16.3, which has a published vulnerability (CVE-2026-54502). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade oj to a patched release ($\geq$ 3.17.3) with <code>bundle update oj</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54502
Estimate	4 hours

MEDIUM	Known vulnerability in oj
Evidence	Gemfile.lock pins oj 3.16.3, which is affected by CVE-2026-54896: Oj - Heap Buffer Overflow in Oj.dump Exception Serialization via Large Indent.
Where	Gemfile.lock : oj (3.16.3)
Impact	The application runs oj 3.16.3, which has a published vulnerability (CVE-2026-54896). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade oj to a patched release ($\geq$ 3.17.3) with <code>bundle update oj</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54896
Estimate	4 hours

MEDIUM Known vulnerability in oj	
Evidence	Gemfile.lock pins oj 3.16.3, which is affected by CVE-2026-54897: Oj - Use-After-Free in Oj::Doc Iterators via Reentrant Close.
Where	Gemfile.lock : oj (3.16.3)
Impact	The application runs oj 3.16.3, which has a published vulnerability (CVE-2026-54897). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade oj to a patched release ($\geq$ 3.17.3) with <code>bundle update oj</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54897
Estimate	4 hours

MEDIUM Known vulnerability in oj	
Evidence	Gemfile.lock pins oj 3.16.3, which is affected by CVE-2026-54898: Oj - Use-After-Free in Oj::Parser SAJ Callback via Input Mutation.
Where	Gemfile.lock : oj (3.16.3)
Impact	The application runs oj 3.16.3, which has a published vulnerability (CVE-2026-54898). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade oj to a patched release ($\geq$ 3.17.3) with <code>bundle update oj</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54898
Estimate	4 hours

MEDIUM Known vulnerability in oj	
Evidence	Gemfile.lock pins oj 3.16.3, which is affected by CVE-2026-54899: Oj - Use-After-Free in Oj::Parser Symbol Key Cache Toggle.
Where	Gemfile.lock : oj (3.16.3)
Impact	The application runs oj 3.16.3, which has a published vulnerability (CVE-2026-54899). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade oj to a patched release ($\geq$ 3.17.3) with <code>bundle update oj</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54899
Estimate	4 hours

MEDIUM	Known vulnerability in oj
Evidence	Gemfile.lock pins oj 3.16.3, which is affected by CVE-2026-54900: Oj - Negative-Size memcpy in 'Oj::Parser' create_id Attribute Handling.
Where	Gemfile.lock : oj (3.16.3)
Impact	The application runs oj 3.16.3, which has a published vulnerability (CVE-2026-54900). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade oj to a patched release ($\geq$ 3.17.3) with <code>bundle update oj</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54900
Estimate	4 hours

MEDIUM	Known vulnerability in oj
Evidence	Gemfile.lock pins oj 3.16.3, which is affected by CVE-2026-54901: Oj - Use-After-Free in 'Oj::Parser' array_class/hash_class GC Marking.
Where	Gemfile.lock : oj (3.16.3)
Impact	The application runs oj 3.16.3, which has a published vulnerability (CVE-2026-54901). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade oj to a patched release ($\geq$ 3.17.3) with <code>bundle update oj</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54901
Estimate	4 hours

MEDIUM	Known vulnerability in oj
Evidence	Gemfile.lock pins oj 3.16.3, which is affected by CVE-2026-54902: Oj - Use-After-Free in 'Oj::Parser' SAJ Long Key Callback.
Where	Gemfile.lock : oj (3.16.3)
Impact	The application runs oj 3.16.3, which has a published vulnerability (CVE-2026-54902). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade oj to a patched release ($\geq$ 3.17.3) with <code>bundle update oj</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54902
Estimate	4 hours

MEDIUM	Known vulnerability in oj
Evidence	Gemfile.lock pins oj 3.16.3, which is affected by CVE-2026-54903: Oj - Integer Overflow in Oj.load 2GB String Handling.
Where	Gemfile.lock : oj (3.16.3)
Impact	The application runs oj 3.16.3, which has a published vulnerability (CVE-2026-54903). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade oj to a patched release ($\geq$ 3.17.3) with <code>bundle update oj</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54903
Estimate	4 hours

MEDIUM	Known vulnerability in rails-html-sanitizer
Evidence	Gemfile.lock pins rails-html-sanitizer 1.7.0, which is affected by GHSA-cj75-f6xr-r4g7: Possible XSS vulnerability with certain configurations of rails-html-sanitizer.
Where	Gemfile.lock : rails-html-sanitizer (1.7.0)
Impact	The application runs rails-html-sanitizer 1.7.0, which has a published vulnerability (GHSA-cj75-f6xr-r4g7). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade rails-html-sanitizer to a patched release ($\geq$ 1.7.1) with <code>bundle update rails-html-sanitizer</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/rails/rails-html-sanitizer/security/advisories/GHSA-cj75-f6xr-r4g7
Estimate	4 hours

MEDIUM	Known vulnerability in rexml
Evidence	Gemfile.lock pins rexml 3.4.0, which is affected by CVE-2025-58767: REXML has DoS condition when parsing malformed XML file.
Where	Gemfile.lock : rexml (3.4.0)
Impact	The application runs rexml 3.4.0, which has a published vulnerability (CVE-2025-58767). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade rexml to a patched release ($\geq$ 3.4.2) with <code>bundle update rexml</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/ruby/rexml/security/advisories/GHSA-c2f4-jgmc-q2r5
Estimate	4 hours

MEDIUM	Known vulnerability in sidekiq-cron
Evidence	Gemfile.lock pins sidekiq-cron 1.12.0, which is affected by CVE-2025-67202: Sidekiq-cron is vulnerable to a cross-site scripting (xss) vulnerability via crafted URL.
Where	Gemfile.lock : sidekiq-cron (1.12.0)
Impact	The application runs sidekiq-cron 1.12.0, which has a published vulnerability (CVE-2025-67202). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade sidekiq-cron to a patched release ($\geq 2.4.0$) with <code>bundle update sidekiq-cron</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://github.com/advisories/GHSA-xv9c-mjw8-79gf
Estimate	4 hours

MEDIUM	Known vulnerability in websocket-driver
Evidence	Gemfile.lock pins websocket-driver 0.7.7, which is affected by CVE-2026-54463: Memory exhaustion via abuse of protocol length headers.
Where	Gemfile.lock : websocket-driver (0.7.7)
Impact	The application runs websocket-driver 0.7.7, which has a published vulnerability (CVE-2026-54463). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade websocket-driver to a patched release ($\geq 0.8.1$) with <code>bundle update websocket-driver</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54463
Estimate	4 hours

MEDIUM	Known vulnerability in websocket-driver
Evidence	Gemfile.lock pins websocket-driver 0.7.7, which is affected by CVE-2026-54464: Resource limit bypass via message compression.
Where	Gemfile.lock : websocket-driver (0.7.7)
Impact	The application runs websocket-driver 0.7.7, which has a published vulnerability (CVE-2026-54464). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade websocket-driver to a patched release ($\geq 0.8.1$) with <code>bundle update websocket-driver</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54464
Estimate	4 hours

MEDIUM	Known vulnerability in websocket-driver
Evidence	Gemfile.lock pins websocket-driver 0.7.7, which is affected by CVE-2026-54465: Memory exhaustion in HTTP header parser.
Where	Gemfile.lock : websocket-driver (0.7.7)
Impact	The application runs websocket-driver 0.7.7, which has a published vulnerability (CVE-2026-54465). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade websocket-driver to a patched release ($\geq 0.8.1$) with <code>bundle update websocket-driver</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://www.cve.org/CVERecord/SearchResults?query=CVE-2026-54465
Estimate	4 hours

MEDIUM	Known vulnerability in yard
Evidence	Gemfile.lock pins yard 0.9.36, which is affected by CVE-2026-49342: YARD static cache reads raw traversal paths before router sanitization.
Where	Gemfile.lock : yard (0.9.36)
Impact	The application runs yard 0.9.36, which has a published vulnerability (CVE-2026-49342). Whether it can be used against this application depends on how the gem is used, but the flaw is public and automated scanners look for exactly this version.
Remediation	Upgrade yard to a patched release ($\geq 0.9.44$) with <code>bundle update yard</code> , run the test suite, and deploy. If the patched release is a major version ahead, read its changelog first. Advisory: https://nvd.nist.gov/vuln/detail/CVE-2026-49342
Estimate	4 hours

Also reviewed

The areas below were reviewed as a whole. Each line is the result as recorded.

AREA	RESULT
Known vulnerabilities in JavaScript dependencies	153 JS vulnerabilities (3 critical, 86 high, 54 medium, 10 low) Node 20 (eol) via yarn.lock
Automated tests	RSpec suite: 847 specs for 774 code files (0.59 ratio). 85 system/integration tests. SimpleCov, FactoryBot, WebMock, Capybara, Faker, Shoulda configured.
Continuous integration	6/7 CI/CD checks passed (1 not implemented: 1 medium)
Deployment	7 of 10 deployment checks passed (score: 75). Kamal deployment configured, with Docker, sidekiq for background jobs. Issues: no health check endpoint, no encrypted credentials, local file storage only.
Monitoring and error tracking	Sentry error tracking. Datadog performance monitoring. Logtail structured logging. Sidekiq job monitoring (weak signal). 4 of 5 monitoring categories covered.
Dependency freshness	58/170 gems current. 53 major versions behind, 59 minor. 1 git-sourced gem not compared.
Database schema	129 tables, 1397 columns. 18 foreign key column(s) missing indexes (badge_achievements.rewarder_id, credits.organization_id, credits.user_id, display_ad_events.article_id, display_ads.audience_segment_id). 9 foreign key column(s) covered only as trailing column of a composite index (badge_achievements.badge_id, identities.user_id, mentions.mentionable_id, organization_memberships.organization_id, podcast_episode_appearances.user_id). 16 commonly-queried column(s) missing indexes (audit_logs.slug, classified_listings.slug, data_update_scripts.status). Wide tables: articles (94 cols), display_ads (45 cols), feed_configs (38 cols), organizations (48 cols), users (91 cols).
Code quality tooling	6 code quality tools detected: RuboCop or StandardRB, Linter configuration file, ERB linting, Brakeman, bundler-audit, .editorconfig. Score: 75.