Raising The Security Bar with Guardr

BALTIMORE
DRUPALCON 2017
APRIL 24-28, 2017

Mediacurrent

Mark Shropshire

Open Source Security Lead

Mark is the lead maintainer of Guardr, a suite of modules predicated around Drupal security. He is passionate about architecting systems to solve workflow problems and improve efficiencies using open source software.

Over his 20 year career leading technical teams, Mark gained experience in IT roles at a large urban research university and nationally recognized, award winning graphic communications company. Through these experiences, Mark has learned to lead others with an eye on the big picture, while getting into the details as a software developer, systems architect and system administrator.

@shrop

/in/markshropshire

shrop

About Mediacurrent

Mediacurrent helps organizations build highly impactful, elegantly designed Drupal websites that achieve the strategic results they need.

- Single-source provider
- Specializing in Drupal since 2007
- Headquartered in Atlanta, GA
- Team of 70+ Drupal Experts including development, design and strategy
- Clients include: Large Enterprise and high-profile global brands

Support
Design
Training
Development
Strategy

Agenda

I. What is Guardr?
II. Why Use Guardr?
III. Security Features
IV. Demonstration
V. How to Contribute

What is Guardr?

Distribution

Guardr is a Drupal distribution with a combination of modules and settings to enhance a Drupal application's security and availability to meet enterprise security requirements.

https://drupal.org/project/guardr

Philosophy

Guardr follows the **CIA Information Security Triad**: confidentiality, integrity and availability. From Wikipedia:

> For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.

Philosophy

OWASP Top 10 Most Critical Web Application Security Risks

- Injection
- Weak authentication and session management
- XSS
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross Site Request Forgery
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards

OWASP
Open Web Application
Security Project

Source: OWASP

How Modules Are Selected

- Does the module fulfill a part of the CIA Information Security Triad?
- Does the module address an OWASP Top 10
- Previous experience with the module?
- Is the additional module worth the attack surface increase?
- Stable release?

What to Expect After Installation

- Fully working Drupal installation
- Based on the Standard Drupal install profile
- Select Guardr modules enabled by default
- Other optional Guardr modules can be enabled as desired
- Guardr recommended settings

Why Use Guardr?

Security Is Hard!

Source: CC Image by Alan Levine on Flickr

Users, system complexity, and the balance between **security** and **usability** make infosec is very **challenging**.

By 2020, 60% of businesses will suffer a security breach based on internal IT's inability to manage risk, paying an average of $551,000 to recover.

Source: Gartner, Inc.,CC Image by Sébastien Launay on Flickr

NIST

PCI DSS

CISSP

Guardr incorporates industry **best practices** from security standards, regulatory controls, and security certifications.

HIPAA

FERPA

ISO/IEC 27001

Drupal 7 Guardr

For new project installs. Existing installs currently need to borrow settings and recommendations from Guardr.

- Stable release
- Continued support
- Limited new feature releases

Drupal 8 Security Enhancements

Twig template engine
(Prevents SQL injection and XSS)

PHP can only send one query to MySQL at a time (Prevents SQL injection)

Improved session ID and user session management

Default clickjacking prevention

CSRF token protection for the routing system

Configurable trust host patterns (Protects HTTP HOST Header attacks)

Drupal 8 Guardr

For new and existing project installs. Build on top of Drupal 8’s security enhancements.

- Alpha release
- Continued support and new feature releases
- Composer based installs and updates

Security Features

Guardr Recommended Core Configurations

Guardr Core

- **Logging and errors**
  - Database log messages to keep: 1,000,000
- **Account settings**
  - Disable the personal contact form by default for new users.
  - Who can register accounts? Administrators only
- **Update Manager settings**
  - Check for updates of uninstalled modules and themes
  - Email notification threshold: Only security updates

Login Security

Password Policy module

- "A password policy can be defined with a set of constraints which must be met before a user password change will be accepted. Each constraint has a parameter allowing for the minimum number of valid conditions which must be met before the constraint is satisfied."

Login Security module

- "Login Security module improves the security options in the login operation of a Drupal site. By default, Drupal introduces only basic access control denying IP access to the full content of the site."

Login Security

Mass Password Reset module

- “This module allows users with "Administer users" permission to reset all user accounts and notify all users”

Session Management

Automated Logout module

- “This module provides a site administrator the ability to log users out after a specified time of inactivity. It is highly customisable and includes "site policies" by role to enforce logout.“

Session Limit module

- “Session Limit allows administrators to limit the number of simultaneous sessions per user.”

Security Kit

Security Kit module

- “SecKit provides Drupal with various security-hardening options. This lets your mitigate the risks of exploitation of different web application vulnerabilities.”
- Techniques to prevent
  - Cross-site Scripting
  - Cross-site Request Forgery
  - Clickjacking
  - SSL/TLS

System Monitoring, Auditing, and Logging

Login History module

- "Login History adds a new table which stores information about individual user logins, including a timestamp, IP address, user agent information, and whether or not the login was via a reset password link."

Security Review module

- "The Security Review module automates testing for many of the easy-to-make mistakes that render your site insecure."

Additional Features

Diff module

- “This module adds a tab for sufficiently permissioned users. The tab shows all revisions like standard Drupal but it also allows pretty viewing of all added/changed/deleted words between revisions.”

Redirect 403 to User Login module

- “Redirect the HTTP 403 error page to the Drupal /user/login page”

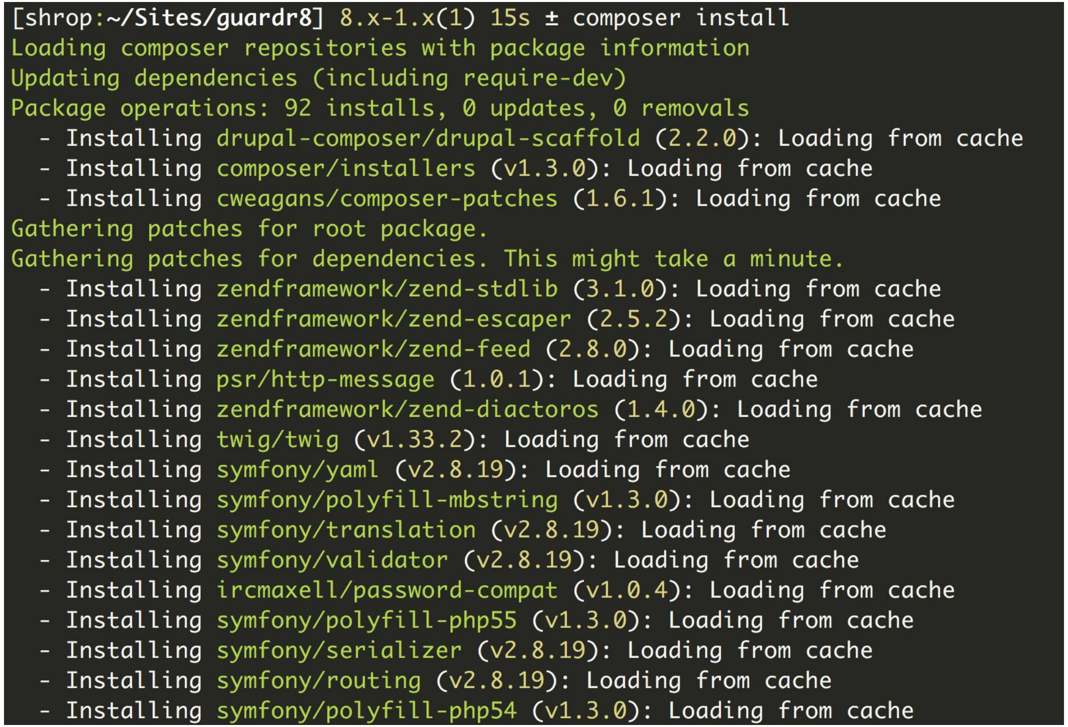
Additional Features

Username Enumeration Prevention module

- “Attackers can easily find usernames that exist by using the forgot password form and a technique called “username enumeration.” This module prevents this from happening.

Demonstration

Guardr Build with Composer



```
[shrop:~/Sites/guardr8] 8.x-1.x(1) 15s ± composer install
Loading composer repositories with package information
Updating dependencies (including require-dev)
Package operations: 92 installs, 0 updates, 0 removals
  - Installing drupal-composer/drupal-scaffold (2.2.0): Loading from cache
  - Installing composer/installers (v1.3.0): Loading from cache
  - Installing cweagans/composer-patches (1.6.1): Loading from cache
Gathering patches for root package.
Gathering patches for dependencies. This might take a minute.
  - Installing zendframework/zend-stdlib (3.1.0): Loading from cache
  - Installing zendframework/zend-escaper (2.5.2): Loading from cache
  - Installing zendframework/zend-feed (2.8.0): Loading from cache
  - Installing psr/http-message (1.0.1): Loading from cache
  - Installing zendframework/zend-diactoros (1.4.0): Loading from cache
  - Installing twig/twig (v1.33.2): Loading from cache
  - Installing symfony/yaml (v2.8.19): Loading from cache
  - Installing symfony/polyfill-mbstring (v1.3.0): Loading from cache
  - Installing symfony/translation (v2.8.19): Loading from cache
  - Installing symfony/validator (v2.8.19): Loading from cache
  - Installing ircmaxell/password-compat (v1.0.4): Loading from cache
  - Installing symfony/polyfill-php55 (v1.3.0): Loading from cache
  - Installing symfony/serializer (v2.8.19): Loading from cache
  - Installing symfony/routing (v2.8.19): Loading from cache
  - Installing symfony/polyfill-php54 (v1.3.0): Loading from cache
```

Guardr Installation with Drush Quick Drupal

- git clone --branch 8.x-1.x https://git.drupal.org/project/guardr.git
- cd guardr
- composer install
- drush qd --root=<full-path-to-webroot> --use-existing --profile=guardr --cache --watchdog --yes

Guardr Tour

Tour completed installation

Upcoming roadmap items

- Continue working through the D7 to D8 module crosswalk plan
- Evaluate additional Drupal core hardening and implement in Guardr Core
- Feature: Ability to add certain Guardr recommendations to existing Drupal 8 installs
- Update documentation for Guardr 8
    - Related project pages
    - Add new Guardr 8 specific documentation

How to Contribute

A big thanks to all of the Guardr contributors, supporting organizations, and Drupal security module contributors!

Source: CC Image courtesy of Alan Levine on Flickr

Thanks to The Drupal Security Team

- Resolves reported security issues in a Security Advisory
- Provides assistance for contributed module maintainers in resolving security issues
- Provides documentation on how to write secure code
- Provides documentation on securing your site
- Help the infrastructure team to keep the drupal.org infrastructure secure

https://www.drupal.org/security-team

How Can I help?

- Writing documentation
- Supporting Guardr users
- Testing patches and updates
- Developing new features and updates

How Can I Get involved?

- Issue queue: https://www.drupal.org/project/issues/guardr
- Documentation: https://www.drupal.org/node/2412899
- IRC: #drupal-guardr on irc.freenode.net

@guardrproject

Thank you!

Mediacurrent

@Mediacurrent

facebook.com/mediacurrent

Mediacurrent.com