



Sleep Better at Night with a Secure Drupal Site

February 19, 2021



Please abide by our Code of Conduct

All attendees, speakers, sponsors, and volunteers at our conference are required to agree with the our code of conduct.

We do not tolerate harassment of conference participants in any form.



Code of Conduct Contacts

#florida Drupal Slack channel

Or

email info@fldrupalcamp.org



AmyJune Hinline
831-406-1130



Mike Anello
321-396-2340

email info@fldrupalcamp.org

<https://www.fldrupal.camp>



Today's Agenda


1. What's Security-First?
2. Security and The Drupal Community
3. OWASP Top 10 Web Vulnerabilities
4. Drupal Best Practices and Solutions
5. Q&A



Mark Shropshire

Senior Director of Development

 /in/markshropshire

 @shrop

- From Concord, North Carolina
- 20+ years of experience as a technical team leader
- Loves empowering teams to excel while using best of class open source technology solutions.
- Passionate about personal and team growth through mentorship, aligning individual purpose with Mediacurrent's vision
- Plays sax, drums, keys, and bass and has a list of other instruments that he would love to learn!

Skills

- Drupal
- Security
- DevOps
- Flutter
- Acquia Site Factory
- Leadership

Open Source Expansion Partner

Our Mission

To bring together the most talented team members to provide world-class solutions for the web.



What's Security-First?



What's Security-First?

Security-first means going beyond compliance to assess risk. It's both a cultural mindset and a continuous development approach that's rooted in process automation.



Security-First Planning

- Proactive and collaborative approach with stakeholders
- Layered defense
- Architecture reviews
- Code reviews
- Automated testing
- Continuous improvements
- Security audits (one-offs and ongoing)
- Documentation



Security Throughout the Website Process



Discovery

- Digital strategy
- Wireframes
- Technical Architecture & Functional Specs
- Quality Assurance Test Cases
- Re-estimate Scope of Work

Design

- Style Tiles
- Mood Boards
- Responsive Design Templates
- HTML Prototypes

Development

- Module Configuration
- Custom Module Programming
- Custom Theme Development
- Front-End Framework Implementation

Quality Assurance

- Execute First Test Runs
- User Acceptance Testing (UAT)
- Execute Final Test Run

Deployment

- Prepare Production Environment
- Sync Latest Files and Data
- Finalize Cache Settings
- Switch DNS

Support

- Analytics/ Performance Evaluation
- Feature Enhancements
- Module Updates
- A/B Testing

Security and The Drupal Community





Drupal Security Team

- Resolves reported security issues in Security Advisories
- 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 secure
- <https://www.drupal.org/security-team>



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.

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

<https://drupal.org/project/guardr>

Drupal Slack: [#contrib-guardr](#)





OWASP Top 10 Web Vulnerabilities

Top 10 Web Application Security Risks

Injection

Broken Authentication

Sensitive Data Exposure

XML External Entities (XXE)

Broken Access Control

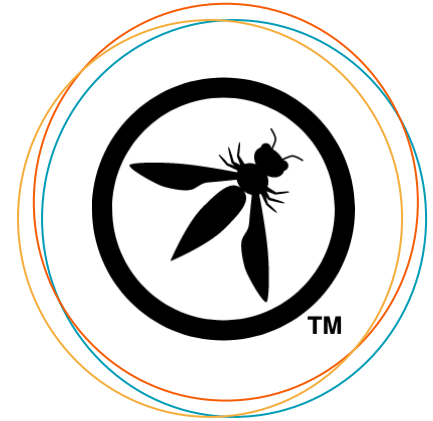
Security Misconfiguration

Cross-Site Scripting XSS

Insecure Deserialization

Using Components with Known Vulnerabilities

Insufficient Logging & Monitoring



<https://owasp.org/www-project-top-ten>

Drupal Best Practices and Solutions



Module Selection

- Module Usage
- Issue Queue Activity
- Security
- Manual Review and Testing
- Release Status
- Commit Activity
- Project information
- Risk Assessment
- Benefit

[A Guide to Drupal Module Evaluation](#)



Use Drupal APIs

Use Drupal APIs to secure your contrib and custom code.

<https://api.drupal.org/api/drupal>

[Writing secure code for Drupal](#)



Monitor Drupal Security Advisories

- Drupal core
- Drupal contrib projects
- Public service announcements
- Notifications via email and RSS
- Follow [@drupalsecurity](https://twitter.com/drupalsecurity) on Twitter
- Drupal Slack [#security-questions](https://www.drupal.org/slack)
- Read SA documentation

<https://www.drupal.org/security>

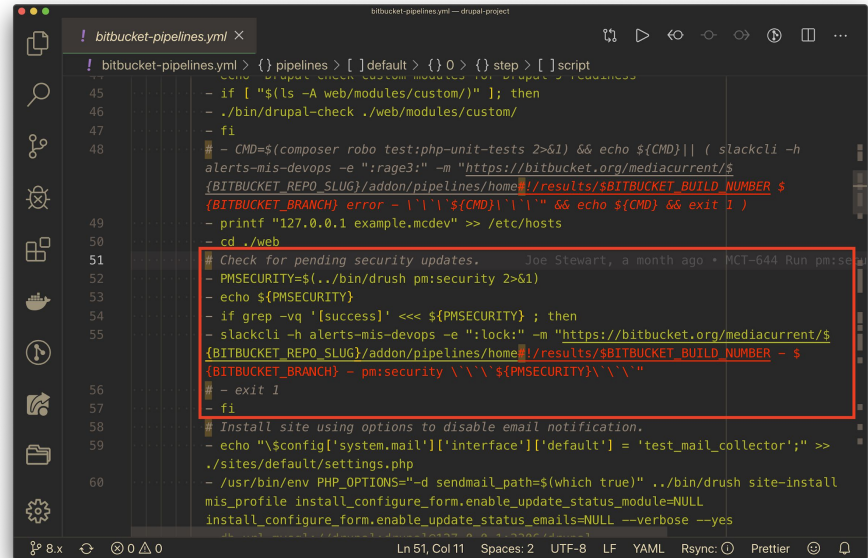


Automated Testing

Continuous Integration Examples

- drush pm:security
- Security Review
- OWASP Zap Baseline Scan

[Mediacurrent Bitbucket Pipelines](#)



```
! bitbucket-pipelines.yml < {} pipelines > [ ] default < {} 0 > {} step > [ ] script
45 - if [ "$(ls -A web/modules/custom/)" ]; then
46   ./bin/drupal-check ./web/modules/custom/
47 - fi
48 # - CMD=$(composer robo test:php-unit-tests 2>&1) && echo ${CMD} | ( slackcli -h
alerts-mis-devops -e ":rage3:" -m "https://bitbucket.org/mediacurrent/s
{BITBUCKET_REPO_SLUG}/addon/pipelines/home#!/results/${BITBUCKET_BUILD_NUMBER} $
{BITBUCKET_BRANCH} error - '\`${CMD}`' ) && echo ${CMD} && exit 1 )
49 - printf "127.0.0.1 example.mcdev" >> /etc/hosts
50 - cd ./web
51 # Check for pending security updates. Joe Stewart, a month ago • NCI-644 Run pm:se
52 - PMSECURITY=$(./bin/drush pm:security 2>&1)
53 - echo ${PMSECURITY}
54 - if grep -vq '[success]' <<< ${PMSECURITY} ; then
55   - slackcli -h alerts-mis-devops -e ":lock:" -m "https://bitbucket.org/mediacurrent/$
{BITBUCKET_REPO_SLUG}/addon/pipelines/home#!/results/${BITBUCKET_BUILD_NUMBER} - $
{BITBUCKET_BRANCH} - pm:security \`${PMSECURITY}\`"
56 - exit 1
57 - fi
58 # Install site using options to disable email notification.
59 - echo "$\nconfig['system.mail']['interface']['default'] = 'test_mail_collector';" >>
./sites/default/settings.php
60 - /usr/bin/env PHP_OPTIONS="-d sendmail_path=$(which true)" ./bin/drush site-install
mis_profile install_configure_form.enable_update_status_module=NULL
install_configure_form.enable_update_status_emails=NULL --verbose --yes
```

Demos

- Drupal project page
- Security Advisories
- Attack surface reduction
- Broken Access Control
- Cross-Site Scripting XSS
- Insufficient logging & monitoring
- Password policies
- Security misconfiguration
- Using components with known vulnerabilities



CMO's Guide to Open Source Security

Secure your open source-based martech stack with this resource for best practices.

What's inside:

- Three foundations for maintaining and securing your website and tech stack
- Checklist to define a security policy for your team
- How to monitor for Drupal and WordPress security releases
- Security incident response report (free template)

<https://www.mediacurrent.com/ebooks/cmos-guide-open-source-security>



Q&A

Thank you! Reach out with any questions!

mediacurrent.com/contact-us

mediacurrent.com/security





Contribution Day

Saturday, February 20, 2021

12:00pm - 3:30pm

First-time contributor workshop • Mentored contribution • General contribution

#DrupalContributions

<https://www.fldrupal.camp/conference/contribution-day>



Contribution Day

Saturday, February 20, 2021

12:00pm - 3:30pm

Planned Workshops

- First-time contributor workshop
- Introduction to Merge Requests
- Mentored Tooling

Planned Initiatives

- Olivero Theme
- SimplyTest
- Drupal Recipes



Thank You!



Mediacurrent.com



Mediacurrent



@Mediacurrent



@Mediacurrent



@Mediacurrent



MediacurrentDrupal