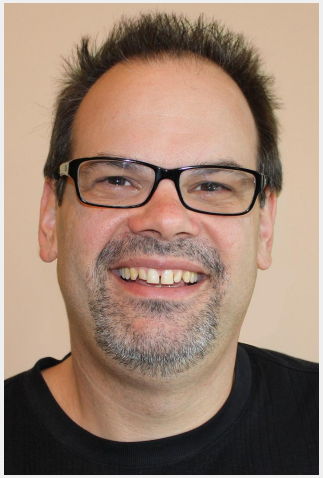
The Story of an Insecure Module

Secure Drupal Development

Mark Shropshire (shrop)

Open Source Security Lead



Mark brings 20 years of experience leading technical teams to his role as Mediacurrent's Open Source Security Lead. He is a leader in tech community organizing, blogging, podcasting, and public speaking within the Drupal community. Mark is passionate about architecting systems to solve workflow problems and improve efficiencies using open source software. Mark is the maintainer of the Gaurdr Drupal security module suite.

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.

shrop @shrop /in/markshropshire

About

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

Contents

1 Web Application Security Risks

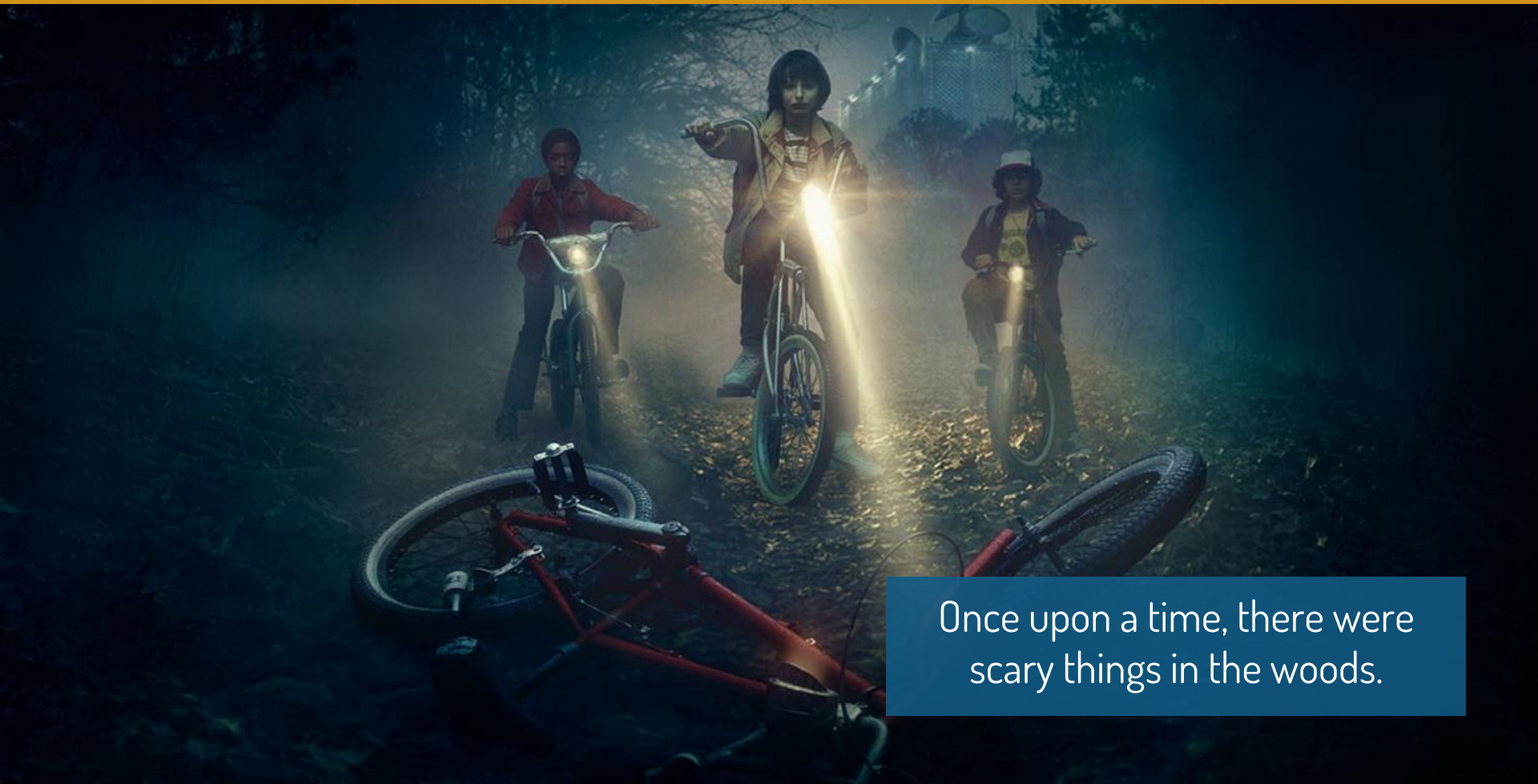
2 Module Security Audit

3 Security in the Drupal Community

4 Additional Considerations


SECURITY
THINGS

1 Web Application Security Risks


Once upon a time, there were
scary things in the woods.

Web Application Security Risks

Security risks are real.

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.

On June 12, 2013 the OWASP Top 10 for 2013 was officially released. This version was updated based on numerous comments received during the comment period after the release candidate was released in Feb. 2013.

- OWASP Top 10 2013 document (PDF).
- OWASP Top 10 2013 - Wiki.
- OWASP Top 10 2013 - Arabic (PDF).
- OWASP Top 10 2013 - Chinese (PDF).
- OWASP Top 10 2013 - Czech (PDF).
- OWASP Top 10 2013 - French (PDF).
- OWASP Top 10 2013 - German (PDF)
- OWASP Top 10 2013 - Hebrew (PDF)
- OWASP Top 10 2013 - Italian (PDF)
- OWASP Top 10 2013 - Japanese (PDF).
- OWASP Top 10 2013 - Korea (PDF).
- OWASP Top 10 2013 - Brazilian Portuguese (PDF).
- OWASP Top 10 2013 - Spanish (PDF)
- OWASP Top 10 2013 - Ukrainian (PDF)
- - Focusing on What Changed Since 2010 (PPTX)
- OWASP Top 10 2013 Presentation - Presenting Each Item in the Top 10 (PPTX).

OWASP Top Ten Project

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

SQL Injection

"Injection flaws occur when an application sends untrusted data to an interpreter. Injection flaws are very prevalent, particularly in legacy code."
https://www.owasp.org/index.php/Top_10_2013-A1-Injection

Broken Authentication and Session Management

"Developers frequently build custom authentication and session management schemes, but building these correctly is hard."

https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management

Cross-site Scripting (XSS)

"XSS flaws occur when an application includes user supplied data in a page sent to the browser without properly validating or escaping that content."

https://www.owasp.org/index.php/Top_10_2013-A3-Cross-Site_Scripting_(XSS)

Insecure Direct Object References

"Applications frequently use the actual name or key of an object when generating web pages. Applications don't always verify the user is authorized for the target object."

https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References

Security Misconfiguration

"Security misconfiguration can happen at any level of an application stack, including the platform, web server, application server, database, framework, and custom code."

https://www.owasp.org/index.php/Top_10_2013-A5-Security_Misconfiguration

Sensitive Data Exposure

"The most common flaw is simply not encrypting sensitive data."

https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure

Missing Function Level Access Control

"Applications do not always protect application functions properly. Sometimes, function level protection is managed via configuration, and the system is misconfigured."

https://www.owasp.org/index.php/Top_10_2013-A7-Missing_Function_Level_Access_Control

Cross-Site Request Forgery (CSRF)

"CSRF takes advantage the fact that most web apps allow attackers to predict all the details of a particular action."

https://www.owasp.org/index.php/Top_10_2013-A8-Cross-Site_Request_Forgery_(CSRF)

Using Components with Known Vulnerabilities

"Virtually every application has these issues because most development teams don't focus on ensuring their components/libraries are up to date."

https://www.owasp.org/index.php/Top_10_2013-A9-Using_Components_with_Known_Vulnerabilities

Unvalidated Redirects and Forwards

"Applications frequently redirect users to other pages, or use internal forwards in a similar manner. Sometimes the target page is specified in an unvalidated parameter."

https://www.owasp.org/index.php/Top_10_2013-A10-Unvalidated_Redirects_and_Forwards

Guess what?

The **Drupal** content management framework can help defend against many of these risks

Secure Drupal Development

- Utilize the Drupal API
- Keep modules, themes, and libraries up to date
- Follow Drupal Coding Standards
- Check that permissions and roles are properly configured
- Follow these references
  - https://www.drupal.org/docs/7/security/
  - https://www.drupal.org/docs/8/security/

Drupal 8 Security

Twig template engine
(Prevents SQL injection and XSS)

Improved session ID and
user session management

CSRF token protection for the
routing system

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

Default clickjacking prevention

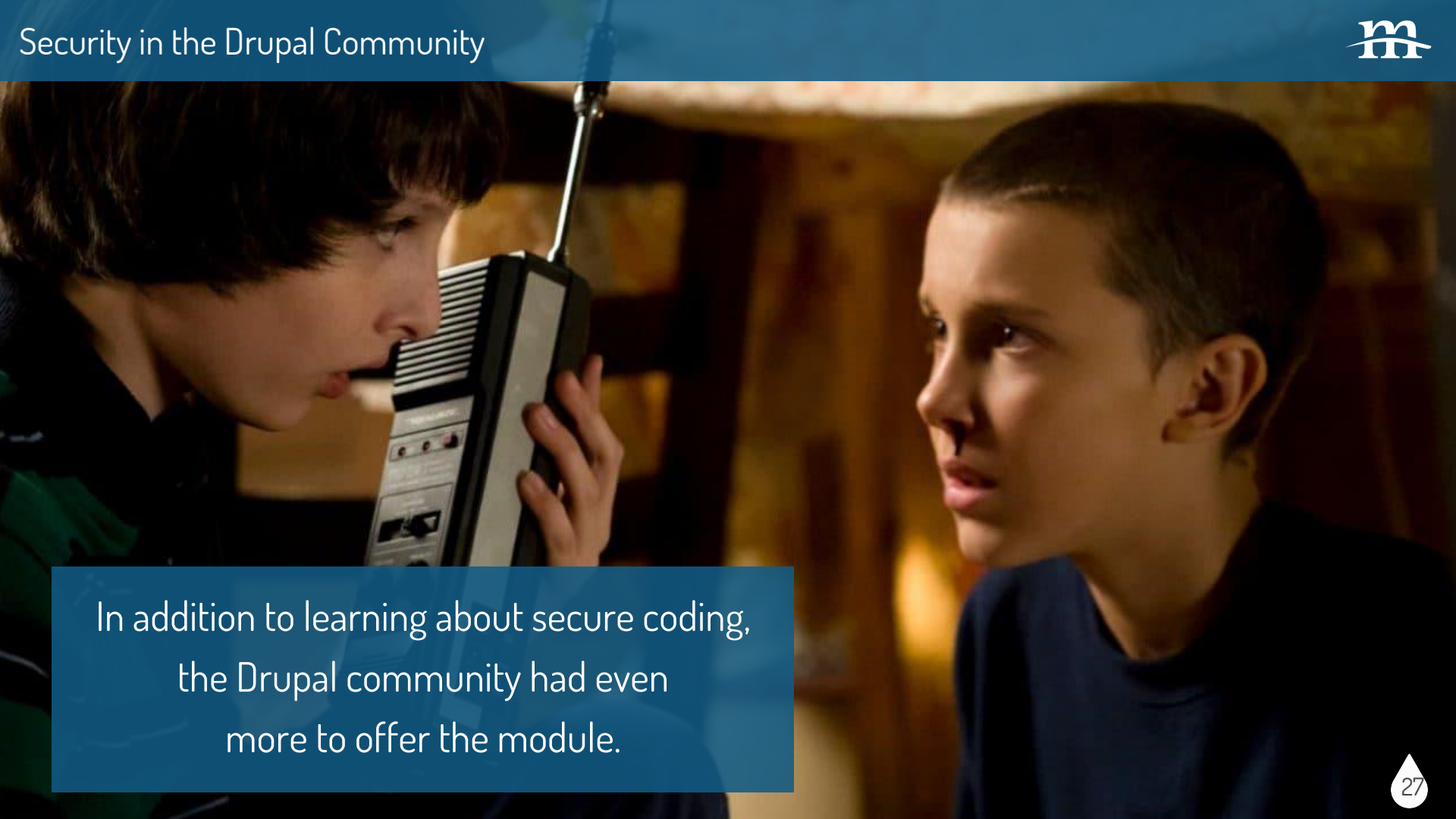
Configurable trust host patterns
(Protects HTTP HOST Header attacks)

2 Module Security Audit

While the woods were scary, there was a module that wanted to have a stable release.

Code Demo

3 Security in the Drupal Community



In addition to learning about secure coding, the Drupal community had even more to offer the module.

The Drupal Security Team

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

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

Leverage the **drupal.org** project issue queues for community **testing** and **code reviews**

Best practices for creating and maintaining projects

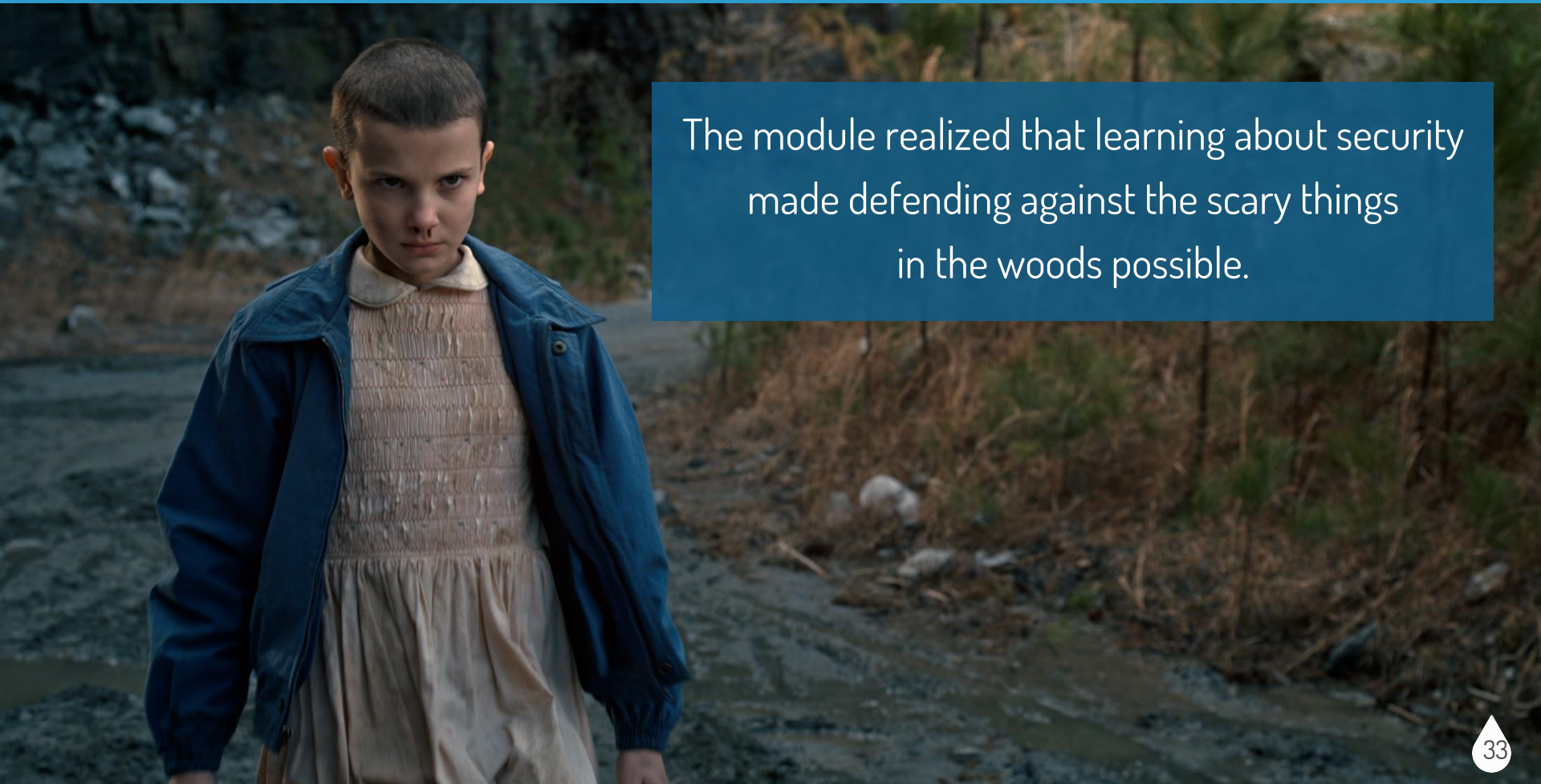
Guardr

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

4 Additional Considerations

Additional Considerations



The module realized that learning about security made defending against the scary things in the woods possible.

The CIA Information Security Triad

Confidentiality, integrity and availability.

> 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.

https://en.wikipedia.org/wiki/Information_security#Key_concepts

✔ Security first strategy using a modern technology stack

Security Building Blocks

- Consider the entire application stack
  - Including hosting infrastructure
- Use HTTPS
- Limit attack surface
- Testing
- Documentation
- Periodic 3rd party security audits

Security Related Tools

- Coder
- Hacked
- Observatory by Mozilla
- OWASP ZAP
- Security Review
- Site Audit

Thank you!

And then everyone in the Drupal community lived happily ever after.

@Mediacurrent

slideshare.net/mediacurrent

Mediacurrent.com