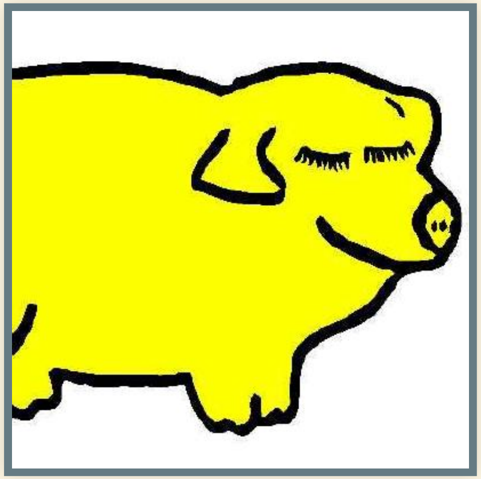
SECURITY IN DRUPAL: WHAT CAN GO WRONG?

Benji Fisher

May 27, 2022 - DrupalCamp NJ

INTRODUCTION

ABOUT ME



- Benji Fisher
- @benjifisher on d.o
- @benjifisher on GitHub
- @benjifisher on GitLab
- @benji17fisher on Twitter

Migration subsystem, Usability group, Security team (provisional member)

ABOUT FRUITION

FRUITION®

Build. Grow. Protect.

- Digital Marketing
- Website Design
- Development
- Security & Hosting

https://fruition.net/

FOLLOW ALONG

Find a link to this presentation on my GitLab Pages:

- https://slides.benjifisher.info/

OUTLINE

- Introduction
- What is the OWASP Top Ten?
- What is Drupal?
- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- ...

OUTLINE (CONTINUED)

- ...
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery
- Conclusion

ATTRIBUTION

These slides borrow a lot of text from https://owasp.org/. According to the standard footer,

> *Unless otherwise specified, all content on the site is Creative Commons Attribution-ShareAlike v4.0 and provided without warranty of service or accuracy.*

All of my slide decks have a similar license: see the last slide.

WHAT IS THE OWASP TOP TEN?

OPEN WEB APPLICATION SECURITY PROJECT® (OWASP)

> *The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software.*

source: https://owasp.org/

OWASP is not Drupal-specific. Let's "get off the island"!

OWASP TOP TEN

> *The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.*

source: https://owasp.org/www-project-top-ten/

The list is updated every few years. The most recent version is from 2021.

WHAT IS DRUPAL?

DRUPAL: A CONTENT MANAGEMENT SYSTEM

Drupal is a web-based content management system (CMS):

> *Enter data in my forms. I will save it to the database, then generate web pages.*

Hacker:

DRUPAL: AN ACTIVE, INTERNATIONAL OSS PROJECT

> *The Drupal community is one of the largest open source communities in the world. We’re more than 1,000,000 passionate developers, designers, trainers, strategists, coordinators, editors, and sponsors working together.*

source: https://www.drupal.org/about

DRUPAL: TAKE SECURITY SERIOUSLY

> *The security team is an all-volunteer group of individuals who work to improve the security of the Drupal project. Members of the team come from countries across 3 continents … The team was formalized in 2005 with a mailing list and has had 3 team leads in that time period.*

source: https://security.drupal.org/team-members

A01:2021-BROKEN ACCESS CONTROL

A02:2021-CRYPTOGRAPHIC FAILURES

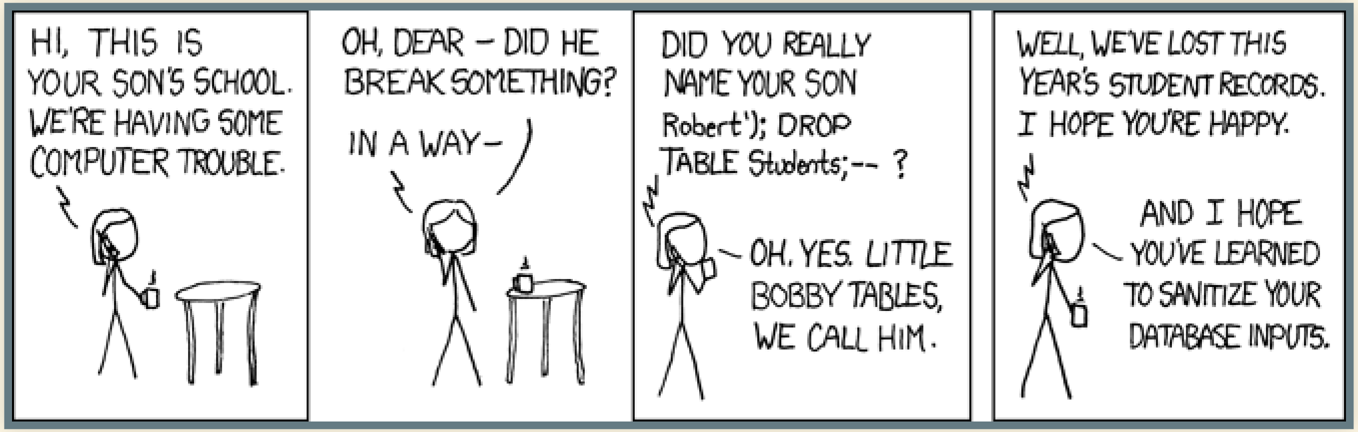
A03:2021-INJECTION

INJECTION: WHAT GOES WRONG

- User-supplied data is not validated, filtered, or sanitized by the application.
- Dynamic queries … are used directly in the interpreter.
- Hostile data is used within … search parameters to extract additional, sensitive records.
- Hostile data is directly used or concatenated. …

source: A03:2021 - Injection

INJECTION: XKCD 327


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

source: https://xkcd.com/327/

INJECTION IN DRUPAL: SA-CORE-2014-005

Drupal 7 includes a database abstraction API to ensure that queries executed against the database are sanitized to prevent SQL injection attacks.

A vulnerability in this API allows an attacker to send specially crafted requests resulting in arbitrary SQL execution. … this can lead to privilege escalation, arbitrary PHP execution, or other attacks.

This … can be exploited by anonymous users.

source: SA-CORE-2014-005

INJECTION: MY RESPONSE

> *Because of the severity of the vulnerability and the simplicity of the update, we tested … and updated the site today.*

source: my e-mail to boss and site owner (paraphrase)

INJECTION: THE UPDATE

VULNERABLE CODE

```
foreach ($data as $i => $value) {
  $new_keys[$key . '_' . $i] = $value;
}
```

FIXED CODE

```
foreach (array_values($data) as $i => $value) {
  $new_keys[$key . '_' . $i] = $value;
}
```

(comment snipped from both)

INJECTION: THE NEXT STEP

```
    // Update the query with the new placeholders.
    // preg_replace is necessary to ensure the replacement
does not affect
    // placeholders that start with the same exact text. For
example, if the
    // query contains the placeholders :foo and :foobar, and
:foo has an
    // array of values, using str_replace would affect both
placeholders,
    // but using the following preg_replace would only affect
:foo because
    // it is followed by a non-word character.
    $query = preg_replace(
      '#' . $key . '\b#',
      implode(', ', array_keys($new_keys)),
```

(line breaks added)

A04:2021-INSECURE DESIGN

A05:2021-SECURITY MISCONFIGURATION

A06:2021-VULNERABLE AND OUTDATED COMPONENTS

THE BEST KEPT SECRET IN WEB SECURITY

The secret:

The most important thing is to do all the boring stuff you *already know*.

It is a lot like …

CLICK BAIT?

How to live a longer, healthier life!

It takes just 4 minutes a day!

Does that seem too good to be true?

BRUSH YOUR TEETH!

- Two minutes, two times a day.
- Best advice you will get today.
- Also floss.
- You really will live a longer, healthier life.

WEB SECURITY HYGIENE

- Use good passwords. Have a policy.
- Keep your software up to date.
- Unless hosting is your core business, do not run your own servers.

DRUPAL: KNOW THE SCHEDULE

- Security release windows: Wednesdays 12-5 ET
- Drupal core updates (patch versions): third Wednesdays
- Drupal core updates (minor versions): June and December
- Minor versions are supported for one year.

DRUPAL: KNOW THE CHANNELS

- Web: Security advisories
- RSS: https://drupal.org/security/rss.xml, https://drupal.org/security/contrib/rss.xml, https://drupal.org/security/psa/rss.xml
- Email: https://www.drupal.org/user (Edit > My newsletters)
- Slack: `#security-questions` channel in Drupal Slack

Unofficial: @drupalsecurity on Twitter (other?)

DRUPAL: KNOW THE DIFFERENCE

- Major version (Drupal 9 to Drupal 10): disruptive
- Minor version (9.3 to 9.4): less disruptive, new features
- Patch version (9.3.6 to 9.3.7): should not be disruptive, bug fixes
- Security release (9.3.7 to 9.3.8): not disruptive (best effort)

DRUPAL AND SYMFONY

Q: Why is Drupal 9 EOL scheduled for Nov. 2023?

A: Drupal 9 uses Symfony 4, which is EOL in Nov. 2023.

A07:2021- IDENTIFICATION AND

AUTHENTICATION FAILURES

A08:2021-SOFTWARE AND DATA INTEGRITY FAILURES

A09:2021-SECURITY LOGGING AND MONITORING FAILURES

A10:2021-SERVER-SIDE REQUEST FORGERY

CONCLUSION

SUMMARY

- Introduction
- What is the OWASP Top Ten?
- What is Drupal?
- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- ...

SUMMARY (CONTINUED)

- …
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery
- Conclusion

REFERENCES

- Benji’s slide decks and source files
- OWASP Top Ten and OWASP Top 10:2021
- Drupal Security Team
- Drupal core release cycle: major, minor, and patch releases
- Security advisories

QUESTIONS

COPYLEFT