

Drupal与Web应用安全

上海外国语大学 信息技术中心

张文正

本作品采用[知识共享署名-相同方式共享 4.0 国际许可协议](https://creativecommons.org/licenses/by-sa/4.0/)进行许可



Web应用安全的重要性与脆弱性

- 研发水平：国内Web开发从业人员薪水较低，代码安全水平较差
- 病从口入：Web应用用户最多，出了事情影响面最广

[CyberSecurity2015第三季度报告](#)指出：低水平的软件开发实践也许是最大的网络威胁！

Poor software development practices may be the biggest cyber-threat of all

谁在用Drupal

- 白宫、美国/加拿大/法国/澳大利亚中央政府
- 全世界约2000+政府网站
- 美国国防部、美国航空航天局（军方背景）

Drupal 遵守严谨的软件工程

- [编码标准](#)
- [单元测试](#)
- [代码安全](#)
- [审查评估](#)
- [Bug提交](#)
- [补丁提交](#)
- [沙盒机制](#)
- [文档手册](#)
- [产品生命周期管理](#)

- Sandbox->alpha->beta->release candidate->正式版
- 小版本演进: 6.37, 7.41, 8.0.0

Issues to be Reviewed / tested / committed before release:

- *+ #2155825: Add UUID generation functionality to CTools / #813754: Ability to use variant machine name in Panels UI which uses UUID
- #1669756: Provide a contextual link for view panes
- #1482968: Open modal on form submission is broken
- #2175403: Don't skip pane cache on empty content
- #1482968: Open modal on form submission is broken
- #1360310: Undefined index notices: complete form, process input, programme #array_parents, #parents, invalid arguments in form_builder
- #1630020: entity_field_value is completely broken, then take a look at #1903 error on custom pane preview, if using a Entity:Field-Value-access-plugin
- #2155443: Enhancement of content type "List of related terms" (term-list)
- #1032218: Optional context is always empty for content type plugins
- #1058786: Caveat About Plugin Name Length and Export UI
- #1259430: Convert entity_field to use #ajax for formatter options
- #1549934: IE9 bug causing 'fllickering' of modal forms at initialisation -- Patch

Files:

Comment	File	Size	Author
#175	2454439-revert-991e143.patch	1.1 KB	catch
	PHP 5.5 & MySQL 5.5 14,312 pass		
	PHP 7 & MySQL 5.5 14,261 pass, 11 fail	PHP 7 & MySQL 5.5 14,306 pass	
	Add test		
#175	2454439-revert-5dc2bd0.patch	1.08 KB	catch
	PHP 5.5 & MySQL 5.5 14,312 pass	PHP 7 & MySQL 5.5 14,306 pass	
		Add test	
#137	php7-core-report.txt	9.1 KB	Chi
#131	php7_results15_without_passes.txt	3.06 KB	Berdir
#131	php7_results15.txt	184.96 KB	Berdir

```
FILE: ...pareview/pareview_temp/modules/offsite/commerce_paystand_offsite.s
-----
FOUND 0 ERRORS AND 10 WARNINGS AFFECTING 10 LINES
-----
34 | WARNING | A comma should follow the last multiline array item. Found:
   | | 'live'
90 | WARNING | A comma should follow the last multiline array item. Found:
106 | WARNING | A comma should follow the last multiline array item. Found:
   | | FALSE
121 | WARNING | A comma should follow the last multiline array item. Found:
   | | $shipping_same
129 | WARNING | A comma should follow the last multiline array item. Found:
133 | WARNING | A comma should follow the last multiline array item. Found:
   | | uid
135 | WARNING | A comma should follow the last multiline array item. Found:
166 | WARNING | A comma should follow the last multiline array item. Found:
218 | WARNING | A comma should follow the last multiline array item. Found:
   | | 'success'
223 | WARNING | A comma should follow the last multiline array item. Found:
   | | 'consumer_id'
-----
FILE: /var/www/drupal-7-...
-----
ACTIONS
-----
Run tests Return to list
-----
FOUND 1 ERROR AND 10 WARNINGS AFFECTING 11 LI
-----
3 | WARNING | Line exceeds 80 characters; cont
7 | WARNING | Line exceeds 80 characters; cont
8 | WARNING | Line exceeds 80 characters; cont
9 | WARNING | Line exceeds 80 characters; cont
10 | WARNING | Line exceeds 80 characters; cor
11 | WARNING | Line exceeds 80 characters; cor
12 | WARNING | Line exceeds 80 characters; cor
13 | WARNING | Line exceeds 80 characters; cor
16 | WARNING | Line exceeds 80 characters; cor
18 | WARNING | Line exceeds 80 characters; cor
19 | ERROR | Files must end in a single new li
-----
RESULTS
-----
20 passes, 6 fails, and 0 exceptions
- CHECK PLAIN
-----
6 passes, 3 fails, and 0 exceptions
MESSAGE
-----
Nothing gets replaced that doesn't
-----
Quotes are replaced with their esca
-----
Ampersands are replaced with their
```

Drupal编码安全1：防止SQL注入

数据库抽象层机制：

- 传参：

```
db_query("SELECT t.s FROM {table} t WHERE t.field  
IN (:users)", array(':users' => $from_user));
```

- Or使用面向对象的方法：

```
$result = db_select('table', 't')  
->fields('t', array('s'))  
->condition('t.field', $from_user, 'IN')  
->execute();
```

Drupal编码安全2：防止跨站脚本攻击

过滤用户所有输入

- [check_plain](#), [check_markup](#)
- [filter_xss](#), [filter_xss_admin](#)

Drupal编码安全4：其他

- [正则表达式替换](#)
- [使用私有、受管理的文件，防止下载](#)
- [服务器端数据验证，不依赖于浏览器的Javascript验证](#)
- [使用sha-256而非md5或sha1散列数据](#)
- [加密数据](#)（提供抽象接口，更灵活）
- 尽可能少地使用eval()函数
- 耗时操作使用Drupal queue队列机制，无需修改PHP的max_execution_time，减少安全风险

防止其他恶意攻击

- [IP访问黑白名单](#)（后台可配置）
- 利用安全众包平台：[Bad behavior](#)、[Xortify.com](#)
- [缓存安全](#)
- [防暴力破解](#)
- [尽可能使用HTTPS协议](#)
- [双因子登录](#)、[扫二维码登录](#)、[USB-Key登录](#)、[划屏手势登录](#)、[Smart Card登录](#)

用户个人隐私保护

- 实现了支付卡产业标准：Payment Card Industry, 达到金融行业安全级别要求
- 用户账号防劫持（session、identity劫持）
- 防Email爬虫，邮件地址仍可点击
- 防注册机器人，同时不影响正常用户体验

敏感词过滤与举报

- 正则表达式过滤敏感词、音近词
- 禁止用户注册敏感的用户名
- 用户可以举报，如：反动、色情、粗鲁等各种类型（可灵活增删）

WORD TO FILTER ▲	REPLACEMENT TEXT	STANDALONE	操作
法轮功	*	否	Edit word Delete word

删除 编辑 回复 **举报**

Web服务器配置安全

- [文件系统安全权限设置](#)
- [Apache配置](#)，配合各类缓存、反向代理等
- [Nginx配置](#)，配合各类缓存、反向代理等
- 各类缓存安全配置：[Varnish](#)、[MemCached](#)等
- [Drupal可以运行在启用mod-security的Apache上：](#)
或使用[入侵防御功能模块](#)，适合未部署IPS/WAF的网络环境
- [防止DDoS](#)
- [静态化](#)
- [内外网分离+反向代理+负载均衡部署](#)

Drupal安全检查、日志和监控

- [生产环境中全面安全检测模块](#)
- 核心自带提醒模块安全更新（邮件、短信）
- 核心支持syslog日志输出
- 自动记录日志：用户登陆注销、代码异常、内容增删、表单修改及任何模块代码中写入日志的操作
- [支持Nagios](#)、[Zabbix](#)、[Munin](#)等第三方监控
- [原生的Drupal监控](#)（包括安全、日志、性能）

User registration Visitors can create accounts and no administrator approval is required.

Your *User registration* settings are set to Visitors can create accounts and no administrator approval is required. Are you sure this is what you want and did not mean to use Visitors can create accounts but administrator approval is required? With improperly setup access rights, this can be dangerous...

Site e-mail Global site e-mail address OK: himiko@himekankankal.com

Your *Site e-mail* settings are OK for production use.

Server
Checks certain server site parameters such as APC.

APC Disabled

APC does not appear to be running.

Performance
Checks if performance settings are OK for production use.

Page caching Disabled

Your *Page caching* settings are disabled. You should at least set page caching to Normal on production sites!

Page compression Enabled

Your *Page compression* settings are OK for production use.

Block cache Disabled

Your *Block cache* settings are disabled. You should really enable this for production as it can cause huge performance increases, especially on high traffic sites.

Optimize CSS files Disabled

Your *Optimize CSS files* settings are disabled, they should be enabled on a production environment! This should not cause trouble if you steer clear of minified files.

Optimize JavaScript files Disabled

Your *Optimize JavaScript files* settings are disabled, ideally they should be enabled on a production environment but this requires testing first, since minification can break some scripts.

```
malcolm@:~/workspace/drupal-6.26$ drush pchk
Production Check status

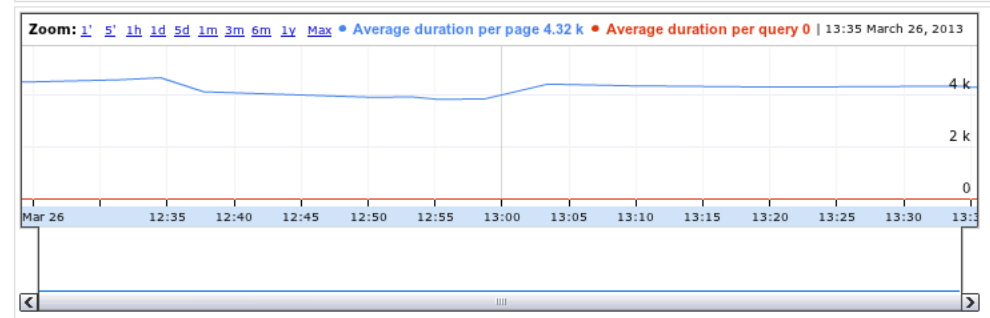
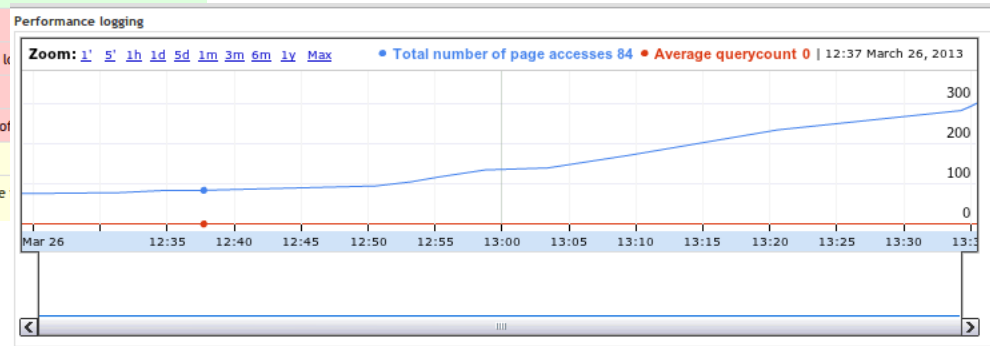
Settings
Error reporting Write errors to the log
User registration Visitors can create accounts and no administrator approval is required
Site e-mail Global site e-mail address set to try.to@

Server
APC Disabled
Release notes Release note .txt files still present on disk

Performance
Page caching Enabled
Page compression Enabled
Block cache Enabled
Optimize CSS files Enabled
Optimize JavaScript files Enabled

Security
Is /node available? Secure
User passwords Secure
Anonymous user rights Secure

Modules
Contact Contact e-mail addresses are Website feed category: jules@hotmail.com
Devel Enabled
```



Drupal官方安全运维

- [安全小组](#)
- [核心、社区贡献模块漏洞补丁发布](#)（不断更新升级）
- [Drupal官网提供最佳安全实践指南](#)（经常更新）

老生常谈：开源是否安全？ 1

开源会让坏蛋也能看到代码，可能干坏事

But，请考虑：

- 闭源软件做手脚你很难知道（窃取密码、修改浏览器主页等等）
- 就算乙方把自己的商业产品的源代码交付给甲方，甲方有时间看吗？能都看懂吗？搞清楚乙方源代码都给了吗？
- 使用人数众多的开源软件社区里总有一些人发现并热心修复问题（最最典型的就是Linux，Drupal也类似）
- 更不用说开源的无厂商锁定、跨越式直接达到国际前沿水准、成本较低等好处了

开源是否安全？ 2

不管闭源还是开源，安全性更取决于：

- 设计要尽可能完善
- 测试要尽量全面
- 维护和跟踪及时持续
- 问题解决要快速
- 信息发布要及时透明

以目前国内软件产业发展阶段和环境来讲：

极少有厂商在实践中达到这个要求和标准；所以，选择经过实践证明是安全可靠的、流行开源的软件是更可取的方法

重要的事情说两遍：谁在用Drupal

- [白宫](#)、[美国](#)/[加拿大](#)/[法国](#)/[澳大利亚](#)中央政府
- [全世界约2000+政府网站](#)
- [美国国防部](#)、[美国航空航天局](#)（军方背景）

结论：Drupal完全满足国家等保要求
(特别是应用安全、数据安全及信息安全)，
对于其他Web-based App开发具有很大的借鉴参考意义

Q&A

Thank you!



我的微信



Drupal在高校QQ群