Чистый код

Чистый код

или WordPress

Что такое чистый код?

Что такое чистый код?

- максимум стандартного PHP

Что такое чистый код?

- максимум стандартного PHP
- никаких фреймворков, систем управления контентом

Что такое чистый код?

- максимум стандартного PHP
- никаких фреймворков, систем управления контентом
- ноль объектно-ориентированной архитектуры

Что такое чистый код?

- максимум стандартного PHP
- никаких фреймворков, систем управления контентом
- ноль объектно-ориентированной архитектуры
- никаких крупных библиотек, всё с нуля

Внимание! Вопрос:

Внимание! Вопрос:

- Кто писал проект на чистом коде?

Внимание! Вопрос:

- Кто писал проект на чистом коде?
- Кто писал свой фреймворк?

Внимание! Вопрос:

- Кто писал проект на чистом коде?
- Кто писал свой фреймворк?

Преимущества чистого кода

Преимущества чистого кода

- быстрый

Преимущества чистого кода

- быстрый
- не нужно изучать чужую документацию

Преимущества чистого кода

- быстрый
- не нужно изучать чужую документацию
- легко воплотить любые хотелки

Преимущества чистого кода

- быстрый
- не нужно изучать чужую документацию
- легко воплотить ~~любые~~ хотелки

Преимущества чистого кода

- быстрый
- не нужно изучать чужую документацию
- легко воплотить **простые** хотелки

Недостатки чистого кода

Недостатки чистого кода

- небезопасный

Недостатки чистого кода

- небезопасный (MySQLi, XSS, R/LFI, …)

Недостатки чистого кода

- небезопасный (MySQLi, XSS, R/LFI, …)
- долго для более сложных решений

Недостатки чистого кода

- небезопасный (MySQLi, XSS, R/LFI, …)
- долго для более сложных решений
- не для больших команд

Недостатки чистого кода

- небезопасный (MySQLi, XSS, R/LFI, …)
- долго для более сложных решений
- не для больших команд
  - недокументированый, нетестированый
  - нет стандартов разработки
  - нет разделения обязанностей (аморфная архитектура)

Недостатки чистого кода

- небезопасный (MySQLi, XSS, R/LFI, …)
- долго для более сложных решений
- не для больших команд
  - недокументированый, нетестированый
  - нет стандартов разработки
  - нет разделения обязанностей (аморфная архитектура)
- developer lock-in

Недостатки чистого кода

- небезопасный (MySQLi, XSS, R/LFI, …)
- долго для более сложных решений
- не для больших команд
  - недокументированый, нетестированый
  - нет стандартов разработки
  - нет разделения обязанностей (аморфная архитектура)
- developer lock-in

Недостатки чистого кода

- небезопасный (MySQLi, XSS, R/LFI, …)
- долго для более сложных решений
- не для больших команд
  - недокументированый, нетестированый
  - нет стандартов разработки
  - нет разделения обязанностей (аморфная архитектура)
- developer lock-in
- закрытый исходный код

Преимущества WordPress и другого открытого кода

- богатая, открытая история создания

Преимущества WordPress и другого открытого кода

- богатая, открытая история создания
- сравнительно безопасный

Wordpress » Wordpress : Vulnerability Statistics

Vulnerabilities (277) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (0) Patches (20) Inventory Definitions (0) Compliance Definitions (0)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2004	2						1		1						
2005	10		5			3	2				3				
2006	16	1	2			1	5	1			3				
2007	40	2	13			7	19			3	5		2		1
2008	27	2	4			3	9	4		1	2		2		
2009	14	3	1				3			1	3	1			4
2010	2		1			1									
2011	11					1	2				4				
2012	24	2	2			2	9			5	3		3		7
2013	19	1	1				8			3	2		1		
2014	29	3	3			1	8	1		6	2		3	1	
2015	11	1	2			1	7			1	1		1		
2016	20	1					9			6	1		1		
2017	46	1	1			4	17	4		5	3		5		
2018	6	1					2								
Total	277	18	35			24	101	10	1	31	32	1	18	1	12
% Of All		6.5	12.6	0.0	0.0	8.7	36.5	3.6	0.4	11.2	11.6	0.4	6.5	0.4	

Joomla : Vulnerability Statistics

Products (**162**) Vulnerabilities (**350**) Search for products of Joomla CVSS Scores Report Possible matches for this vendor Related Metasploit Modules

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2005	4	1	1			1	1								
2006	51	3	19			2	4			2	3	1		17	
2007	59		41			18	9	1	1		3			22	
2008	96		80			77	2	1				1	1	3	3
2009	25		15			15	6	1			1		1		1
2010	10		6			5	4							1	12
2011	16		5			5	4				5				5
2012	25		2			2	10				8	1			3
2013	11	1				1	4			3	3				2
2014	10	1	3			2	5			3					1
2015	13		6			4	1	2			2		2		
2016	6		1			1						1			
2017	19		1			1	6			1	5		1		
2018	5					2	3								
Total	350	6	180			136	59	5	1	9	30	4	5	43	27
% Of All		1.7	51.4	0.0	0.0	38.9	16.9	1.4	0.3	2.6	8.6	1.1	1.4	12.3	

Bitrix : Vulnerability Statistics

Products (4) Vulnerabilities (10) Search for products of Bitrix CVSS Scores Report Possible matches for this vendor Related Metasploit Modules

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2005	2		1								1			1	
2006	4		1				2				2				
2008	1														
2014	1									1					
2015	2	1						2			1				
Total	10	1	2				2	2		1	4			1	
% Of All		10.0	20.0	0.0	0.0	0.0	20.0	20.0	0.0	10.0	40.0	0.0	0.0	10.0	

Верю не верю...

Преимущества WordPress и другого открытого кода

- богатая, открытая история создания
- сравнительно безопасный
- сообщество вокруг кода

Преимущества WordPress и другого открытого кода

- богатая, открытая история создания
- сравнительно безопасный
- **целые сообщества** вокруг кода

Преимущества WordPress и другого открытого кода

- богатая, открытая история создания
- сравнительно безопасный
- целые сообщества вокруг кода
- низкий порог входа

Преимущества WordPress и другого открытого кода

- богатая, открытая история создания
- сравнительно безопасный
- целые сообщества вокруг кода
- низкий порог входа (...недостаток?)

Преимущества WordPress и другого открытого кода

- богатая, открытая история создания
- сравнительно безопасный
- целые сообщества вокруг кода
- низкий порог входа (...недостаток?)
- документирован, тестирован, многофункционален

Примеры

```php
$postData = array(
    'login' => 'acogneau',
    'pwd' => 'secretpassword',
    'redirect_to' => 'http://example.com',
    'testcookie' => '1'
);

curl_setopt_array($ch, array(
    CURLOPT_URL => 'http://example.com/wp-login.php',
    CURLOPT_RETURNTRANSFER => true,
    CURLOPT_POST => true,
    CURLOPT_POSTFIELDS => $postData,
    CURLOPT_FOLLOWLOCATION => true
));

$output = curl_exec($ch);
echo $output;
```

Примеры

wp_remote_post()

```php
$postData = array(
    'login' => 'acogneau',
    'pwd' => 'secretpassword',
    'redirect_to' => 'http://example.com',
    'testcookie' => '1'
);

curl_setopt_array($ch, array(
    CURLOPT_URL => 'http://example.com/wp-login.php',
    CURLOPT_RETURNTRANSFER => true,
    CURLOPT_POST => true,
    CURLOPT_POSTFIELDS => $postData,
    CURLOPT_FOLLOWLOCATION => true
));

$output = curl_exec($ch);
echo $output;
```

Примеры

```
$mysqli = new mysqli("localhost", "my_user", "my_password", "world");
/* check connection */
if ($mysqli->connect_errno) {
    printf("Connect failed: %s\n", $mysqli->connect_error);
    exit();
}
/* Create table doesn't return a resultset */
if ($mysqli->query("CREATE TEMPORARY TABLE myCity LIKE City") ===
TRUE) {
    printf("Table myCity successfully created.\n");
}
/* Select queries return a resultset */
if ($result = $mysqli->query("SELECT Name FROM City LIMIT 10")) {
    printf("Select returned %d rows.\n", $result->num_rows);
    /* free result set */
    $result->close();
}
/* If we have to retrieve large amount of data we use
MYSQLI_USE_RESULT */
if ($result = $mysqli->query("SELECT * FROM City",
MYSQLI_USE_RESULT)) {
    /* Note, that we can't execute any functions which interact with the
       server until result set was closed. All calls will return an
       'out of sync' error */
    if (!$mysqli->query("SET @a:='this will not work'")) {
        printf("Error: %s\n", $mysqli->error);
    }
```

Примеры

get_posts()

```
$mysqli = new mysqli("localhost", "my_user", "my_password", "world");
/* check connection */
if ($mysqli->connect_errno) {
    printf("Connect failed: %s\n", $mysqli->connect_error);
    exit();
}
/* Create table doesn't return a resultset */
if ($mysqli->query("CREATE TEMPORARY TABLE myCity LIKE City") ===
TRUE) {
    printf("Table myCity successfully created.\n");
}
/* Select queries return a resultset */
if ($result = $mysqli->query("SELECT Name FROM City LIMIT 10")) {
    printf("Select returned %d rows.\n", $result->num_rows);
    /* free result set */
    $result->close();
}
/* If we have to retrieve large amount of data we use
MYSQLI_USE_RESULT */
if ($result = $mysqli->query("SELECT * FROM City",
MYSQLI_USE_RESULT)) {
    /* Note, that we can't execute any functions which interact with the
       server until result set was closed. All calls will return an
       'out of sync' error */
    if (!$mysqli->query("SET @a:='this will not work'")) {
        printf("Error: %s\n", $mysqli->error);
    }
```

Примеры

```
function generateRandomString($length = 10) {
    $characters =
'0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLM
NOPQRSTUVWXYZ';
    $charactersLength = strlen($characters);
    $randomString = '';
    for ($i = 0; $i < $length; $i++) {
        $randomString .= $characters[rand(0,
$charactersLength - 1)]; } return $randomString;
    }
}
```

Примеры

```
function generateRandomString($length = 10) {
    $characters =
'0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLM
NOPQRSTUVWXYZ';
    $charactersLength = strlen($characters);
    $randomString = '';
    for ($i = 0; $i < $length; $i++) {
        $randomString .= $characters[rand(0,
$charactersLength - 1)]; } return $randomString;
    }
}
```

wp_generate_password()

API, только API...

- Dashboard Widgets API
- Database API
- HTTP API
- REST API
- File Header API
- Filesystem API
- Metadata API
- Options API
- Plugin API
- Quicktags API
- Rewrite API
- Settings API
- Shortcode API
- Theme Modification API
- Theme Customization API
- Transients API
- Widgets API
- XML-RPC WordPress API

API, только API... (продолжение)

- ACF, Carbon Fields, Metabox.io
- WooCommerce, bbPress, buddyPress
- Visual Composter, Elementor
- Cavalcade, TLC
- composer.phar для всего остального

Принципы всего “нечистого” кода

Принципы всего “нечистого” кода

До вас всё уже написали!

Принципы всего “нечистого” кода

До вас всё уже написали!

легко писать и понимать...
...сложно выстрелить себе в ногу

(но можно...)

Когда можно писать чистый код

- Правда нет подходящего решения
  или решение не по душе
- Ради развлечения, челленджа
- Если вы патчите ядро и библиотеки

Чистый код

или **WordPress**

~~Чистый код~~

или **WordPress**

~~Чистый код~~

или **WordPress**

или любой другой открытый фреймворк

Спасибо

что протестировали меня