

静的アプリケーションセキュリティテスト 報告書

acme/app

不合格	18 指摘	0 緊急	6 高	12 中	0 低
-----	----------	---------	--------	---------	--------

対象

検査したパス	src templates
検査したファイル	6
ルール	pieceofcake2/security-sast (CakePHP 2) p/php
設定	APP_ENV=prod で検査
不合格の基準	高以上

実行

実行日時	2026-10-17 10:05:48 ~ 10:05:53 (UTC)
所要時間	5秒
ソフトウェア	PHP 8.5.11 Semgrep 1.180.0 pieceofcake2/security-sast 1.x-dev

リスク別の指摘

1. 高

No.	ルール	リスク	箇所
1-1	find() に変数を含む条件の文字列	高	1箇所
1-2	既定値、サンプル、または短い Security.salt	高	1箇所
1-3	Model::query() に変数を含む SQL	高	2箇所
1-4	リクエストの値で指定したビューやエレメント	高	1箇所
1-5	リクエストの値の unserialize()	高	1箇所

2. 中

No.	ルール	リスク	箇所
2-1	既定値またはサンプルの Security.cipherSeed	中	1箇所
2-2	'cipher' で暗号化した Cookie	中	1箇所
2-3	リクエストの値へのリダイレクト	中	2箇所
2-4	CSRF やフォーム改ざんのチェックの無効化	中	2箇所
2-5	ビューで h() を通さない変数の出力	中	5箇所
2-6	変数を渡した Xml::build()	中	1箇所

1. 高

1-1 find() に変数を含む条件の文字列

高

ルール	cakephp2-conditions-string
リスク	高
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
OWASP Top 10	A03:2021 - Injection
確度	MEDIUM
箇所	1箇所

変数を含む条件の文字列を find() に渡しています。値がエスケープされるように、条件の配列 (['Post.title' => \$title]) にしてください。

src/Controller/PostsController.php:22

```
$found = $this->Post->find('all', ['conditions' => "Post.title = '$q'"]);
```

1. 高

1-2 既定値、サンプル、または短い Security.salt

高

ルール	cakephp2-config-salt
リスク	高
CWE	CWE-1188: Initialization of a Resource with an Insecure DefaultCWE-330: Use of Insufficiently Random Values
OWASP Top 10	A02:2021 - Cryptographic Failures
確度	HIGH
箇所	1箇所

Security.salt が、配布時の既定値かドキュメントのサンプルの値、または 32 文字未満です。ハッシュや署名した値 (フォームのトークンなど) を偽造できます。SECURITY_SALT に 32 バイト以上のランダムな値を設定してください。

config/core.php:3

```
Configure::write('Security.salt', 'DYhG93b0qyJfIxfS2guVoUubWwvniR2G0FgaC9mi');
```

1. 高

1-3 Model::query() に変数を含む SQL

高

ルール	cakephp2-query-concatenation
リスク	高
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
OWASP Top 10	A03:2021 - Injection
確度	MEDIUM
箇所	2箇所

変数を含む文字列で組み立てた SQL を Model::query() に渡しています。query() の値の配列（\$this->Model->query('... WHERE id = ?', [\$id])）か、条件の配列を使う find() にしてください。

src/Controller/PostsController.php:19

```
$posts = $this->Post->query("SELECT * FROM posts WHERE title LIKE '%" . $q . "%'");
```

src/Controller/PostsController.php:20

```
$more = $this->Post->query("SELECT * FROM posts WHERE id = $q");
```

1. 高

1-4 リクエストの値で指定したビューやエレメント

高

ルール	cakephp2-render-request
リスク	高
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
OWASP Top 10	A01:2021 - Broken Access Control
確度	HIGH
箇所	1箇所

リクエストの値を render() や element() に渡しています。パスを含めると、どのテンプレートでも表示できます。許可したビューの一覧に対応させてください。

src/Controller/PostsController.php:39

```
$this->render($this->request->query('page'));
```

1. 高

1-5 リクエストの値の unserialize()

高

ルール	cakephp2-unserialize-request
リスク	高
CWE	CWE-502: Deserialization of Untrusted Data
OWASP Top 10	A08:2021 - Software and Data Integrity Failures
確度	HIGH
箇所	1箇所

リクエストの値を unserialize() に渡しています。どのクラスのオブジェクトでも作られます。json_decode() にしてください。

src/Controller/PostsController.php:46

```
$data = unserialize($this->request->data('payload'));
```

2. 中

2-1 既定値またはサンプルの Security.cipherSeed

中

ルール	cakephp2-config-cipher-seed
リスク	中
CWE	CWE-1188: Initialization of a Resource with an Insecure Default
OWASP Top 10	A02:2021 - Cryptographic Failures
確度	HIGH
箇所	1箇所

Security.cipherSeed が、配布時の既定値かドキュメントのサンプルの値です。CookieComponent の 'cipher' で使われます。SECURITY_CIPHER_SEED にランダムな数を設定し、Cookie を 'aes' に移してください。

config/core.php:4

```
Configure::write('Security.cipherSeed', '76859309657453542496749683645');
```

2. 中

2-2 'cipher' で暗号化した Cookie

中

ルール	cakephp2-config-cookie-cipher
リスク	中
CWE	CWE-327: Use of a Broken or Risky Cryptographic Algorithm
OWASP Top 10	A02:2021 - Cryptographic Failures
確度	HIGH
箇所	1箇所

CookieComponent が 'cipher' で暗号化しています (Cookie.type が未設定か 'cipher')。'cipher' は安全ではありません。Cookie.type を 'aes'、Cookie.key を 32 バイト以上のランダムな値、Security.useOpenSsl を true にしてください。

config/core.php:5

```
Configure::write('Cookie.type', 'cipher');
```

2. 中

2-3 リクエストの値へのリダイレクト

中

ルール	cakephp2-redirect-request
リスク	中
CWE	CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
OWASP Top 10	A01:2021 - Broken Access Control
確度	HIGH
箇所	2箇所

リクエストの値を redirect() に渡しています。ルートの配列の Router::url() などでアプリケーション内のパスにだけリダイレクトするか、URL を許可リストで確かめてください。

src/Controller/PostsController.php:29

```
return $this->redirect($this->request->query('url'));
```

src/Controller/PostsController.php:34

```
return $this->redirect($this->request->data['Post']['url']);
```

2. 中

2-4 CSRF やフォーム改ざんのチェックの無効化

中

ルール	cakephp2-security-csrf-disabled
リスク	中
CWE	CWE-352: Cross-Site Request Forgery (CSRF)
OWASP Top 10	A01:2021 - Broken Access Control
確度	MEDIUM
箇所	2箇所

SecurityComponent の CSRF のチェック、またはフォームの改ざんのチェックを無効にしています。
unlockedActions など、必要なアクションだけ無効にしてください。

src/Controller/PostsController.php:12

```
$this->Security->csrfCheck = false;
```

src/Controller/PostsController.php:13

```
$this->Security->validatePost = false;
```

2. 中

2-5 ビューで h() を通さない変数の出力

中

ルール	cakephp2-view-unescaped-output
リスク	中
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
OWASP Top 10	A03:2021 - Injection
確度	LOW
箇所	5箇所

ビューで変数を h() を通さずに出力しています。h() でエスケープするか、エスケープするヘルパーを使ってください。

templates/Posts/edit.ctp:10

```
<div><?= $body_html ?></div>
```

templates/Posts/edit.ctp:12

```
<p><?= $summary ?></p>
```

templates/Posts/index.php:2

```
<p><?= $title ?></p>
```

templates/Posts/view.ctp:2

```
<div><?= $post['Post']['body'] ?></div>
```

templates/Posts/view.ctp:3

```
<p><?php echo $post['Post']['summary']; ?></p>
```

2. 中

2-6 変数を渡した Xml::build()

中

ルール	cakephp2-xml-build-variable
リスク	中
CWE	CWE-918: Server-Side Request Forgery (SSRF)
OWASP Top 10	A10:2021 - Server-Side Request Forgery (SSRF)
確度	MEDIUM
箇所	1箇所

Xml::build() に変数を渡しています。変数が URL やパスなら、その中身が読み込まれます。XML の文字列には ['readFile' => false] を渡し、リクエストの値は渡さないでください。

src/Controller/PostsController.php:44

```
$xml = Xml::build($this->request->data('xml'));
```