

Static Application Security Testing Report

acme/app

FAILED	18 Findings	0 Critical	6 High	12 Medium	0 Low
--------	----------------	---------------	-----------	--------------	----------

Target

Scanned paths	src templates
Scanned files	6
Rules	pieceofcake2/security-sast (CakePHP 2) p/php
Configuration	Checked with APP_ENV=prod
Fails on	High or higher

Run

Date	2026-10-17 10:05:39 – 10:05:44 (UTC)
Duration	5s
Software	PHP 8.5.11 Semgrep 1.180.0 pieceofcake2/security-sast 1.x-dev

Findings by risk

1. High

No.	Rule	Risk	Places
1-1	Conditions string with a variable in find()	High	1
1-2	Default, sample or short Security.salt	High	1
1-3	SQL built with a variable in Model::query()	High	2
1-4	View or element named by the request	High	1
1-5	unserialize() of a value of the request	High	1

2. Medium

No.	Rule	Risk	Places
2-1	Default or sample Security.cipherSeed	Medium	1
2-2	Cookies encrypted with 'cipher'	Medium	1
2-3	Redirect to a value of the request	Medium	2
2-4	CSRF or form tampering check turned off	Medium	2
2-5	Variable printed in a view without h()	Medium	5
2-6	Xml::build() with a variable	Medium	1

1. High

1-1 Conditions string with a variable in find()

High

Rule	cakephp2-conditions-string
Risk	High
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
OWASP Top 10	A03:2021 - Injection
Confidence	MEDIUM
Places	1

A conditions string with a variable is passed to find(). Use a conditions array ([Post.title' => \$title]) so that the value is escaped.

src/Controller/PostsController.php:22

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

1. High

1-2 Default, sample or short Security.salt

High

Rule	cakephp2-config-salt
Risk	High
CWE	CWE-1188: Initialization of a Resource with an Insecure Default CWE-330: Use of Insufficiently Random Values
OWASP Top 10	A02:2021 - Cryptographic Failures
Confidence	HIGH
Places	1

Security.salt is the default of the distribution or a sample of the documentation, or shorter than 32 characters. The hashes and the signed values (e.g. the tokens of forms) can be forged. Set SECURITY_SALT to a random value of 32 bytes or more.

config/core.php:3

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

1. High

1-3 SQL built with a variable in Model::query()

High

Rule	cakephp2-query-concatenation
Risk	High
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
OWASP Top 10	A03:2021 - Injection
Confidence	MEDIUM
Places	2

SQL built from a string with a variable is passed to Model::query(). Use the values array of query() (\$this->Model->query('... WHERE id = ?', [\$id])) or find() with conditions arrays.

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. High

1-4 View or element named by the request

High

Rule	cakephp2-render-request
Risk	High
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
OWASP Top 10	A01:2021 - Broken Access Control
Confidence	HIGH
Places	1

A value of the request is passed to render() or element(). A path in it can render any template. Map the value to a list of allowed views.

src/Controller/PostsController.php:39

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

1. High

1-5 unserialize() of a value of the request

High

Rule	cakephp2-unserialize-request
Risk	High
CWE	CWE-502: Deserialization of Untrusted Data
OWASP Top 10	A08:2021 - Software and Data Integrity Failures
Confidence	HIGH
Places	1

A value of the request is passed to unserialize(): it can create objects of any class. Use json_decode().

src/Controller/PostsController.php:46

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

2. Medium

2-1 Default or sample Security.cipherSeed

Medium

Rule	cakephp2-config-cipher-seed
Risk	Medium
CWE	CWE-1188: Initialization of a Resource with an Insecure Default
OWASP Top 10	A02:2021 - Cryptographic Failures
Confidence	HIGH
Places	1

Security.cipherSeed is the default of the distribution or a sample of the documentation. It is used by the 'cipher' type of CookieComponent. Set SECURITY_CIPHER_SEED to a random number, and move the cookies to the 'aes' type.

config/core.php:4

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

2. Medium

2-2 Cookies encrypted with 'cipher'

Medium

Rule	cakephp2-config-cookie-cipher
Risk	Medium
CWE	CWE-327: Use of a Broken or Risky Cryptographic Algorithm
OWASP Top 10	A02:2021 - Cryptographic Failures
Confidence	HIGH
Places	1

CookieComponent encrypts with the 'cipher' type (Cookie.type is not set, or is 'cipher'), which is not secure. Set Cookie.type to 'aes', Cookie.key to a random value of 32 bytes or more, and Security.useOpenSsl to true.

config/core.php:5

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

2. Medium

2-3 Redirect to a value of the request

Medium

Rule	cakephp2-redirect-request
Risk	Medium
CWE	CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
OWASP Top 10	A01:2021 - Broken Access Control
Confidence	HIGH
Places	2

A value of the request is passed to `redirect()`. Redirect only to paths of the application, e.g. with `Router::url()` of a route array, or check the URL against a list.

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. Medium

2-4 CSRF or form tampering check turned off

Medium

Rule	cakephp2-security-csrf-disabled
Risk	Medium
CWE	CWE-352: Cross-Site Request Forgery (CSRF)
OWASP Top 10	A01:2021 - Broken Access Control
Confidence	MEDIUM
Places	2

The CSRF check or the form tampering check of SecurityComponent is turned off. Turn it off only for the actions that need it, e.g. with unlockedActions.

src/Controller/PostsController.php:12

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

src/Controller/PostsController.php:13

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

2. Medium

2-5 Variable printed in a view without h()

Medium

Rule	cakephp2-view-unescaped-output
Risk	Medium
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
OWASP Top 10	A03:2021 - Injection
Confidence	LOW
Places	5

A variable is printed in a view without h(). Escape it with h(), or use a helper that escapes.

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. Medium

2-6 Xml::build() with a variable**Medium**

Rule	cakephp2-xml-build-variable
Risk	Medium
CWE	CWE-918: Server-Side Request Forgery (SSRF)
OWASP Top 10	A10:2021 - Server-Side Request Forgery (SSRF)
Confidence	MEDIUM
Places	1

Xml::build() is called with a variable: a URL or a path in it is read. Pass ['readFile' => false] for a string of XML, and do not pass values of the request.

src/Controller/PostsController.php:44

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