PHP Fixer report

- Target: `demo\site`
- Generated: 2026-10-25 01:52:08 UTC
- Mode: scan only (no changes written)
- Files scanned: 10
- Findings: 31 (17 high, 4 medium, 10 low)
- Auto-fixable: 11
- Runtime: PHP 8.4.27 (verification binary) — patched against PHP2Shell (CVE-2026-109618, CVE-2026-109619)

Findings by rule

Rule	Count
dirname-file	9
removed-function	8
sql-injection	4
request-superglobal	2
header-location	2
extract	1
weak-password-hash	1
unserialize	1
dynamic-include	1
curly-offset	1
interp-braces	1

Findings

Severity	Location	Rule	What was found
high	`admin/login.php:9`	extract	Request array passed to extract().
high	`admin/login.php:10`	sql-injection	$email carries request data into a SQL string passed to a query function.
high	`admin/login.php:11`	weak-password-hash	md5() applied to a value that looks like a password.
high	`admin/reports.php:13`	sql-injection	$since carries request data into a SQL string passed to a query function.
high	`admin/reports.php:15`	unserialize	Request data is unserialized ($_COOKIE).
high	`contact.php:12`	sql-injection	$name carries request data into a SQL string passed to a query function.
high	`includes/db.php:6`	removed-function	mysql_connect() was removed.
high	`includes/db.php:8`	removed-function	mysql_error() was removed.
high	`includes/db.php:10`	removed-function	mysql_select_db() was removed.
high	`includes/db.php:17`	removed-function	mysql_query() was removed.
high	`includes/db.php:19`	removed-function	mysql_error() was removed.
high	`includes/db.php:28`	removed-function	mysql_fetch_assoc() was removed.
high	`includes/db.php:36`	sql-injection	$_GET carries request data into a SQL string passed to a query function.
high	`index.php:10`	dynamic-include	include path is built from request data ($page).
high	`lib/util.php:6`	curly-offset	$name{0} uses a curly offset.
high	`lib/util.php:12`	removed-function	money_format() was removed.
high	`lib/util.php:27`	removed-function	get_magic_quotes_gpc() was removed.
medium	`admin/reports.php:12`	request-superglobal	$_REQUEST read.
medium	`contact.php:14`	header-location	header("Location: ...") is not followed by exit.
medium	`contact.php:24`	request-superglobal	$_REQUEST read.
medium	`lib/util.php:22`	header-location	header("Location: ...") is not followed by exit.

low	admin/login.php:3	dirname-file	dirname(__FILE__)
low	admin/login.php:4	dirname-file	dirname(__FILE__)
low	admin/reports.php:3	dirname-file	dirname(__FILE__)
low	admin/reports.php:4	dirname-file	dirname(__FILE__)
low	contact.php:3	dirname-file	dirname(__FILE__)
low	contact.php:4	dirname-file	dirname(__FILE__)
low	includes/config.php:11	dirname-file	dirname(__FILE__)
low	index.php:3	dirname-file	dirname(__FILE__)
low	index.php:4	dirname-file	dirname(__FILE__)
low	lib/util.php:17	interp-braces	${who}

Detail and recommended fixes

admin/login.php:9:5 — extract() on request data (high)

Request array passed to extract().

Recommended fix: Read the keys you expect: $name = $_POST['name'] ?? ''. Never extract request arrays.

admin/login.php:10:71 — Request data concatenated into SQL (high)

$email carries request data into a SQL string passed to a query function.

Recommended fix: Bind the value: $stmt = $pdo->prepare("SELECT * FROM t WHERE id = ?"); $stmt->execute([$id]); Never interpolate into SQL.

admin/login.php:11:17 — md5/sha1 used for a password (high)

md5() applied to a value that looks like a password.

Recommended fix: password_hash($pw, PASSWORD_DEFAULT) on write, password_verify($pw, $hash) on login. Rehash on next successful login to migrate existing users.

admin/reports.php:13:63 — Request data concatenated into SQL (high)

$since carries request data into a SQL string passed to a query function.

Recommended fix: Bind the value: $stmt = $pdo->prepare("SELECT * FROM t WHERE id = ?"); $stmt->execute([$id]); Never interpolate into SQL.

admin/reports.php:15:11 — unserialize() on untrusted data (high)

Request data is unserialized ($_COOKIE).

Recommended fix: Use JSON: json_decode($input, true). If the format is fixed, pass ["allowed_classes" => false] as the second argument.

contact.php:12:65 — Request data concatenated into SQL (high)

$name carries request data into a SQL string passed to a query function.

Recommended fix: Bind the value: $stmt = $pdo->prepare("SELECT * FROM t WHERE id = ?"); $stmt->execute([$id]); Never interpolate into SQL.

includes/db.php:6:13 — Function removed from PHP (high)

mysql_connect() was removed.

Recommended fix: Replace with mysqli_connect or PDO.

includes/db.php:8:37 — Function removed from PHP (high)

mysql_error() was removed.

Recommended fix: Replace with mysqli_error($link).

`includes/db.php:10:5` **— Function removed from PHP (high)**

mysql_select_db() was removed.

Recommended fix: Replace with the database name in mysqli_connect/PDO DSN.

`includes/db.php:17:15` **— Function removed from PHP (high)**

mysql_query() was removed.

Recommended fix: Replace with mysqli_query or PDO::query.

`includes/db.php:19:14` **— Function removed from PHP (high)**

mysql_error() was removed.

Recommended fix: Replace with mysqli_error($link).

`includes/db.php:28:19` **— Function removed from PHP (high)**

mysql_fetch_assoc() was removed.

Recommended fix: Replace with $result->fetch_assoc().

`includes/db.php:36:59` **— Request data concatenated into SQL (high)**

$_GET carries request data into a SQL string passed to a query function.

Recommended fix: Bind the value: $stmt = $pdo->prepare("SELECT * FROM t WHERE id = ?"); $stmt->execute([$id]); Never interpolate into SQL.

`index.php:10:1` **— Request data in include/require (high)**

include path is built from request data ($page).

Recommended fix: Map a request key to a fixed list of files: $page = ['home' => __DIR__ . '/home.php']; then include $page[$key] ?? $page['home'];

`lib/util.php:6:19` **— Curly-brace string offset (removed in PHP 8) (high)**

$name{0} uses a curly offset.

Fix applied: Use square brackets: $str[$i].

`lib/util.php:12:12` **— Function removed from PHP (high)**

money_format() was removed.

Recommended fix: Replace with NumberFormatter::formatCurrency.

`lib/util.php:27:9` **— Function removed from PHP (high)**

get_magic_quotes_gpc() was removed.

Recommended fix: Replace with stripslashes() only where input is still escaped.

`admin/reports.php:12:10` **— $_REQUEST used (medium)**

$_REQUEST read.

Recommended fix: Read the intended channel: $_GET[...] or $_POST[...] with a default.

`contact.php:14:5` **— Redirect header without exit (medium)**

header("Location: ...") is not followed by exit.

Recommended fix: Follow every header("Location: ...") with exit; and only redirect to a fixed or whitelisted URL.

`contact.php:24:47` **— $_REQUEST used (medium)**

$_REQUEST read.

Recommended fix: Read the intended channel: $_GET[...] or $_POST[...] with a default.

`lib/util.php:22:5` — **Redirect header without exit (medium)**

header("Location: ...") is not followed by exit.

Recommended fix: Follow every header("Location: ...") with exit; and only redirect to a fixed or whitelisted URL.

`admin/login.php:3:14` — **dirname(__FILE__) instead of __DIR__ (low)**

dirname(__FILE__)

Fix applied: Replace dirname(__FILE__) with __DIR__.

`admin/login.php:4:14` — **dirname(__FILE__) instead of __DIR__ (low)**

dirname(__FILE__)

Fix applied: Replace dirname(__FILE__) with __DIR__.

`admin/reports.php:3:14` — **dirname(__FILE__) instead of __DIR__ (low)**

dirname(__FILE__)

Fix applied: Replace dirname(__FILE__) with __DIR__.

`admin/reports.php:4:14` — **dirname(__FILE__) instead of __DIR__ (low)**

dirname(__FILE__)

Fix applied: Replace dirname(__FILE__) with __DIR__.

`contact.php:3:14` — **dirname(__FILE__) instead of __DIR__ (low)**

dirname(__FILE__)

Fix applied: Replace dirname(__FILE__) with __DIR__.

`contact.php:4:14` — **dirname(__FILE__) instead of __DIR__ (low)**

dirname(__FILE__)

Fix applied: Replace dirname(__FILE__) with __DIR__.

`includes/config.php:11:9` — **dirname(__FILE__) instead of __DIR__ (low)**

dirname(__FILE__)

Fix applied: Replace dirname(__FILE__) with __DIR__.

`index.php:3:14` — **dirname(__FILE__) instead of __DIR__ (low)**

dirname(__FILE__)

Fix applied: Replace dirname(__FILE__) with __DIR__.

`index.php:4:14` — **dirname(__FILE__) instead of __DIR__ (low)**

dirname(__FILE__)

Fix applied: Replace dirname(__FILE__) with __DIR__.

`lib/util.php:17:19` — **${var} interpolation (deprecated in PHP 8.2) (low)**

${who}

Fix applied: Use {$var} inside the string.

Proposed patch (not applied)

admin\login.php

```
--- a/admin\login.php
+++ b/admin\login.php
@@ -1,7 +1,7 @@
 <?php
 // Admin login. Passwords were hashed with md5 before the move to PHP 8.
```

```
-require_once dirname(__FILE__) . '/../includes/config.php';
-require_once dirname(__FILE__) . '/../includes/db.php';
+require_once __DIR__ . '/../includes/config.php';
+require_once __DIR__ . '/../includes/db.php';

 session_start();
```

admin\reports.php

```
--- a/admin\reports.php
+++ b/admin\reports.php
@@ -1,7 +1,7 @@
 <?php
 // Admin reports. Runs shell tools to export and emails the result.
-require_once dirname(__FILE__) . '/../includes/config.php';
-require_once dirname(__FILE__) . '/../includes/db.php';
+require_once __DIR__ . '/../includes/config.php';
+require_once __DIR__ . '/../includes/db.php';

 session_start();
 if (empty($_SESSION['uid'])) {
```

contact.php

```
--- a/contact.php
+++ b/contact.php
@@ -1,7 +1,7 @@
 <?php
 // Handles the contact form. Posts to itself.
-require_once dirname(__FILE__) . '/includes/config.php';
-require_once dirname(__FILE__) . '/includes/db.php';
+require_once __DIR__ . '/includes/config.php';
+require_once __DIR__ . '/includes/db.php';

 $sent = false;
 if ($_SERVER['REQUEST_METHOD'] == 'POST') {
```

includes\config.php

```
--- a/includes\config.php
+++ b/includes\config.php
@@ -8,6 +8,6 @@
 $db_pass = 'plumb2014';
 $db_name = 'rivera_site';

-$root = dirname(__FILE__);
+$root = __DIR__;
 $uploads = $root . '/uploads';
```

index.php

```
--- a/index.php
+++ b/index.php
@@ -1,7 +1,7 @@
 <?php
 // Site entry point. Routes ?p= to a page file.
-require_once dirname(__FILE__) . '/includes/config.php';
-require_once dirname(__FILE__) . '/includes/db.php';
+require_once __DIR__ . '/includes/config.php';
+require_once __DIR__ . '/includes/db.php';

 $page = $_GET['p'];
```

```
$title = 'Rivera Plumbing';
```

lib\util.php

```
--- a/lib\util.php
+++ b/lib\util.php
@@ -3,7 +3,7 @@

 function initials($name)
 {
-    $first = $name{0};
+    $first = $name[0];
     return strtoupper($first) . '.';
 }

@@ -14,7 +14,7 @@

 function greeting($who)
 {
-    return "Hello ${who}, thanks for calling Rivera Plumbing.";
+    return "Hello {$who}, thanks for calling Rivera Plumbing.";
 }

 function redirect_back()
```

Method and limits

- Only mechanically provable rewrites are applied; anything touching business logic is reported.
- Each patched file is written to a temporary copy, checked with `php -l`, and only then replaced.
- Original bytes are kept in the backup directory; `phpfixer restore <dir>` puts them back.
- The scanner reads code, strings, comments and inline HTML separately, so matches inside comments or quoted text are not treated as code.
- A clean report is not a security guarantee: findings are pattern-level, and a manual review still applies.