lfi1.php

* **总漏洞数**: 1

1. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 使用 include($\_GET["page"]); 直接包含用户输入的文件，存在本地文件包含（LFI）或远程文件包含（RFI）漏洞。攻击者可以利用这个漏洞读取敏感文件或执行任意代码。
   * **修复建议**: 验证和限制用户输入，只允许包含预定义的文件。可以使用白名单方式或者基于文件名的严格验证。

lfi2.php

* **总漏洞数**: 1

1. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 使用 include("includes/".$\_GET['library'].".php"); 直接包含用户输入的文件，存在本地文件包含（LFI）或远程文件包含（RFI）漏洞。攻击者可以通过操控 library 参数包含任意文件，导致代码执行或信息泄露。
   * **修复建议**: 验证和限制用户输入，只允许包含预定义的文件。可以使用白名单方式或者基于文件名的严格验证。

lfi3.php

* **总漏洞数**: 2

1. **漏洞类型**: 任意文件读取 (Arbitrary File Read)
   * **CWE 标号**: CWE-73
   * **描述**: 使用 file\_get\_contents($\_GET['file']); 直接读取用户指定的文件，存在任意文件读取漏洞。攻击者可以通过操控 file 参数读取服务器上的任意文件，获取敏感信息。
   * **修复建议**: 限制文件读取的路径，并确保只能读取预定义的文件。可以使用白名单方式或者基于文件名的严格验证。

lfi4.php

* **总漏洞数**: 1

1. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 使用 include('includes/class\_'.addslashes($\_GET['class']).'.php'); 直接包含用户输入的文件，存在本地文件包含（LFI）漏洞。尽管使用了 addslashes() 函数，这不足以防止文件包含漏洞，攻击者仍可能通过构造特殊输入绕过保护。
   * **修复建议**: 验证和限制用户输入，只允许包含预定义的文件。可以使用白名单方式或者基于文件名的严格验证。

lfi5.php

* **总漏洞数**: 2

1. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 使用 include("pages/$file"); 直接包含用户输入的文件，存在本地文件包含（LFI）漏洞。尽管使用了 str\_replace('../', '', $\_GET['file']); 来防止目录遍历，但攻击者仍可能通过其他路径操作绕过保护。
   * **修复建议**: 验证和限制用户输入，只允许包含预定义的文件。可以使用白名单方式或者基于文件名的严格验证。
2. **漏洞类型**: 目录遍历 (Directory Traversal)
   * **CWE 标号**: CWE-22
   * **描述**: 尽管使用了 str\_replace() 来去除 ../，这并不足以完全防止目录遍历攻击。攻击者可以通过构造特殊输入绕过该检查，访问任意文件。
   * **修复建议**: 使用 realpath() 函数并确保文件路径在允许的目录内。

lfi6.php

* **总漏洞数**: 1

1. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 使用 include($\_POST["page"]); 直接包含用户输入的文件，存在本地文件包含（LFI）漏洞。攻击者可以通过操控 page 参数包含任意文件，导致代码执行或信息泄露。
   * **修复建议**: 验证和限制用户输入，只允许包含预定义的文件。可以使用白名单方式或者基于文件名的严格验证。

lfi7.php

* **总漏洞数**: 1

1. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 使用 include("includes/".$\_POST['library'].".php"); 直接包含用户输入的文件，存在本地文件包含（LFI）漏洞。攻击者可以通过操控 library 参数包含任意文件，导致代码执行或信息泄露。
   * **修复建议**: 验证和限制用户输入，只允许包含预定义的文件。可以使用白名单方式或者基于文件名的严格验证。

lfi8.php

* **总漏洞数**: 2

1. **漏洞类型**: 任意文件读取 (Arbitrary File Read)
   * **CWE 标号**: CWE-73
   * **描述**: 使用 file\_get\_contents($\_POST['file']); 直接读取用户指定的文件，存在任意文件读取漏洞。攻击者可以通过操控 file 参数读取服务器上的任意文件，获取敏感信息。
   * **修复建议**: 限制文件读取的路径，并确保只能读取预定义的文件。可以使用白名单方式或者基于文件名的严格验证。
2. **漏洞类型**: 信息泄露 (Information Exposure)
   * **CWE 标号**: CWE-200
   * **描述**: 尽管代码中阻止了 .php 文件的读取，但没有其他额外的文件类型检查，仍然可能导致信息泄露。例如，攻击者可以读取配置文件或其他敏感数据文件。
   * **修复建议**: 使用 realpath() 函数并确保文件路径在允许的目录内。

lfi9.php

* **总漏洞数**: 1

1. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 使用 include('includes/class\_'.addslashes($\_POST['class']).'.php'); 直接包含用户输入的文件，存在本地文件包含（LFI）漏洞。尽管使用了 addslashes() 函数，这不足以防止文件包含漏洞，攻击者仍可能通过构造特殊输入绕过保护。
   * **修复建议**: 验证和限制用户输入，只允许包含预定义的文件。可以使用白名单方式或者基于文件名的严格验证。

lfi10.php

* **总漏洞数**: 2

1. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 使用 include("pages/$file"); 直接包含用户输入的文件，存在本地文件包含（LFI）漏洞。尽管使用了 str\_replace('../', '', $\_POST['file']); 来防止目录遍历，但攻击者仍可能通过其他路径操作绕过保护。
   * **修复建议**: 验证和限制用户输入，只允许包含预定义的文件。可以使用白名单方式或者基于文件名的严格验证。
2. **漏洞类型**: 目录遍历 (Directory Traversal)
   * **CWE 标号**: CWE-22
   * **描述**: 尽管使用了 str\_replace() 来去除 ../，这并不足以完全防止目录遍历攻击。攻击者可以通过构造特殊输入绕过该检查，访问任意文件。
   * **修复建议**: 使用 basename() 函数来防止目录遍历，并确保文件路径在允许的目录内。

lfi11.php

* **总漏洞数**: 1

1. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 使用 include($\_POST['stylepath']); 直接包含用户输入的文件，存在本地文件包含（LFI）漏洞。攻击者可以通过操控 stylepath 参数包含任意文件，导致代码执行或信息泄露。
   * **修复建议**: 验证和限制用户输入，只允许包含预定义的文件。可以使用白名单方式或者基于文件名的严格验证

lfi12.php

* **总漏洞数**: 1

1. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 使用 include($\_GET['stylepath']); 直接包含用户输入的文件，存在本地文件包含（LFI）漏洞。攻击者可以通过操控 stylepath 参数包含任意文件，导致代码执行或信息泄露。
   * **修复建议**: 验证和限制用户输入，只允许包含预定义的文件。可以使用白名单方式或者基于文件名的严格验证。

lfi13.php

* **总漏洞数**: 2

1. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 使用 include("pages/$file"); 直接包含用户输入的文件，存在本地文件包含（LFI）漏洞。尽管使用了 str\_replace('../', '', $\_GET['file']); 来防止目录遍历，但攻击者仍可能通过其他路径操作绕过保护。
   * **修复建议**: 验证和限制用户输入，只允许包含预定义的文件。可以使用白名单方式或者基于文件名的严格验证。
2. **漏洞类型**: 目录遍历 (Directory Traversal)
   * **CWE 标号**: CWE-22
   * **描述**: 尽管使用了 str\_replace() 来去除 ../，这并不足以完全防止目录遍历攻击。攻击者可以通过构造特殊输入绕过该检查，访问任意文件。
   * **修复建议**: 使用 basename() 函数来防止目录遍历，并确保文件路径在允许的目录内。

lfi14.php

* **总漏洞数**: 2

1. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 使用 include("pages/$file"); 直接包含用户输入的文件，存在本地文件包含（LFI）漏洞。尽管使用了 str\_replace('../', '', $\_POST['file']); 来防止目录遍历，但攻击者仍可能通过其他路径操作绕过保护。
   * **修复建议**: 验证和限制用户输入，只允许包含预定义的文件。可以使用白名单方式或者基于文件名的严格验证。
2. **漏洞类型**: 目录遍历 (Directory Traversal)
   * **CWE 标号**: CWE-22
   * **描述**: 尽管使用了 str\_replace() 来去除 ../，这并不足以完全防止目录遍历攻击。攻击者可以通过构造特殊输入绕过该检查，访问任意文件。
   * **修复建议**: 使用 basename() 函数来防止目录遍历，并确保文件路径在允许的目录内。