Example1.php

* **总漏洞数**: 3

1. **漏洞类型**: 文件上传路径遍历 (File Upload Path Traversal)
   * **CWE 标号**: CWE-22
   * **描述**: 使用 basename($\_FILES['uploaded']['name']) 来确定目标路径，攻击者可以通过上传带有路径遍历字符（例如 ../）的文件名，将文件上传到服务器上的任意位置。
   * **修复建议**: 只允许上传预定义的文件类型，并确保文件名不包含路径遍历字符。
2. **漏洞类型**: 文件上传任意代码执行 (Unrestricted File Upload)
   * **CWE 标号**: CWE-434
   * **描述**: 未对上传的文件类型进行严格验证，攻击者可以上传恶意脚本文件并在服务器上执行。
   * **修复建议**: 验证文件类型，确保只允许上传特定的文件类型（例如图像文件），并且在保存文件时使用安全的文件扩展名。
3. **漏洞类型**: 信息泄露 (Information Exposure)
   * **CWE 标号**: CWE-200
   * **描述**: 上传失败时的错误信息可能会泄露服务器的文件路径信息。
   * **修复建议**: 在错误消息中避免包含敏感的路径信息，只显示通用的错误信息。

Example2.php

* **总漏洞数**: 2

1. **漏洞类型**: 文件上传路径遍历 (File Upload Path Traversal)
   * **CWE 标号**: CWE-22
   * **描述**: 使用 basename($\_FILES['uploaded']['name']) 来确定目标路径，攻击者可以通过上传带有路径遍历字符（例如 ../）的文件名，将文件上传到服务器上的任意位置。
   * **修复建议**: 只允许上传预定义的文件类型，并确保文件名不包含路径遍历字符。
2. **漏洞类型**: 文件上传任意代码执行 (Unrestricted File Upload)
   * **CWE 标号**: CWE-434
   * **描述**: 尽管验证了文件类型和大小，但没有验证上传文件的实际 MIME 类型和扩展名，攻击者仍可能上传带有恶意代码的文件。
   * **修复建议**: 验证文件的实际 MIME 类型和扩展名，并确保上传文件目录和名称的安全性。

Example3.php

* **总漏洞数**: 2

1. **漏洞类型**: 文件上传路径遍历 (File Upload Path Traversal)
   * **CWE 标号**: CWE-22
   * **描述**: 使用 basename($\_FILES['uploaded']['name']) 来确定目标路径，攻击者可以通过上传带有路径遍历字符（例如 ../）的文件名，将文件上传到服务器上的任意位置。
   * **修复建议**: 使用 basename() 函数对文件名进行处理，并确保文件名不包含路径遍历字符。
2. **漏洞类型**: 文件上传任意代码执行 (Unrestricted File Upload)
   * **CWE 标号**: CWE-434
   * **描述**: 尽管验证了文件类型和大小，但没有验证上传文件的实际 MIME 类型和扩展名，攻击者仍可能上传带有恶意代码的文件。
   * **修复建议**: 验证文件的实际 MIME 类型和扩展名，并确保上传文件目录和名称的安全性。

Insomnihack\_2019\_l33t-hoster.php

* **总漏洞数**: 4

1. **漏洞类型**: 路径遍历 (Path Traversal)
   * **CWE 标号**: CWE-22
   * **描述**: 使用用户提供的文件名并将其保存到服务器目录中，存在路径遍历风险。攻击者可以通过构造特殊文件名将文件保存到未预期的目录。
   * **修复建议**: 使用 basename() 函数处理文件名，并严格验证上传目录。
2. **漏洞类型**: 文件包含漏洞 (File Inclusion Vulnerability)
   * **CWE 标号**: CWE-98
   * **描述**: 上传文件中如果包含 PHP 代码，可能被执行，导致远程代码执行。
   * **修复建议**: 验证上传文件的实际 MIME 类型，并确保不允许上传 PHP 文件。可以使用 exif\_imagetype() 函数来验证图像文件类型。
3. **漏洞类型**: 会话固定 (Session Fixation)
   * **CWE 标号**: CWE-384
   * **描述**: 在会话开始后，没有重新生成会话 ID，可能导致会话固定攻击。
   * **修复建议**: 在用户登录后立即调用 session\_regenerate\_id(true) 以生成新的会话 ID。
4. **漏洞类型**: 信息泄露 (Information Exposure)
   * **CWE 标号**: CWE-200
   * **描述**: 上传失败时返回的错误信息可能会泄露系统的内部信息。
   * **修复建议**: 返回通用的错误信息，而不是直接显示系统的内部信息。

WishList.php

* **总漏洞数**: 2

1. **漏洞类型**: 文件上传路径遍历 (File Upload Path Traversal)
   * **CWE 标号**: CWE-22
   * **描述**: 使用用户提供的文件名并将其保存到服务器目录中，存在路径遍历风险。尽管使用了白名单检查，但白名单检查针对的是文件名的具体值而不是文件扩展名和路径。
   * **修复建议**: 使用 basename() 函数对文件名进行处理，并确保文件名不包含路径遍历字符。还应将白名单检查扩展到文件扩展名。
2. **漏洞类型**: 不安全的反序列化 (Insecure Deserialization)
   * **CWE 标号**: CWE-502
   * **描述**: 在 PHP 中，通过魔术方法 \_\_destruct() 来执行文件上传操作，如果对象被反序列化，可能导致代码执行漏洞。
   * **修复建议**: 避免在魔术方法中执行安全敏感操作，并使用专门的方法进行文件处理。