1. PHP – скрипт: читает и выводит содержимое файлы, имя файла через параметр file в URL.
2. Функция Path Filter удаляет последовательности типа «://» и обратные слэши, удаляет относительные пути «../». Проблема в том, что это можно обойти, введя, например, запасные символы.
3. Содержимое считается с помощью file\_get\_contents. Уязвимость в том, что если злоумышленник передаст путь к файлу, он получит доступ к содержимому.
4. Так же в коде в целом нет ограничения на чтения файлов только с определённой директории.

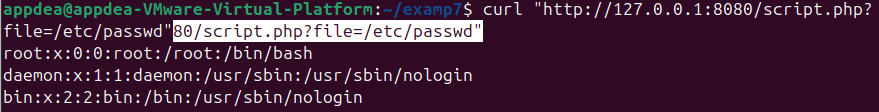
**КАК ВОСПРОИЗВЕСТИ:**

1. Запускаем php - сервер:

*php -S localhost:8080*

1. Используем curl для отправки запроса по абсолютному пути к серверу:

*curl http://127.0.0.1:8080/script.php?file=/etc/passwd*



**Как защитить:**

1. Может ограничить используемую директорию. Например, при помощи realpath:

*$baseDir = "/var/www/html/files/"; // Разрешенная директория*

*if (isset($\_GET['file']) && $\_GET['file'] != "") {*

*$file = $\_GET['file'];*

*$filePath = realpath($baseDir . $file);*

*// Проверяем, что файл находится в разрешенной директории*

*if (strpos($filePath, $baseDir) !== 0) {*

*die("Access denied");*

*}*

*} else {*

*$filePath = $baseDir . "index.html"; // Файл по умолчанию*

*}*

1. Можно использовать белый список для допустимых файлов, если мы знаем, чем именно мы будем пользоваться:

*$allowedFiles = ["index.html", "about.html", "contact.html"]; // Белый список*

1. Можем использовать fopen с проверкой пути

*$baseDir = "/var/www/html/files/";*

*if (isset($\_GET['file']) && $\_GET['file'] != "") {*

*$file = basename($\_GET['file']);*

*$filePath = $baseDir . $file;*

*if (!file\_exists($filePath)) {*

*die("File not found");*

*}*

*$content = file\_get\_contents($filePath);*

*} else {*

*$filePath = $baseDir . "index.html"; // Файл по умолчанию*

*}*

1. Можно использовать basename, которая в целом удалит весь путь и оставит только имя файла

*if (isset($\_GET['file']) && $\_GET['file'] != "") {*

*$file = basename($\_GET['file']); // Удаляем путь, оставляя только имя файла*

*$filePath = "/var/www/html/files/" . $file;*

*} else {*

*$filePath = "/var/www/html/files/index.html"; // Файл по умолчанию*

*}*