Professor’s computer

- 문제 이름: Professor’s computer
- 카테고리: Web
- 난이도: Easy

문제 배경 및 설명

교수님의 컴퓨터를 뚫어라.

교수님의 컴퓨터에는 학생들이 `ping` 테스트를 할 수 있는 기능이 존재합니다. 이 기능은 내부적으로 입력된 값을 시스템 명령어에 그대로 붙여 사용하기 때문에 악의적인 명령어를 삽입할 수 있습니다.

사용된 취약점**: Command Injection (**명령어 삽입**)**

이 문제는 사용자의 입력을 리눅스 시스템 명령어로 검증 없이 실행하는 `system()` 또는 `shell_exec()` 함수를 통해 발생하는 Command Injection 취약점을 이용한 문제입니다. 사용자가 `host=127.0.0.1;cat grades.txt`와 같은 입력을 보내면 세미콜론 뒤의 명령어가 시스템에서 함께 실행됩니다.

풀이 방법

목표

`/flag/grades.txt` 파일 안에 숨겨진 flag를 확인하는 것

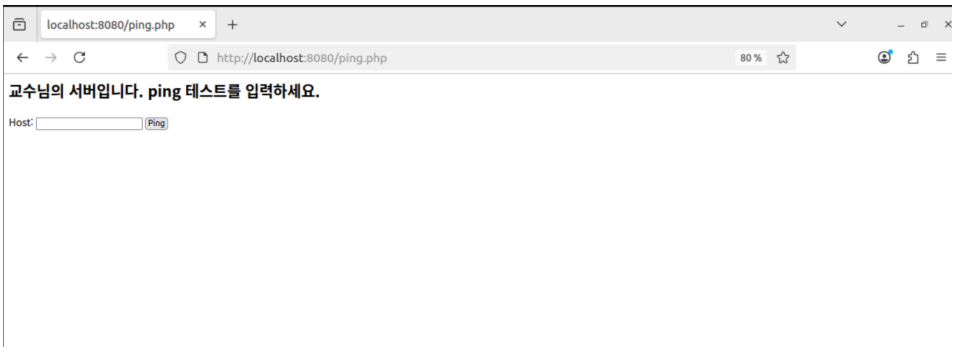
예시:

```
http://localhost:8080/ping.php?host=127.0.0.1;cat grades.txt 1337
```

- ; → . `ping` 뒤에 다른 명령어를 실행하도록 만듭니다.
- `cat grades.txt` → 숨겨진 파일 내용을 출력하는 명령어처럼 보이게 합니다.
- 1337 → 아무 의미 없는 숫자. 그러나 이 숫자가 포함되지 않으면 플래그가 출력되지 않습니다.
- 단순히 `;cat grades.txt`만 입력하면 실패 페이지(`fail.php`)로 이동되며, 플래그가 출력되지 않습니다.
- 정규표현식을 통해 입력 값에 포함된 4자리 이상의 숫자 중 1337이 있을 경우에만 php 내부에서 플래그 파일을 읽어 출력됩니다.

1. 처음 화면

2. ping.php



3. 잘못 입력 시

4. /flag/grades.txt 입력시

5. flag 출력화면