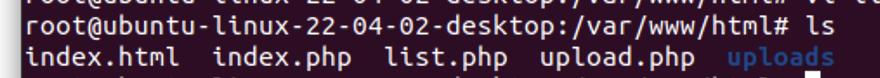
WHS\_8반\_신지연3293

0. 웹쉘은 공격자가 원격지에서 피해 서버에 명령을 수행할 수 있게 작성한 server side 파일이다. 이렇게 악의적으로 작성한 스크립트 파일인 웹쉘을 업로드하여 웹 서버를 장악할 수 잇다.

1. 웹서버 구축 후 웹쉘을 사용해서 시스템 명령 실행한 후 캡쳐

환경 (ubuntu 22.04.02, apache2, php)



우분투에 아파치 웹서버와 php를 설치한다. /var/www/html에 uploads.php, list.php와 uploads폴더를 만든다.

- uploads.php : 파일 업로드하는 페이지

- list.php : 업로드한 파일을 보여주고 접속할 수 있는 페이지

- uploads : 업로드한 파일을 보관하는 페이지

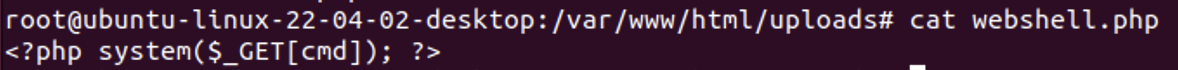
|  |  |
| --- | --- |
| 텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진  자동 생성된 설명 | 스크린샷, 텍스트, 소프트웨어이(가) 표시된 사진  자동 생성된 설명 |
| Localhost/upload.php | Localhost/list.php |

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명텍스트, 스크린샷, 메뉴, 폰트이(가) 표시된 사진

자동 생성된 설명

웹쉘 코드가 작성되어있는 webshell.php를 업로드한다.



Localhost/list.php에서 Webshell.php를 클릭하면 파일 업로드 위치가 나오게 되어 실제 파일의 저장시 업로드 위치 유추가 가능하다. Hello.txt같은 경우 uploads라는 폴더 아래에 있다는 것을 알 수 있다.

텍스트, 스크린샷, 폰트, 화이트이(가) 표시된 사진

자동 생성된 설명

파일 위치를 알아내고 해당 경로에서 cmd=ls;로 하위 파일들을 볼 수 있다. 처음부터 upload.php를 만들때 추가 보안 검증 및 파일 유형 검사를 수행하지 않아서 webshell.php뒤에 get 파라미터로 cmd에 시스템 명령어를 보내면 그 결과를 받아 볼 수 있지만 500에러가 나왔다.

텍스트, 스크린샷, 소프트웨어, 컴퓨터 아이콘이(가) 표시된 사진

자동 생성된 설명

Webshell.php를 로드하는 과정을 살펴보니 upgrade-insecure -requests라는 헤더가 1로 설정디어 있어서 혹시 몰라 0으로 변경하였지만 같은 오류가 나왔다. 찾아보니 php는 보안상의 이유로 외부에서 시스템 명령을 실행하려는 시도를 차단한다고 한다.

텍스트, 스크린샷, 소프트웨어, 번호이(가) 표시된 사진

자동 생성된 설명

2. 웹쉘 실행을 막으려면 어떤 방법을 사용할 수 있을지 고민후 적용하고 캡쳐

파일 업로드를 통한 웹쉘을 막으려면 먼저 업로드할 수 있는 파일의 확장자를 제한하고 허용되지 않는 파일 유형을 걸러내야 한다. 위의 실습과 같이 웹쉘을 실행할 수 있는 PHP, ASP, JSP 등의 파일 확장자를 업로드하지 못하도록 제한해야 한다. 그렇기 위해서는 uploads.php에 다음과 같은 코드를 추가해야 한다.

텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

또한 파일의 디렉토리 정보가 url에 나오지 않도록 웹 루트 디렉토리를 이용하여 루트 디렉토리 이하에 파일을 저장하면 URL에 해당 디렉토리 경로가 나타나지 않게 한다. 또는 .htaccess 파일을 사용하여 디렉토리에서 직접 파일에 대한 접근을 금지하고 디렉토리의 내용만 표시하도록 한다.