파라미터 변조

파라미터 변조는 파라미터로 전달되는 정보를 변조하여 명령어 삽입/ 원격지 파일 삽입 / 타인 글 수정/삭제 등 다양한 취약점을 발생시킬 수 있다.

사례분석

1. 타인의 비밀 글 보기

사용자는 자신이 작성한 글을 비밀 글로 등록하여 작성자 및 관리자만이 볼 수 있도록 설정한 경우가 있은 이를 우회하는 방법도 존재한다.

Ex) /bbs/qna\_view.asp?seq=13

/bbs/qna\_view.asp?seq=11

이처럼 파라미터로 변화를 주는 경우 변화가 있는 부분을 취약점으로 예측하여 취약한부분에 접근할 수 있다.

1. 공지사항 글 변조

일반적으로 관리자만이 접근가능한 공지사항의 경우는 보기기능 밖에 제공되지 않기 때문에 기능에 따른 페이지 이름 등을 추측하여 접근을 시도해 본다.

/bbs/notice\_view.asp 가 공지사항 읽기라면

/bbs/notice\_write.asp 등

혹은, 공지사항 글 작성을 자바 스크립트로 통제하는 경우의 우회방법을 확인해 본다.

<http://www.xxx.xxxx/bbs.do?cmd=view&no=21>

이런 경우 1. 파라미터를 write로 변경한다 2. 프록시로 데이터를 가로챈 후 자바스크립트 로직 삭제 후 웹서버로 전송하여

1. 자바스크립트로 구성된 수정/삭제페이지 정보노출

Function jsDelete(){

If(confirm(‘선택한 게시물을 삭제합니까?’)){

Document.dForm.action=”bbs.Delete.do”;

Document.dForm.submit();

}

}

1. 파일 삽입

외부파일 혹은 내부파일을 삽입하는 경우 웹 쉘 파일 등을 내부 파일처럼 인식 시키거나 시스템 파일에 접근하는 취약점을 의미한다. 취약점이 있는 경우 널 바이트 인잭션을 통한 공격을 한다.

1. 명령어 삽입

-윈도우 cmd에서 &사용 가능한점

-exec()로 변수로서 들어가서 사용되는 경우

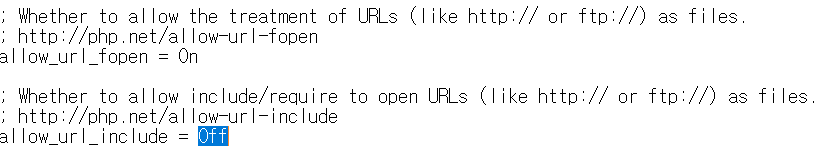
|  |  |
| --- | --- |
| 구분 | 취약한함수 |
| PHP | Require(), include(), eval(), exec(), passthru(), system(), fopen()등 |
| PERL | Open(), sysopen(), glob(), system() |
| JAVA | System.\* |
| C | System(), exec(), strcpy(), strcat(), sprint() |
| PYTHON | Exec(), eval(), execfile(), compile(), input() |

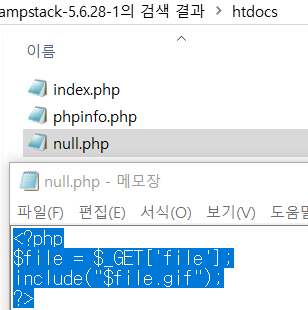
1. URL Redirection

파라미터에 ?target=http://malicious.com 등 추가

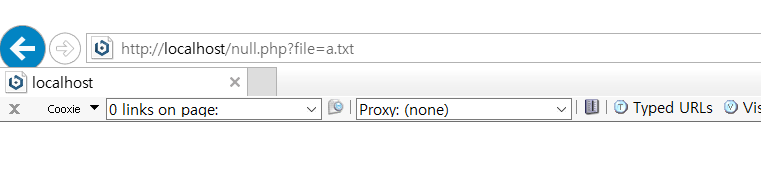
모의실습

1. 파일 삽입





상기소스는 GET방식으로 file변수를 입력받고 해당변수를 include함수에 삽입하기에 전형적인 RFI. LFI취약점이 발생되는 코드이다.



1. 명령어 삽입
2. 웹서버의 버퍼 오버 플로우 점검

298~322