webhacking.kr 60번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-04
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

Access Denied와 함께 index.phps를 가리킨다.

들어가보면 소스는 다음과 같다.

```
<?
sleep(1);
if(eregi("[0-9]",$_COOKIE[PHPSESSID])) exit("Access Denied<br><a
href=index.phps>index.phps</a>");
if($_GET[mode]=="auth")
{
echo("Auth~<br>");
    $f=@file("readme/$_SESSION[id].txt");
    for($i=0;$i<=strlen($f);$i++)
        {
        $result.=$f[$i];
        }
    if(eregi("$_SESSION[id]",$result))
    {
    echo("Done!");
    @unlink("readme/$_SESSION[id].txt");
    @clear();
    exit();
    }
}
$f=@fopen("readme/$_SESSION[id].txt","w");
@fwrite($f,"$_SESSION[id]");
@fclose($f);
if($_SERVER[REMOTE_ADDR]!="127.0.0.1")
{
sleep(1);
@unlink("readme/$_SESSION[id].txt");
}
?>
```

우선 쿠키의 PHPSESSID에 숫자가 있다면 종료한다.

그리고 GET형식으로 받은 mode값이 auth라면 SESSION[id].txt 파일을 읽고 그 값이 SESSION[id]와 같다면 클리어이다.

또한 아래에선 SESSION[id].txt를 만들어서 안에 SESSION[id]를 쓴다.

ip가 127.0.0.1이 아니라면 1초 대기한 후 파일을 지운다.

지우기 전 1초를 대기하므로 크롬과 익스플로러로 동시에 접속해보기로 했다.
우선 크롬의 PHPSESSID쿠키를 a로 바꿔서 맨 위의 if구문을 통과한다.
익스플로러의 PHPSESSID쿠키도 aa로 바꾼다.
그리고 크롬으로는 그냥 접속을, 익스플로러론 ?mode=auth로 접속을 빠르게 하게 되면 다음과 같이 클리어된다.