마법봉

해쉬에 마법을 부여하면 그 어떤 것도 뚫릴지어니...

If you enchant a hash, Anything will breakthrough...





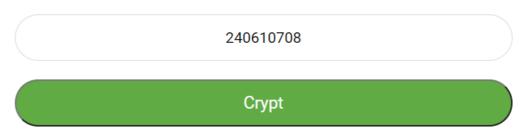
```
<?php
show_source(__FILE__);
$flag = "if_you_solved";
$input = $_GET['flag'];
if(md5("240610708") == sha1($input)){
    echo $flag;
}
else{
    echo "Nah...";
}
?>
Nah...
```

마법봉 1

코드를 보면 240610708을 md5로 암호화한 값과 input값을 sha1으로 암호화한 값을 비교한다.

MD5 Encryption

Enter a word here to get its MD5 hash:



먼저 240610708을 md5로 암호화해보면

The MD5 hash for 240610708 is: 0e462097431906509019562988736854

라고 나온다.

php에서는 비교연산자에 대한 취약점이 나타나는데

A == B 를 비교하면 두개의 자료형이 달라도 데이터가 일치하면 true를 반환하기 때문에 여기서 지수를 이용하면 0e로 시작되는 값이 모두 0으로 인식된다.

따라서 sha1로 암호화한 값도 0이 되게 하기 위해서 sha1의 매직해쉬를 만들어 주는 값을 찾으면

Hash Type	Hash Length	"Magic" Number	Magic Hashes	Found By
md2	32	505144726	0e015339760548602306096794382326	WhiteHat Security, Inc.
md4	32	48291204	0e266546927425668450445617970135	WhiteHat Security, Inc.
md5	32	240610708	0e462097431906509019562988736854	Michal Spacek
shal	40	10932435112	0e07766915004133176347055865026311692244	Independently found by Michael A.
				Cleverly & Michele Spagnuolo &
				Rogdham
		<u> </u>		

마법봉 2

10932435112인 것을 알 수 있다.

← → C ▲ 주의 요함 | ctf.j0n9hyun.xyz:2029/flag.php?flag=10932435112

 ${\bf HackCTF\{magic_makes_everything_possible\}}$

마법봉 3