2018.7.16 Plit00 김두형

MD5_COMPARE

wargame.kr

다시 살펴보자

- 맨날 워게임 풀이하면 제자리를 머무는거같다.
- 외주를 해보자.
- 나와있는 CTF 문제들을 최대한 다 풀어보자.
- CTF Write-up도 많이보자

Return

- 취약점 찾고있어요
- Root-me web-client, web-sever 올클
- Pawnable . Kr dragon까지

md5_compare

Index

1.분석
2.풀이
3.QnA

분석

- ctype_alpha($v1)
- is_numeric($v2)
- v1 != v2

  chk = false
  or
  chk = true

```php
<?php
    if (isset($_GET['view-source'])) {
         show_source(__FILE__);
         exit();
    }

    if (isset($_GET['v1']) && isset($_GET['v2'])) {
        sleep(3); // anti brute force

        $chk = true;
        $v1 = $_GET['v1'];
        $v2 = $_GET['v2'];

        if (!ctype_alpha($v1)) {$chk = false;}
        if (!is_numeric($v2) ) {$chk = false;}
        if (md5($v1) != md5($v2)) {$chk = false;}

        if ($chk){
            include("../lib.php");
            echo "Congratulations! FLAG is : ".auth_code("md5_compare");
        } else {
            echo "Wrong...";
        }
    }
?>
```

지식

- Php magic hash

▲ PHP: md5('240610708') == md5('QNKCDZO') (3v4l.org)

240 points by dbrgn on May 4, 2015 | hide | past | web | favorite | 175 comments

▲ dietrichepp on May 4, 2015 [-]

I'm not exactly clear on how PHP == works, but you can see the MD5 for yourself:

```
$ echo -n 240610708 | md5sum
0e462097431906509019562988736854  -
$ echo -n QNKCDZO | md5sum
0e830400451993494058024219903391  -
$ echo -n aabg7XSs | md5sum
0e087386482136013740957780965295  -
```

- String => float && 0=0 true!

"혼자 다시 풀어보세요"

–dudu

QnA