

Challenge - PHP serial cracking



Description

- A secure application is using a unique algorithm to validate Serial Numbers in a PHP Web Application.
- You were able to gain access to the PHP source code of the application.

Challenge

Analyze the Serial Number Validation method algorithm and try to find valid serial numbers.

Details

Serial Validation Method:

```
1
2 function VSSG($pwd)
3 {
4     $hash= hash('MD5', $pwd);
5     for ($x = 0; $x < 8; $x++)
6     {
7         $xored[$x]=substr($hash, $x*4, 4);
8     }
9     foreach ($xored as $v)
10    {
11        $final=dechex(hexdec($v) ^ hexdec($final))
12    }
13
14    if (($final=="fd56") && (strlen($pwd)==16))
15        return true;
16    return false;
```