Webwob First to solve this challenge!

Web - 100 points

# Soal

|  |
| --- |
| <http://128.199.96.39/> |

# Solusi

Di halaman web kita diberi source codenya:

|  |
| --- |
| <?php  **function** length($x) {  **if** (is\_array($x))  **return** count($x);  **return** strlen($x);  }  **require**("flag.php");  $pass = $\_GET["password"];  $ok = length($pass)==4;  **for** ($i=0; $i<length($pass); $i++) {  **if** (strcmp($pass[$i], $password[$i])!=0) {  $ok = **false**;  **print** "invalid **$i**";  **break**;  } }  **if** ($ok) {  **echo** "The Flag is: ".$FLAG;  **exit**(0); } **else** {  **if** (isset($\_GET["password"]))  **print** "Invalid"; } |

Beberapa hal yang bisa ditangkap dari source tersebut:

* Input parameter password (GET) bisa berupa array atau string, kalau array harus 4 elemen, kalau string harus 4 huruf
* Perbandingan satu per satu huruf dengan password pakai fungsi strcmp()

Kita sebenarnya bisa bruterforce password karena cuma 4 huruf, tapi itu agak lama. Kelemahannya, fungsi strcmp di PHP bisa di-bypass dengan memasukkan array (strcmp($var1, $var2) akan bernilai benar jika $var1 atau $var2 berupa array, apapun isinya). Maka idenya adalah memasukkan password dalam bentuk array di dalam array seperti ini.

|  |
| --- |
| $pass = array(array(“a”), array(“b”), array(“c”), array(“d”)) |

Hal ini supaya ketika diambil $pass[0] maka akan dapat suatu array(“a”) yang lolos strcmp(array(“a”), $pass[i]). Maka kita susun request seperti ini supaya di program jadi struktur array seperti di atas:

|  |
| --- |
| http://128.199.96.39/?password[0][0]=a&password[1][0]=b&password[2][0]=c&password[3][0]=d |

Dapat flagnya:

**The Flag is: flag{AVariant\_Of\_Strcmp}**