2019年09月28日

<http://edu.wargame.dyns.cx/>

Level 1

MD5雜湊 - rainbow tables

hash lookup online

(加鹽- password + random value)

Level 2

靜態分析

非雜湊、加密內容

編碼運算

常見到等號(=)

BASE 64

Level 3

imagehide

encrypt text in picture

Level 4

注意字串長度(Simple Authentication Algorithm)

Julius Caesar (Caesar Cipher)

A-C、C-E、C-G

Level 1

1. Level1.exe 丟入記事本
2. 找到可能的字串(2215eb57bf0ff4dab5b89d3d45186bd2)
3. 用[MD5解碼網站](https://crackstation.net/)解題
4. 得到密碼 : biconditional

Level 2

1. 因為有=後綴，且字母有大小寫，判斷為Base 64
2. 丟入[Base 64 解碼網站](https://www.base64decode.org/)，

得到

<?

$content="ER2XGZLSNZWWCZJ5EJWGK5TFNQZCEOYKERYGC43THURGG6LCMVZGG43JEI5QU2LGEAUCQJDMN5TWS3R5HUSHK43FOJXG2YLFFEQCMJRAFASHAYLTON3W64TEHU6SI4DBONZSSKIKPMFCAIBAEAQCAIBAER3GC3DJMRPXK43FOI6TCOYKEAQCAIBAEAQCALZPEBDWC5LOOQQECY3DMVZXGIB5EBHUWCT5EBSWY43FEB5QUIBAEAQCAIBAEASHMYLMNFSF65LTMVZD2MB3BIQCAIBAEAQCAIDFMNUG6IBCKBEFAICXMFZG42LOM45CAICQJBICAU3UMFZHI5LQHIQCA2LOEBKW423ON53W4IDPNYQGY2LOMUQDAIR3BIQCAIBAEAQCAIBPF4QEOYLVNZ2CAQLDMNSXG4ZAHUQEKUSSJ5JAU7I=";

$valid\_user=0;

$code=\*\*\*\*\*\*\_decode($content); // I am not sure!

eval($code);

// Couples lines of PHP code

?>

1. 擷取紅字部分，因有=後綴，且字母只有大寫

判斷為Base 32，丟入[Base 32解碼網站](https://emn178.github.io/online-tools/base32_decode.html)

得到 :

$usernmae="level2";

$pass="cybercsi";

if (($login==$usernmae) && ($password==$pass))

{

$valid\_user=1;

// Gaunt Access = OK

} else {

$valid\_user=0;

echo "PHP Warning: PHP Startup: in Unknown on line 0";

// Gaunt Access = ERROR

}

1. 得到密碼 : cybercsi

Level 3

1. Yahoo!

Level 4