Sara Nowak

Nr albumu: 226068

Bezpieczeństwo systemów i usług informatycznych 2

Laboratorium nr 2

Podczas ostatnich zajęć mieliśmy wejść na stronę uw-team.org, na której znajdują się gry z serii Hackme. Mieliśmy przejść przez kolejne poziomy gier 1.0 i 2.0. Hasła odgadywaliśmy dzięki wyświetleniu źródła strony.

1) Hackme 1.0, uw-team.org/hackme

a) Level 1

W źródle strony na dole jest funkcja zawierająca wyrażenie:

if (document.getElementById('haslo').value=='a jednak umiem czytac')

czyli hasło to: a jednak umiem czytac

b) Level 2

if (document.getElementById('haslo').value==has)

w skrypcie hasełko.js:

var has='to bylo za proste'

czyli hasło to: to było za proste

c) Level 3

var dod='unknow'

var literki='abcdefgh'

ost=literki.substring(2,4)+'qwe'+dod.substring(3,6);

if (document.getElementById('haslo').value==ost)

hasło to: cdqwenow

d) Level 4

wynik=(Math.round(6%2)*(258456/2))+(300/4)*2/3+121;

if (zaq==wynik)

hasło to: 171

e) Level 5

ile=((seconds*(seconds-1))/2)*(document.getElementById('pomoc').value%2)

if (ile==861)

wynik modulo nie może wynosić 0, więc musimy podać liczbę nieparzystą

861 = ((seconds*(seconds-1))/2*1

861 = ((seconds*(seconds-1))/2

861*2 = ((seconds*(seconds-1))

1722 = ((seconds*(seconds-1))

1722 = seconds^2 – seconds

seconds^2-seconds-1722=0

seconds=42

hasło to: dowolna liczba nieparzysta wpisana w 42 sekundzie

f) Level 6

```
var licznik=0;

var hsx=' ';
var znak=' ';
zaq=document.getElementById('haslo').value;
for (i=1; i<=5; i+=2){
licznik++;
if ((licznik%2)==0) {znak='_';} else {znak='x';}
hsx+=lit.substring(i,i+1)+znak;
}
hsx+=hsx.substring(hsx.length-3,hsx.length);
if (zaq==hsx) {self.location.href=hsx+'.htm';
```

wartości licznika: 1,3,5

licznik=1, więc modulo = 1, wartość z if false, pierwszy znak 'x'

hsx.substring(1,2)= 'b'; hsx = 'bx'

i=3,licznik=2, znak='_'

hsx.substring(3,4) = 'd'

hsx = 'bxd_'

i=5,licznik=3, znak='x'

hsx.substring(5,6) = 'e'

hsx = 'bxd_ex'

następnie po wyjściu z pętli:

hsx+=hsx.substring(hsx.length-3,hsx.length)

hsx = hsx + hsx.substring(3,6)

hsx = 'bxd_ex' + '_ex'

hsx = 'bxd_ex_ex'

hasło to: bxd_ex_ex

g) Level 7

Przy użyciu „tabeli" if'ów z zmieniając litery z ciągu plxszn_xrv i otrzymujemy hasło.

hasło to: kocham cie

h) Level 8

Na podstawie skryptu otrzymujemy hasło: qrupjf162

2) Hackme 2.0

a) Level 1

<input type="password" name="haslo" id="haslo"><input value="text" name="formularz" id="formularz" type="hidden">

hasło to: text

b) Level 2

if (document.getElementById('haslo').value==unescape('%62%61%6E%61%6C%6E%65'))

hasło to: banalne

c) Level 3

if (binary(parseInt(document.getElementById('haslo').value))==10011010010)

hasło to: 1024

d) Level 4

liczbę decymalną zamieniamy na liczbę heksadecymalną

hasło to 102

e) Level 5

Na podstawie kodu php, w url wpisujemy 102.php?has=1&log=1

f) Level 6

link do następnej strony w pliku cookie

ciastka.htm

g) Level 7

W katalogu hm2/include znajduje się plik cosik.js z linkiem do następnego etapu

listing.php

e) Level 8

Wystarczy ustawić referenta na onet.pl albo wyłączyć obsługę JavaScript. Hasło można znaleźć w kodzie źródłowym. W tym etapie należało ustawić referenta (strony z której przechodzimy) na onet.pl. Hasło znajdowało sie w kodzie źródłowym. Otrzymujemy adres następnego etapu.

f) Level 9

Wyłączamy obsługę JavaScript albo zmieniamy godzinę na komputerze. Widzimy wiadomość zakodowaną w postaci binarnej.

„Gratuluje :) Udalo ci sie rozkodowac ten etapik :] Nie bylo to specjalnie trude... Wystarczylo zrobic sobie program konwertujacy, lub wejsc na www.google.pl i wpisac "text to binary". To byl juz ostatni etap tej gry. Aby byc wpisanym na liste zwyciezcow przeslij haslo "bezkvu6r" na adres unkn0w@wp.pl”