Bezpieczeństwo Systemów i Usług Informatycznych

Laboratorium 3 - HackMe i HackMe2

1. Treść zadania.

Naszym zadaniem było rozwiązanie zagadek programistycznych umieszczonych na stronach http://uw-team.org/hackme/ oraz http://uw-team.org/hm2/. Poniżej zaprezentowane zostaną rozwiązania poszczególnych etapów.

1. HackMe.

- Poziom 1

Pierwszym krokiem było podejrzenie źródła strony w przeglądarce. Z kodu można wyczytać, że kliknięcie przycisku OK obsługuje funkcja sprawdz(). Z jej treści wynika, że hasło to "a jednak umiem czytac". Trudność polegała na tym, że treść tej funkcji została umieszczona po wielu znakach nowych linii. Problematyczna też była obecność funkcji o bliźniaczo podobnej nazwie sprawdz () (dodatkowa spacja).

- Poziom 2

Po podejrzeniu źródła strony zauważyć można dołączony zewnętrzny plik "haselko.js". W nim znajduje się zmienna z którą porównujemy wprowadzane dane. Hasło to "to bylo za proste".

- Poziom 3

Do generowania zmiennej z którą porównywane są nasze dane wejściowe używana jest funkcja losuj. Przypisuje ona zmiennej "ost" wartość opierając się na fragmentach łańcuchów znaków jakimi są zmienne "literki" oraz "dod". Pomocne okazuje się sprawdzenie w dokumentacji funkcji substring języka JavaScript. Hasło to: "cdqwenow".

- Poziom 4

Aby wyznaczyć hasło musimy obliczyć równanie.

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

Hasło to 171.

- Poziom 5

Musimy obliczyć kolejne równanie, tym razem kwadratowe.

Po uproszczeniu wygląda ono mniej więcej tak:

(x*(x-1))/2 * Y%2 = 861

x - wartość licznika działającego na stronie

y- wartość wpisywana przez nas

x = 42

Musimy w 42 sekundzie wpisać liczbę nieparzystą.

- Poziom 6

Na tym poziomie utrudnieniem jest wprowadzona pętla. Poniżej rozpisanie poszczególne iteracje.

lit = abcdqepolsrc

hsx = lit.substring(i, i+1)

Iteracja 1.

i = 1
licznik = 1
znak = x
hsx = bx

i = 3
licznik = 2
znak = _
hsx = bxd_

i = 5
licznik = 3
znak = x
hsx = bxd_ex

Następnie jeszcze prosta modyfikacja hsx na podstawie podłańcucha.

hsx = bxd_ex_ex

- Poziom 7

Kolejna pętla. Tym razem jej długość jest zależna od długości łańcucha przez nas wprowadzanego. Wiemy, że wynik ma wynosić "plxszn_xrv". W kodzie znajduje się ciąg instrukcji warunkowych kodujących dane wejściowe. Po rozszyfrowaniu wyniku okazuje się, że dane wejściowe potrzebne do jego uzyskania to "kocham cie".

- Poziom 8

Kolejna zabawa pętlami. Tym razem głównym utrudnieniem jest użycie w kodzie zmiennych get i qet, co ma nas zmylić. Poniżej kolejne iteracje.

Iteracja 1

i = 0
qet = 0
wyn = q

i = 2
qet = 1
wyn = qr

i = 4
qet = 2
wyn = qru

i = 6
qet = 3
wyn = qrup

i = 8
qet = 4
wyn = qrupj

i = 10
qet = 5
wyn = qrupjf

Dane potrzebne do wykonania funkcji eval znajdują się w zewnętrznym pliku .js, którego lokalizacja zapisana została szesnastkowo.

wyn = wyn + 162 = qrupjf162

3. HackMe 2

- Poziom 1

W źródle strony zauważyć można okryte pole z wartością "text", która jest hasłem.

- Poziom 2

Hasło zapisane jest szesnastkowo w kodzie strony. Hasło to "banalne".

- Poziom 3

Hasło zapisane jest binarnie w kodzie strony. Hasło to 1234.

- Poziom 4

Kolejna sztuczka z "ukryciem" fragmentu źródła strony poprzez zastosowanie wielu nowych linii. Zmienna cos zawiera liczbę zakodowaną liczbę 258. Hasłem jest liczba 258 zapisana szesnatkowo, czyli 102.

- Poziom 5

Aby przejść dalej należy uzupełnić adres url o zmienne i ich wartości (metoda GET).

?has=1&log=1

- Poziom 6

Link do następnej strony zawarty jest w ciasteczku. Plik: ciastka.htm.

- Poziom 7

Hasłem jest nazwa pliku .js, którą poznać możemy odwiedzając katalog /include. Hasło: cosik.

Aby obejść dalsze zabezpieczenie należy wyłączyć obsługę JavaScriptu w przeglądarce. Hasło do następnego etapu zawarte jest w źródle w divie "ukryte". Hasło: kxnxgxnxa.

- Poziom 8

Gra sugeruje nam otwarcie pliku pokaz.php.

Pierwsze zdanie zaszyfrowane jest szyfrem rot13. Potrzebne jest użycie dekodera. Wiadomość to: "ponizszy adres zostal zakodowany z przesunieciem o 2 ".

Następna linijka zawiera zaszyfrowany link do nieaktualnego translatora binary -> string. Po użyciu innego naszym oczom ukazuje się wiadomość:

" 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 ".