

Gra 2

Abdullah Maou 231001

Level #1

```
<html><head><title>Hackme 2.0 - by Unknown</title></head><body text="white" bgcolor="black" link="yellow" vlink="yellow" alink="yellow">
<script>
function spr(){
if (document.getElementById('formularz').value==document.getElementById('haslo').value){ self.location.href=document.getElementById('haslo').value+'.htm'; } else {alert('Nie, to nie to haselko :(');}
}
</script>
<h3>Hackme 2.0 - level #1</h3>
Podaj haselko: <input type="password" name="haslo" id="haslo"><input value="text" name="formularz" id="formularz" type="hidden"><input type="button" onClick="spr()" value="Go!">
</body></html>
```

Z kodu wynikało, że hasło przypisane jest do elementu formularz.

Hasło to text – można podglądać po zmianie typu elementu z hidden na visible

Level #2

Zamieniamy znaki hex na ASCII string w nawiasie za funkcją unescape

```
<html><head><title>Hackme 2.0 - by Unknown</title></head><body text="white" bgcolor="black" link="yellow" vlink="yellow" alink="yellow">
<script>
function spr(){
if (document.getElementById('haslo').value==unescape('%62%61%6E%61%6C%6E%65')) { self.location=document.getElementById('haslo').value+'.htm'; } else { alert('Zle haslo!');}
}
</script>
<h3>Hackme 2.0 - level #2</h3>
Podaj haslo: <input type="password" name="haslo" id="haslo"> <input type="button" onClick="spr()" value="Break me!">
</body></html>
```

Hasło to "banalne"

Level #3

```
<html><head><title>Hackme 2.0 - by Unknown</title></head><body text="white" bgcolor="black" link="yellow" vlink="yellow" alink="yellow">
<script>
function binary(liczba) {
return liczba.toString(2);
}
function spr(){
if (binary(parseInt(document.getElementById('haslo').value))==10011010010) { self.location=document.getElementById('haslo').value+'.htm'; } else { alert('Zle! \nPodstawy matematyki sie klaniaja :)');}
}
</script>
<h3>Hackme 2.0 - level #3</h3>
Podaj haselko: <input type="password" name="haslo" id="haslo"> <input type="button" onClick="spr()" value="Click me baby!">
</body></html>
```

Zamienić liczbę binarną 10011010010 na decymalną

Hasło to: 1234

Level #4

uw-team.org says

podaj haslo:

wpisz X aby zatrzymać skrypt

OK Cancel

Należy wyłączyć funkcje JavaScriptową w przeglądarce.

Następnie zamieniamy znaki hex na ASCII zgodnie z zadaniem 2gim a wynik to 258

Zamieniamy to na liczbę hexadecymalną – 102

Level #5

Hackme 2.0 - level #5

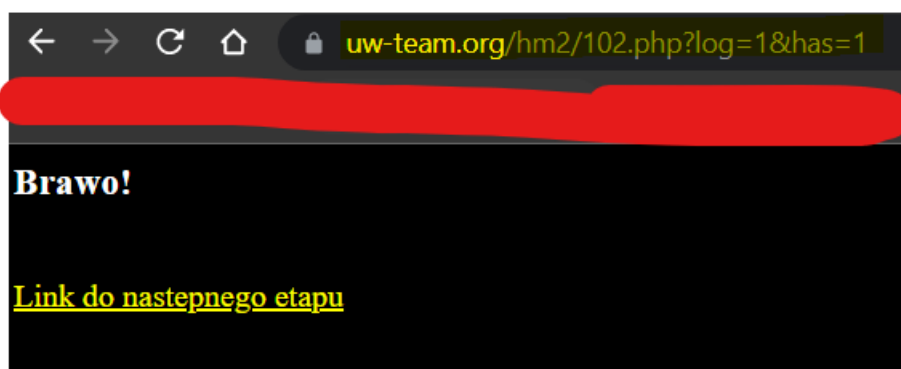
Podaj login:

Podaj hasło:

Ten etap napisany jest w PHP, więc nie możesz podglądać jego źródła.
Oto źródło skryptu:

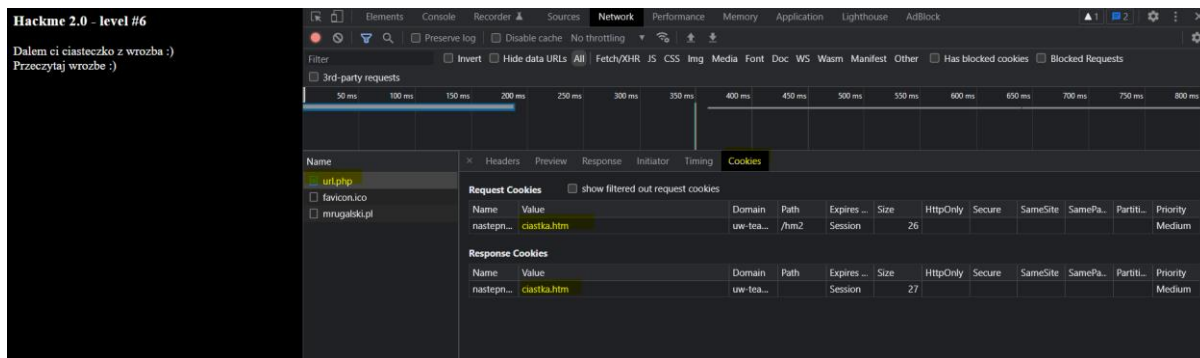
```
if (!isset($haslo)) {$haslo='';}  
if (!isset($login)) {$login='';}  
if ($haslo=="tu jest haslo") {$has=1;}  
if ($login=="tu jest login") {$log=1;}  
if (($has==1) && ($log==1)) { laduj nastepny level } else { powroc do tej strony }
```

Należy zgodnie ze skryptem zedytować link żeby uzyskać rozwiązanie



Level #6

W tekście znajduje się podpowiedź o plikach cookies.



Po otwarciu widzimy link do kolejnego etapu /ciastka.htm

Level #7

Trzeba ponownie wyłączyć obsługę JavaScriptu w przeglądarce

Po przejściu w podany adres /zle.htm



```
<html><head><title>Hackme 2.0 - by Unknow</title></head><body text="white" bgcolor="black" link="yellow" vlink="yellow" alink="yellow">
<h3>Podano złe hasło!</h3>
<!-- A może by tak wykorzystać pewną właściwość serwera apache? //-->
</body></html>
```

Zgodnie z podpowiedzią wpisujemy /include w link i dzięki temu dostajemy się do katalogu include.

Zgodnie ze skryptem na stronie ciastka.htm

Włączamy wtyczkę i wpisujemy hasło

Index of /hm2/include

Name	Last modified	Size	Description
 Parent Directory		-	
 cosik.js	2008-11-19 16:39	21	

Hasło to cosik

Level #8

Potrzebujemy wyłączyć wtyczkę JavaScript

Hackme 2.0 - level #8

Podaj hasło:

```
<br>
... <div id="ukryte" style="display:none"> == $é
    <font color="black">h</font>
    <font color="black">a</font>
    <font color="black">s</font>
    <font color="black">l</font>
    <font color="black">e</font>
    <font color="black">m</font>
    <font color="black"> d</font>
    <font color="black">o</font>
    <font color="black"> t</font>
    <font color="black">e</font>
    <font color="black">g</font>
    <font color="black">o </font>
    <font color="black">e</font>
    <font color="black">t</font>
    <font color="black">a</font>
    <font color="black">p</font>
    <font color="black">u</font>
    <font color="black"> j</font>
    <font color="black">e</font>
    <font color="black">s</font>
    <font color="black">t</font>
    <font color="black"> s</font>
    <font color="black">l</font>
    <font color="black">o</font>
    <font color="black">w</font>
    <font color="black">o </font>
    <font color="black">k</font>
    <font color="black">x</font>
    <font color="black">n</font>
    <font color="black">x</font>
    <font color="black">g</font>
    <font color="black">x</font>
    <font color="black">n</font>
    <font color="black">x</font>
    <font color="black">a</font>
  </div>
</body>
</html>
```

Można przeczytać zdanie „hasłem do tego etapu jest słowo

Następny etapik ukryty jest w pliku pokaz.php

Hackme 2.0 - level #8

Podaj hasło:

Level #9

Zmienimy link na /pokaz.php

Hackme 2.0 - level #9

```
01100111 01110010 01100001 01110100 01110101 01101100 01100001
```

Milego dekodowania :)

Za pomocą binary decoder

The screenshot shows a binary decoder application with two panes. The left pane is titled 'VIEW' and 'Bytes', showing a table of binary data. The right pane is titled 'VIEW' and 'Text', displaying the decoded message.

FORMAT	GROUP BY
Binary	Byte

```
01100111 01110010 01100001 01110100 01110101 01101100
01100001 01100011 01101010 01100101 00100001 00100000
01110101 01100100 01100001 11000101 10000010 01101111
00100000 01000011 01101001 00100000 01110011 01101001
11000100 10011001 00100000 01110101 01101011 01101111
11000101 10000100 01100011 01111010 01111001 11000100
10000111 00100000 01110100 01100101 00100000 01110111
01100101 01110010 01110011 01101010 01100101 00100000
01001000 01100001 01100011 01101011 01101101 01100101
00101110
```

gratulacje! udało Ci się ukończyć tę wersję Hackme.