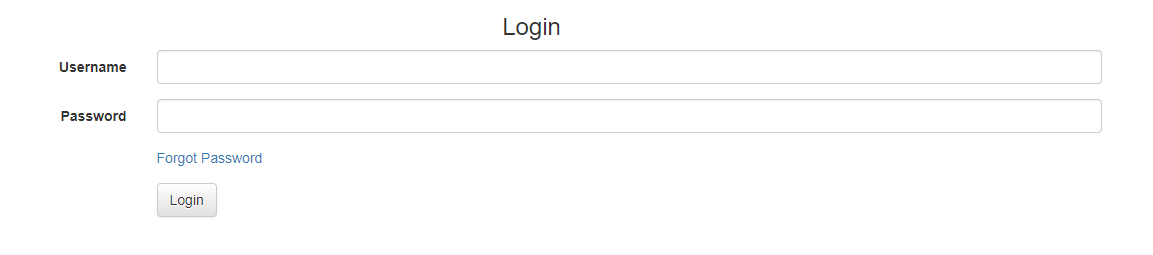
# Web2 Writeup

Login

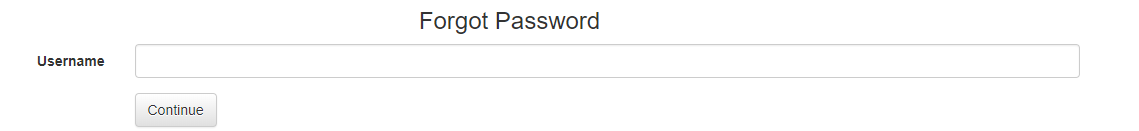


Test test 弱口令



很显然需要管理员登录才行

Forgot password



可爆破用户名



Admin



Login.php

右键查看源代码



Csrf\_token 刷新



后面有 == 猜测为 base64



a:1:{s:10:"csrf\_token";i:555440116;} 这是序列化的结果 注意数字

猜测为 php 生成的随机数

生成随机数的函数有两个 rand() 和 mt\_rand()

其中生成前需要设置种子 srand() 和 mt\_srand()

**种子可爆破 (请看 <白帽子讲 web 安全> 伪随机数安全)**

如果直接调用生成函数, 种子最大则为 2^32 (x86),

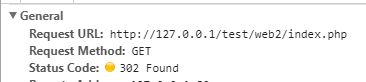
让我们爆破肯定是不可能的

那么就需要知道种子的取值范围

地址栏

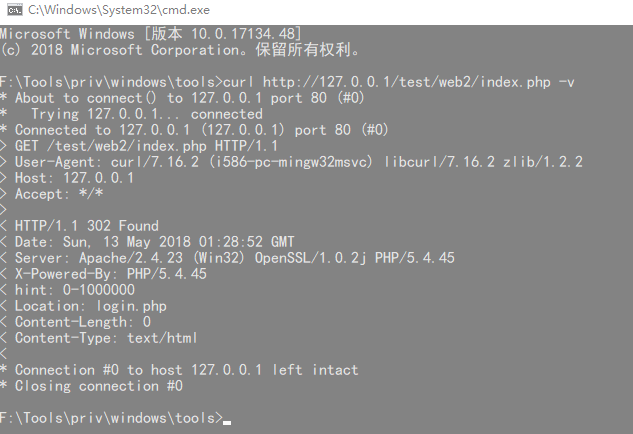


访问 index.php



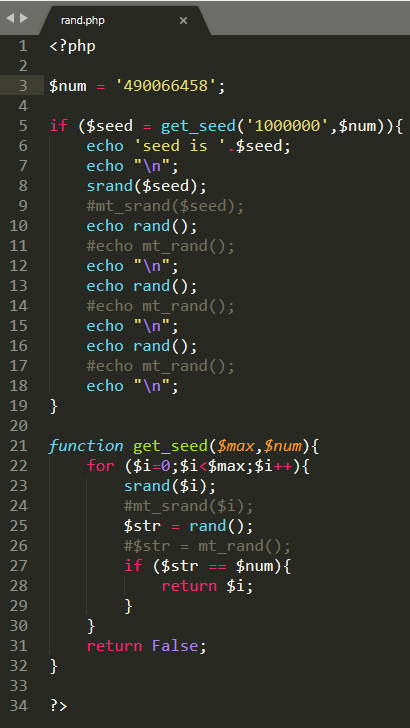
302 跳转

查看响应头



Hint: 1-1000000 一百万

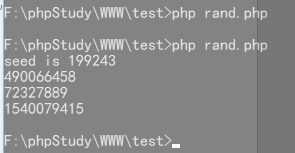
下面就简单了, for 循环 100万次, 把 rand() 和 mt\_rand() 都跑一遍



Rand()



Mt\_rand()



Seed is 199243

Csrf\_token 刷新会变化, 也就是说 seed 会重新设置

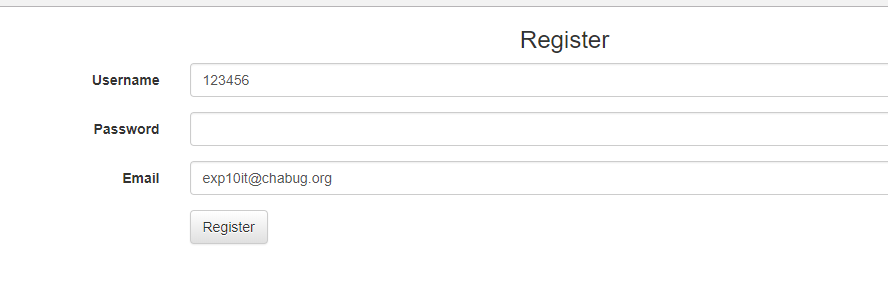


Forgot password 没有 token

那么 login.php 生成的 seed 和 forgot password 里的 seed 可能是一样的

下面 找回 admin 密码 需要知道邮件里链接的格式

Register.php 猜都能猜出来



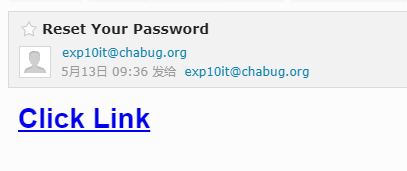
123456 123456



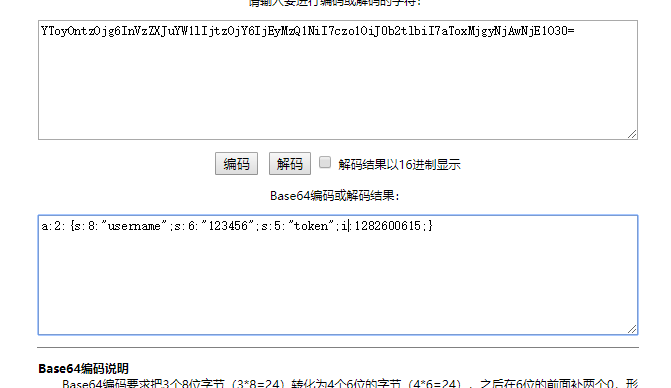
找回密码



邮箱



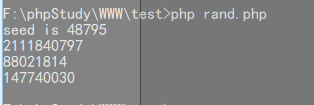
<http://127.0.0.1/submit.php?token=YToyOntzOjg6InVzZXJuYW1lIjtzOjY6IjEyMzQ1NiI7czo1OiJ0b2tlbiI7aToxMjgyNjAwNjE1O30>=



Payload

a:2:{s:8:"username";s:5:"admin";s:5:"token";i:XXXXXX;}

访问 login.php 重新生成 token

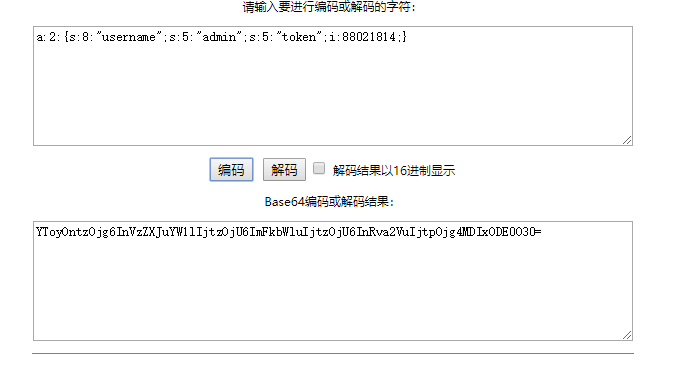


88021814

找回 admin 密码



Base64



Submit.php?token= YToyOntzOjg6InVzZXJuYW1lIjtzOjU6ImFkbWluIjtzOjU6InRva2VuIjtpOjg4MDIxODE0O30= X

登录

