/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

/\* 程序作者：爱的伊苏 \*/

/\* 程序完成时间：2019/2/6 \*/

/\* 有任何问题请联系：740531307@qq.com \*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//@永远得意的笑下去

首先阅读题目源码

<?php

session\_start();

if (isset ($\_GET['password'])) {

if ($\_GET['password'] == $\_SESSION['password'])

die ('Flag: '.$flag);

else

print '<p>Wrong guess.</p>';

}

mt\_srand((microtime() ^ rand(1, 10000)) % rand(1, 10000) + rand(1, 10000));

?>

Session是位于服务端的客户端数据，判断session对应哪个客户端通过http请求头中的cookie来判断。

解题思路：通过删除所有cookie和password

使得二者在判断是都为空满足判断条件，从而得到flag

推荐插件 BrupSuite