实验吧 天网管理系统writeup

原创

qq_41497476 于 2019-04-28 19:50:18 发布 69 收藏

分类专栏： 简单 文章标签： web

本文链接：https://blog.csdn.net/qq_41497476/article/details/89644560

实验吧 天网管理系统writup

仅提供过程：

1.使用Burpsuit查看网页有一段隐秘的提示`****<!-- $test=$_GET['username']; $test=md5($test); if($test=='0') -->****`

2.按照要求，输入一个经过md5加密后php脚本识别为0的字符串作为username

3.有一些字符串经md5加密后显示为0e......php识别为科学计数法，值为0

4.response页面提示

$unserialize_str = $_POST['password']; $data_unserialize = unserialize($unserialize_str); if($data_unserialize['user'] == '???' && $data_unserialize['pass']=='???') { print_r($flag); } 伟大的科学家php方言道：成也布尔，败也布尔。 回去吧骚年

5.密码需要满足要求：在unserialize成一个序列后有两个字段：user,pass且都满足=="???"条件，php双等号有许多特殊性，这里利用***0==“非1开头的任意字符串”***构造数据，成功获取flag。