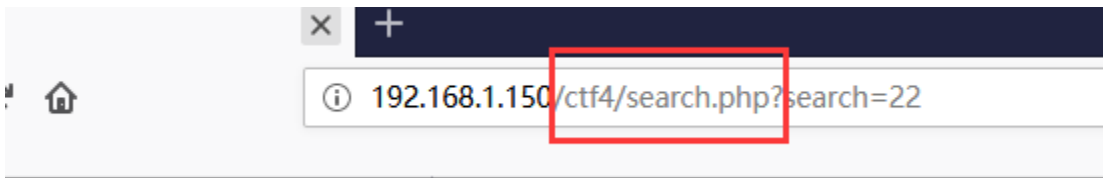


网络安全与防护实训(6/4/19)

一、弄点课上能用上的最 basic 手工注入

因为讨论原理所以就不讲解前期的猜代码结构的步骤了 直接看源代码 不然太费事了说起来

首先



这个是注入地址可以看出后台是 search.php 处理请求
所以我们先找到并打开 search.php 看一下

```
txt13 php.txt13 search.php
<?php
include_once('sys/config.php');
include_once('header.php');
if (!empty($_GET['search'])) {
    $query = "SELECT * FROM comment WHERE comment_text LIKE '%".$_GET['search']."'";
    $data = mysqli_query($dbc,$query);
}
?>
<div class="bs-example table-responsive">
    <?php echo 'The result for'.$_GET['search'].'is:'?>
    <table class="table table-striped table-hover ">
    <tr>
        <th>#</th>
        <th>Column heading</th>
    </tr>
    <?php
    while($com = mysqli_fetch_array($data)) {
        //净化输出变量
```

很容易找到 sql 查询语句

代码:

SELECT * FROM comment WHERE comment_text LIKE '%".\$_GET['search']."'

其中我们的输入 search 变量可以理解为替换了下方↓代码中的红框部分

```

define_once('header.php');
empty($_GET['search'])) {
    query = "SELECT * FROM comment WHERE comment_text LIKE '%" . $_GET['search'] . "%'";
    data = mysqli_query($dbc, $query);
}

```

也就是说我们加入输入 22 也就是 <http://IP/ctf4/search.php?search=22>

执行的时候就是把`{$_GET['search']}`部分换成 22 了

有了这个思路我们就可以尝试提交一些别的东西看看我们的猜想对不对

这里需要了解一个注释符号 `--` 也就是两个减号

功能是注释掉后面的查询代码 但是一般我们习惯输入 `--+`

(习惯问题以前去上课听别人讲的)

我们尝试输入 `22% '--+`

注: *****

此时代码相当于

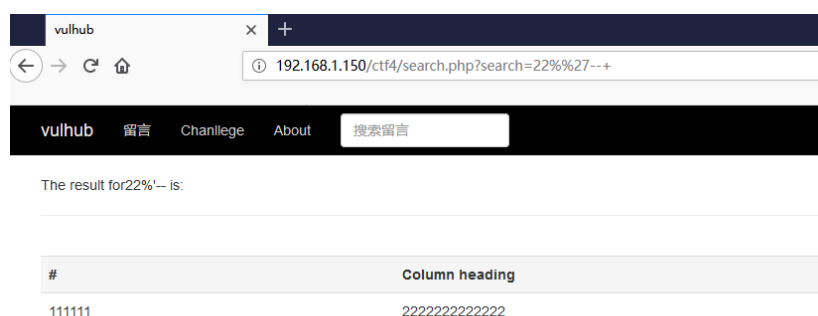
`SELECT * FROM comment WHERE comment_text LIKE '%22% '--+ %'`

之前的情况:

`SELECT * FROM comment WHERE comment_text LIKE '%22 %'`

用心对比不难发现规律

下面验证发现结果会和上次相同



#	Column heading
111111	222222222222

成功

原理其实就是这个

后面的部分就比较复杂了 答案我传到 <ftp://192.168.9.200/> 的 NS 文件夹下了
复杂原理我也上传过了 看到基础篇也有 10 多页。。。

这东西很烦的 我感觉打字 说不明白，实在谁想探讨白天真人互动吧

