Http 头注入之 UA 头注入

一、http 头注入介绍

在安全意识越来越重视的情况下，很多网站都在防止漏洞的发生。例如 SQL 注入中，用户提交的参数都会被代码中的某些措施进行过滤。

过滤掉用户直接提交的参数,但是对于 HTTP 头中提交的内容很有可能就没有进行过滤。例如 HTTP 头中 User-Agent、Referer、Cookies 等。

二、User-Agent 注入(INSERT 提交的参数)

1 获得头信息
2 没过滤
3 数据库操作
查看 Less-18 代码

```
$row1 = mysql_fetch_array($result1);
    if($row1)
            {
            echo '<font color= "#FFFF00" font size = 3 >';
            $insert="INSERT INTO `security`.`uagents` (`uagent`, `ip_address`, `username`) VALUES ('$uagent', '$IP', $uname)";
            mysql_query($insert);
            //echo 'Your IP ADDRESS is: ' .$IP;
            echo "</font>";
            //echo "<br>";
            echo '<font color= "#0000ff" font size = 3 >';
            echo 'Your User Agent is: ' .$uagent;
            echo "</font>";
            echo "<br>";
            print_r(mysql_error());
            echo "<br><br>";
            echo '<img src="../images/flag.jpg"  />';
            echo "<br>";

            }
    else
            {
            echo '<font color= "#0000ff" font size="3">';
            //echo "Try again looser";
            print_r(mysql_error());
```

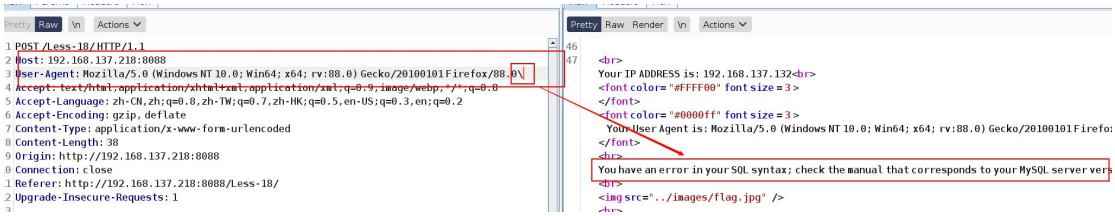
```
    $uagent = $_SERVER['HTTP_USER_AGENT'];
    $IP = $_SERVER["REMOTE_ADDR"];
    echo "<br>";
    echo 'Your IP ADDRESS is: ' .$IP;
    echo "<br>";
    //echo 'Your User Agent is: ' .$uagent;
ake the variables
sset($_POST['uname']) && isset($_POST['passwd']))

    {
    $uname = check_input($_POST['uname']);
    $passwd = check_input($_POST['passwd']);
```

可以看到注入点

$insert="INSERT INTO `security`.`uagents` (`uagent`, `ip_address`, `username`) VALUES ('$uagent', '$IP', $uname)";

实验演示：
在输入正确的用户名密码之后发现提示 useragent 信息

然后对 useragent 进行尝试注入，发现有 sql 错误



用 payload 进行渗透

那么该如何获得响应的信息呢？

利用报错函数