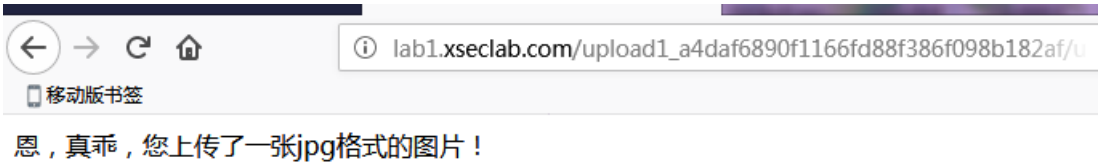
网络安全实验室_上传关writeup

转载

a173262565 于 2018-03-22 11:03:00 发布 179 收藏
文章标签： php
原文链接：http://www.cnblogs.com/Ragd0ll/p/8622306.html

请上传一张jpg格式的图片

先传个图片码试试



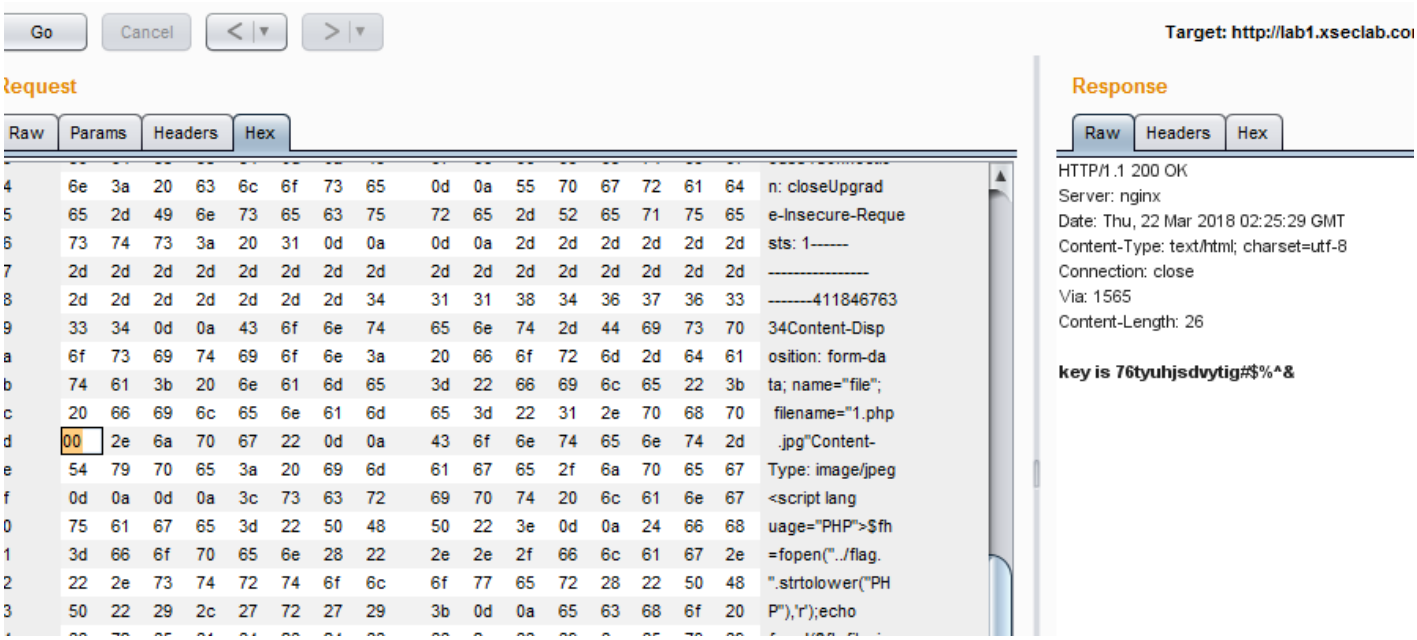
我肯定乖嘛(#`Д´)ノ

气到改后缀

请上传一张jpg格式的图片

我猜是00截断，不信来试试

先在赋值1.php .jpg，接着去hex中找到空格改成00就成了

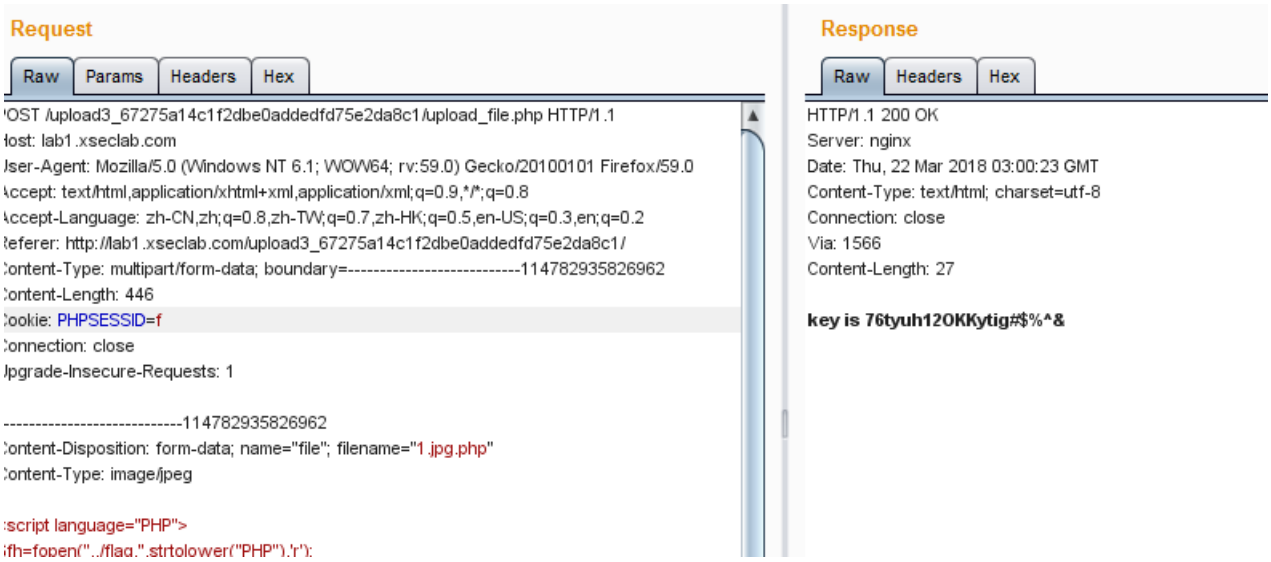


请上传一张jpg格式的图片

名字跟前面一样，试试截断果然不行了，看看源码竟然还发现给出了代码

```
function check(){
    var filename=document.getElementById("file");
    var str=filename.value.split(".");
    var ext=str[1];
    if(ext==='jpg'){
        return true;
    }else{
        alert("请上传一张JPG格式的图片！");
        return false;
    }
    return false;
}
```

看的出来他用.来分割传入的数据，如果第一个.后面是jpg就成了



转载于:https://www.cnblogs.com/Ragd0ll/p/8622306.html