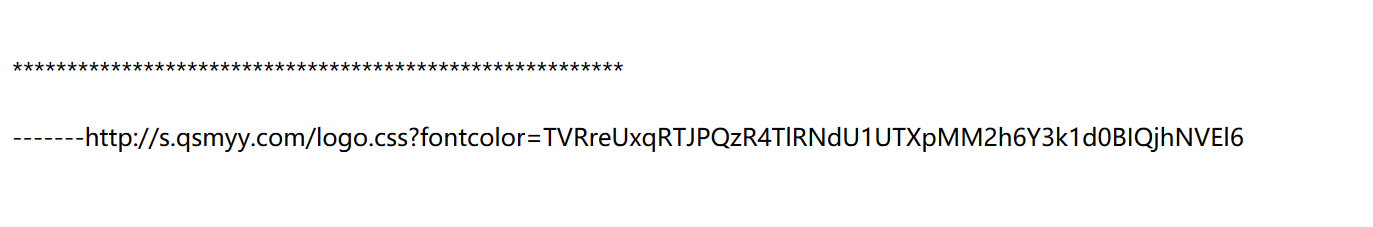
之前在应急中发现了一个5678.php后门程序，后来在发到论坛上，有朋友提醒说该后门还带有后门，于是速速拆开看看。分析该木马，发现存在css\_font函数，具体代码如下：



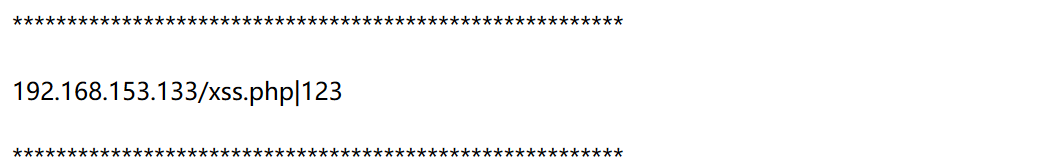
输出rawtargetu如下



fontcolor主要组成如下：后门访问路径url+后门密码，首先经过了base64编码，获取值如下：MTkyLjE2OC4xNTMuMTMzL3hzcy5waHB8MTIz，接着利用str\_replace函数将编码参数中的a替换为@，在继续将参数中的=替换为?，然后在进行base64编码，根据此规律最终解码函数如下：

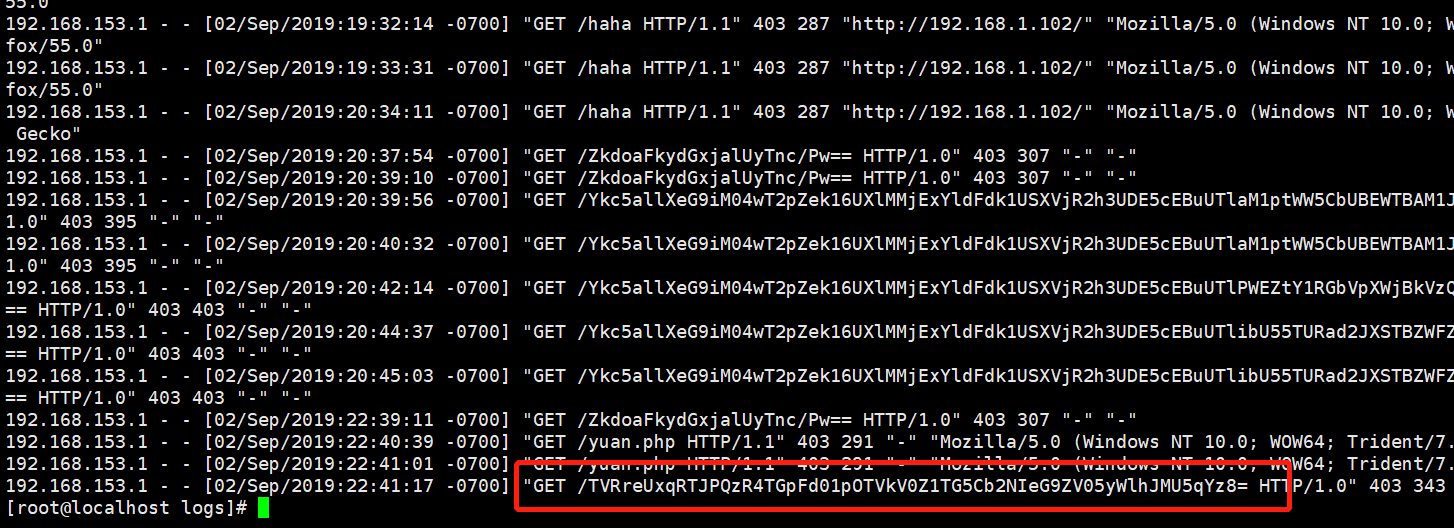
$jiema=base64\_decode(str\_replace('?','=',str\_replace('@','a',base64\_decode('TVRreUxqRTJPQzR4TlRNdU1UTXpMM2h6Y3k1d0BIQjhNVEl6'))));

输出解码结果如下：

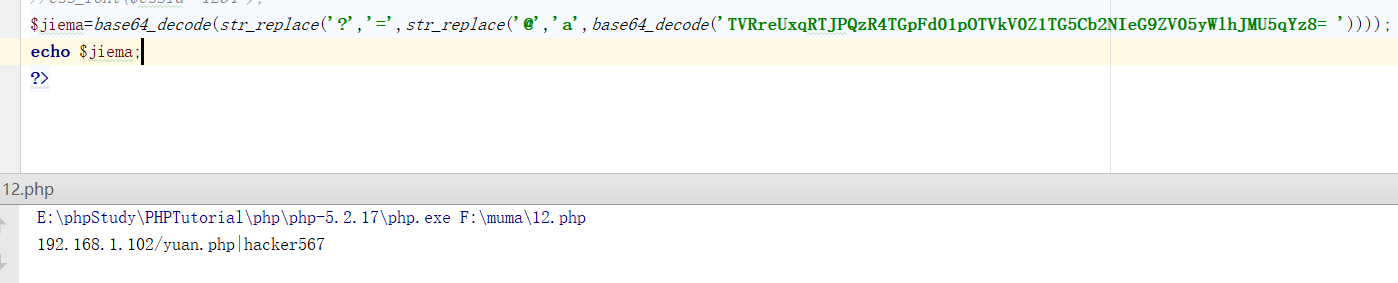


很显然，向http://s.qsmyy.com/logo.css?传递的主要内容为后门的访问地址和访问密码，只需要在后门服务器上搭建个web服务，定时去查看日志就可以了，正所谓鹬蚌相争，渔翁得利。

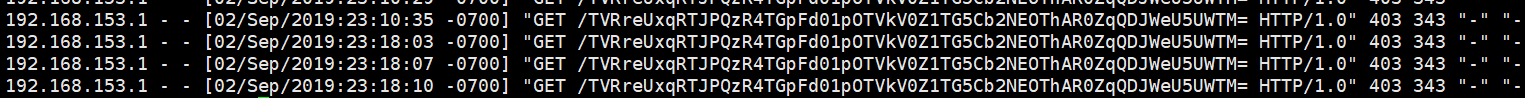
把后门地址修改为本地搭建的web服务器进行测试，可成功接收到相关日志。



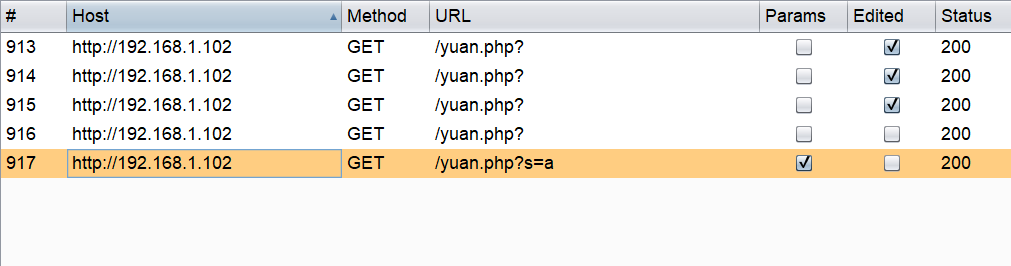
将接收到的信息进行解码，可成功获取后门访问地址以及密码信息。



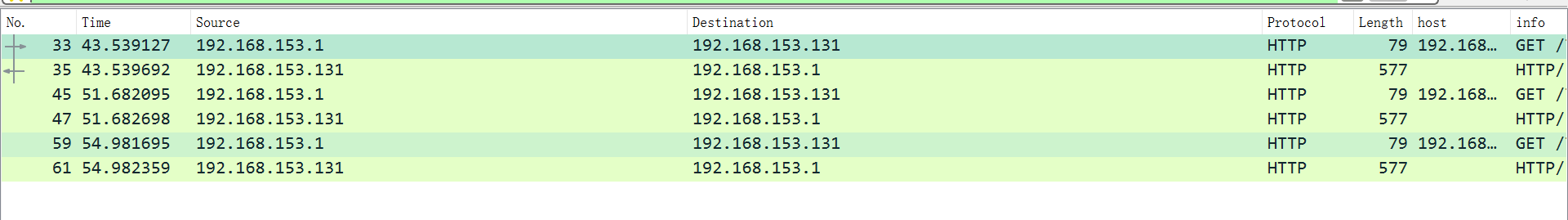
接下来看看该后门有没有什么网络行为，在不进行源码分析的情况能不能被发现，先利用burp抓浏览器包，此时观察web日志，已经接收到相关数据



但是burp抓取的数据包中却什么也看不到



尝试利用wireshark抓包查看，通过过滤发现后门链接的迹象



Follow一下，可追踪到该后门链接



顺便查了下黑吃黑的相关资料，这还是很普遍的，尤其是免费的一些工具、木马，菜刀工具之前就出现过一个有后门的版本，所以在拿到一个shell或是新工具还是很有必要对其进行分析的，免得我们成为他人的黑手。