**宝塔Liunx面板存在xss漏洞**

**官网地址**：https://www.bt.cn/

**项目地址：**https://www.bt.cn/bbs/thread-1186-1-1.html

Linux面板6.0安装命令(暂时仅兼容Centos7.x，其它系统版本请安装5.9稳定版)：

yum install -y wget && wget -O install.sh http://download.bt.cn/install/install\_6.0.sh && bash install.sh



**宝塔简介：**

宝塔面板是一款服务器管理软件，支持windows和linux系统，可以通过Web端轻松管理服务器，提升运维效率。例如：创建管理网站、FTP、数据库，拥有可视化文件管理器，可视化软件管理器，可视化CPU、内存、流量监控图表，计划任务等功能。

宝塔面板拥有极速方便的一键配置与管理，可一键配置服务器环境（LAMP/LNMP/Tomcat/Node.js），一键部署SSL，异地备份；提供SSH开启关闭服务，SSH端口更改，禁ping，防火墙端口放行以及操作日志查看；CPU、内存、磁盘IO、网络IO数据监测，可设置记录保存天数以及任意查看某天数据；计划任务可按周期添加执行，支持SHELL脚本，提供网站、数据库备份以及日志切割，且支持一键备份到又拍云存储空间，或者其他云存储空间里；通过web界面就可以轻松管理安装所用的服务器软件，还有实用的扩展插件；集成方便高效的文件管理器，支持上传、下载、打包、解压以及文件编辑查看

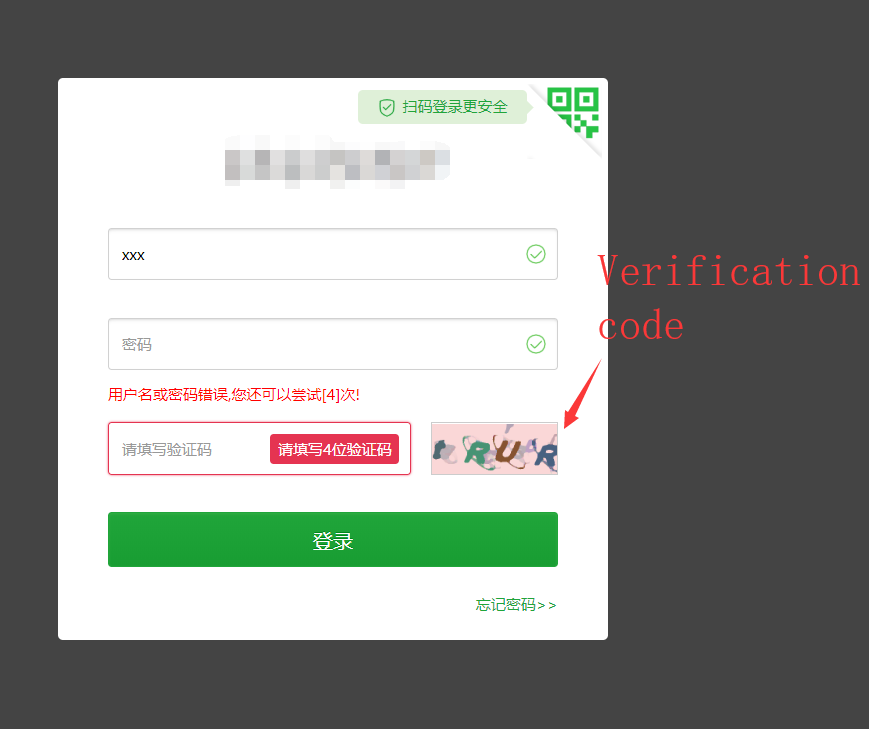
**漏洞利用：**

1. 安装完成后，访问登录地址

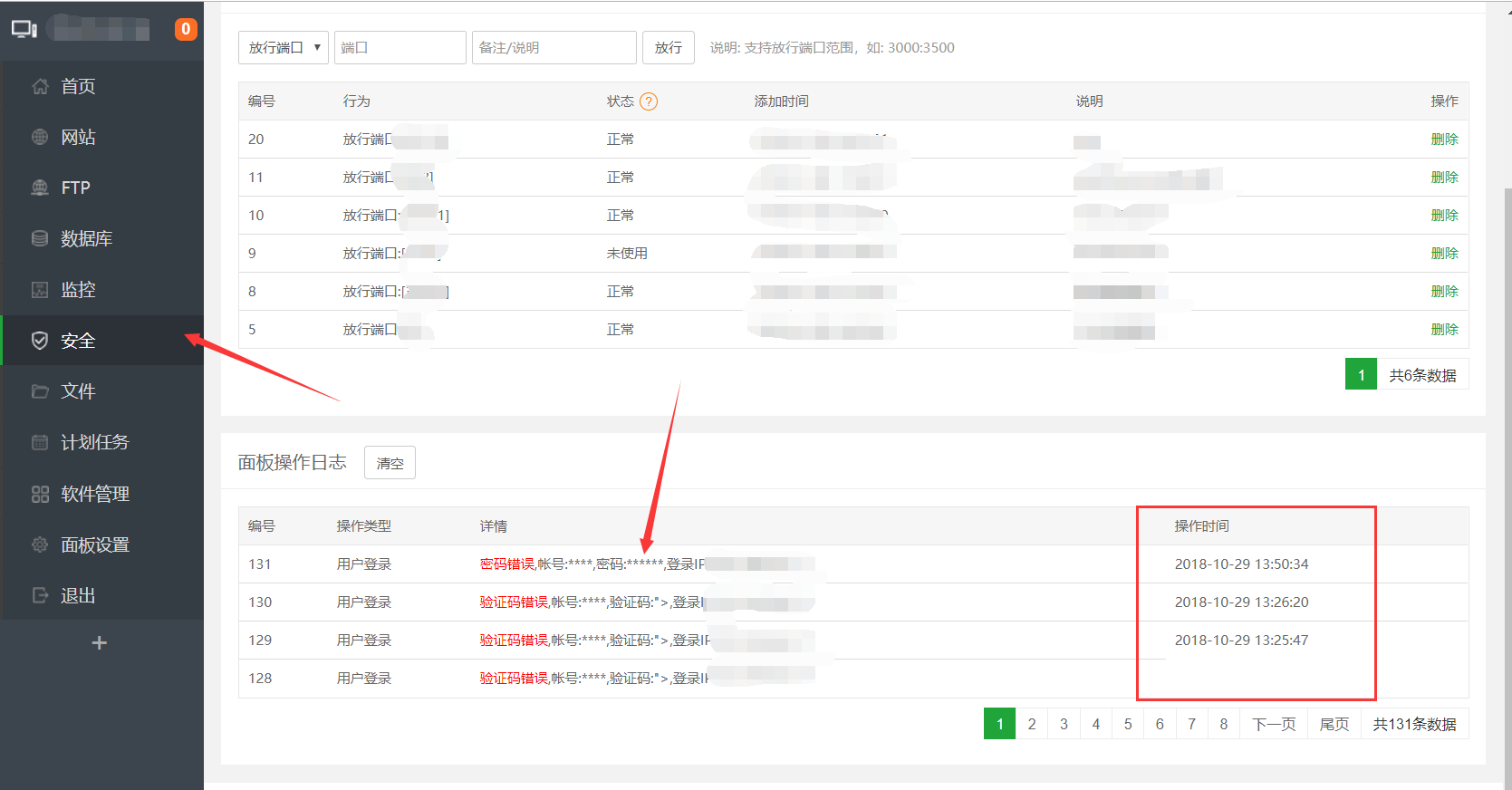


1. 当使用错误的账号密码登录时，要求使用验证码登录

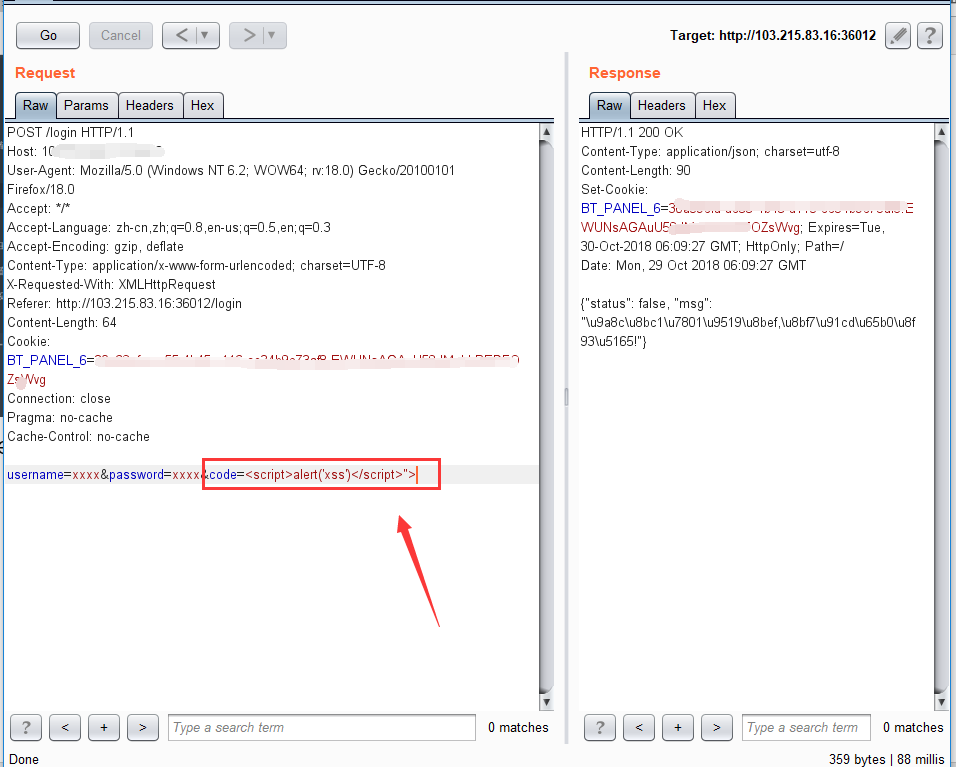
Tips：漏洞就存在验证码处



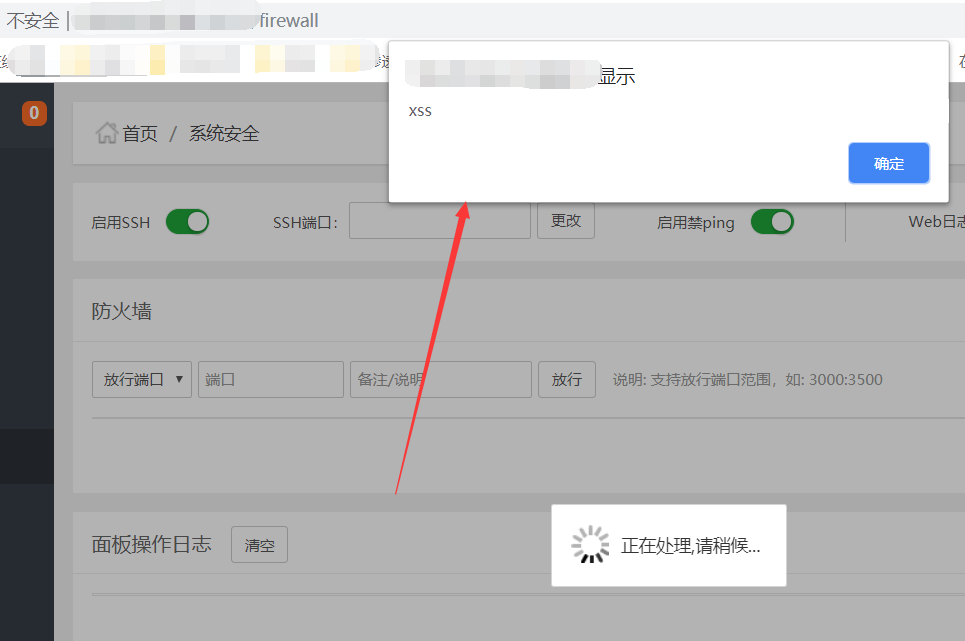
1. 使用正确的账号密码登录面板后，可以看见在面板《安全》这记录了登录操作日志



1. 这时候我们在使用burp截获登录时的数据包，对数据包进行相关修改，插入我们的payload”code=<script>alert(‘xss’)</script>”



1. 重放数据包后，再次访问安全这一栏目，可以看见js代码成功执行，窗体成功弹出！



Tips：如有不足之处请指正。