**Pagoda Linux panel exists xss**

**Home**：https://www.bt.cn/

**Installation documentation：**https://www.bt.cn/bbs/thread-1186-1-1.html

Linux Panel 6.0 installation command (temporarily only compatible with Centos7.x, other system versions please install 5.9 stable version):

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



**Project Description：**

The Pagoda Panel is a server management software that supports windows and linux systems. It can easily manage servers through the Web and improve operation and maintenance efficiency. For example: create a management website, FTP, database, have a visual file manager, visual software manager, visualize CPU, memory, traffic monitoring charts, schedule tasks and other functions.

Pagoda panel has a fast and convenient one-button configuration and management, one-click configuration server environment (LAMP/LNMP/Tomcat/Node.js), one-click deployment of SSL, offsite backup; SSH open and close service, SSH port change, ban ping , firewall port release and operation log view; CPU, memory, disk IO, network IO data monitoring, can set the record save days and arbitrarily view the data of a certain day; scheduled tasks can be added by cycle, support SHELL script, provide website, database backup And log cutting, and support one-click backup to shoot cloud storage space, or other cloud storage space; through the web interface can easily manage the server software used for installation, as well as practical extensions; integrated convenient and efficient file manager Support upload, download, package, unzip and file editing.

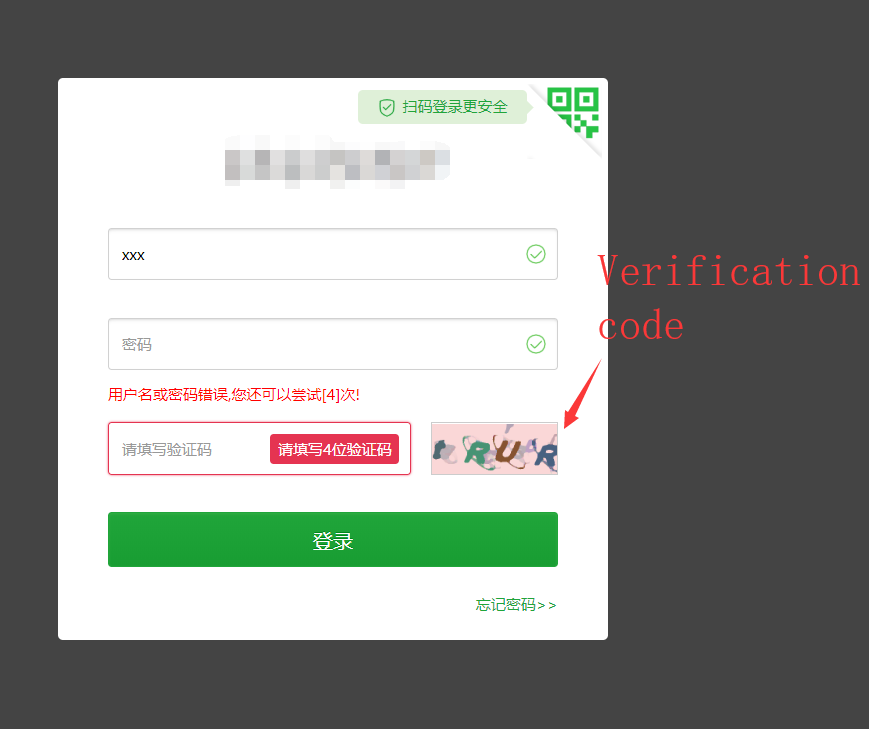
**Example：**

1. Access login address after installation is complete

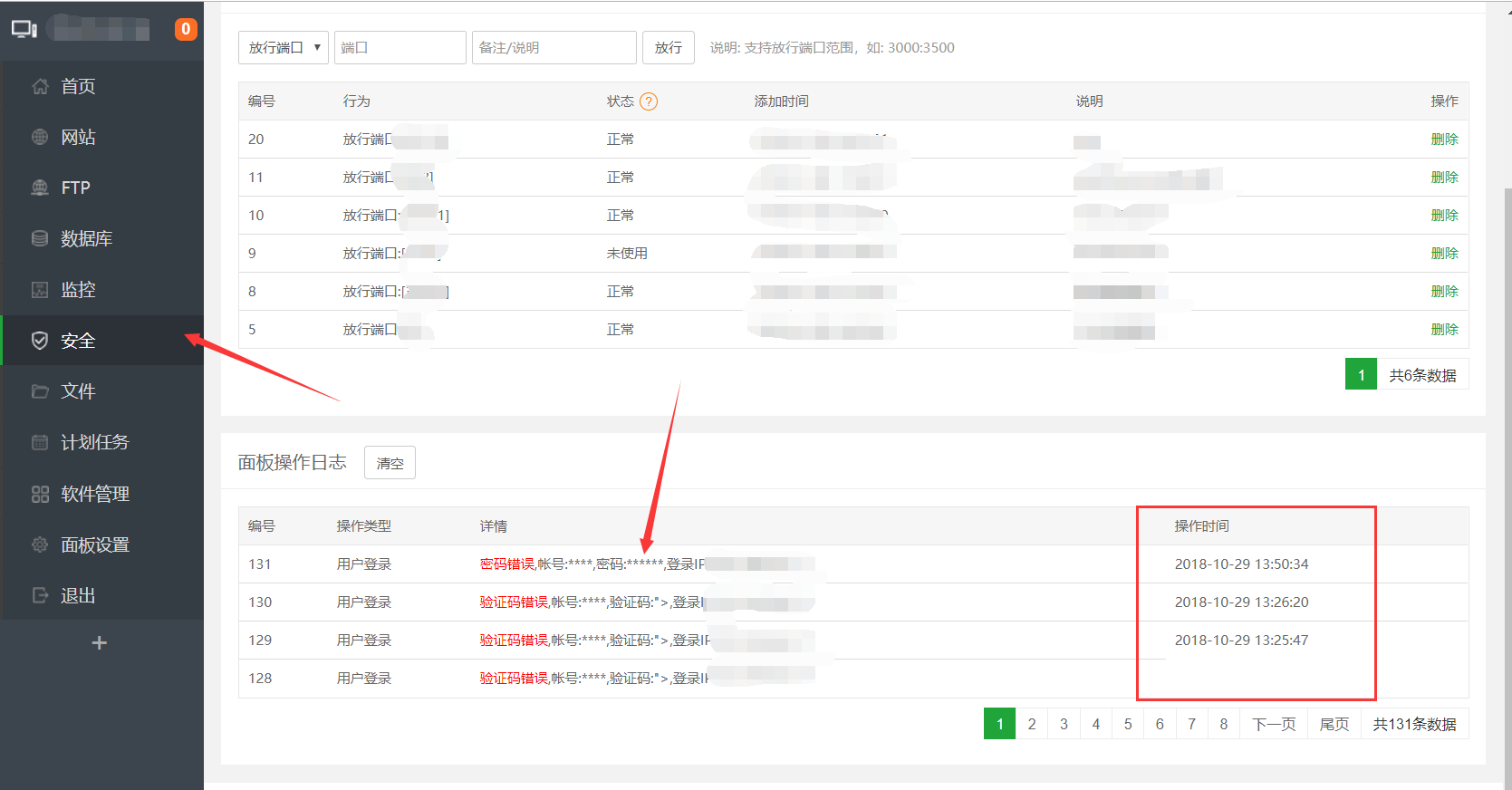


1. A verification code appears after trying to log in with an invalid account

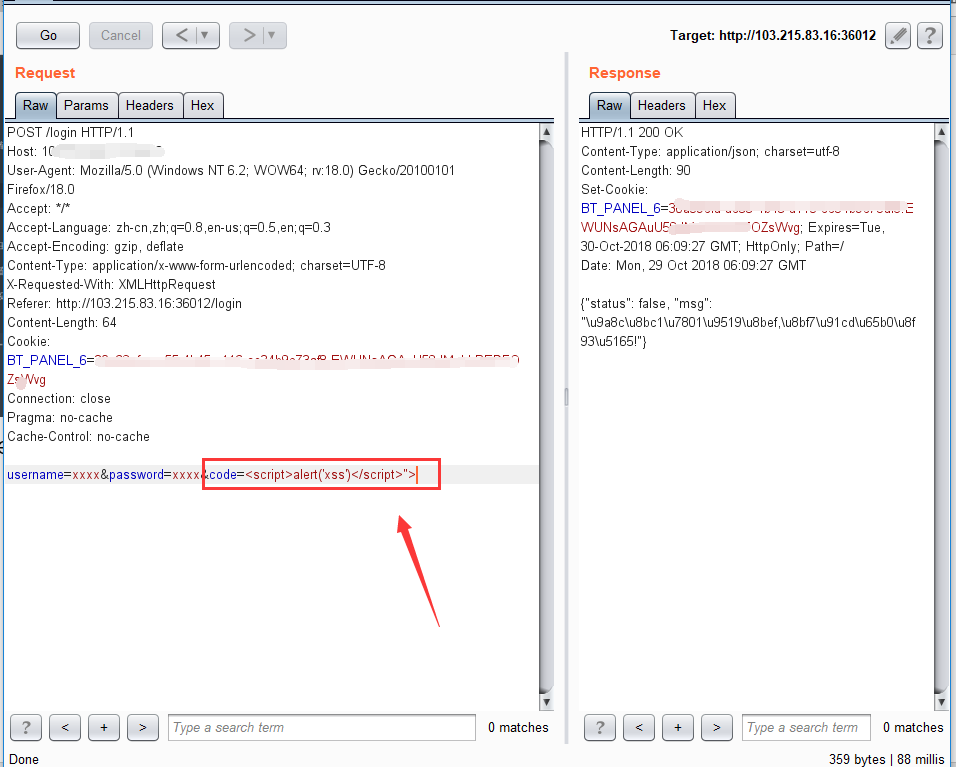
Tips：This vulnerability appears at the verification code.



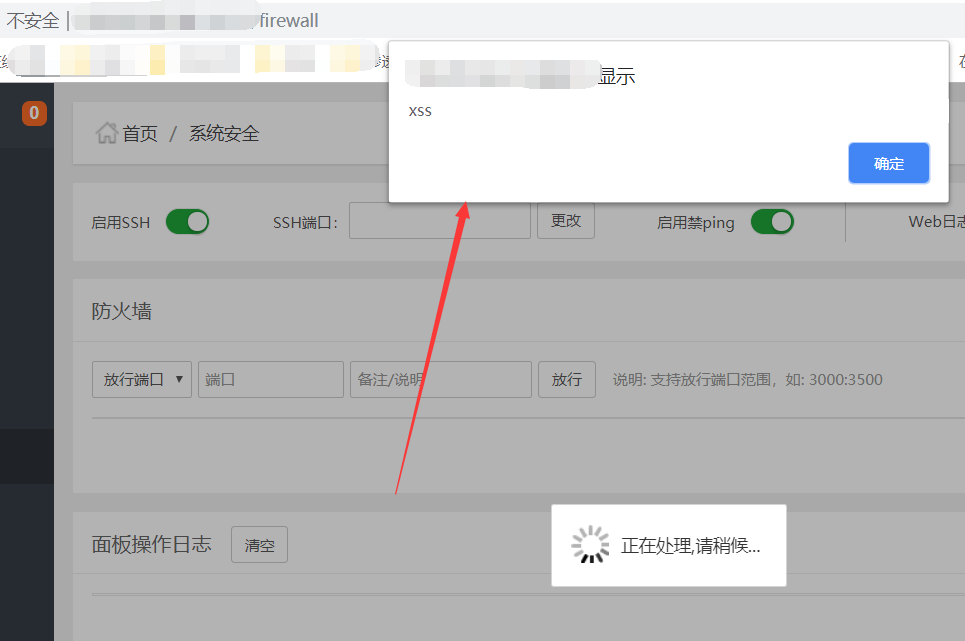
1. We can clearly see in the background of the panel, our login log



1. At this time, we use the packet interception tool (burp) to intercept the packet of this login. And make some modifications, insert malicious code



1. Visit the background again, you can see that the javascript code we inserted successfully executed（Do not use it in depth to prove that the vulnerability exists.）.



Tips：Inadequacies, please correct me