[Entity Description]

The PHP Cloud Talent System is designed and developed specifically for Chinese users, with 100% open source code. It is an efficient talent and enterprise recruitment and hiring solution built on PHP and MySQL databases, which can greatly meet the needs of webmasters for secondary development of website programs while respecting copyright.

[Vulnerability Description]

Without filtering malicious data submitted by users, malicious characters can be directly concatenated into SQL statements, causing SQL injection vulnerabilities and allowing access to database data.

[Impact Description]

Attackers can obtain sensitive information in applications and databases, such as user credentials, personal information, bank accounts, etc., by injecting malicious SQL queries. You can modify data in the database, including inserting, updating, or deleting records. This may result in the application performing incorrect data operations, disrupting data integrity.

[Physical download address]

<https://www.phpyun.com/bbs/thread-17296-1-1.html>

Vulnerability code

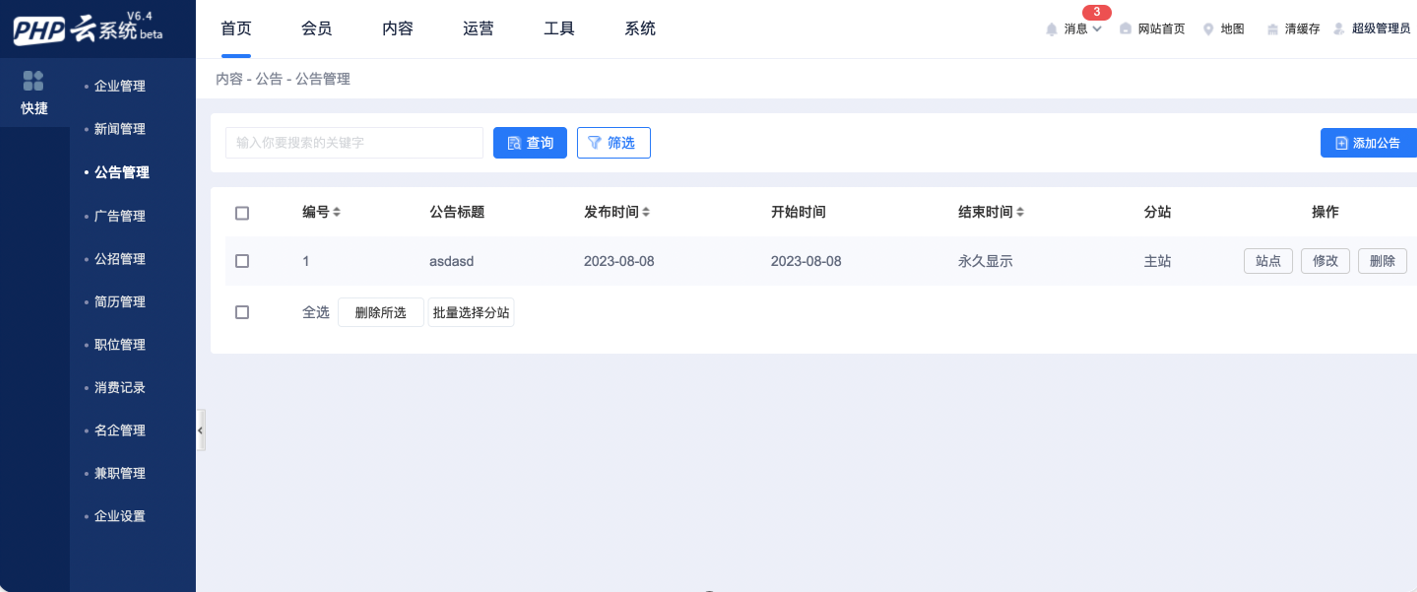
admin/model/advertise.class.php



Accessing the backend (the domain name in the URL is the local test domain name, not the real domain name)

hhttp://www.phpyuntest.cc/admin/index.php

Log in using admin admin

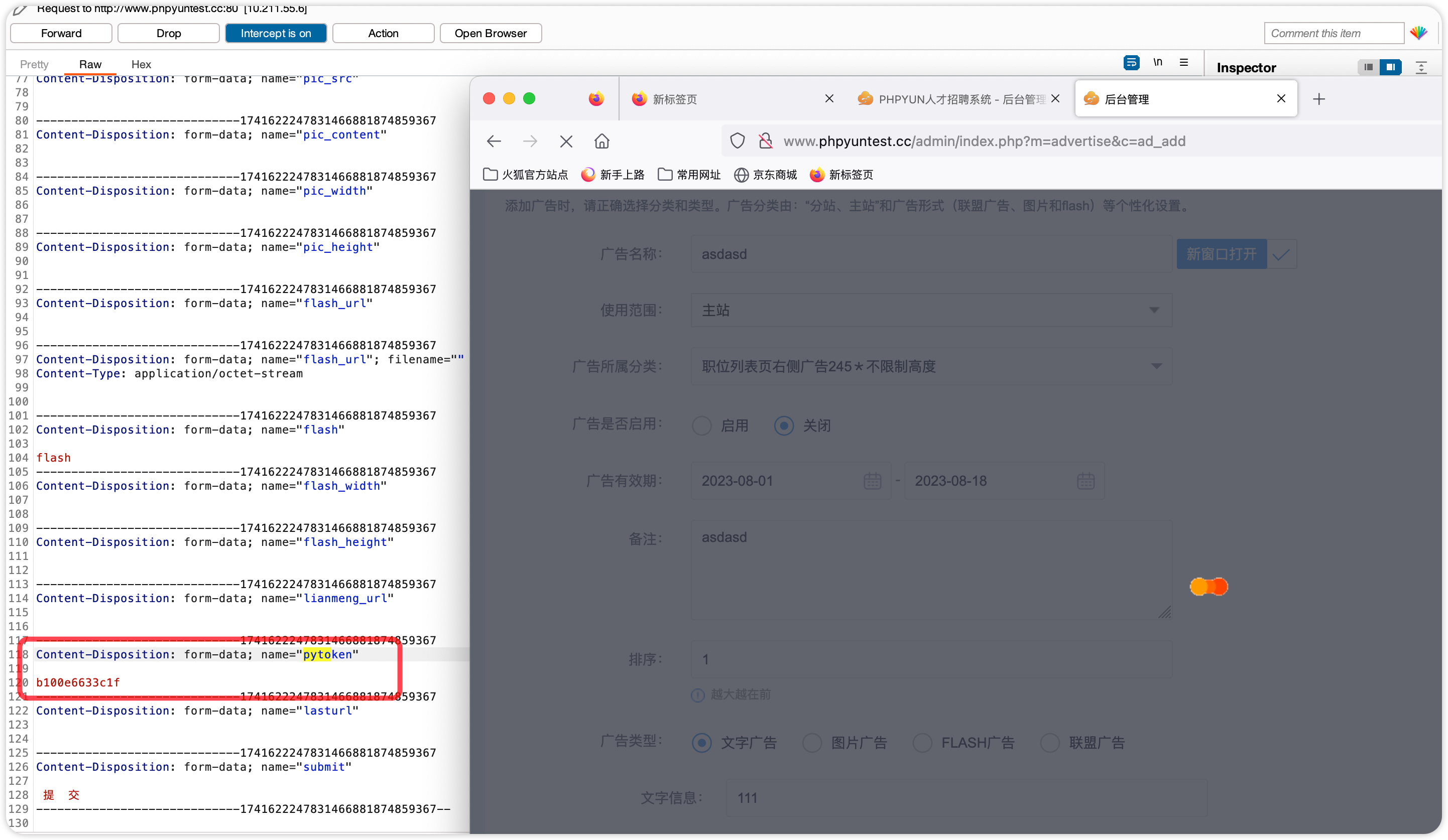


Vulnerability location: Operations - Advertising - Advertising Management - Add Ads (This feature may not be displayed on the frontend, but can be accessed directly by constructing a URL):

http://www.phpyuntest.cc/admin/index.php?m=advertise&c=ad\_add



Randomly fetch a data packet in the background to obtain the pytoken corresponding to the current session



This pytoken corresponds one-to-one with PHPSESSID and remains valid throughout the current login session,

Afterwards, pytoken and cookie in the data package can be replaced to construct the data package for SQL injection:

