

进来一个登录框

用户名  
密码  
登录

发现login.php，存在一个init参数为true时会初始化数据库，初始化了账号密码

正在重置数据库...  
数据库检查/创建成功  
users表已删除  
users表重新创建成功  
管理员用户创建成功  
普通用户创建成功  
数据库users表重置成功!  
[返回登录页面](#)

初始化后存在弱口令admin/admin123,user1/user123,user2/user123  
登录普通用户，发现只有一个文件上传的位置，尝试了一下是白名单

欢迎, user1!  
U  
[浏览...] 未选择文件。  
上传头像  
当前为普通用户  
退出登录

登录admin账号，有数据库备份和导入功能。

The screenshot shows a web-based database management interface. At the top, it displays the URL <http://127.0.0.1/dashboard.php>. Below the header, there's a message: '必须登录此网络才能访问互联网。 打开网络登录页面' (You must log in to access the network). The main content area has two sections: '数据库备份' (Database Backup) and '数据库导入' (Database Import). The '数据库备份' section contains a blue button labeled '创建数据库备份' (Create Database Backup). The '数据库导入' section contains a yellow warning box stating: '注意: 导入数据库将覆盖现有数据, 请确保在操作前已创建备份!' (Warning: Importing the database will overwrite existing data, please ensure a backup is created before operation!). It also includes a file upload input field with the placeholder '浏览... 未选择文件.' (Browse... No file selected.) and a green button labeled '导入数据库' (Import Database).

创建一个数据库备份看一下，发现uploadfile表中字段extension字段存放了白名单，尝试将其中一个改成php，然后导入sql文件，将白名单重置允许上传php文件

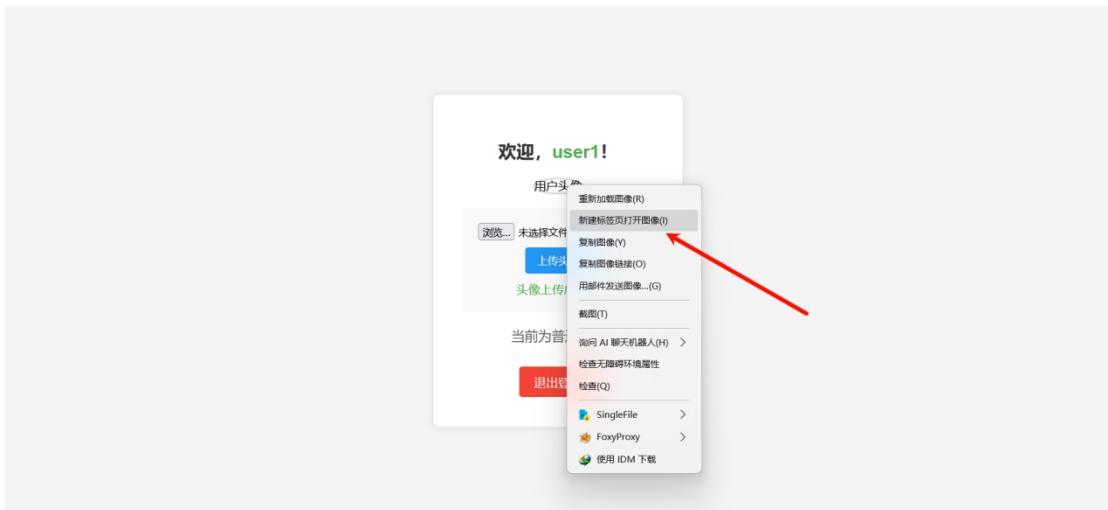
```
45 DROP TABLE IF EXISTS `uploadfile`;
46 /*!40101 SET @saved_cs_client      = @@character_set_client */;
47 /*!40101 SET character_set_client = utf8mb4 */;
48 CREATE TABLE `uploadfile` (
49   `id` int(11) NOT NULL AUTO_INCREMENT,
50   `extension` varchar(10) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
51   PRIMARY KEY (`id`),
52   UNIQUE KEY `extension` (`extension`)
53 ) ENGINE=MyISAM AUTO_INCREMENT=7 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;
54 /*!40101 SET character_set_client = @saved_cs_client */;
55
56
57 -- Dumping data for table `uploadfile`
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
```

导入成功

The screenshot shows a confirmation message: '导入成功' (Import successful). Above this, there's a download link for a SQL file named 'backup\_user\_management\_20251022181518.sql' (4.49 KB, 2025-10-22 18:15:19). Below the download link, there's a '数据库导入' (Database Import) section with a yellow warning box: '注意: 导入数据库将覆盖现有数据, 请确保在操作前已创建备份!' (Warning: Importing the database will overwrite existing data, please ensure a backup is created before operation!). It includes a file upload input field and a green '导入数据库' (Import Database) button. At the bottom, there's a '管理员功能' (Administrator Functions) section with a list of items:

- 管理用户账户
- 查看系统日志
- 配置系统设置
- 管理所有内容

再次尝试文件上传



成功上传webshell

必须登录此网络才能访问互联网。 打开网站登录页面

PHP Version 7.3.4	
System	Windows NT ZHENHONGRUI 10.0 build 22631 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	configure --log=configure.log --enable-snapshot-build --enable-debug-pack --disable-zts --with-pdo-oci=c:\php-snap-build\deps\aux\oracle\vs64\instantclient_12_1\vc14\shared --with-oci8-12c=c:\php-snap-build\deps\aux\oracle\vs64\instantclient_12_1\vc14\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:\generation_testing_tools\PHP\phpStudy_64\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	API20180731,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

读取.flag

HECTF{90ed1f77c-0f30384c34270fa-e4d4ff93626e7f27}