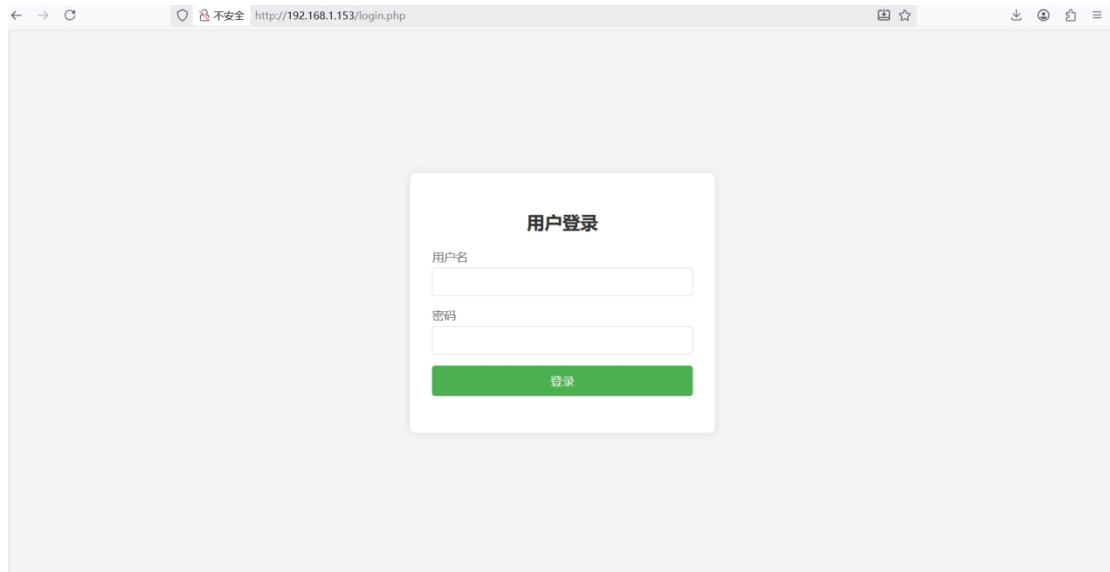


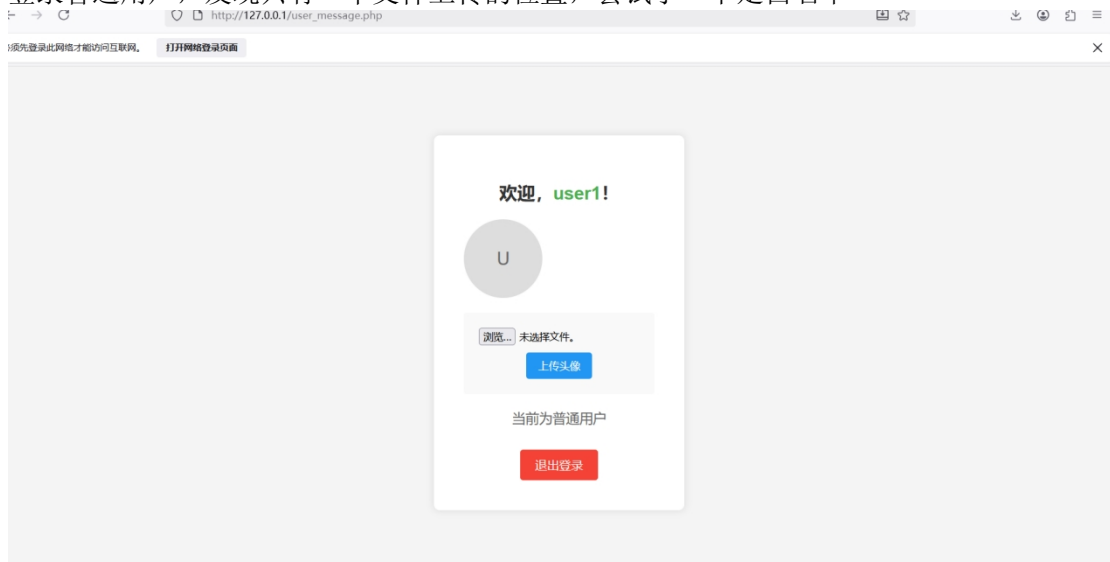
进来一个登录框



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



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



登录admin账号，有数据库备份和导入功能。



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

```
49 DROP TABLE IF EXISTS `uploadfile`;  
50 /*!40101 SET @saved_cs_client = @@character_set_client */;  
51 /*!50503 SET character_set_client = utf8mb4 */;  
52 CREATE TABLE `uploadfile` (  
53   `id` int(11) NOT NULL AUTO_INCREMENT,  
54   `extension` varchar(10) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,  
55   PRIMARY KEY (`id`),  
56   UNIQUE KEY `extension` (`extension`)  
57 ) ENGINE=MyISAM AUTO_INCREMENT=1 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;  
58 /*!40101 SET character_set_client = @saved_cs_client */;  
59  
60 --  
61 -- Dumping data for table `uploadfile`  
62 --  
63  
64  
65 LOCK TABLES `uploadfile` WRITE;  
66 /*!40000 ALTER TABLE `uploadfile` DISABLE KEYS */;  
67 INSERT INTO `uploadfile` VALUES (1,'jpg'),(2,'jpeg'),(3,'png'),(4,'gif'),(5,'webp');  
68 /*!40000 ALTER TABLE `uploadfile` ENABLE KEYS */;  
69 UNLOCK TABLES;  
70  
71 --  
72 -- Table structure for table `users`  
73 --  
74  
75 DROP TABLE IF EXISTS `users`;  
76 /*!40101 SET @saved_cs_client = @@character_set_client */;  
77 /*!50503 SET character_set_client = utf8mb4 */;  
78 CREATE TABLE `users` (  
79   `id` int(11) NOT NULL AUTO_INCREMENT,  
80   `username` varchar(50) COLLATE utf8mb4_unicode_ci NOT NULL,  
81   `password` varchar(255) COLLATE utf8mb4_unicode_ci NOT NULL,  
82   `role` enum('admin','user') COLLATE utf8mb4_unicode_ci NOT NULL DEFAULT 'user',  
83   `avatar` varchar(255) COLLATE utf8mb4_unicode_ci DEFAULT NULL,  
84   `created_at` timestamp NULL DEFAULT CURRENT_TIMESTAMP,  
85   PRIMARY KEY (`id`),  
86   UNIQUE KEY `username` (`username`)  
87 ) ENGINE=MyISAM AUTO_INCREMENT=1 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;  
88 /*!40101 SET character_set_client = @saved_cs_client */;  
89  
90 --  
91 -- Dumping data for table `users`  
92 --
```

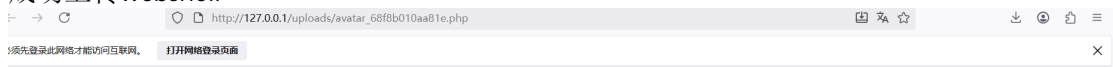
导入成功



再次尝试文件上传



成功上传webshell



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	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,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:\penetration_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	API320180731,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}