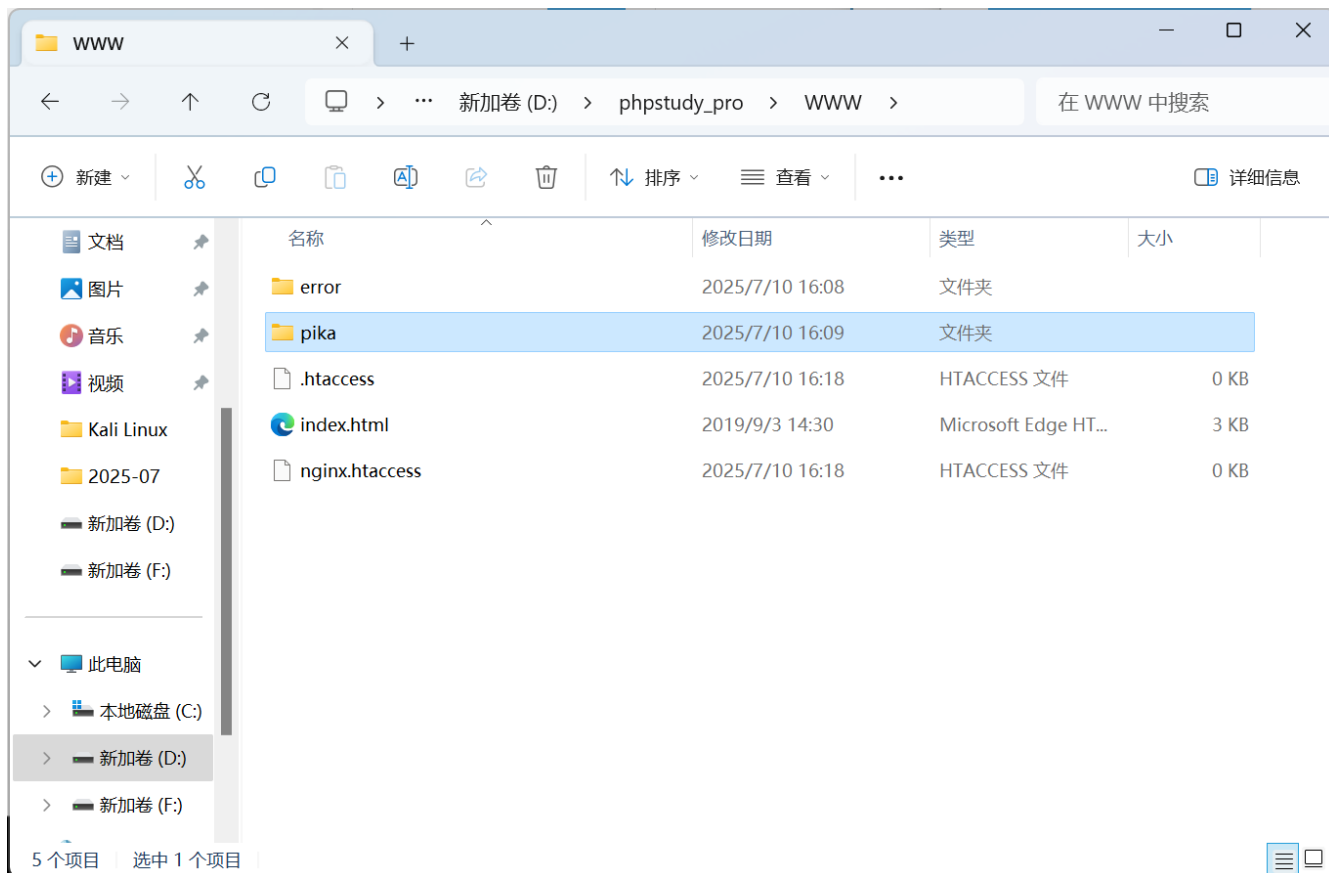


使用小皮面板搭建Pikachu靶场

1.在小皮面板中打开Apache和MySQL



2.将Pikachu文件夹复制到小皮面板安装目录的WWW文件夹下



3.在浏览器网址栏中输入Localhost



站点创建成功

目录说明:

- 1: 网站目录: /phpstudy安装目录/www/站点域名/
- 2: 错误提示页面: /phpstudy安装目录/www/站点域名/error/
- 3: 你可以删除或者修改该目录下的所有文件

操作注意事项:

- 1: 新建站点、数据库、FTP可在phpstudy面板操作, 数据库可在环境中下载数据库管理软件等;
- 2: 将网站程序放到站点目录时请使用复制, 剪切可能造成程序文件权限不正确;

使用手册, 视频教程, BUG反馈, 官网地址: www.xp.cn

4.在后方添加/pika, 进入pikachu

Get the pikachu

localhost/pika/

Pikachu 漏洞练习平台 pika-pika~

系统介绍

漏洞类型

系统介绍

Pikachu是一个带有漏洞的Web应用系统。在这里包含了常见的web安全漏洞。如果你是一个Web渗透测试学习人员且正发愁没有合适的靶场进行练习，那么Pikachu可能正合你意。

Pikachu上的漏洞类型列表如下：

- Burt Force(暴力破解漏洞)
- XSS(跨站脚本漏洞)
- CSRF(跨站请求伪造)
- SQL-Inject(SQL注入漏洞)
- RCE(远程命令/代码执行)
- Files Inclusion(文件包含漏洞)
- Unsafe file downloads(不安全的文件下载)
- Unsafe file uploads(不安全的文件上传)
- Over Permission(越权漏洞)
- ./././ (目录遍历)
- I can see your ABC(敏感信息泄露)
- PHP反序列化漏洞
- XXE(XML External Entity attack)
- 不安全的URL重定向
- SSRF(Server-Side Request Forgery)
- More...(找找看?, 有彩蛋)
- 管理工具里面提供了一个简易的xss管理后台,供你测试钓鱼和劫cookie~
- 后续会持续更新一些新的漏洞进来,也欢迎你提交漏洞案例给我,最新版本请关注pikachu

每类漏洞根据不同的情况又分别设计了不同的子类

同时,为了让这些漏洞变的有意思一些,在Pikachu平台上为每个漏洞都设计了一些小的场景,点击漏洞页面右上角的"提示"可以查看到帮助信息。

如何安装和使用

Pikachu使用世界上最好的语言PHP进行开发-, 数据库使用的是mysql, 因此运行Pikachu你需要提前安装好"PHP+MySQL+中间件"的基础环境, 建议在你的测试环境直接使用 一些集成软件来搭建这些基础环境比如XAMPP,WAMP等,作为一个搞安全的人,这些东西对你来说应该不是什么难事。接下来:

->把下载下来的pikachu文件夹放到web服务器根目录下;

->根据实际情况修改inc/config.inc.php里面的数据库连接配置;

->访问http://x.x.x.x/pikachu,会有一个红色的热情提示"欢迎使用,pikachu还没有初始化",点击进行初始化安装",点击即可完成安装。

我为Pikachu创建了一个QQ群(ID:532078894), 欢迎加进来和大家一起学习讨论。

如果阁下对Pikachu有什么建议或者想找我聊聊可以发个邮件给我: 1061321987@qq.com, 谢谢。

切记

5.继续在后方添加/install.php，进入安装界面

Get the pikachu

localhost/pika/install.php

Pikachu 漏洞练习平台 pika-pika~

系统介绍

漏洞类型

系统初始化安装

Setup guide:

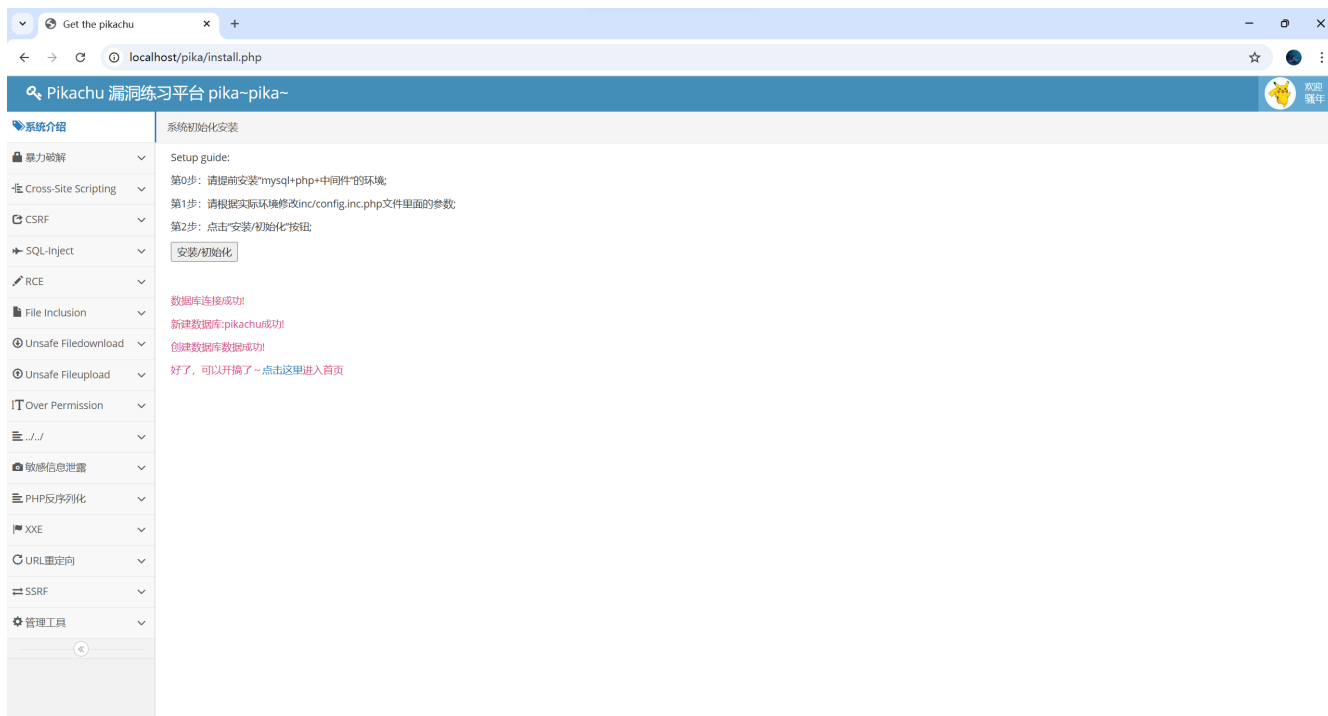
第0步: 请提前安装"mysql+php+中间件"的环境

第1步: 请根据实际情况修改inc/config.inc.php文件里面的参数;

第2步: 点击"安装/初始化"按钮;

安装/初始化

6.点击完成安装



7.如果出现报错（如：请仔细检查inc/config.inc.php的配置），可检查config文件中的数据库是否在小皮面板中存在，小皮面板是否连接到mysql