

FineCMS 的跨站脚本攻击实验

一【实验目标】

- 掌握 FineCMS 的使用；
- 掌握 FineCMS 跨站脚本攻击原理。

二【实验环境】

- Windows 10 操作系统
- phpStudy, AntSword, ASCII 码转化工具

三【实验原理】

FineCMS 是一款基于 PHP+MySql 开发的内容管理系统，采用 MVC (Model View Controller，模型-视图-控制器) 设计模式实现业务逻辑与表现层的适当分离，使网页设计师能够轻松设计出理想的模板，插件化方式开发功能易用且便于扩展，支持自定义内容模型和会员模型，系统表单功能可轻松扩展出留言、报名、咨询等功能，实现与内容模型、会员模型相关联，FineCMS 可面向中小型站点提供重量级网站建设解决方案。

跨站脚本攻击 (XSS) 指网站没有对用户输入数据进行编码、转义、过滤限制等处理，导致攻击者的输入可能被输出到页面中当作 HTML 代码和客户端脚本被浏览器执行，从而形成攻击。

四【实验步骤】

实验具体操作步骤如下：

注意：实验时使用 IE 或者 edge 浏览器。

1. 进入系统，输入密码“Admin123456”，如图 1 所示。

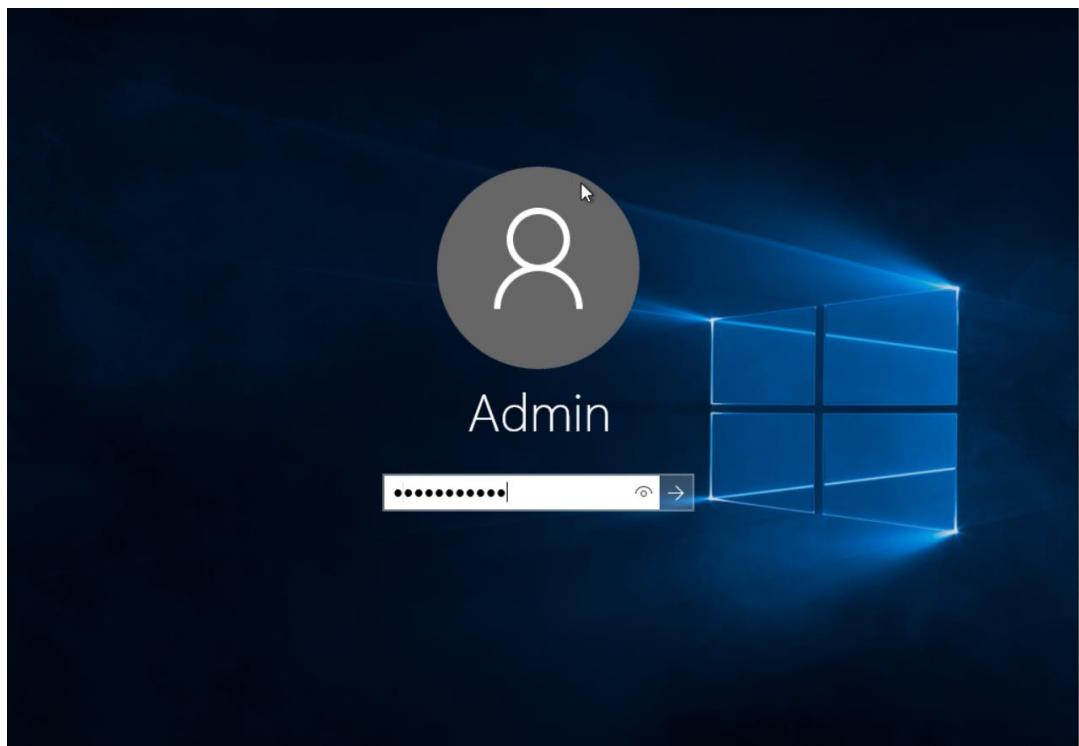


图 1

2. 点击“文件资源管理器”进入【C:\phpStudy\WWW】文件夹下，新建 dede 文件夹，如图 2 所示。

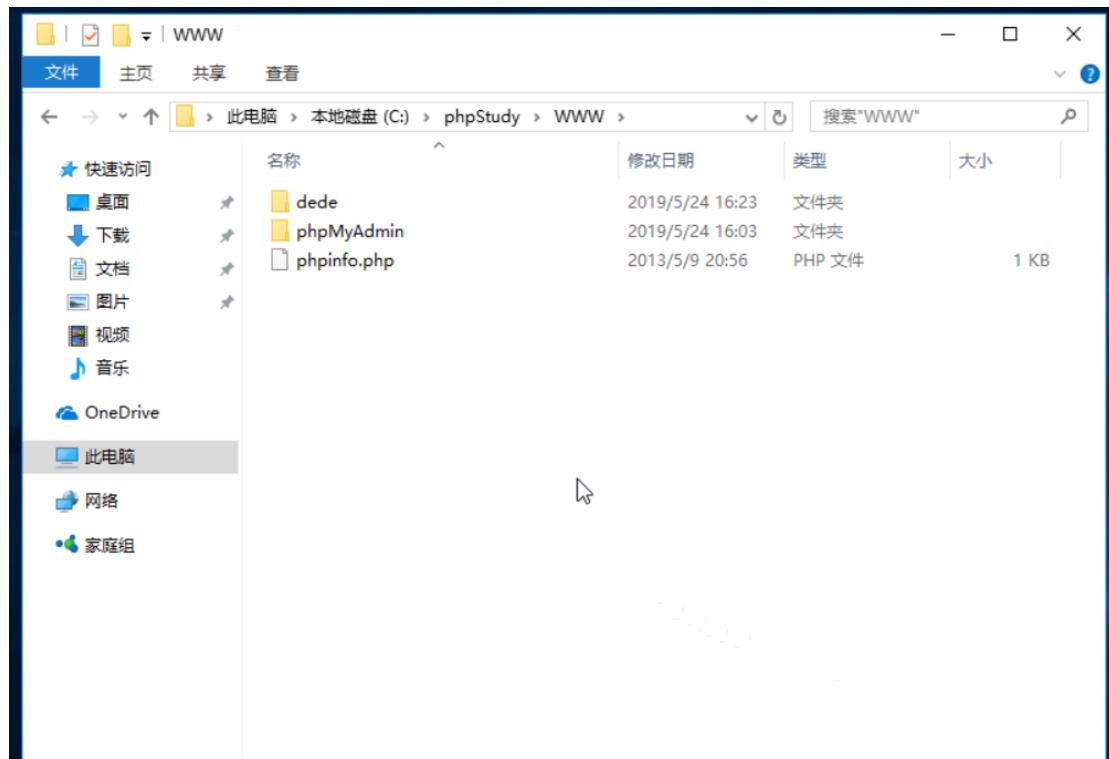


图 2

3. 将【C:\tools】文件夹中 DedeCMS-V5.7-UTF8-SP1-Full 中的 uploads 中的内

容，拷贝到 dede 文件夹。如图 3 所示。

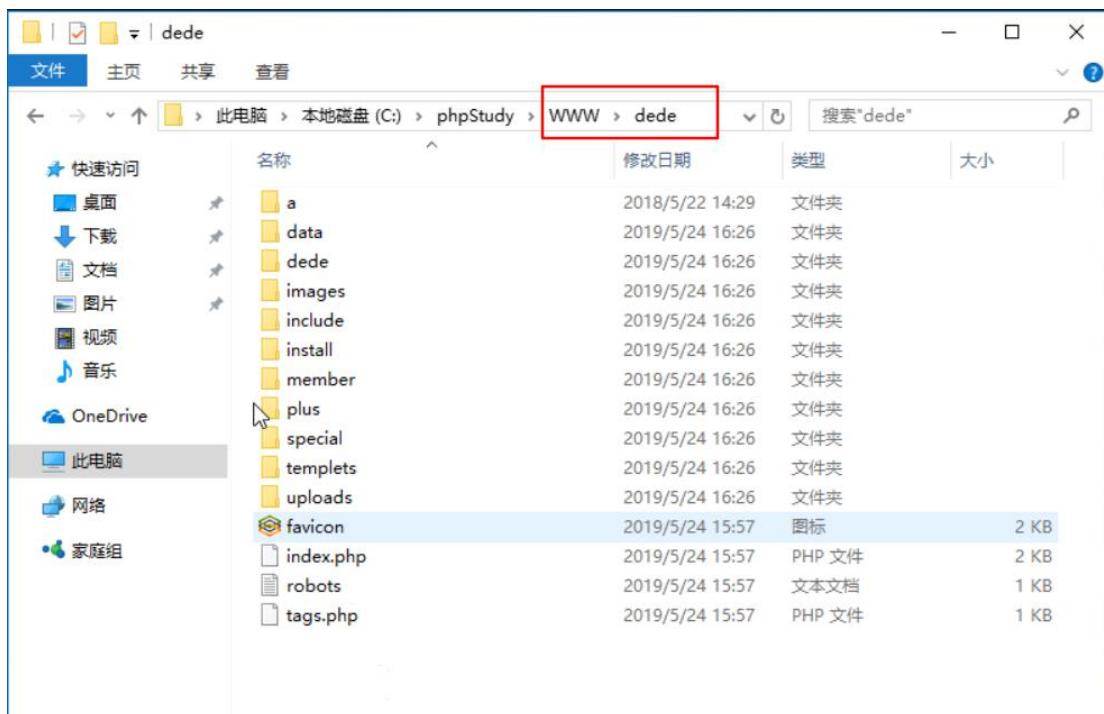


图 3

4. 进入 phpStudy 文件夹，双击打开 phpStudy.exe。点击【其他选项管理】→【MyHomePage】进入浏览器。如图 4 所示。



图 4

5. 首页信息如下，点击【dede/】开始安装，如图 5 所示。

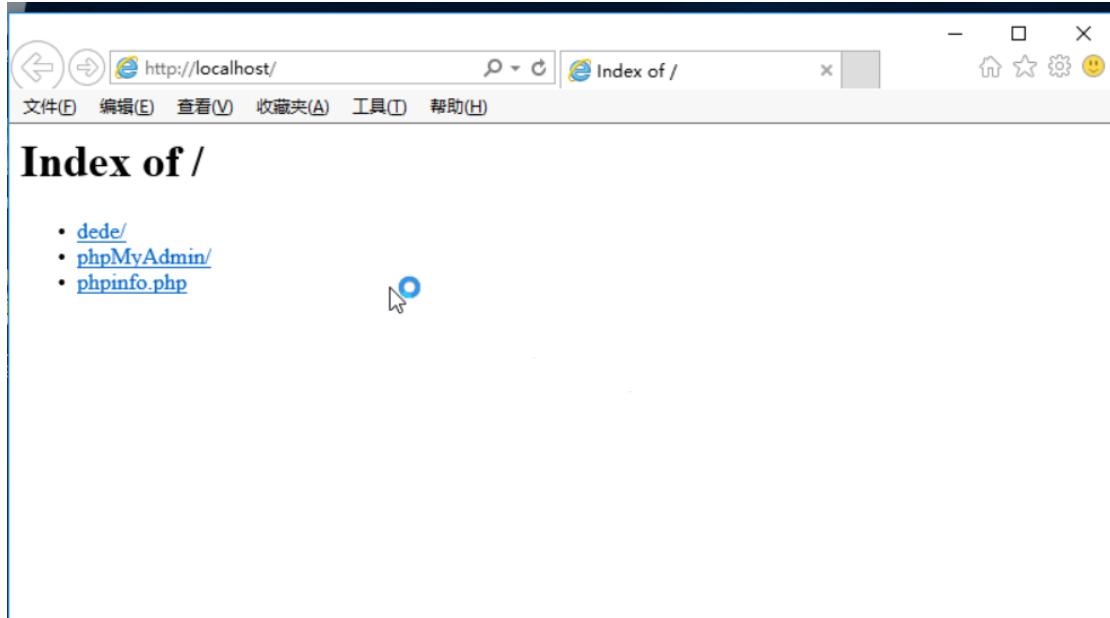


图 5

6. 按照默认完成安装，数据库密码设置为“root”如图 6 所示。

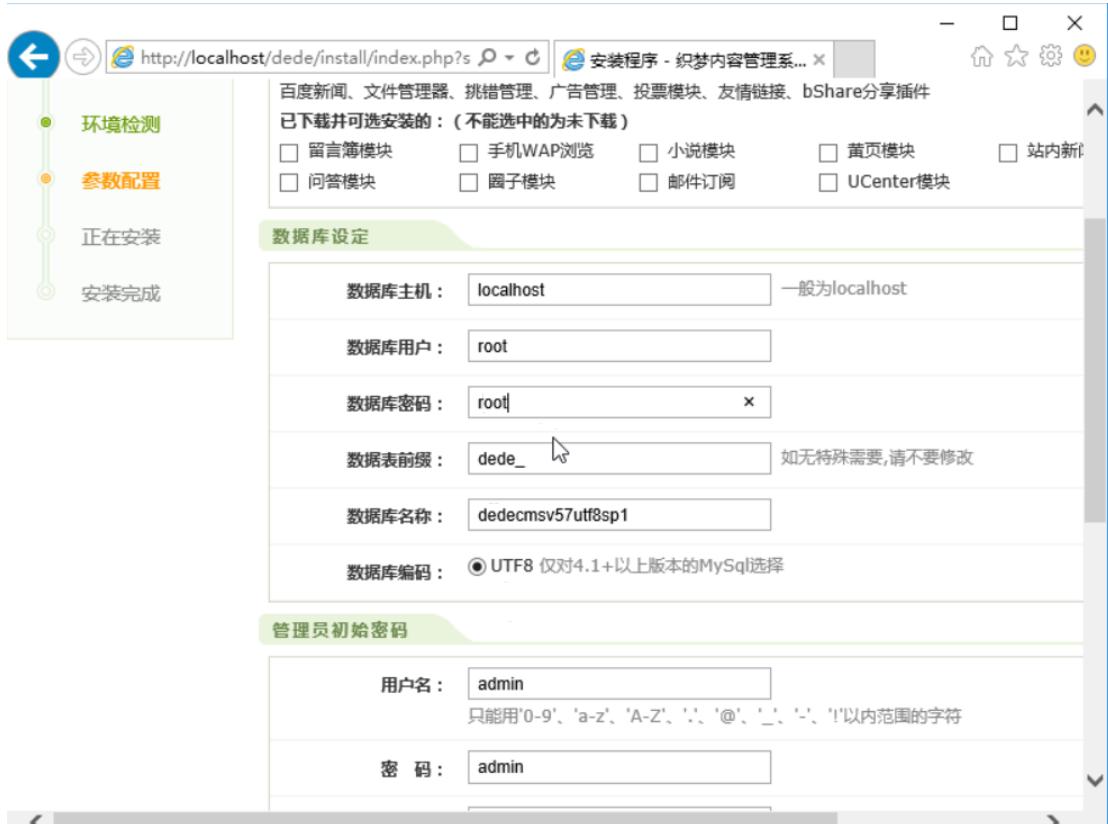


图 6

7. 安装完成后点击【访问网站首页】。如图 7 所示。

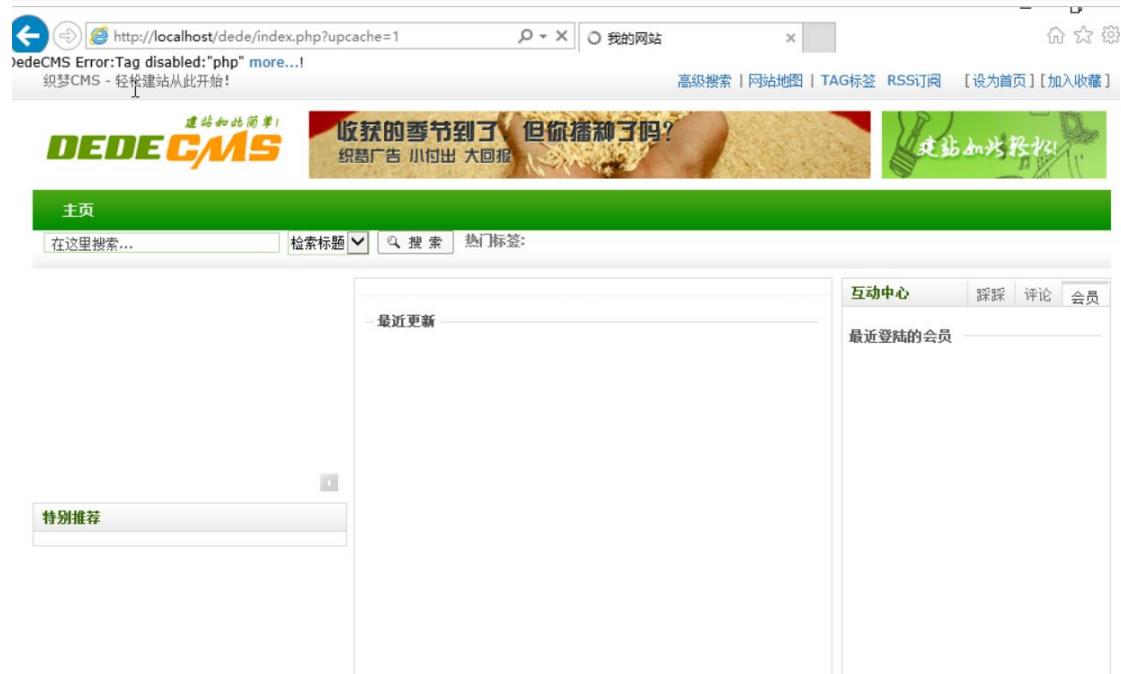


图 7

8. 在浏览器中输入【http://localhost /dede/dede/login.php】访问网站后台，输入用户名和密码（按照前面设置的输入，没有更改则都是 admin），点击【登录】。如图 8 所示。



图 8

9. 进入管理页面后，在最左侧点击【系统】→【系统基本参数】→【会员设置】中的【是否开启会员功能】选择【是】，点击【确定】保存更改。如图 9 所示。

The screenshot shows the DedeCMS 5.7 management interface. On the left sidebar, under the 'System' category, the 'Basic Parameters' item is selected. In the main content area, the 'User Settings' tab is highlighted with a red box. The configuration table lists several parameters, with the first one, '是否开启会员功能' (Enable Member Function), having its 'Yes' radio button selected and highlighted with a red box.

参数说明	参数值	变量名
是否开启会员功能:	<input checked="" type="radio"/> 是 <input type="radio"/> 否	cfg_mb_open
是否开启会员图集功能:	<input checked="" type="radio"/> 是 <input type="radio"/> 否	cfg_mb_album
是否允许会员上传非图片附件:	<input checked="" type="radio"/> 是 <input type="radio"/> 否	cfg_mb_upload
会员上传文件大小(X):	1024	cfg_mb_upload_size
是否开放会员对自定义模型投稿:	<input checked="" type="radio"/> 是 <input type="radio"/> 否	cfg_mb_sendall
是否把会员指定的远程文档下载到本地:	<input checked="" type="radio"/> 是 <input type="radio"/> 否	cfg_mb_rardown
会员附件许可的类型:	swf mp3 m3u rmbv wmv wma wav mid mov zip rar doc xsl ppt wps	cfg_mb_addontype
会员附件总大小限制(MB):	500	cfg_mb_max
不允许注册的会员id:	www,bbs,ftp,mail,user,users,admin,administrator	cfg_mb_notallow
用户id最小长度:	3	cfg_mb_idmin

图 9

10. 点击注销。如图 10 所示。

The screenshot shows the DedeCMS 5.7 management interface. The top navigation bar includes a 'Logout' link, which is highlighted with a red box. The left sidebar shows the 'System' category with various sub-options like 'Basic Parameters', 'User Management', etc.

图 10

11. 在浏览器中输入【<http://localhost/dede/index.php>】，点击【注册账号】进行注册。如图 11 所示。

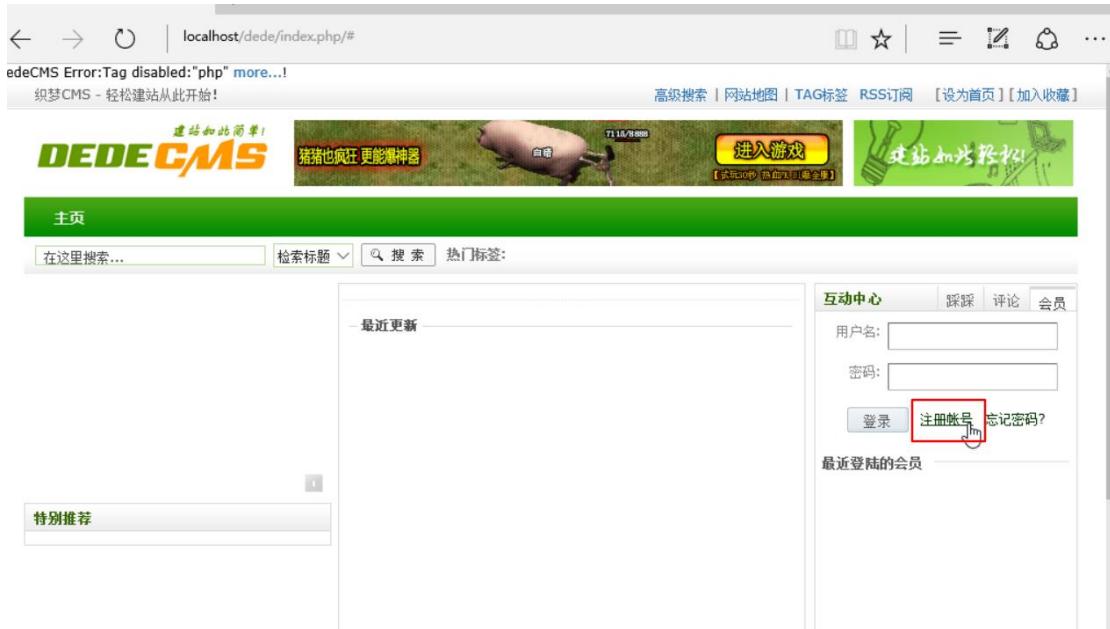


图 11

12. 输入资料，点击【完善信息】，完成注册。如图 12 所示。

A screenshot of a user registration form. At the top, there are three green arrows pointing right with the text "填写基本信息", "完善详细资料", and "恭喜 注册成功". Below this, a note says "(带 * 号的表示为必填项目，用户名必须大于3位小于20位，密码必须大于3位)". The form fields include:

- 帐号类型: 个人 企业
- 用户名: * (可以使用中文，但禁止除[@].]以外的特殊符号)
- 用户笔名: *
- 登陆密码: *
- 密码强度: 较弱
- 确认密码: * *两次输入密码不一致
- 电子邮箱: *(每个电子邮箱只能注册一个帐号)
- 安全问题: (忘记密码时重设密码用)
- 问题答案:
- 性别: 男 女 保密
- 验证码:  看不清? [点击更换](#)
- 会员注册协议: 1、在本站注册的会员，必须遵守《万能网电子商务服务管理规定》，不得在本站发表违法信息，侵犯他人隐私，侵犯他人知识产权，[转到“设置”以激活 Windows](#)。

图 12

13. 修改数据库字段长度，以实现 XSS 攻击效果。点击 phpStudy 控制面板的【MySQL 管理器】。输入账号密码“root”，“root”如图 13 所示。



图 13

14. 进入数据库配置页面，选择【dedecms57utf8sp1】数据库。在展开的数据表中找到 dede_flink，选择【结构】，点击 url 后的【修改】，将 url 一栏中的 60 修改为 255，点击【保存】。如图 14，15 所示。

图 14



图 15

15. 返回网站首页，在浏览器中输入【<http://localhost/dede/index.php>】，点击网站右下角的【申请加入】，如图 16 所示。

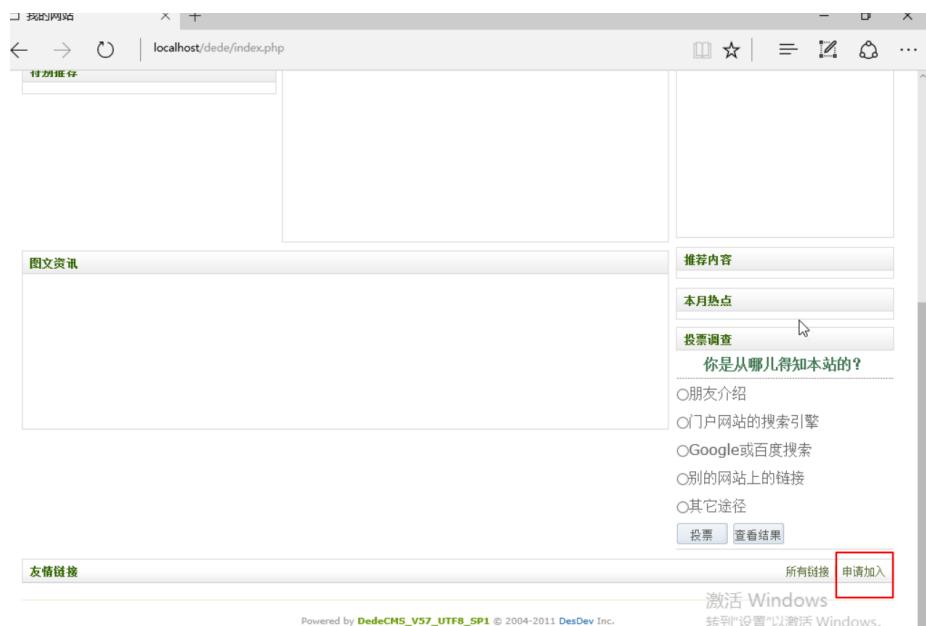


图 16

16. 在网址一行输入 javascript:alert(1)，输入验证码，点击【提交】。如图 17 所示。

The screenshot shows a web browser window with the URL `localhost/dede/plus/flink_add.php`. The page title is "DEDECMS" with the subtitle "建站如此简单!". The main content area is titled "申请链接". It contains several input fields: "网址" (Address) with the value "javascript:alert(1)", "网站名称" (Website Name), "网站Logo" (Website Logo) with the note "(88*31 gif或jpg)", "网站简介" (Website Description), "站长Email" (Administrator Email), "网站类型" (Website Type) set to "综合网站" (Comprehensive Website), and "验证码" (Captcha) with the text "GRAN". Below the form are two buttons: "提交" (Submit) and "重置" (Reset). At the bottom of the page, there is a footer with the text "Powered by DedeCMSV57_UTF8_SP1 © 2004-2011 DesDev Inc." and "Copyright © 2002-2011 DEDECMS. 织梦科技 版权所有 Power by DedeCms".

图 17

17. 发现可以正常提交申请，说明可能存在跨站脚本攻击漏洞。如图 18 所示。



图 18

18. 通过构造编码，对该网站进行跨站脚本攻击，同时构造一句话木马，生成一个网页。进入【C:\phpStudy\WWW\dede】，找到 a.js 文件，这段代码可以创建并保存一句话木马网页，木马连接口令为 cmd。如图 19 所示。

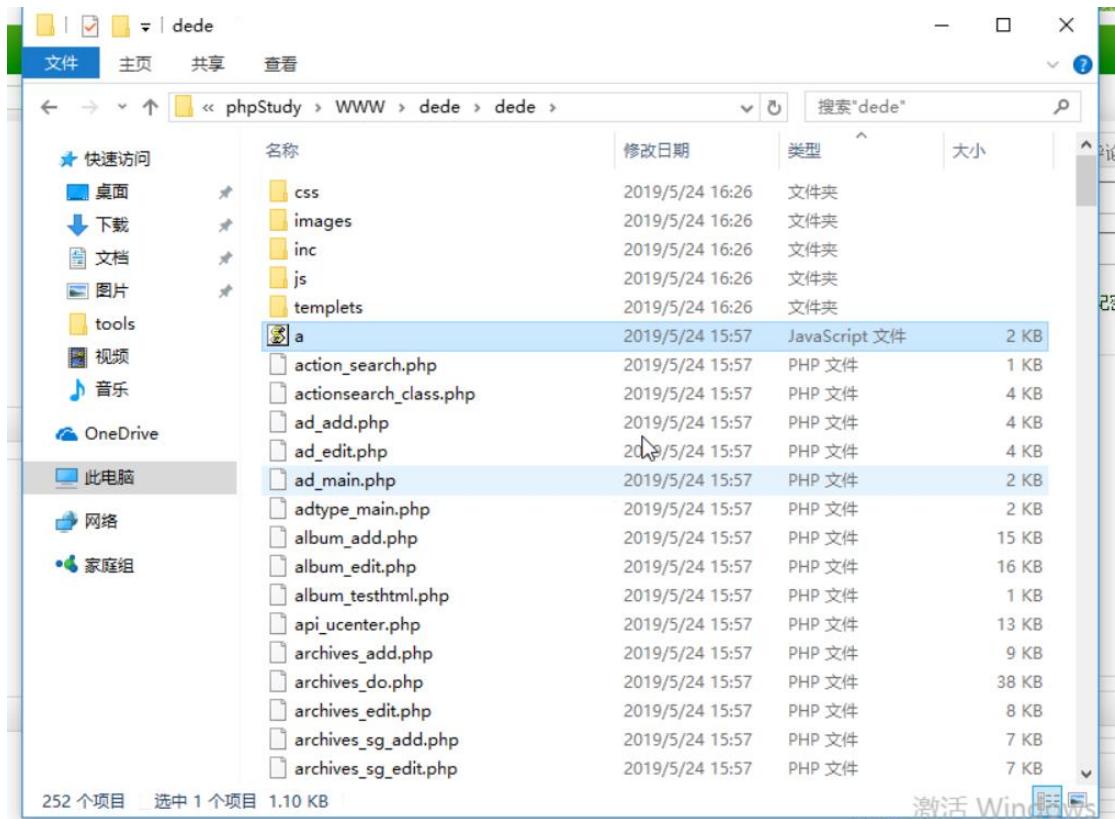


图 19

19. 由于需要调用脚本和执行命令，所以需要对注入的 `xss` 进行转码，打开【C:\tools\ASCII 码转换工具】将`<script src=http://localhost: 80/dede/a. js></script>`这段脚本转换为十进制 ASCII 码，将结果复制。如图 20 所示。



图 20

20. 再次在申请友情链接部分进行 XSS 攻击，输入【Javascript :
document.write(String.fromCharCode(上一步复制的结果))】，再次提交该
申请。如图 21 所示。

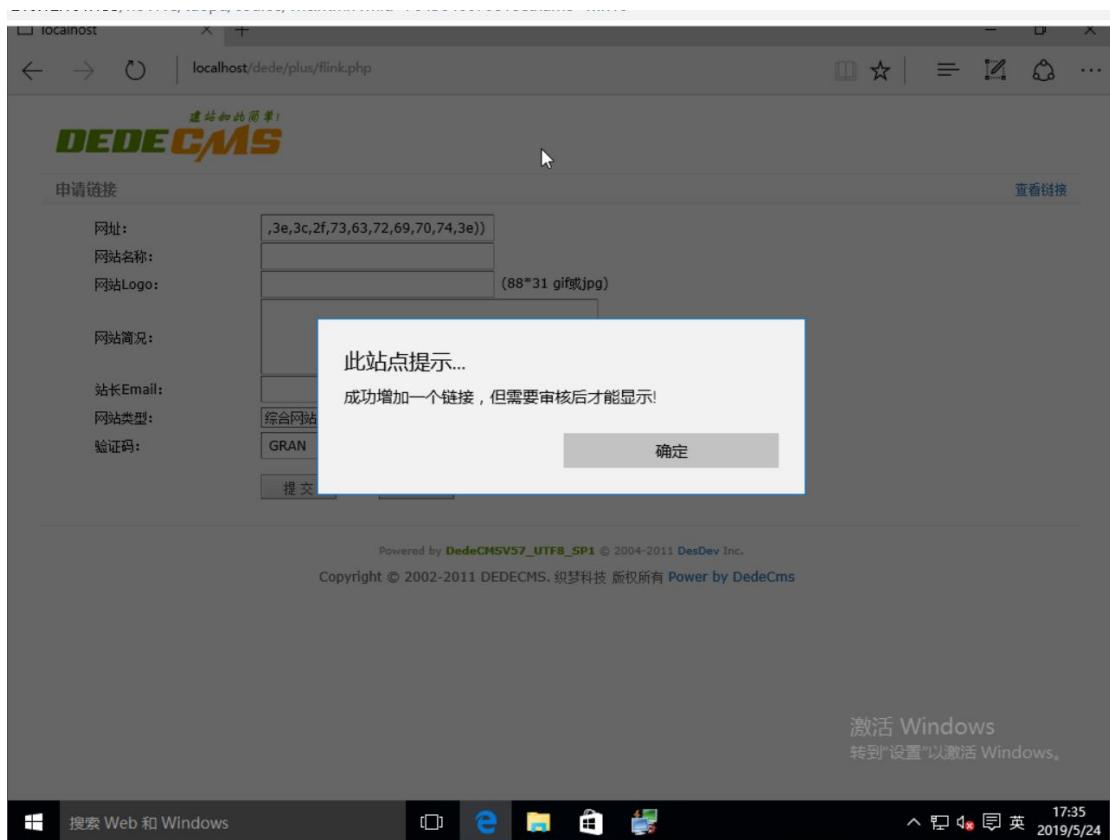


图 21

21. 提交的申请需要由管理员进行申请，管理员登录，点击【模块】-【友情链接】，
此处为方便显示，点击更改设置网站名称为“123”，之后点击该申请。如图
22 所示。

您好：admin , 欢迎使用DedeCMS ! 主菜单 内容发布 内容维护 系统主页 网站主页 会员中心 注销 快捷方式 +

功能搜索 搜索 官方论坛 在线帮助

选择	网站名称	网站Logo	站长Email	时间	状态	顺序	管理
<input type="checkbox"/>	123	无图标		2019-05-24	内页	1	[更改] [删除]

图 22

22. 显示如图界面。如图 23 所示。

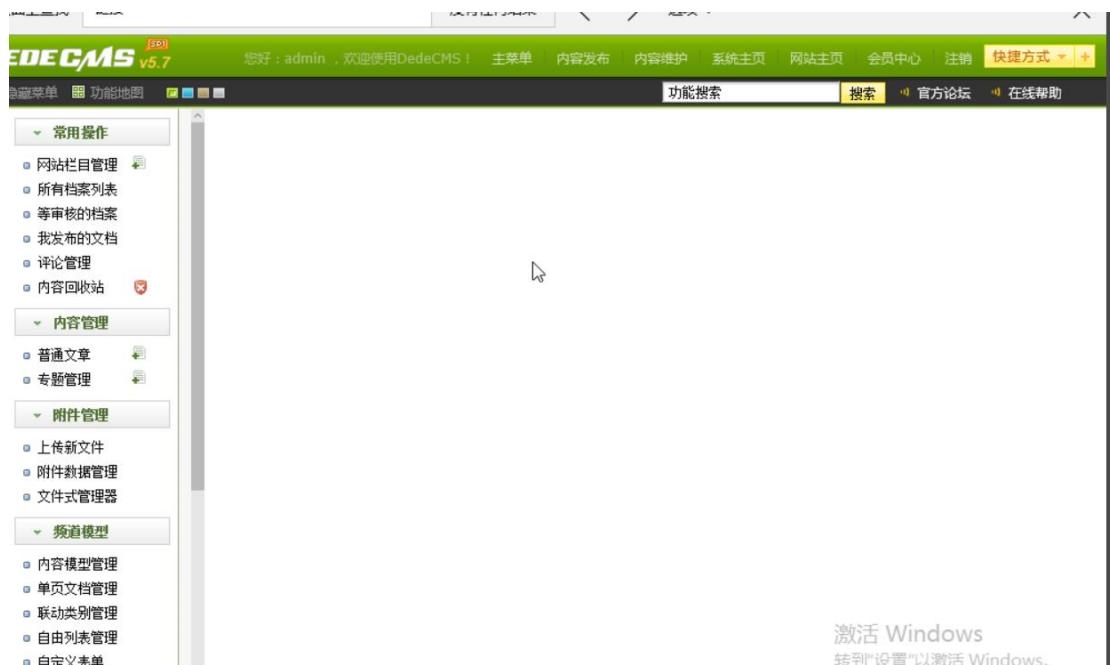


图 23

23. 在网站根目录【dede】文件夹下会下生成一个文件，文件名为【paxmac.php】。如图 24 所示。

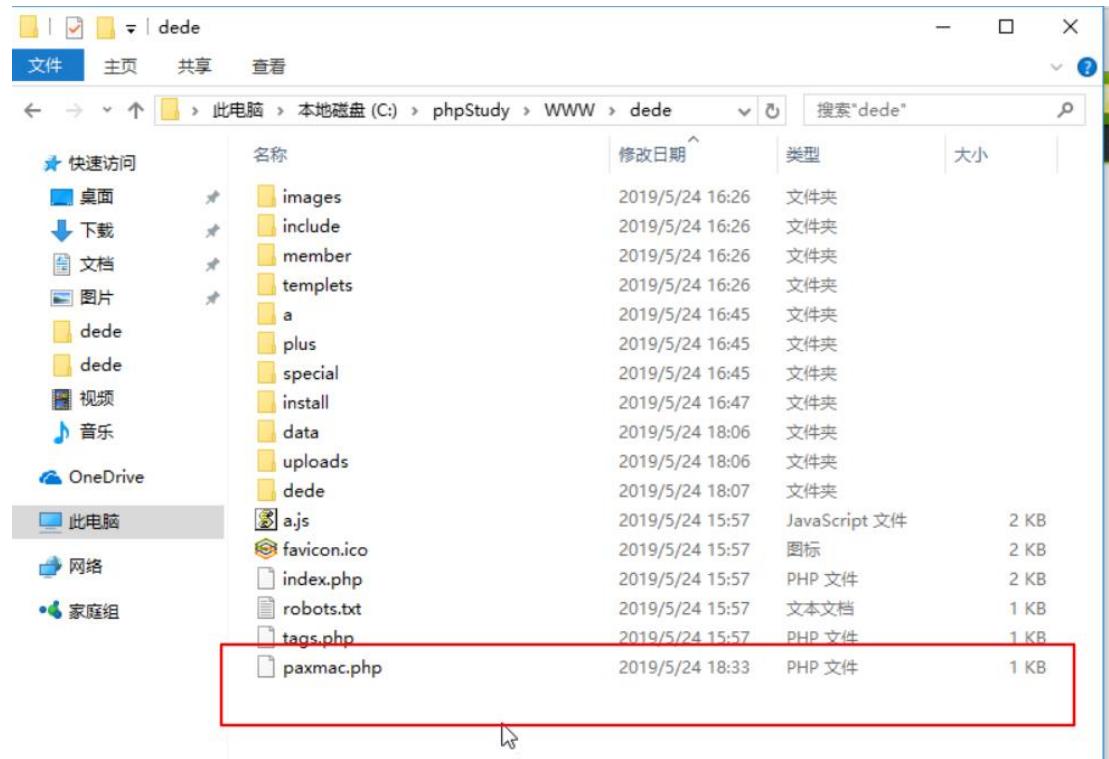


图 24

24. 生成一句话木马网页后，进入【C:\tools\AntSword】，打开【AntSword.exe】。如图 25 所示。

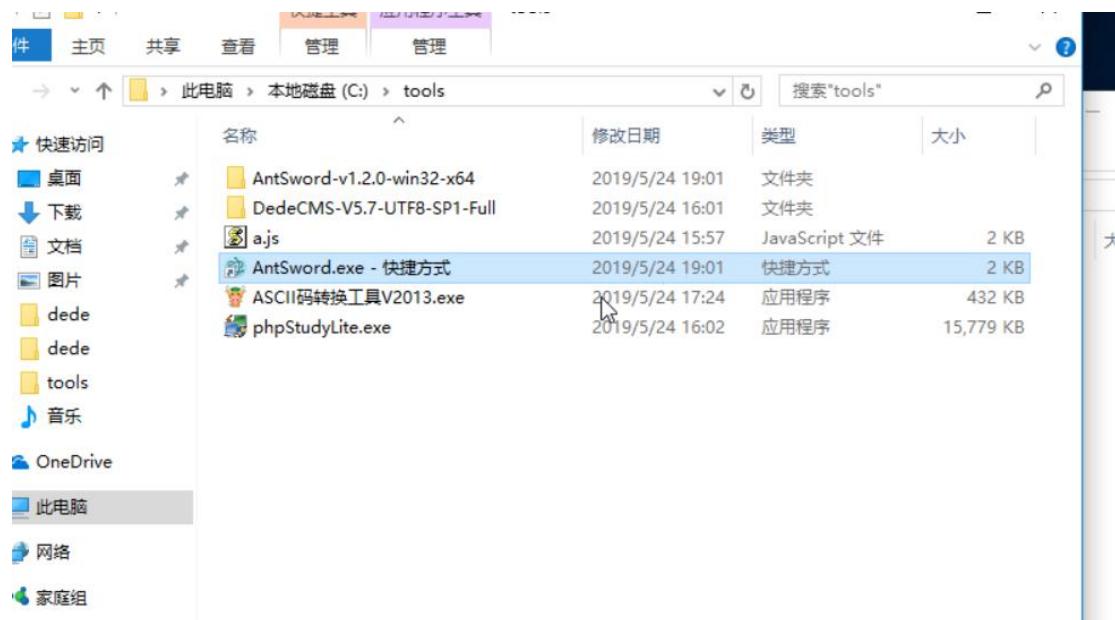


图 25

25. 右键点击【Add】，输入地址【<http://localhost:80/dede/paxmac.php>】连接该网站，连接口令为 cmd，点击【Add】。连接成功，完成对网站文件的渗透。如图 26 所示。

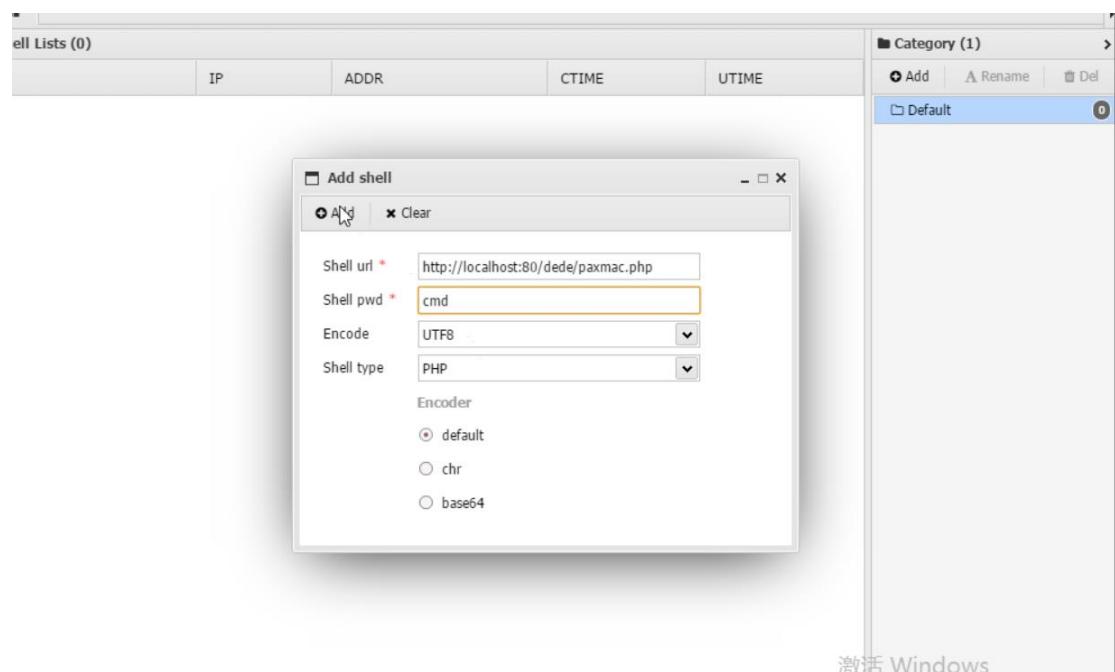


图 26

26. 渗透成功如图 27 所示。



图 27

五【实验思考】

- 思考如何利用了解其他可能存在的 FineCMS 漏洞？