第13章实验报告

1 实验名称

实现本地Web攻击和防御

2 实验原理

攻击者利用网页开发时留下的漏洞,向其中注入恶意代码,使用户加载并执行恶意制造的网页程序。

• XSS: 攻击者将恶意脚本注入到Web页面中,用户访问时恶意脚本被执行,用于窃取用户的敏感信息;

3 实验环境

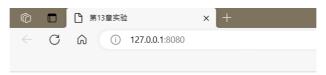
Python3.9.13 , 调用库见附件 requirements.txt

4 实验步骤

4.1 XSS的攻击和防御

利用Flask框架设计网页的代码见文件 ./13/1.py

运行结果如下图



本地 Web 攻击与防御

1. 反射型攻击(查询功能)

查询内容	查询
所有内容如下:	
ABC	
DEF	
HIJ	

2. 持久型攻击(提交功能)

提交内容

4.1.1 反射型攻击

```
1
   query = ""
2
   # 查询
3
   if request.method == "GET":
4
       if request.args.get("submit") == "查询":
5
           query = request.args.get("content").strip()
6
           if query:
7
               sub_dataset = [x for x in dataset if query in x]
8
               return render_template("index.html", query=query, comments=sub_dataset)
```

该程序对用户的输入未进行处理,因此存在XSS漏洞,可对网页进行XSS反射型攻击。

```
查询框输入
```

1 <script>alert("/XSS/")</script>

结果如下

```
127.0.0.1:8080 says
/XSS/
```

4.1.2 持久型攻击

```
1 # 提交
2 elif request.method == "POST":
3 if request.form.get("submit") == "提交":
4 comment = request.form.get("input").strip()
5 if comment:
6 dataset.append(comment) # 模拟将提交写入数据库
```

程序直接将提交内容加入dataset,并未作处理。

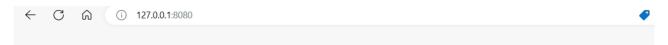
在提交框输入下述代码

1 <script>alert("/XSS/")</script>

结果如下:



当再次提交时,这段恶意代码会被执行,进行了持久型攻击。(下图是动图,请点击此处查看)



本地 Web 攻击与防御

1. 反射型攻击(查询功能)

查询内容	查询
所有内容如下:	
ABC	
DEF	
HIJ	

2. 持久型攻击(提交功能)



4.1.3 XSS攻击的防御

对XSS攻击的防御措施是对用户输入的内容进行处理,修改后的代码如下:

```
query = ""
    # 查询
3
    if request.method == "GET":
4
        if request.args.get("submit") == "查询":
5
            query = request.args.get("content").strip()
6
            # 防御反射型攻击
            query = ''.join(q for q in query if q.isalnum())
8
9
            if query:
10
                sub_dataset = [x for x in dataset if query in x]
11
                return render_template("index.html", query=query, comments=sub_dataset)
12
            # 提交
13
        elif request.method == "POST":
14
            if request.form.get("submit") == "提交":
15
                comment = request.form.get("input").strip()
16
                # 防御持久型攻击
17
                comment = ''.join(c for c in comment if c.isalnum())
18
                if comment:
19
                    dataset.append(comment) # 模拟将提交写入数据库
20
21
                    return render_template("index.html", query=query, comments=dataset)
```

其中第7行和第17行的目的是只保留输入中字母和数字, 删去特殊字符

再次进行反射型攻击和持久型攻击失败:

本地 Web 攻击与防御

1. 反射型攻击(查询功能)

查询内容 **查询**

查询 scriptalertXSSscript 结果如下:

2. 持久型攻击(提交功能)

提交内容

1. 反射型攻击(查询功能)

本地 Web 攻击与防御

查询内容 **查询**

所有内容如下:

ABC DEF

HIJ

scriptalertXSSscript

2. 持久型攻击(提交功能)

提交内容 提交