

北京邮电大学

网络空间安全学院



测试及结果展示报告

项目：基于源代码检测和动态执行的二阶 SQL 注入漏洞检测

组员：王硕、彭致远、李懿飞、王晨旭

2020 年 12 月 10 日

目录

1 引言	3
1.1 目的	3
1.2 背景及范围	3
1.3 定义、术语和缩写	3
2 测试概述	4
2.1 测试环境与配置	4
2.2 测试内容	4
2.2.1 PHP 和 SQL 解析树	4
2.2.2 CFG 的正确生成	4
2.2.3 扫描结果验证	5
3 运行结果与分析	5
3.1 PHP 和 SQL 解析树	5
3.2 CFG 的正确生成	7
3.3 扫描结果验证	10
4 结论	15

1 引言

1.1 目的

本测试报告为大三上学期网络分析实践课程的“基于源代码检测和动态执行的二阶 SQL 注入漏洞检测工具”的测试报告，目的在于测试工具的基本功能并分析测试结果，判断系统是否符合需求。

1.2 背景及范围

- 项目名称：基于源代码检测和动态执行的二阶 SQL 注入漏洞检测工具
- 项目成员：北京邮电大学网络空间安全学院“网络安全分析实践”课程开发小组
 - ◆ 王硕（组长）：2018213641
 - ◆ 彭致远：2018213646
 - ◆ 李懿飞：2018213632
 - ◆ 王晨旭：2018213636
- 系统范围：具有 PHP7.4 环境的 Windows 系统计算机
- 用户：无限制
- 实现项目的计算机网络：校园网

本测试报告预期参考人员包括测试工具的同学、开发工具的同学、验收工具的老师。

1.3 定义、术语和缩写

序号	术语或缩写	解释
1	SQL	结构化查询语言(Structured Query Language)简称 SQL，是一种特殊目的的编程语言，是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统。
2	AST	抽象语法树（Abstract Syntax Tree，AST），是源代码语法结构的一种抽象表示。它以树状的形式表现编程语言的语法结构，树上的每个节点都表示源代码中的一种结构。
3	CFG	控制流程图，是一个过程或程序的抽象表现，是用在编译器中的一个抽象数据结构，由编译器在内部维护，代表了一个程序执行过程中会遍历到的所有路径。它用图的形式表示一个过程内所有基本块执行的可能流向，也能反映一个过程的

		实时执行过程。本项目用于描述变量在流动过程的执行过程
4	PHP-Parser	开源工具，用于生成 PHP 文件的语法分析树
5	SQL-Parser	开源工具，用于生成 SQL 语句的语法分析树

2 测试概述

2.1 测试环境与配置

- 操作系统：Windows 10
- PHP 环境：PHP7.4，有 x-debug 调试测试工具
- 运行软件：PhpStorm 2020.2.3
- 虚拟机：kali linux 2020
- 待扫描的项目：一个自己搭建的 demo 网站、三个从 github 网站下载的 PHP Web 项目（两个具有二阶 SQL 注入漏洞、一个没有）

2.2 测试内容

2.2.1 PHP 和 SQL 解析树

序号	功能	要求
1	PHP AST 的生成	对特定 PHP 文件，对比是否能完全分析 PHP 文件并生成对应语法分析树
2	SQL AST 的生成	是否能扫描出所有 SQL 语句，并均能生成对应的语法分析树

2.2.2 CFG 的正确生成

序号	功能	要求
1	PHP 内变量的流动	查找出所有的变量、并准确的分析变量的来源、去向和变化
2	SQL 内变量的流动	定位数据库的表格和表项；并查找出所有的变量、并准确的分析变量的来源、去向和变化

2.2.3 扫描结果验证

序号	功能	要求
1	检测出网站内潜在的二阶 SQL 注入漏洞	对存在二阶 SQL 注入漏洞的网站能准确定位到二阶 SQL 注入漏洞更多注入点与触发点，对于不存在二阶 SQL 注入漏洞的网站，报告安全。
2	安全检查	用户输入命令不合法，会有回显，不报错； 用户文件项目不存在，提示用户

3 运行结果与分析

3.1 PHP 和 SQL 解析树

(1) PHP 文件的 AST，测试用例为 demo 项目内的 change.php 文件，源码和生成的 AST 如下：（由于语法分析树很大，故截图只截了一部分，详细的输出保存在文件夹：/输入项目/demo/parser 文件夹内对应的语法分析树）

```
01. <?php
02. session_start();
03. $username = $_SESSION["username"];
04. echo $username;
05. echo '<form method="post">
06.     原来的密码<input type="password" name="old_password" required="required">
07.     修改后的密码<input type="password" name="new_password" required="required">
08.     <input type="submit" name="change" value="修改">
09. </form>';
10.
11.
12. if(isset($_POST['change'])){
13.     // 创建连接
14.     $conn = new mysqli("10.122.241.50", "root", "123456", "sql_test");
15.
16.     // 检测连接
17.     if ($conn->connect_error) {
18.         die("数据库连接失败: " . $conn->connect_error);
19.     }
20.
21.     $old_pass = $_POST["old_password"];
22.     $new_pass = $_POST["new_password"];
23.
24.     $old_password = mysqli_real_escape_string($conn, $old_pass);
25.     $new_password = mysqli_real_escape_string($conn, $new_pass);
26.
27.     $sql = "select distinct *
28.         from user
29.         where username = '$username' and password = '$old_password'";
30.     $result = $conn->query($sql);
31.
32.     if ($result->num_rows > 0) {
33.         mysqli_query($conn,"UPDATE user SET password='$new_password'
34.             WHERE username = '$username'");
35.         echo "<script>alert('修改成功')</script>";
36.         session_destroy();
37.         echo "<script>window.location.href='index.html';</script>";
38.     } else {
39.         echo "<script>alert('原密码错误')</script>";
40.     }
41.     $conn->close();
42. }
43. ?>
```

```

Scan Files:
change.php
register.php
submit.php
array(
  0: Stmt_Expression(
    expr: Expr_FuncCall(
      name: Name(
        parts: array(
          0: session_start
        )
      )
      args: array(
      )
    )
  )
  1: Stmt_Expression(
    expr: Expr_Assign(
      var: Expr_Variable(
        name: username
      )
      expr: Expr_ArrayDimFetch(
        var: Expr_Variable(
          name: _SESSION
        )
        dim: Scalar_String(
          value: username
        )
      )
    )
  )
  2: Stmt_Echo(
    exprs: array(
      0: Expr_Variable(

```

(2) SQL 语句的 AST, 输出如下:

```

SELECT DISTINCT * FROM user WHERE username = 'username'

object(PhpMyAdmin\SqlParser\Statements\SelectStatement)#1284 (17) {
  ["expr"]=>
  array(1) {
    [0]=>
    object(PhpMyAdmin\SqlParser\Components\Expression)#1286 (7) {
      ["database"]=>
      NULL
      ["table"]=>
      NULL
      ["column"]=>
      NULL
      ["expr"]=>
      string(1) "*"
      ["alias"]=>
      NULL
      ["function"]=>
      NULL
      ["subquery"]=>
      NULL
    }
  }
}

```

```

["from"]=>
array(1) {
  [0]=>
  object(PhpMyAdmin\SqlParser\Components\Expression)#1287 (7) {
    ["database"]=>
    NULL
    ["table"]=>
    NULL
    ["column"]=>
    NULL
    ["expr"]=>
    string(4) "user"
    ["alias"]=>
    NULL
    ["function"]=>
    NULL
    ["subquery"]=>
    NULL
  }
}

```

```

["where"]=>
array(1) {
  [0]=>
  object(PhpMyAdmin\SqlParser\Components\Condition)#1288 (3) {
    ["identifiers"]=>
    array(1) {
      [0]=>
      string(8) "username"
    }
    ["isOperator"]=>
    bool(false)
    ["expr"]=>
    string(21) "username = 'username'"
  }
}

```

3.2 CFG 的正确生成

- 1、测试 demo 项目，生成的 CFG 的每个结点的信息打印如下：

```
    请将php项目放入桌面
请输入项目名称: demo

正在进行扫描项目demo...

Scan Files:
change.php
register.php
submit.php

Variable Count:
29

[cmd]
[1]输出扫描结果
[2]输出变量流
[3]退出系统
2

Variable Info:
29
0: username change.php db(user(username)) [1, ] db(user(username)) [] 0
1: _SESSION change.php db [] db(user(username)) [0, ] 0
2: _POST change.php web [] db(user(password)) [4, 5, ] 0
3: conn change.php php [] db(user(password)) [6, 7, 9, ] 0
4: old_pass change.php web_form(old_password) [2, ] db(user(password)) [6, ] 0
5: new_pass change.php web_form(new_password) [2, ] [7, ] 0
6: old_password change.php web_form(old_password) [3, 4, ] db(user(password)) [] 0
7: new_password change.php web_form(new_password) [3, 5, ] [] 0
8: sql change.php php [] [9, ] 0
9: result change.php [3, 8, ] [] 0
10: conn register.php php [] db(user(username)) [14, 15, 17, ] 0
11: name register.php web_form(username) [12, ] db(user(username)) [14, ] 0
12: _POST register.php web [] db(user(username)) [11, 13, ] 0
13: pass register.php web_form(password) [12, ] [15, ] 0
14: username register.php web_form(username) [10, 11, ] db(user(username)) [] 0
15: password register.php web_form(password) [10, 13, ] [] 0
16: sql register.php php [] [17, ] 0
17: result register.php [10, 16, ] [] 0
18: sql1 register.php php [] [] 0
19: conn submit.php php [] [26, ] 0
20: _POST submit.php web [] [21, 22, ] 0
21: name submit.php web_form(username) [20, ] [] 0
22: pass submit.php web_form(password) [20, ] [] 0
23: username submit.php [] db(user(username)) [] 0
24: password submit.php [] db(user(password)) [] 0
25: sql submit.php php [] [26, ] 0
26: result submit.php [19, 25, ] [27, ] 0
27: row submit.php php [26, ] [28, ] 0
28: _SESSION submit.php php [27, ] [] 0
```

通过简单的分析，可以看出此 CFG 是合法的。

2、测试 github 项目 netdisk，一个简单的网盘系统，生成的 CFG 的每个节点的信息打印如下：

请将php项目放入桌面
请输入项目名称: netdisk

正在进行扫描项目netdisk...

Scan Files:

GetPwd.php
classTable.php
conn.php
download.php
fTable.php
fileIndex.php
forgetPwd.php
index.php
login_confirm.php
register.php
register_user.php
sTable.php
search.php
upload.php

Variable Count:

142

[cmd]

[1]输出扫描结果

[2]输出变量流

[3]退出系统

2

Variable Info:

142

0: conn GetPwd.php php [] [4,] 0
1: uName GetPwd.php web_form(uName) [2,] db(user(uname)) [] 0
2: _GET GetPwd.php web [] db(user(uname)) [1,] 0
3: sql GetPwd.php php [] [4,] 0
4: result GetPwd.php [0, 3,] [5,] 0
5: rows GetPwd.php [4,] [] 0
6: newUrl GetPwd.php [] [] 0
7: conn classTable.php php [] db(file(uid)) [11, 16,] 0
8: uName classTable.php [] db(user(uname)) [] 0
9: _GET classTable.php web [] db(file(ftype)) [14,] 0
10: sql3 classTable.php php [] db(file(uid)) [11,] 0
11: result3 classTable.php [7, 10,] db(file(uid)) [12,] 0
12: rows3 classTable.php [11,] db(file(uid)) [13,] 0
13: uId classTable.php [12,] db(file(uid)) [] 0
14: fType classTable.php web_form(ftype) [9,] db(file(ftype)) [] 0
15: sql4 classTable.php php [] [16,] 0
16: result4 classTable.php [7, 15,] [] 0
17: set classTable.php [] [] 0
18: dbhost conn.php [] [] 0
19: dbport conn.php [] [] 0
20: dbuser conn.php [] [] 0

.....

121: myFileError upload.php web_file(error) [120,] [123,] 0
122: myTmpFile upload.php web_file(tmp_name) [120,] [] 0
123: notError upload.php web_file(name) [119, 121,] [] 0
124: fileName upload.php [] [] 0
125: fileError upload.php [] [] 0
126: errorMsg upload.php [] [] 0
127: tmpName upload.php [] [] 0
128: dirName upload.php [] [] 0
129: secondDirName upload.php [] [] 0
130: _POST upload.php web [] db(file(uid)) [133,] 0
131: thirdDirName upload.php [] [] 0
132: uploadedFilePath upload.php [] [] 0
133: uId upload.php web_form(uId) [130,] db(file(uid)) [] 0
134: fName upload.php web_file(name) [120,] db(file(fname)) [] 0
135: fType upload.php web_file(type) [120,] db(file(ftype)) [] 0
136: fSize upload.php php [] db(file(fsize)) [] 0
137: fTime upload.php php [] db(file(ftime)) [] 0
138: fPath upload.php [] db(file(fpath)) [] 0
139: conn upload.php php [] [] 0
140: sql upload.php php [] [] 0

3、测试 github 项目 shopping，输出如下：

只截取了部分结点信息：

```
Variable Count:
363
...

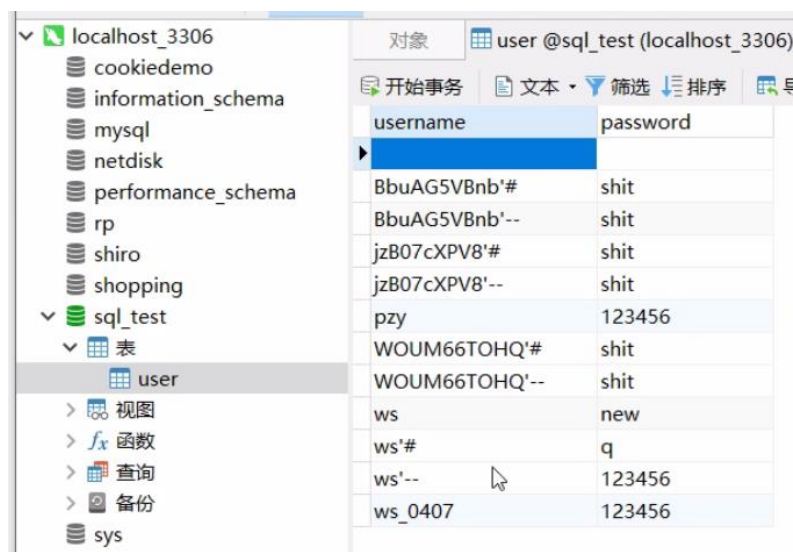
170: link database.php php [] [] 0
171: cn1 forget_ok.php web_form(username3) [172, ] db(customer(c_name)) [] 0
172: _POST forget_ok.php web [] [171, 174, 175, 176, ] 0
173: _SESSION forget_ok.php db [] [] 0
174: tp1 forget_ok.php web_form(telphone2) [172, ] db(customer(c_phone)) [] 0
175: q1 forget_ok.php web_form(question2) [172, ] db(customer(c_question)) [] 0
176: a1 forget_ok.php web_form(answer2) [172, ] db(customer(c_answer)) [] 0
177: sql forget_ok.php php [] [179, ] 0
178: link forget_ok.php php [] [179, ] 0
179: rs forget_ok.php [178, 177, ] [] 0
180: n head2.php db(user(n)) [20, ] db(customer(c_name)) [] 0
181: sql head2.php php [] [183, ] 0
182: link head2.php php [] [183, ] 0
183: rs head2.php [182, 181, ] [] 0
184: result head2.php [] [] 0
185: _SESSION index.php db [] [] 0
186: link index.php php [] [188, ] 0
187: sql index.php [] [188, ] 0
188: rs index.php [186, 187, ] [] 0
189: result index.php [] [] 0
190: n login_ok.php web_form(username) [191, ] db(customer(c_name)) [] 0
191: _POST login_ok.php web [] [190, 192, ] 0
192: p login_ok.php web_form(password) [191, ] db(customer(c_pass)) [] 0
193: sql login_ok.php php [] [195, ] 0
194: link login_ok.php php [] [195, ] 0
195: rs login_ok.php [194, 193, ] [196, ] 0
196: r login_ok.php [195, ] [197, ] 0
197: _SESSION login_ok.php db [196, ] [] 0
198: _SESSION loginout.php db [] [] 0
199: i look.php web_form(id) [200, 200, ] db(product(p_id)) [] 0
...

```

3.3 扫描结果验证

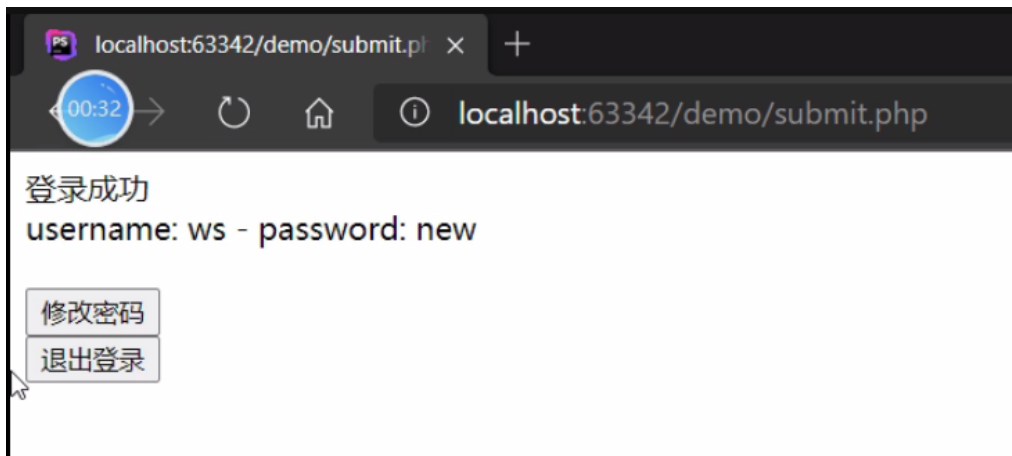
1、demo 项目

(1) 数据库内容：



username	password
BbuAG5VBnb'#	shit
BbuAG5VBnb'--	shit
jzB07cXPV8'#	shit
jzB07cXPV8'--	shit
pzy	123456
WOUM66TOHQ'#	shit
WOUM66TOHQ'--	shit
ws	new
ws'#	q
ws'--	123456
ws_0407	123456

(2) 网站运行效果：



(3) 含有一个登陆-注册-修改密码的二阶 SQL 注入漏洞，检测结果如下：

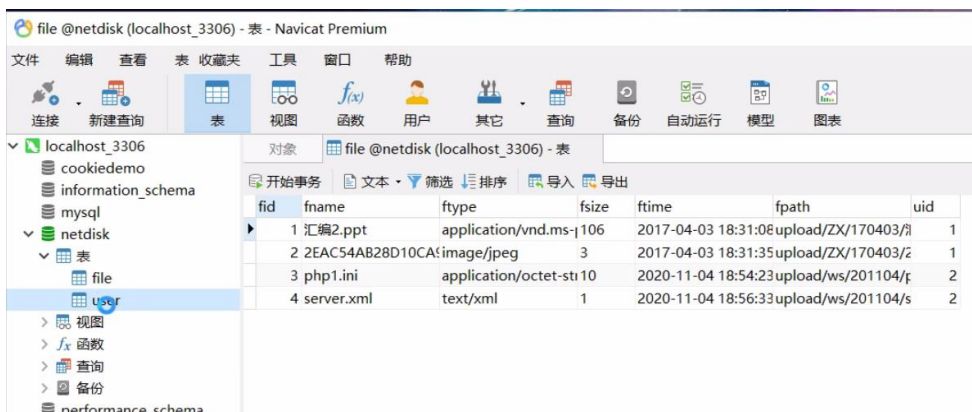
```
[cmd]
[1]输出扫描结果
[2]输出变量流
[3]退出系统

1 result(s) found
register.php -> web_form(username) -> change.php -> db(user(username))
```

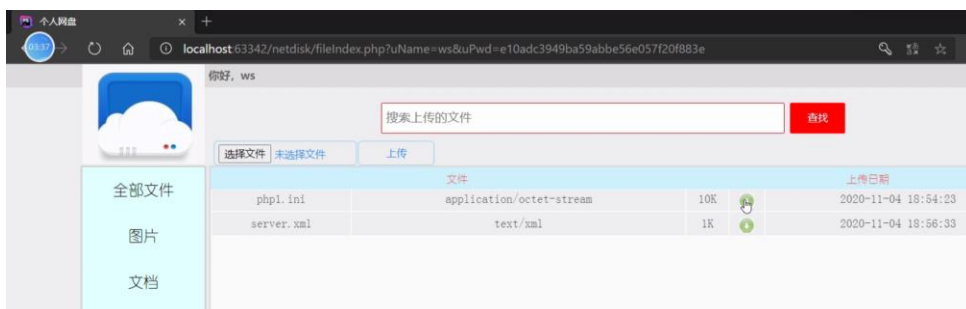
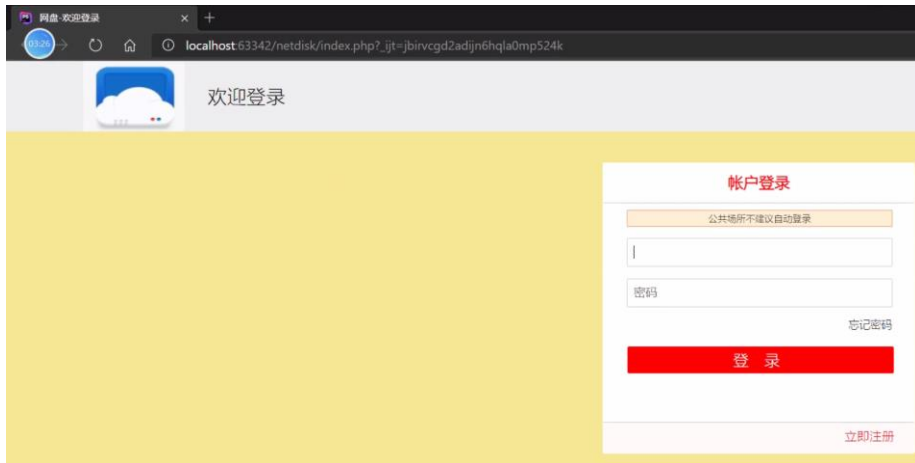
可以得知注入点在 register.php 界面，触发点在 change.php 界面，来自用户的输入，最终存到数据库内，又被拿出来执行。故存在二阶 SQL 注入漏洞。

2、netdisk 项目

(1) 数据库信息：



(2) 网站运行效果：



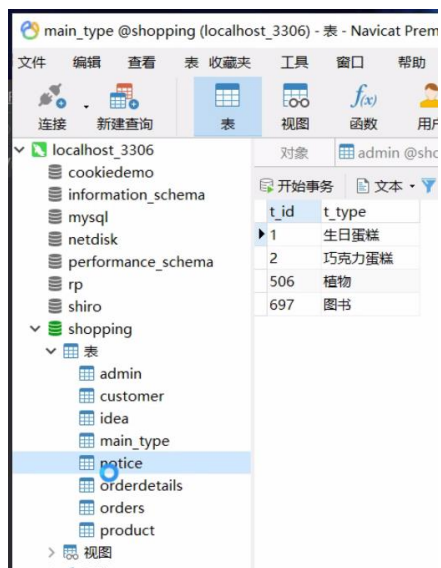
(3) 网站含有一个二阶的文件 SQL 注入漏洞，文件名作为用户的上传的文件，直接被后端读取存到数据库内，又重新在下载界面获取到下载的文件的文件名，到后端查找文件的存储地址，故存在二阶 SQL 注入漏洞。

```
[cmd]
[1]输出扫描结果
[2]输出变量流
[3]退出系统
j

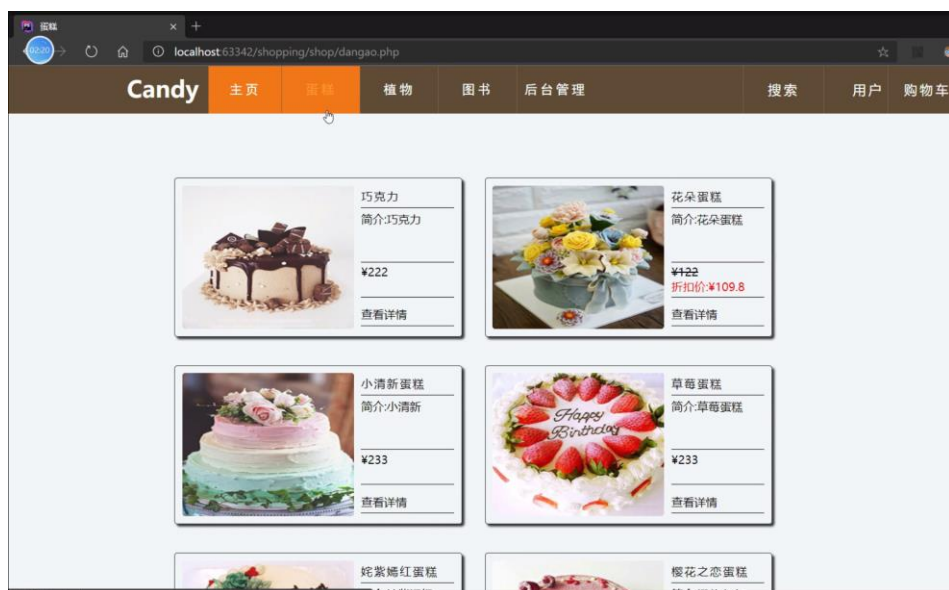
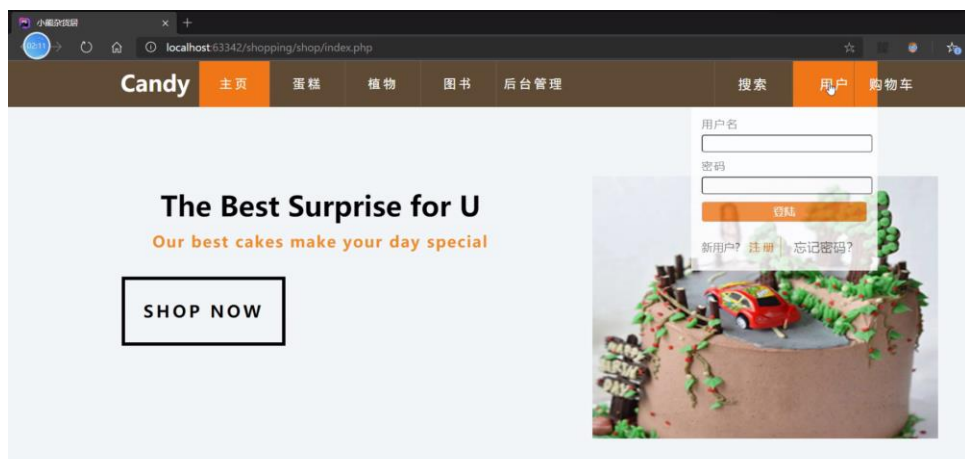
3 result(s) found
sTable.php -> web_form(fName) -> download.php -> db(file(fname))
search.php -> web_form(fName) -> download.php -> db(file(fname))
upload.php -> web_file(name) -> download.php -> db(file(fname))
```

3、shopping 项目

(1) 数据库信息：



(2) 网站运行效果:



(3) 由于网站只是一个简单的加购物车，没有涉及到数据库内的操作，所以 0 result，结果正确：

```
[cmd]
[1]输出扫描结果
[2]输出变量流
[3]退出系统
1
0 result(s) found
```

4、最后测试项目的安全性

(1) 错误的命令输入：

```
[cmd]
[1]输出扫描结果
[2]输出变量流
[3]退出系统
4
[cmd]
[1]输出扫描结果
[2]输出变量流
[3]退出系统
5
[cmd]
[1]输出扫描结果
[2]输出变量流
[3]退出系统
3
欢迎下次使用，bye-bye!
Process finished with exit code 0
```

(2) 没有项目文件：

```
请将php项目放入桌面
请输入项目名称： bad_location
项目文件不存在，请重新输入???
项目文件不存在，请重新输入netdisk

正在进行扫描项目netdisk...

Scan Files:
GetPwd.php
```

4 结论

- 1、项目功能达到要求, 对于提供的项目文件能够准确的扫描出存在的二阶 SQL 注入漏洞。
- 2、能够定位到二阶 SQL 注入漏洞的注入点和触发点, 提醒项目管理者注入防范。
- 3、项目运行良好, 不会出现报错, 用户友好性程度高。