上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

PHP-WEB漏洞挖掘
测试文档

小组成员：金子本、王新忠、洪逸杰、张泽挥、杨景犀、钟一鸣

项目名称：PHP-WEB漏洞挖掘

指导老师：黄征

日期：2022年5月27日

目录

第一章 前端设计

前端的测试工作分为两部分：前端页面的测试工作以及与后端页面交互的测试工作。

前端页面的测试工作通过vscode中自带的html预览插件结合浏览器预览完成。测试工作随页面开发工作同步进行，对html、CSS的修改都可以在vscode的预览插件或浏览器中见到测试效果。因为预览的方便性，前端可以一边开发一边测试以达到满意的效果。

最开始的时候只是完成了一个大致的文件上传页面。基本可以实现需要的功能，如文件上传，输入代码的上传等。但文件上传框，代码输入框的分布，各种按钮的布局都比较混乱。这一时期主要进行的是与后端交互的测试。

与后端的交互效果的测试过程通过JavaScript语言中的console命令进行。Console命令可以在浏览器的控制台页面输出用户指定输出的内容，我们可以通过这一功能输出变量的值，变量的类型来判断特定操作是否完成。在这一功能的开发过程中，我们还与后端开发同学积极沟通协作，通过共享屏幕的方式完成协作编程，调试bug.这使我们很有效率地解决问题与困难。

在完成与后端的交互后，我们重新对页面的布局进行了设计，并添加了一个海报页面。此时的优化主要是对css文件进行修改。因为能够看到预览，测试时可以及时看到修改后的效果，所以进行起来较为顺利。

第二章 后端设计

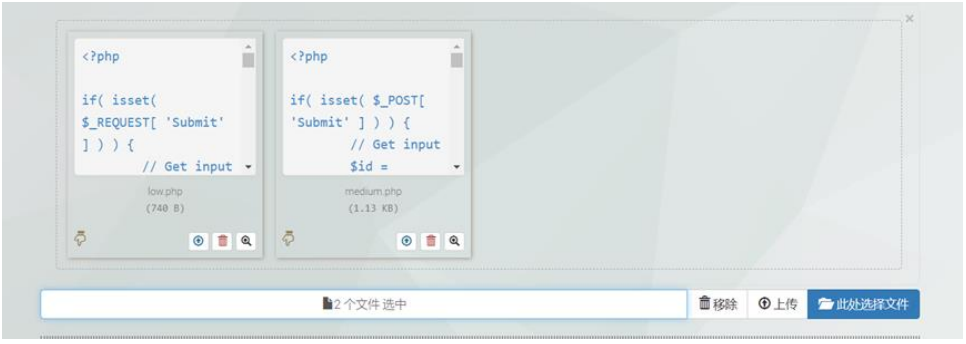
2.1 测试思路

因为后端的进度比前端稍慢，所以我们后端的代码完成时前端的功能也已完成，所以后端的测试直接利用前端做好的页面进行测试。我们首先分别测试三个函数的功能，分别为上传文件的功能，输入代码的功能，检测的功能。这三个功能测试好了之后我们测试了整个网页的功能，确保从上传文件以及输入代码后后端能够正确的检测出结果并返回。

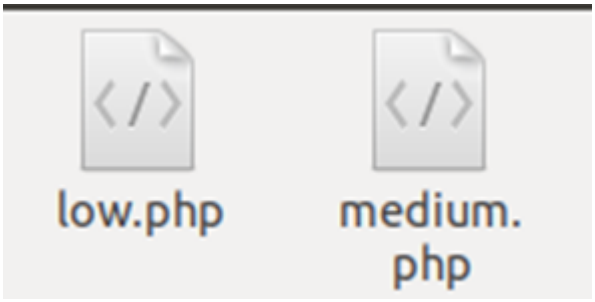
2.2 函数功能测试

2.2.1 上传文件功能测试

我们在前端选择文件并上传，上传后在后端的目录中去寻找文件是否已经进行存储，文件的内容和拓展名是否仍保持一致：



前端选择的文件



后端接受的文件

经测试，上传文件函数功能正常。

2.2.2 输入代码功能测试

我们在前端输入代码并上传，在后端目录中打开default.php文件查看文件中的内容与用户输入的代码是否相同：

用户输入的代码

default.php

经比较，二者内容一致，输入代码并上传函数功能正常

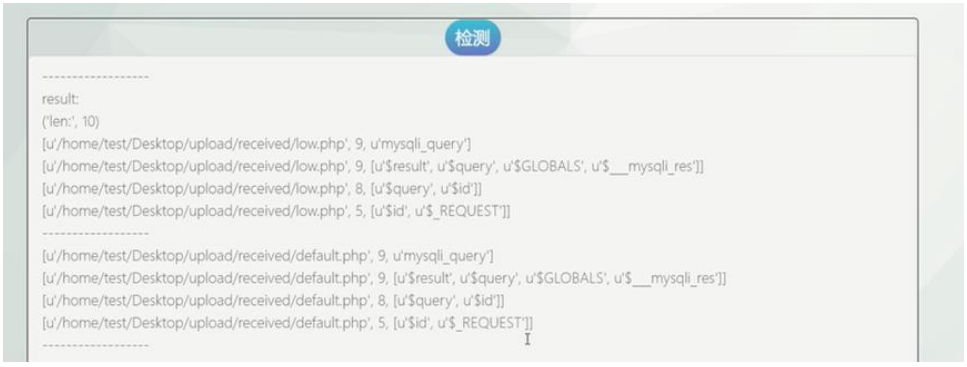
2.2.3 检测函数功能测试

前端点击检测后，后端调用脚本并返回结果。我们通过观看前端的页面文本框中是否显示结果即可检测该函数是否功能正常：

经检测，检测函数功能正常

2.3 整体功能测试

我们上传了文件并检测得到了一个结果，我们同时将这些文件直接输入到我们的漏洞检测系统中也得到了一个结果：



网页显示的结果

```
result:
('len:', 10)
[u'/home/test/Desktop/upload/received/low.php', 9, u'mysqli_query']
[u'/home/test/Desktop/upload/received/low.php', 9, [u'$result', u'$query', u'$GLOBALS', u'$___mysqli_res']]
[u'/home/test/Desktop/upload/received/low.php', 8, [u'$query', u'$id']]
[u'/home/test/Desktop/upload/received/low.php', 5, [u'$id', u'$_REQUEST']]
------------------
[u'/home/test/Desktop/upload/received/default.php', 9, u'mysqli_query']
[u'/home/test/Desktop/upload/received/default.php', 9, [u'$result', u'$query', u'$GLOBALS', u'$___mysqli_res']]
[u'/home/test/Desktop/upload/received/default.php', 8, [u'$query', u'$id']]
[u'/home/test/Desktop/upload/received/default.php', 5, [u'$id', u'$_REQUEST']]
------------------
```

漏洞检测系统检测的结果

经过比较，二者之间完全一致，我们的网站实现了上传文件或者输入代码并获得检测的结果并显示的功能，网站的预期功能基本实现。

第三章 图卷积神经网络

在卷积神经网络判别漏洞文件的测试过程中，我们使用了90个已知类型的漏洞，在这些漏洞中总体上识别出了82个漏洞，识别的准确率是0.91。从每个漏洞的角度来看对于SQLI、XSS漏洞的识别都十分有效，分别达到了0.933和1.000，但是对于OSCI（系统命令执行漏洞）的识别准确率只有0.200，从结果中可以看到在识别OSCI漏洞的过程中，将其中的6个漏洞识别为SQLI漏洞，18个漏洞识别为XSS漏洞。这说明我们的神经网络对于OSCI的学习是存在一定问题的，需要后续的改进分析，并且需要排查对于XSS漏洞的特征分析是否存在过拟合的情况。

	漏洞个数	识别出的漏洞个数	识别准确率
OSCI	30	6	0.200
XSS	30	30	1.000
SQLI	30	28	0.933
总体	90	82	0.911

```
(dt) PS C:\Users\Shen\Desktop\GNN> python run_model.py
Found Vuln:
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-email_filter__cat-concatenation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-email_filter__cat-interpretation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-email_filter__cat-sprintf_%s_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-email_filter__ls-concatenation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-email_filter__ls-interpretation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-email_filter__ls-sprintf_%s_simple_quote.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-full_special_chars_filter__cat-concatenation_simple_quote.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-full_special_chars_filter__cat-interpretation_simple_quote.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-full_special_chars_filter__cat-sprintf_%s_simple_quote.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-full_special_chars_filter__ls-concatenation_simple_quote.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-full_special_chars_filter__ls-interpretation_simple_quote.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-full_special_chars_filter__ls-sprintf_%s_simple_quote.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-special_chars_filter__cat-concatenation_simple_quote.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-special_chars_filter__cat-interpretation_simple_quote.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-special_chars_filter__cat-sprintf_%s_simple_quote.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-special_chars_filter__ls-concatenation_simple_quote.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-special_chars_filter__ls-interpretation_simple_quote.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-CLEANING-special_chars_filter__ls-sprintf_%s_simple_quote.php
CI  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-VALIDATION-email_filter__cat-concatenation_simple_quote.php
CI  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-VALIDATION-email_filter__cat-interpretation_simple_quote.php
CI  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-VALIDATION-email_filter__cat-sprintf_%s_simple_quote.php
CI  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-VALIDATION-email_filter__ls-concatenation_simple_quote.php
CI  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-VALIDATION-email_filter__ls-interpretation_simple_quote.php
CI  in    C:/Users/Shen/Desktop/GNN/test\CWE_78__array-GET__func_FILTER-VALIDATION-email_filter__ls-sprintf_%s_simple_quote.php
```

```
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_79__array-GET__func_FILTER-CLEANING-email_filter__Use_untrusted_data_propertyValue_CSS-span_Style_Property_Value.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_79__array-GET__func_FILTER-CLEANING-email_filter__Use_untrusted_data_script-quoted_Event_Handler.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_79__array-GET__func_FILTER-CLEANING-email_filter__Use_untrusted_data_script-quoted_String.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_79__array-GET__func_FILTER-CLEANING-email_filter__Use_untrusted_data_script-side_Quoted_Expr.php
XSS  in    C:/Users/Shen/Desktop/GNN/test\CWE_79__array-GET__func_FILTER-CLEANING-email_filter__Use_untrusted_data_script-window_SetInterval.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-email_filter__join-concatenation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-email_filter__join-interpretation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-email_filter__join-sprintf_%s_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-email_filter__select_from-concatenation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-email_filter__select_from-interpretation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-email_filter__select_from-sprintf_%s_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-full_special_chars_filter__join-concatenation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-full_special_chars_filter__join-interpretation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-full_special_chars_filter__join-sprintf_%s_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-full_special_chars_filter__select_from-concatenation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-full_special_chars_filter__select_from-interpretation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-full_special_chars_filter__select_from-sprintf_%s_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-special_chars_filter__join-concatenation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-special_chars_filter__join-interpretation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-special_chars_filter__join-sprintf_%s_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-special_chars_filter__select_from-concatenation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-special_chars_filter__select_from-interpretation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-CLEANING-special_chars_filter__select_from-sprintf_%s_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-VALIDATION-email_filter__join-concatenation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-VALIDATION-email_filter__join-interpretation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-VALIDATION-email_filter__join-sprintf_%s_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-VALIDATION-email_filter__select_from-concatenation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-VALIDATION-email_filter__select_from-interpretation_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_FILTER-VALIDATION-email_filter__select_from-sprintf_%s_simple_quote.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_mysql_real_escape_string__multiple_select-concatenation.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_mysql_real_escape_string__multiple_select-interpretation.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_mysql_real_escape_string__select_from_where-concatenation.php
SQLi  in    C:/Users/Shen/Desktop/GNN/test\CWE_89__array-GET__func_mysql_real_escape_string__select_from_where-interpretation.php

Total predicted as vulnerable:  82
Total functions:  90

Predicted distribution:
Safe    8
dtype: int64
```

第四章 静态代码分析

在静态代码分析的测试阶段，因为传入的文件为神经网络认为存在的漏洞文件，所以在测试过程中，我们并未选用很大量的数据，只是选择了一些典型文件，来分析是否能够完整地查找出源节点到污点节点的路径。在下图的结果文件中，我们可以分析最常见的SQLI漏洞。从漏洞的原始文件可以看出源节点为$id = $_REQUEST['id']，污点节点为$result = mysqli_query()函数，可以从结果中看出静态分析过程中，首先定位到了污点函数，然后通过后向遍历的方法定位到了$query，再到$id，此时到达源节点，一条完整的路径输出。

```
result:
('len:', 20)
[u'../php_src/dvwa/vulnerabilities/sqli_blind/source/low.php', 9, u'mysqli_query']
[u'../php_src/dvwa/vulnerabilities/sqli_blind/source/low.php', 9, [u'$result', u'$getid', u'$GLOBALS']]
[u'../php_src/dvwa/vulnerabilities/sqli_blind/source/low.php', 8, [u'$getid', u'$id']]
[u'../php_src/dvwa/vulnerabilities/sqli_blind/source/low.php', 5, [u'$id', u'$_GET']]
------------------
[u'../php_src/dvwa/vulnerabilities/sqli_blind/source/high.php', 9, u'mysqli_query']
[u'../php_src/dvwa/vulnerabilities/sqli_blind/source/high.php', 9, [u'$result', u'$getid', u'$GLOBALS']]
[u'../php_src/dvwa/vulnerabilities/sqli_blind/source/high.php', 8, [u'$getid', u'$id']]
[u'../php_src/dvwa/vulnerabilities/sqli_blind/source/high.php', 5, [u'$id', u'$_COOKIE']]
------------------
[u'../php_src/dvwa/vulnerabilities/sqli/source/low.php', 9, u'mysqli_query']
[u'../php_src/dvwa/vulnerabilities/sqli/source/low.php', 9, [u'$result', u'$query', u'$GLOBALS', u'$___mysqli_res']]
[u'../php_src/dvwa/vulnerabilities/sqli/source/low.php', 8, [u'$query', u'$id']]
[u'../php_src/dvwa/vulnerabilities/sqli/source/low.php', 5, [u'$id', u'$_REQUEST']]
------------------
[u'../php_src/dvwa/vulnerabilities/brute/source/low.php', 13, u'mysqli_query']
[u'../php_src/dvwa/vulnerabilities/brute/source/low.php', 13, [u'$result', u'$query', u'$GLOBALS', u'$___mysqli_res']]
[u'../php_src/dvwa/vulnerabilities/brute/source/low.php', 12, [u'$query', u'$pass', u'$user']]
[u'../php_src/dvwa/vulnerabilities/brute/source/low.php', 5, [u'$user', u'$_GET']]
------------------
```

```php
<?php

if( isset( $_REQUEST[ 'Submit' ] ) ) {
    // Get input
    $id = $_REQUEST[ 'id' ];

    // Check database
    $query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) : (

    // Get results
    while( $row = mysqli_fetch_assoc( $result ) ) {
        // Get values
        $first = $row["first_name"];
        $last  = $row["last_name"];

        // Feedback for end user
        $html .= "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }

    mysqli_close($GLOBALS["___mysqli_ston"]);
}

?>
```