上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

PHP-WEB漏洞挖掘
部署文档

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

在部署方面，我们的项目仍然运行在本地服务器localhost上，在后续的开发过程中。我们会尝试将该项目部署到服务器上。

因为只有两个界面，并且调用的图片，css等文件都是使用的相对路径，所以下载后直接打开就可以看到前端的页面。

通过改变Ajax中url的值，我们可以实现与后端服务器的交互。

```
function upload() {
var code = $("#file-zh-input").val();
$.ajax({
type: "POST",
url: "http://127.0.0.1:8080/upload",
data: {
    "code" : code
},
dataType: "json",
success: function(data) {
    alert("上传成功");
}
});
```

第二章 后端设计

因为我们后端的检测系统是部署在ubuntu系统上的，为了方便进行测试等，网站后端springboot也部署在虚拟机上，系统为ubuntu18.04。后端开启后会在虚拟机的8080端口开始监听前端传输过来的数据和请求并返回相应的结果。后端检测函数需要使用检测系统，也可直接通过脚本调用即可。

第三章 图卷积神经网络

运行：

python run_model.py

安装相关的依赖：

pip install -r requirements.txt

依赖包括：

ase==3.19.2

certifi==2020.6.20

chardet==3.0.4

cycler==0.10.0

decorator==4.4.2

future==0.18.2

googledrivedownloader==0.4

h5py==2.10.0

idna==2.10

intervaltree==3.0.2

isodate==0.6.0

Jinja2==2.11.2

joblib==0.16.0

kiwisolver==1.2.0

llvmlite==0.33.0

lxml==4.5.2

MarkupSafe==1.1.1

matplotlib==3.3.0

networkx==2.4

numba==0.50.1

numpy==1.19.1

pandas==1.0.5

phply==1.2.5

Pillow==7.2.0

ply==3.11

pyparsing==2.4.7

python-dateutil==2.8.1

pytorch-nlp==0.5.0

pytz==2020.1

rdflib==5.0.0

requests==2.24.0

scikit-learn==0.23.1

scipy==1.5.2

six==1.15.0

sortedcontainers==2.2.2

threadpoolctl==2.1.0

torch==1.5.1

torch-geometric==1.6.0

torch-scatter==2.0.5

torch-sparse==0.6.6

tqdm==4.48.0

urllib3==1.25.10

wandb

第四章 静态代码分析

以分析dvwa网站漏洞为例。

```
APP_NAME=dvwa
mkdir workspace && cd $_
../phpjoern/php2ast ../php_src/$APP_NAME
../joern/phpast2cpg nodes.csv rels.csv

HEAP=3G
JEXP_HOME=../batch-import/
PHPJOERN_HOME=../phpjoern/
java -classpath "$JEXP_HOME/lib/*" -Dfile.encoding=UTF-8
org.neo4j.batchimport.Importer $PHPJOERN_HOME/conf/batch.properties
graph.db nodes.csv rels.csv,cpg_edges.csv

cp -R graph.db ../neo4j-community-2.1.8/data/
```

启动Neo4j：

```
cd neo4j-community-2.1.8/bin
./neo4j console
```

使用python-joern进行查询：

```
cd python-joern
python main_test.py
```