The background is a traditional Chinese ink wash painting. It depicts a serene landscape with misty, layered mountains in shades of green and blue. A calm lake reflects the scene, with a small red boat carrying a person in the lower left. Several birds, including a large white crane with black wings and a red beak, are shown in flight against a pale, hazy sky. A large, bright red sun or moon is visible in the upper left corner.

一种基于多视角特征融合的 Webshell检测方法

汇报人：

2024-01-13



目录

- 引言
- Webshe11概述与分类
- 多视角特征提取方法
- 基于多视角特征融合的Webshe11检测模型
- 实验结果与分析
- 总结与展望



01

引言





研究背景与意义



Webshell概述

Webshell是一种恶意脚本，攻击者通过上传Webshell实现对目标服务器的远程控制，进而窃取数据或进行其他非法操作。

研究背景

随着互联网的普及和Web应用的广泛使用，Webshell攻击事件不断增多，给企业和个人用户带来了巨大的安全威胁。

研究意义

研究Webshell检测方法对于提高网络安全防护能力、保护用户隐私和财产安全具有重要意义。

国内外研究现状及发展趋势



国内外研究现状

目前，国内外学者已经提出了一些Webshell检测方法，如基于静态特征、动态行为、机器学习等方法。然而，这些方法存在误报率高、漏报率高等问题。

发展趋势

随着深度学习技术的不断发展，基于深度学习的Webshell检测方法逐渐成为研究热点。同时，多视角特征融合技术也被引入到Webshell检测中，以提高检测准确率。

WEB DEVELOPMENT PROCESS

nam rerum facilis est et expedita distinctio. Nam libero tempore, cum soluta nobis est eligendi optio, cumque nihil impedit, quoque nihil voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debet necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae.



本文研究内容与创新点



01

研究内容：本文提出了一种基于多视角特征融合的Webshell检测方法。首先，从静态和动态两个视角提取Webshell的特征；然后，利用深度学习技术对特征进行学习和融合；最后，通过分类器对Webshell进行分类识别。

02

创新点：本文的创新点主要包括以下几个方面

03

1. 提出了基于多视角特征融合的Webshell检测方法，综合考虑了静态和动态特征，提高了检测准确率。

04

2. 设计了一种基于深度学习的特征学习和融合方法，能够自动学习Webshell的特征表示，避免了手工提取特征的繁琐和主观性。

05

3. 在公开数据集上进行了实验验证，结果表明本文方法具有较高的检测准确率和较低的误报率。



02

Webshell概述与分类



Webshell定义及功能

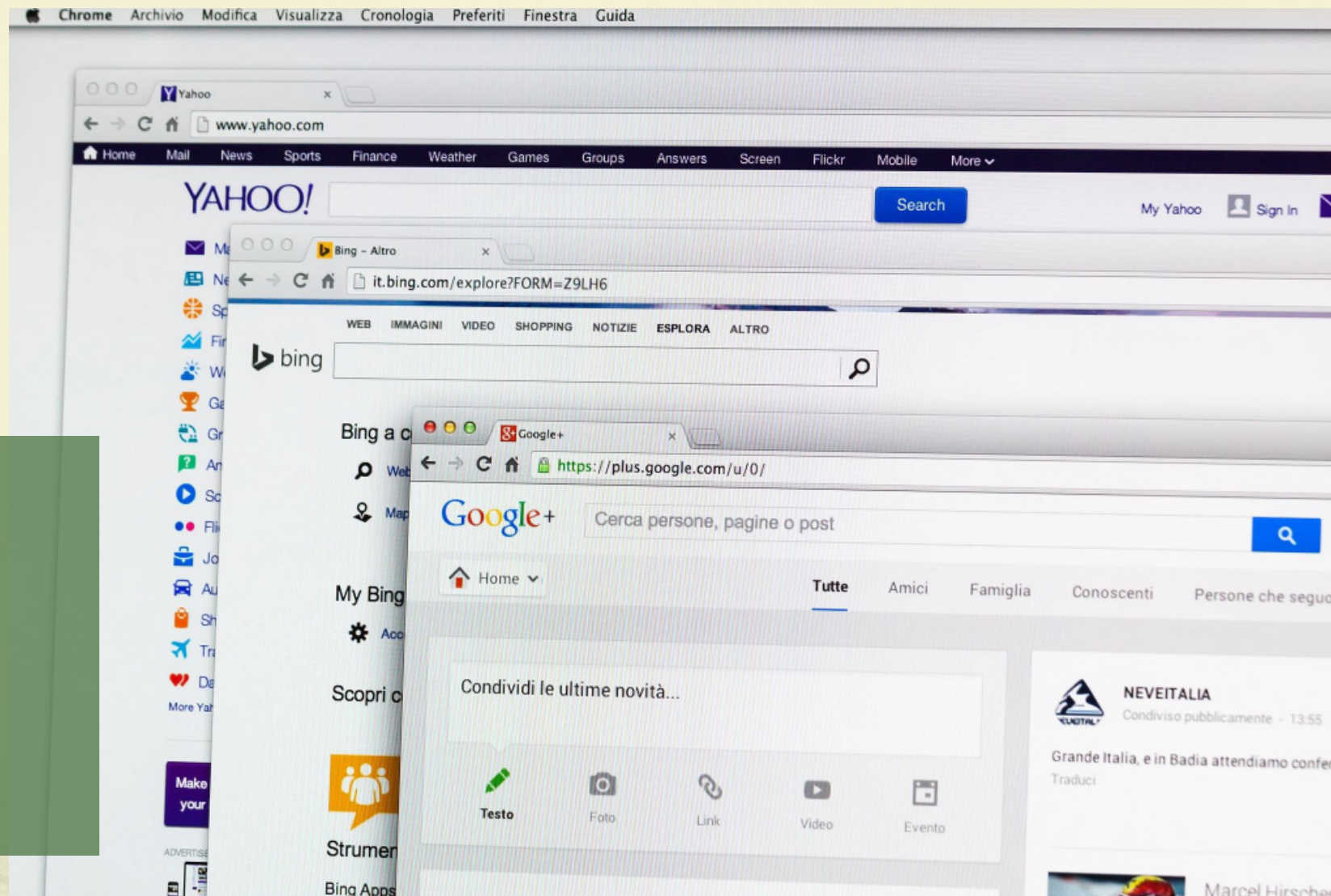


Webshell定义

Webshell是一种通过Web服务器上的漏洞或配置不当上传的恶意脚本，用于远程控制服务器并执行攻击者指定的命令。

Webshell功能

Webshell能够实现文件上传、下载、执行命令、查看系统信息、反弹Shell等功能，为攻击者提供对目标服务器的完全控制。





常见Webshell类型与特点



PHP Webshell

利用PHP语言编写的恶意脚本，通过URL参数传递命令并执行。

ASP Webshell

利用ASP语言编写的恶意脚本，通过HTTP请求传递命令并执行。

JSP Webshell

利用Java语言编写的恶意脚本，通过Servlet容器解析并执行命令。

跨站脚本攻击（XSS）型Webshell

将恶意脚本嵌入到Web页面中，当用户访问该页面时，恶意脚本会在用户浏览器中执行。



Webshell攻击原理及危害



```

...($clientLast || $DbLast - $clientLast
= $clientLast;
... Replace(
n_encode(array("id"; => $DbLast, "r" => $o->Ge
... $i < count($words); $i++) {
n($words[$i]) > 7){
t($_POST['get']))
... echo $o->GetStart
(int)$_POST['get'];
... self(isset($_POST
) = (int)$_POST['update'];
n_encode($o->GetLinkData($id, false));
... GetLinkData($id, false);
... mysql_query("SELECT MAX(id)"
... getM')));
... if(isset($_POST
... encode($o->GetLinksData($_POST['getM']));
... $clientLast);
... $clientLast;
... $o->RateLink($_POST['linkClass'], (int)$_PO
... $o->GetReserve
... escape_string($show));
... stripslashes
... escape_string($what));
... specialchars
... get')) $_POST['linkClass'], (int)$_PO

```

攻击原理

攻击者通过寻找目标Web服务器上的漏洞或配置不当，上传恶意Webshell脚本。一旦Webshell上传成功，攻击者可以通过访问特定的URL地址来执行恶意脚本中的命令，从而实现目标服务器的远程控制。

危害

Webshell攻击可以导致服务器被完全控制，攻击者可以窃取敏感信息、篡改网站内容、发起DDoS攻击等。同时，Webshell还可能被用于传播恶意软件、发起网络钓鱼攻击等，给企业和个人带来严重的安全威胁和财产损失。



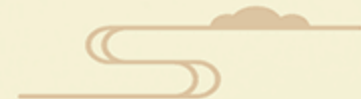
03

多视角特征提取方法





文本特征提取



1

词汇特征

通过词袋模型、TF-IDF等方法提取Webshell脚本中的词汇特征，包括关键词、特殊字符等。

2

语法特征

利用编程语言语法分析技术，提取Webshell脚本中的语法结构特征，如函数调用、变量声明等。

3

语义特征

基于深度学习技术，如词向量、循环神经网络等，提取Webshell脚本的语义特征，理解代码含义。





文件结构特征

分析Webshell脚本的文件结构，提取文件类型、编码方式、压缩方式等特征。

代码结构特征

研究Webshell脚本的代码结构，提取函数数量、代码行数、注释比例等特征。

控制流结构特征

通过控制流图等方法，提取Webshell脚本的控制流结构特征，如循环、条件语句等。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：
<https://d.book118.com/816220233111010141>