Web 系统测试

3.5 Web安全测试—文件上传漏洞

河北师范大学软件学院
Software College of Hebei Normal University

目 录

概述

- Web应用程序通常会有文件上传功能
- 解析漏洞
  - 攻击者在利用上传漏洞时，通常会与Web容器的解析漏洞配合在一起

Web解析漏洞

➢IIS解析文件

- ●在IIS根目录建立文件夹parsing.asp
- ●在该文件夹内创建文本文档test.txt
- ●在文本文档上写如下内容

<%=Now()%>

访问http://localhost/parsing.asp/test.txt

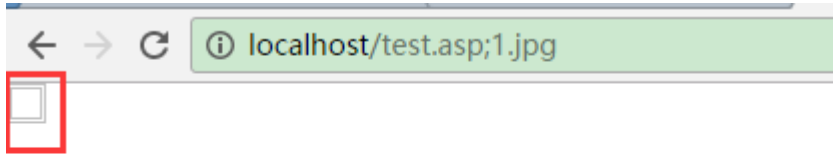
原因：IIS不解析.txt文件，应该直接显示内容，而在parsing.asp中却被当做ASP脚本执行

Web解析漏洞

当文件为文件名为*.asp;1.jpg

访问http://localhost/test.asp;1.jpg

原因：当做.asp文件被解析



认识解析漏洞

➢Apache解析漏洞

- ●新建文本文件，写如下内容

```
<?php
        phpinfo();
?>
```

- ●保存文件为1.php.rar
- ●浏览器地址栏输入 http://localhost/1.php.rar，正常应该提示文件下载框，但此时显示phpinfo()的内容
- ●Apache解析文件时，当碰到不认识的扩展名时，将会从后向前解析直到碰到认识的扩展名为止，如果都不认识，则会暴露其源代码

绕过上传漏洞

➢防止上传漏洞两种策略

- 客户端检测：客户端使用JS检测，在文件未上传时，就对文件进行验证
- 服务器端检测：检测文件扩展名是否合法，检测文件中是否嵌入恶意代码

文件上传漏洞预防

- 白名单与黑名单过滤
- MIME（MultiPupose Internet Mail Extensions）验证（用来设定某种扩展名文件的打开方式）类型验证
  - CSS文件MIME类型为text/css
  - gif图片MIME类型为text/gif
- 目录验证
  - 接收文件后，对目录进行判断

如何检验有没有解析漏洞

- 上传要求（正确的）的文件类型
- 上传带有脚本的伪造成 txt,jpg 文件上传验证

总结

- 什么是文件上传漏洞
- 文件上传漏洞解析
- 文件上传漏洞预防

Question