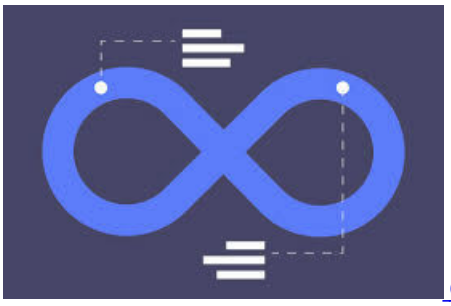
渗透测试 & 网络 & CTF 面试题整理

原创

OceanSec 于 2022-02-10 10:47:40 发布 3512 收藏 17

分类专栏： # Other # 考证考核 文章标签： 网络 web安全 面试

本文链接：https://blog.csdn.net/q20010619/article/details/122855958



Other 同时被 2 个专栏收录

32 篇文章 2 订阅

订阅专栏

考证考核

12 篇文章 12 订阅

订阅专栏

开卷！！！

之前整理的关于 web 安全的面试题

□ 宏观题

个□介绍

后□□可能会问

□次有趣的渗透测试经历

给你□个站怎么渗透

owasp top 10

挖过的CNVD证书

挖过本公司什么洞

你了解的安全漏洞

如果给你□个cms，如何给开发□员□些建议

护□期间做了什么

平常如何学习□安
CTF□赛经历&做题经验
记忆深刻的□道CTF题
出过的CTF题
AWD□□做题&出题
CTF运维
□ 渗透测试
□ 思路&流程
常□端□漏洞
公司的□络安全具体指什么
owasp 漏洞都有哪些？
给你知乎这个站点，你的□站流程，怎么攻击其他客户
邮箱服务SMTP有哪些攻击□式
渗透□企业简单还是□站点简单，为什么
如果已经□下了□个站，你会做什么？
反弹shell的姿势
你擅□打点还是内□？讲讲你打点的习惯，以及最近的□个shell是怎么拿到的？
如果你发现这个地□能进□命令执□，有哪些符号是可以的
当你利□命令执□进□反弹shell的时候如何做□较隐蔽，如果不能□bash python 还能□什么，
如果写定时任务反弹shell不成功你会怎么做
shell如何获取内□信息不被发现(翻浏览器记录，看DNS记录等)
getshell的□式
站库分离怎么写shell
怎么判断□前是否是cms
□个成熟并且相对安全的CMS，渗透时扫□录的意义？
为何□个 mysql 数据库的站，只有□个 80 端□开放？
web □□的 js 逆向
浏览器的常□编码
web常□的加密算法有什么
怎样对□个站去挖nday
OOB 带外数据
□ 信息收集
信息搜集的流程和□些□技巧
技术业务与信息分析业务
如何收集企业资产？
旁站及C段收集与利□□式
指纹识别？如何确定□法识别的指纹？
出现问题如何快速确定到问题资产？
在渗透过程中，收集□标站注册□邮箱对我们有什么价值？
□ □站认证机制
cookie和session有什么区别 ，后段session是如何进□保存的
Oauth认证过程中可能会出现什么问题，导致什么样的漏洞?
JWT原理&作□
JWT的安全性问题
JWT漏洞攻击思路
□ sql
SQL的存储引擎
mysql 数什么是事务？
读锁和写锁
MySQL的索引
mysql 的□户名密码是存放在那张表□□？mysql密码采□哪种加密□式？

mysql 的□户名密码是存放在那张表□□？mysql 密码采□哪种加密□式？
mysql 安全要如何做？
绕过
宽字节注□的实现条件，利□POC？
宽字节注□修复
报错注□的□种□式？
□回显如何检测注□成功？
□次注□的原理？
那么order by处如何修复
sql注□过滤逗号
**时间盲注ban掉了sleep函数，有哪些可以替换
时间盲注服务器回显□较慢，可以□什么解决
GPC是什么？GPC之后怎么绕过？
mysql的□个艾特@和两个@@有什么区别
框架防sql注□
mysql不知道列名怎么爆字段？
过滤了select怎么注□？
sql注□单引号被过滤了怎么绕过?
limit 后怎么注□？
SQL注□拿shell（不同的系统版本、数据库）
File_priv不为空的时候怎么写shell
outfile和dumpfile的差别？
发现□个sql注□的话:怎么反弹shell(linux和Windows)
SQL注□的后渗透姿势？SQL注□写□件的条件？如果写□□件后□法利□可能是什么情况？
防御
*哪些SQL注□不能通过预编译来防范
pdo防sql注□原理？
预编译具体□法
mysql中like查询会会□常缓慢，如何进□优化
NoSQL优点、□较、MongoDB注□□式
□ xss
xss探测内□
XSS 蠕□的产□条件
反射型和存储型区别在哪□，XSS危害
Dom-XSS和其他XSS区别、CSP了解过吗
XSS的测试思路
浏览器层□的防御
头部防御XSS的思路
特殊情况的xss
xss 后端如何修复像script复写的情况
xss对□户的输□进□实体转义□定能够防御吗？
□户输□在script标签中应该如何进□防御
svg标签利□图□xss有了解过吗
xss中httponly secure 和csp分别是□什么□的，如何实现的
盲注的利□□式
XSS如何配合组合拳进□getshell
secure-file-priv的作□和参数
XSS，能打到后台，但是后台系统处于内□，怎么做内□探测？
DOM型xss在审计中关注的重点
DOM 型 XSS□动化测试或□□测试
有没有了解过突变性XSS

有□个xss输出在href标签□□应该怎么办以及怎么修复
xss除了能盗□cookie还能做啥，对□标站的□久控制
前端xss如果特殊字符输出被htmlscecial过滤了怎么办
XSS可以控制属性怎么利□
有没有了解过突变型XSS
img 标签除了onerror 属性外，还有其他获取管理员路径的办法吗？
对于 XSS 怎么修补建议
cookie 存在哪□？可以打开吗?
Cookie安全□结
□ csrf
原理+防御
token 和 referer 做横向对□，谁安全等级□？
对 referer 的验证，从什么角度去做？如果做，怎么杜绝问题
针对 token, 对 token 测试会注意哪□□，会对 token 的哪□□进□测试？
CSRF，Referer如何绕过？
不同域名怎样通过CSRF拿Cookie
csrf如何getshell
其它格式的csrf
□种特殊的CSRF场景：后端只解析json格式的时候如何利□CSRF(□更改Content-Type)
Cookie 的 samesite
□ ssrf
原理+防御
你真实渗透过程中会去测嘛，怎么测
SSRF的利□□段，哪些协议可以利□
SSRF的DNS重绑定有了解吗，如何修复
gopher+redis攻击有哪些姿势
如果dnslog接受到了dns请求能确保有ssrf吗，请说出为什么
SSRF 如何进□修复
SSRF □回显
SSRF实战攻击内□，隐蔽获取信息
SSRF中302转跳防御（安全包）
ssrf利□过程中如何获取内□ip？
ssrf如何拿shell?
□些技巧和注意事项
csrf□般□什么□具进□检测
□ 反序列化
□ 逻辑漏洞
越权漏洞有没有什么了解
越权漏洞和逻辑漏洞□盒和□盒难以产出，有什么好的□法
逻辑漏洞场景分析
任意密码重置
□付漏洞
越权漏洞
未授权访问
验证码相关
竞争条件漏洞
□ 代码执□&命令执□（注□）
原理+防御
常□的□句话
□ □件上传

□件上传漏洞□般发□在什么场景？
□件上传的绕过□式？
□件上传遇到□名单（00截断之外的）
□件内容验证绕过对□件上传漏洞在□站中会做什么样的安全设计？
解析漏洞
防御
□ □件包含
原理&修复
导致□件包含的函数
已知某□站存在LFI(本地□件包含)，但是□法上传任何□件，针对该情况有哪些利□□式?(★★)
伪协议
本地□件包含拿shell
远程□件包含拿shell
绕过
防御
任意□件读取怎么获得□件的具体位置
读那些□件
□件下载
□ XXE
危害&原理
XXE防御
xxe□回显怎么办
xxe防护如果不能禁□外部实体该怎么做
xxe拿shell?
应该在哪□进□xxe过滤，是xml还是file_get_contents
怎么判断是否存在xxe漏洞
xxe的content-type应该是什么
□ 移动安全
app，逆向有了解过吗
移动端的调试经验 apk,ipa包分析
什么叫脱壳?
□ ELSE
点击劫持
url重定向绕过
Redis未授权访问
修复
□ 前端安全&XSS防御
□ 同源策略&跨域
简单的说□下同源策略
讲□讲内容安全策略CSP？
跨域请求有哪些□式？（jsonp&cors&代理）
总结
跨域可能存在什么漏洞？
CORS跨域漏洞如何利□？
如何对JSONP跨域请求存在的漏洞进□测试？
如何防御跨域请求漏洞？
jsonp referr校验能否百分百防护吗
jsonp 劫持
cors如果是不允许的域发起了请求，cors会进□怎样的返回
jsonp的token跟在哪个位置

Ajax 是什么？
Ajax 是否遵循同源策略？
ajax可以对请求□进□操作么
ajax发送post请求
前端函数如document可以跨域吗
不同浏览器之间，安全策略有哪些不同？□如chrome，firefox，IE
CORS哪个响应头是允许跨域的
jsonp如何实现跨域带第三□cookie？
如果你拿到□个jsonp漏洞你会怎么利□
□ csp
原理
csp常□绕过
csp写在meta标签中的安全问题
http-only作□
http-only,http-sercure
HTTP-Only禁□的是JS读取cookie信息，如何绕过这个获取cookie
csrf如果较验referer，如何伪造referer
xss怎么修改referer
□ 前端代码安全措施
前端加密是如何实现的，以及前端加密的过程是怎么样的
□ □具开发&分析
□ 使□&分析
简要介绍□□常□的扫描器和其实现上的特点
oneforall□域名收集原理
□域名搜集□法
处理泛解析问题
sqlmap流程
sqlmap api
burpsuite
xray
webshell管理□具流量
nmap和masscan的区别？
nmap扫描服务指纹的原理？
sqlmap的使□□法？
os-shell的原理
□burp抓包，有□户数据字段，有sign字段的签名，如何进□步渗透？
burp https抓包相关问题
curl□持的协议
awvs和appscan
dnslog的实现原理
使□DNS泄露数据的限制
□ 开发
□动化漏洞挖掘的思路？
开发经历？如果写□个□盒漏扫检测引擎如何实现？
□盒扫描器
□盒分析
语义waf
□撸□个SQL注□的检测脚本
端□扫描怎么做
□状态扫描
□状态扫描是会省略TCP握□的哪□步

□状态扫描是会留存TCP握□的痕□
□ □络层□
从键盘键□域名发□了什么
□ 协议
HTTP请求□式
HTTP响应码
GET 和POST的区别
HTTPS的实现原理
HTTP和HTTPS的区别
http □连接和短连接的区别
中间□攻击
防御中间□攻击的□案
浅析 HTTPS 中间□攻击与证书校验？
UDP和TCP区别
哪些服务和协议□到UDP那些□TCP
nmap、msf SYN 半握□和全握□实现
TCP三次握□四次挥□流程
DNS欺骗是什么
DNS重绑定&修复
DNS记录中A MX TXT意思
DNS收集□域
DNS域传送漏洞
HTTP请求□私
CLRF
307跳转
ARP欺骗
ARP欺骗防护
DDOS
syn洪流原理
cc攻击原理
Sockstress攻击
dns放□攻击
应□层的拒绝服务
UDP端□探测的有效□式是什么
□ CDN
绕过
证书透明度的危害？