2020/2/19 北京攻防研究员一面

因为曹师傅在北京，就投了一下北京安恒，面试了一个多小时，问了很多问题还是不错。估计是没有内推所以问题很多吧。时间2020/2/19/晚上7点到8点16

一、自我介绍

二、sql注入的原理和预防-sql预编译

其实是想要你举一个例子来说具体原理
写一条sql注入语句
sql预编译-知道东西，但是不知道这个术语，醉了
[数据库预编译为何能防止SQL注入]

三、跨站脚本

跨站脚本产生的原因
三种xss
dom型xss是反射型还是存储型
用xss打管理员cookie
csrf与xss区别

四、ssrf的原理

五、护网打内网的细节

六、反序列化漏洞

七、java-dao层做什么的

DAO接口： 把对数据库的所有操作定义成抽象方法，可以提供多种实现。

八、挖过的逻辑漏洞

九、短信轰炸

十、结合burp绕过waf的姿势

1、大小写 2、url编码 3、一些函数 4、webshell混淆
说一个你写过绕过waf的马
`分块传输` 绕过waf(之前看到过，忘了哈哈)

十一、sqlmap

要求爆库爆表嘚说每一条语句
`python sqlmap.py -u "http://localhost/sqli-labs-master/Less-1/?id=1"  -D security -T users -C id,username,password --dump`
--os-shell原理

十二、wireshark

捕捉过滤器 源ip要 192.168.1.1
`ip src host 10.1.1.1  //捕捉来源IP地址为10.1.1.1的封包。`
`ip.addr == 10.1.1.1  //显示来源或目的IP地址为10.1.1.1的封包。`

十三、英语文献翻译能力

全英文文献能翻译出么

十四、awvs

十五、burpsuite有哪些模块

repeter
intruder
spider
爆破模块有哪些爆破方式
问的是burpsuit里四种爆破模式区别

> sniper:狙击手：如果有两个爆破点，就在原来的基础上，单个修改，把payload值插入，如：字典里的数为3，爆破点为2，总共爆破6次

> battering ram：攻城锤：如果有两个爆破点，那么会同时替换字典里的值，即爆破时两个点的值是相通的，如：字典里有3个，爆破点有两个，爆破3次。

> pitch-fork：插稻草的叉子：可以在每个爆破点载入不同的字典。position1,2……如：pos1载入3个值的字典，pos2载入100个值的字典，它会按顺序匹配，以最少的payload为准，总共爆破3次。

> cluster bomb：集束炸弹：同样可以载入多个字典，是采用排列组合的方式，将每个position的所有情况和其他依次组合，如：pos1有3个值，pos2有100个值，总共爆破300次。若pos1有300，pos2有300，爆破90000次

十六、密码学

对称加密，非对称加密，散列（Hash），分组加密，数字签名（Digital Signature）
讲一下对称加密和非对称加密区别

十七、md5用来干嘛

检测文件完整性

十八、数据类型有哪些

十九、sql注入的类型

（1）基于布尔的盲注：根据页面返回判断条件真假注入

（2）基于时间的盲注：即不能根据页面返回内容判断任何信息，用条件语句查看时间延迟语句是否执行（即页面返回时间是否增加）来判断

（3）基于报错的注入：即页面会返回错误信息，或者把注入的语句的结果直接返回在页面中。

单引号
双引号
基于数字型注入
（4）联合查询注入：可以使用union情况下注入

二十、.net后端框架

二十一、时间盲注函数

```
最简单的就是sleep了，用if(1=1,sleep(5),0)

benchmark函数

heavy query 笛卡尔积 -->具体的方式就是将简单的表查询不断的叠加，使之以指数倍运算量的速度增长，不断增加系统执行 sql 语句的负荷，直到产生攻击者想要的时间延迟

get_lock GET_LOCK有两个参数，一个是key,表示要加锁的字段，另一个是加锁失败后的等待时间(s)，一个客户端对某个字段加锁以后另一个客户端再想对这个字段加锁就会失败，然后就会等待设定好的时间
```

二十二、提权和cobaltstrike

Cobalt Strike 一款以Metasploit为基础的GUI框架式渗透测试工具，集成了端口转发、服务扫描，自动化溢出，多模式端口监听，exe、powershell木马生成等。
https://www.cnblogs.com/ldhbetter/p/10684279.html
提权不太熟了：https://blog.csdn.net/qq_38684504/article/details/91359951

2020/2/20 北京安恒二面

一面结束，第二天二面就来了，也是问了一个多小时，还是不错的比较专业，时间2020/2/20晚上7:51

一、自我介绍

二、实战的经历细节-遇到什么问题-发现了哪些问题

三、ctf主要做什么方向

四、jwt

https://st4ck.gitee.io/2020/01/01/jwt/

五、base32-栅栏密码

六、给你一个jpg-misc常规思路-binwalk-foremost

七、常见的awd网络拓扑

八、sqlmap跑当前数据库名

```
--current-db
```

九、mysql的密码放在哪里

```
UPDATE mysql.user SET password=PASSWORD('新密码') WHERE User='root';
```

十、文件解析漏洞

IIS7.5、apache、nginx都有，回答了iis和apache的
https://www.jianshu.com/p/224ac688d135

iis

在iis6.0下，分号后面的不被解析，所以xx.asp;.jpg被解析为asp脚本得以执行。

形式：www.xxx.com/xx.asp/xx.jpg 服务器默认会把.asp，.asa目录下的文件都解析成asp文件。
IIS6.0 默认的可执行文件除了asp还包含这三种：
/test.asa
/test.cer
/test.cdx

apache解析漏洞

Apache 解析文件的规则是从右到左开始判断解析,如果后缀名为不可识别文件解析,就再往左判断。比如 test.php.owf.rar ".owf"和".rar" 这两种后缀是apache不可识别解析,apache就会把 wooyun.php.owf.rar解析成php。
www.xxxx.xxx.com/test.php.php123

十一、get-post区别

突然问傻了

```
get是从服务器上获取数据，post是向服务器传送数据。
get传送的数据量较小，不能大于2KB。post传送的数据量较大，一般被默认为不受限制
get安全性非常低，post安全性较高
```

十二、head方法

十三、redis开什么端口，有什么漏洞,如何利用

6379-未授权访问getshell的一些方法
写马和写ssh的key

十四、如果辨别一个网站是struct2框架

看url里面的连接，如果是XXX.action结尾或直接XXX？参数1=XXX，应该就是stuts2

十五、linux查看某一个进程的cpu占比

ps aux里面就有

十六、linux历史命令

.bash_history,history

十七、linux下passwd和shadow区别

shadow是root可读
passwd匿名都可读

十八、工资想要多少

ps:然后说-如果两天后晚上打电话给我说明我提的需求一切合理，给offer,如果觉得不合适，就不会打电话

然后就打电话给了offer