2020/2/17 奇安信一面

2020/2/14/周五投在牛客网的，但是两天没有消息，因为周末没上班，2020/2/17/周一上午hr突然直接加了我微信，说面试过两天安排。
然后2020/2/17/下午4点电话就来了，大概持续50分钟。

一、自我介绍

二、实战经验：一次真实的渗透，你在其中具体做了什么

正常回答巴拉巴拉

三、mysql布尔盲注于时间盲注区别

基于布尔的盲注：
Web页面的返回值只有两种， True 和 False ， 所以我们只能通过测试输入的注入语句为 Ture 或 False 来判断注入的效果 ， 并通过这两种可能一步步得出数据库的信息
W基于时间的盲注：
web页面的返回值只有一种，True。
无论我们输入任何值，它的返回情况都会按正确的处理。无法通过返回页面正确或是错误来推断信息
加入特定的时间函数，通过查看是web页面返回的时间来判断注入的语句是否正确，以此得出数据库的信息。

四、mysql+dnslog：

测试一些网站的时候，一些注入都是无回显的，我们可以写脚本来进行盲注，但有些网站会ban掉我们的ip，这样我们可以通过设置ip代理池解决，DNS在解析的时候会留下日志，咱们这个就是读取多级域名的解析日志，来获取信息
简单来说就是把信息放在高级域名中，传递到自己这，然后读取日志，获取信息

五、mysql提权

1、写webshell 2、MOF提权 3、UDF提权

六、mysql没有写权限如何写马

这就真不知道了，可能是我理解错了。回答抱歉这个我真不知道

七、跨域+同源+jsonp

所谓的同源，指的是协议，域名，端口相同。浏览器处于安全方面的考虑，只允许本域名下的接口交互，不同源的客户端脚本，在没有明确授权的情况下，不能读写对方的资源。
当一个请求url的协议、域名、端口三者之间任意一个与当前页面url不同即为跨域
jsonp的核心原理就是目标页面回调本地页面的方法,并带入参数

八、APP脱壳+反编译+流量分析

这个问题比较陌生了
加壳是在二进制的程序中植入一段代码，在运行的时候优先取得程序的控制权
常见的知道upx
反编译和流量分析嘚感谢觅动了，熟悉了一点

九、webshell免杀

就是一些混淆，比如

```
<?php
$c=str_rot13('nffreg');
$c($_REQUEST['x']);
?>
```

还有其他一些混淆

十、redis安全漏洞

（1）写webshell：
（2）写公钥ssh登录（我记得这个，但是面试突然忘记了）
windows下就很麻烦,不过大概记得这篇文章
https://uknowsec.cn/posts/notes/Redis%E5%9C%A8Windows%E7%8E%AF%E5%A2%83%E4%B8%8BGetshell.html

十一、为什么sqlmap能对sqlserver直接getshell而不用直接指定目录

这个就不太熟悉了，好像是sqlserver有命令执行的函数

十二、文件解析漏洞

IIS7.5、apache、nginx都有，回答了iis和apache的

iis

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

十二、struct2、weblogic、shiro等框架的漏洞有了解么

有
j2EE开源框架struts2出现了很多命令执行漏洞，好在昨天刚好挖src,挖到了一个struct2_S016的洞，描述了一下
weblogic rec有利用过，只知道是反序列化，具体原理不熟悉
shiro反序列化漏洞看过：这个up主不错，b站真的啥都有https://www.bilibili.com/video/av57241403,大概讲了一下原理

十三、你有什么问题问我们

一些私人问题，建议这个还是提前想一下，不然到时候你会茫然