各位老师，你们好！

我很荣幸能够参加今天的研究生复试，我叫王国庆，来自重庆忠县，就读于成都东软学院，物联网工程专业。

在我的大学期间，我总是认真学习，在我的大部分专业课程中都取得了较好的成绩，并获得了一些宝贵的学习经验，且具备一定的自学能力。我在大学里自学了web安全方面的一些知识，熟悉渗透测试的基本方法，并且有一些实战经验，但仍然有很多需要学习和提升的地方。我还自学了python，它可以做一些机械化的事情来满足人们的需求，比如批量漏洞探测（挖掘），我曾经编写过python脚本来挖掘漏洞，并获得了CNVD的一些证书。

当我大三的时候，我决定参加研究生入学考试，因为我真的很喜欢网络安全这个专业，希望能够继续深入学习。并且，我认为研究生可以使自己在社会上更有竞争力。

接下来，我想谈谈我未来的读研规划。重庆邮电大学拥有雄厚的师资力量，并享有很高的声誉。在接下来的三年里，我将阅读大量的相关文献，形成更系统的网络安全观。我将专注于我专业领域的学习，努力提高我的研究能力。

以上是我的自我介绍。感谢各位老师！

**老师：四级有没有过？**

"老师您好，我在英语四级考试中没有通过，但是我通过前两次的四级分数意识到了自己在英语学习上的不足，特别是听力和写作方面。我已经制定了详细的学习计划来提升我的英语能力。虽然我目前的水平还有待提高，但我相信通过持续的努力和学习，我一定会取得进步的。如果我能顺利考上研究生，我有信心通过今年12月份的四级考试。

# self-introduction

Good morning, dear professors. I am glad to be here for this interview. My name is Wang Guoqing , 23 years old and I come from Chonqing City, Now I am studying at ChengDu Neusoft University and my major is Internet of Things Engineering.

During my college years, I always take study seriously and did well in most of my specialized courses , and I got some precious learning experience . I learned web security and some software skills on my own in college,especially Python,It can do some mechanized things to meet people's needs ,such as exploring vulnerabilities, I have written python scripts to exploit vulnerabilities and obtained some certificates of China National Vulnerability Database.

When I was a junior , I made the decision to take postgraduate entrance examination because I hope I can get in-depth study in my dream major. In addition , I think to be a postgraduate can make myself more competitive in society.

Next, I want to talk about my future plans. Chongqing University of Posts and Telecommunications has mighty teaching staff for my dream major and enjoys a high reputation, In the next three years, I plan to read vast relevant literature to form a more systematic view of Network and Information Security. And I will concentrate on the study on my professional field and work hard to improve my research ability.

That's all about me. If I am lucky enough to be admitted, I will devote myself to the study and research in the next three years.thank you！

Frankly,I am not prepared for this question.sorry 坦白说我没有准备过这个问题。

That’s all I can think of right now

Sorry, I didn't hear you clearly. Could you please repeat it 重复一遍

1. 你的家乡 Could you tell me something about your hometown?

Thank you for your question.My hometown is Zhongxian County, Chongqing, located in the central part of Chongqing, with a long history and culture. Bai Juyi once served as an official there. There are many specialties in my hometown, such as Zhongzhou Stinky tofu and oranges, which are very delicious. There are also many famous tourist attractions, especially Shibaozhai, which still stand tall after more than 400 years of wind and rain,and attracts a large number of tourists every year. Welcome everyone to visit my hometown when you have time. Thank you again for your question!

2.Why do you choose our university?

Thank you for your question.

Firstly,I chose Chongqing University of Posts and Telecommunications because it is a prestigious university with a long history and an active academic atmosphere. // And I chose the major of network and information security because I like it very much. //

Secondly,the teacher there are all excellent,and they provide innovative approach to academy.

Finally,Because I grew up in Chongqing, Chongqing is a city with a long history and culture.I like the culture here very much, so I am very eager to continue my postgraduate study here, not only academically, but also comprehensively to be a better person.Thank you!

3.Can you talk to us about the food in your hometown？

Thank you for your question. My hometown is Zhongxian County, Chongqing, where there are many delicious foods, such as Stinky tofu, oranges and pig's feet rice. My favorite food is pig's foot rice because it's delicious and affordable. My friends often joke, "A bowl of pig's foot rice can create a romantic for men."Thank you!

4.Why did you choose to pursue postgraduate studies ?

Thank you for your question.When I was a junior , I made the decision to take postgraduate entrance examination because I hope I can get in-depth study in my dream major. In addition , I think to be a postgraduate can make myself more competitive in society.thank you !

1. Can you talk about your graduate study plan ?

Thank you for your question.Chongqing University of Posts and Telecommunications has mighty teaching staff for my dream major and enjoys a high reputation, In the next three years, I plan to read vast relevant literature to form a more systematic view of Network and Information Security. And I will concentrate on the study on my professional field and work hard to improve my research ability.Thank you!

6.Can you introduce your undergraduate school ？

Thank you for your question.My undergraduate school is ChengDu Neusoft University, located in Chengdu, Sichuan , next to Qingcheng Mountain. The campus has beautiful scenery, friendly students and excellent teachers. Our school's foods are very delicious,such as pig’s foot rice,My favorite food is pig's foot rice because it's delicious and affordable. My roommate often joke, "A bowl of pig's foot rice can create a romantic for men."Our school library is very large and has complete infrastructure. Thank you!

7.Talk about your hobby（Key words : in your free time / spare / leisure time favorite sport your hobby

Thank you for your question .My hobbies are playing table tennis and running. Playing table tennis is a sport that I have loved since I was young, and I also enjoy watching table tennis matches. The hobby of running was cultivated during my undergraduate studies. It not only helps to exercise the body, but also relieves stress and relaxes the brain.Thank you!

**8.Keywords : what is your greatest strength and weakness / advantage merit /disadvantage**

Thank you for your question .Every person has his own strength and weakness . My strength is to approach problems with a positive attitude. When I meet some tough things , a good attitude can allow me to keep calm and find an effective way to deal with it.As for my great weakness, I think that I am poor at refusing requests . I need to learn how to say “no” to others when I’m inconvenient . These are my great strength and weakness.Thank you!

**9.Which of your family members influences you most?**

Thank you for your question .Well , as for this question , I think that should be my father. There are two reasons . First of all,my father is the breadwinner of my family .He works hard to support our family. Secondly , my father is an active man . when he meets some tough things , he can clam down and solve them with a positive attitude instead of complaining them . With the influence of him , I become a sunny person and also face difficulties with an optimistic attitude . This is my father who influences me most.Thank you!

POC是⽤来证明漏洞存在的，EXP是⽤来利⽤漏洞的，两者通常不是⼀类，或者说，PoC通常是⽆害的，Exp通常是有害的，有了POC，才有EXP。

POC：全称 ' Proof of Concept '，中⽂ ' 概念验证 ' ，常指⼀段漏洞证明的代码。

EXP：全称 ' Exploit '，中⽂ ' 利⽤ '，指利⽤系统漏洞进⾏攻击的动作。

1、你为什么报考我们学校？

感谢老师的提问。首先我之所以报考重庆邮电大学，是因为重庆邮电大学成立于1950年，拥有深厚的文化底蕴，并且重邮在我梦想的专业方面拥有雄厚的师资力量，并享有很高的声誉。我的回答完毕，谢谢老师！

然后就是因为我是真心喜欢网络安全这个专业，在我上专科的时候，我就对网络安全里的web安全非常感兴趣，那个时候自学了渗透测试，喜欢挖漏洞，为了挖到漏洞我可以一晚上不睡觉。直到现在，我仍然清晰地记得第一次挖掘 CNVD 漏洞的全过程。从信息收集开始，到成功发现一个漏洞，再到批量探索漏洞，总共花费了 3 天的时间。最终漏洞被收录并获得 CNVD 证书时那种喜悦感是由衷而来的。

最后就是因为我是一个重庆人，因为专科和本科都是在成都那边上的，切身体会还是感觉重庆好，每次放假回家，一踏上重庆的这片土地有一种说不出来的安全感，就像是实实在在到了自己家一样。

结合以上几点就是我报考贵校的原因。我的回答完毕。谢谢老师！

1. 你为什么报考网络与信息安全这个专业？

好的， 感谢老师的提问。首先我之所以报考网络安全这个专业，是因为我自己真的非常喜欢这个专业，在我上专科的时候，我就对网络安全里的web安全非常感兴趣，那个时候自学了渗透测试，喜欢挖漏洞，为了挖到漏洞我可以一晚上不睡觉。直到现在，我仍然清晰地记得第一次挖掘 CNVD 漏洞的全过程。从信息收集开始，到成功发现一个漏洞，再到批量探索漏洞，总共花费了 3 天的时间。最终漏洞被收录并获得 CNVD 证书时那种喜悦感是由衷而来的。

然后就是这个专业也算是一个新兴的专业，专业前景广阔，发展空间巨大。

中央网络安全和信息化领导小组组长习近平总书记强调，网络安全就是国家安全是国家发展的重要方面。我相信网络安全在未来一定会得到很好的发展。

综上所述就是我报考这个专业的原因。我的回答完毕，谢谢老师。

1. 你说你曾经挖到过漏洞，谈谈你挖漏洞的经历。

**Cnvd**  资产5000万+通用（必须有10个以上的漏洞示例） 先是手动一个账号密码输入，最后才是写python poc批量探索

**Edusrc**  （fofa+goby）

**逻辑漏洞**（小程序支付 和 未授权访问+sql注入

**前端JS日志文件泄露**

这个漏洞我没找到他后台登录地址，应该是前后端分离的，不然应该可以通过管理员的账号密码 拿到webshell 。所以说渗透测试的本质就是信息收集。

1. 感兴趣的方向 ，

这个问题我目前还欠研究，虽然现在不了解，但是如果能读研究生，一定跟随老师好好吧这个问题专研清除。但我现在对...有了一些了解，不知道能否简单谈谈。

1. 你大学生活中遇到的最大的（印象最深刻）挫折是什么？

SQL注入分类：union注入、bool盲注、宽字节注入、二次注入、报错注入、sleep时间注入

**原理**：利用sql语句获取数据库的敏感信息，一般存在于和数据库交互的地方

**预防**：预编译，正则表达式过滤

## 常见的中间件漏洞

IIS

PUT 漏洞、短文件名猜解、远程代码执行、解析漏洞

Apache

解析漏洞、目录遍历

Nginx

文件解析、目录遍历、CRLF 注入、目录穿越

Tomcat

远程代码执行、war 后门文件部署

JBoss

反序列化漏洞、war 后门文件部署

WebLogic

## XSS

我主要掌握的就是反射型（非持久型）xss 和存储型xss

**反射型：**这种攻击方式是一次性的，通过链接发送給别人，若有人点击这个链接，服务器接收到请求并处理，然后将带有XSS代码的数据返回给用户的浏览器。浏览器解析这段代码，执行攻击者的恶意脚本。从而实现窃取用户信息等

**存储型：**攻击脚本被存储在目标服务器的数据库或文件中，因此具有较高的隐蔽性。比如一些网站的留言板，是存储型xss的重灾区

**预防：**通过对用户输入的数据进行验证，把一些特殊的标签转义或者删除 ‘<’ ’script’

## 逻辑漏洞

越权、未授权访问、支付漏洞

**正则表达式**：是一种文本模式，用于描述和匹配一系列符合某个模式（规则）的文本

**[Socket](https://m.baidu.com/s?word=Socket&sa=re_dqa_zy" \t "https://answer.baidu.com/answer/_self)**是计算机网络中用于不同主机之间进程通信的端点，它提供了应用层进程利用网络协议交换数据的机制。Socket可以看作是两个网络应用程序进行通信时，各自通信连接中的端点，

**Socket通信的类型有两种**：TCP和UDP

## SSRF（服务端请求伪造）

是一种由攻击者构造形成由服务器端发起请求的一个安全漏洞，ssrf的攻击目标是从外网无法访问的内部系统，比如一些链接id？=www.baidu.com

防范：对回显的内容进行加密，设置ip白名单

主站一般都比旁站安全，且主站域名一般有CDN,国外PING

# 未授权+sql注入

关键词：信息收集，通过主域名获取子域名，在通过域名反查ip，主站比较安全，，cdn是什么，怎么绕过，点击进入login界面，判断存在哪些漏洞，第一：F12抓包 看看有没有js文件泄露，搜索后缀为.log的文件。..因为我按了f12一直刷新页面嘛，然后就看到了可能有未授权访问。

CNVD，首先，CNVD收录的前提条件有两个：公司资产5000w+通用漏洞

然后我通过一个网站，里面全是卖路由器的，我一个个找，终于功夫不负有心人，我找到了一个资产大于5000万，而且我能找它到弱口令的路由器，弱口令是我通过搜索：路由器名+应用手册，里面有初始账号密码，然后再用专业的搜索引擎，搜索这个路由器的名字，就出现几十页的地址信息，我前面是一个一个手动去探测有没有漏洞，后面越试越恼火。然后就没有然后了，我是第二天才想起来有python爬虫这个东西，而且之前也学过一点点，然后就百度，找到了个类似的代码，然后一直面向百度编程，最终写了个爬取ip信息的脚本，还写了一个poc 用于批量验证漏洞的，