暑期总结

学习内容

1. owasp top10

> 1. A1 注入injection
> 2. A2 失效的身份验证和会话管理
> 3. A3 跨站请求伪造
> 4. A4 敏感信息泄露
> 5. A5 未验证的重定向和转发
> 6. A6 安全配置错误
> 7. A7 跨站脚本攻击XSS
> 8. A8 跨站请求伪造CSRF
> 9. A9 使用含有已知漏洞的组件
> 10. A10 未验证的文件上传

> 基础
> http协议，
> sql注入，
> xss，
> csrf，
> sqlmap，
> burpsuite，
> coockie
> 等

> 难点
> 需熟悉各种漏洞的利用方式，灵活变通，熟悉漏洞变式。但最底层原理不变，payload需根据题目精心构造。并且变化多端。不易被直接发现。需要进行各种验证。并且不一定能够找到准确答案，需要细心。

2. Crypto

> 1. 密码学基础
> 2. 古典密码
> 3. 现代密码学
> 4. 密码学工具
> 5. 密码学攻击

> 难点
> 需要对各种密码学算法进行了解，并且需要了解各种攻击方式，以及各种攻击方式的特点。
> 各种编码规则要熟悉，能够利用python进行编码，解码。对密文解密，明文加密。明确密码加解密过程

3. pwn

> 1. 基础
>   熟悉二进制文件，以及各种格式，以及各种格式对应的结构体。
>   熟悉各种堆栈，以及堆栈的利用方式。
>   熟悉各种格式化字符串，以及格式化字符串的利用方式。
>   熟悉各种rop，以及rop的利用方式。
>   熟悉各种gadget，以及gadget的利用方式。
>   熟悉各种栈溢出，以及栈溢出的利用方式。
>   熟悉各种堆溢出，以及堆溢出的利用方式。

> 难点
> 需要对各种漏洞进行了解，并且需要了解各种利用方式，以及各种利用方式的特点。对内存地址进行运算，计算出需要覆盖的内存地址，以及需要填充的内存大小。
> 地址覆盖，需要对文件进行反编译。对栈进行处理。
> 需要对各种gadget进行了解，并且需要了解各种gadget的利用方式。构造特定的exp进行攻击。

4. 代码审计

> 1. 基础
>   多为php代码审计，需要熟悉php的语法，以及php的函数。
>   需要熟悉php的变量作用域，以及php的变量类型。
>   需要熟悉php的魔术方法，以及魔术方法的调用方式。
>   需要熟悉php的魔术常量，以及魔术常量的调用方式。

> 难点
> php语句构造，利用协议，执行文件包含。跨目录文件访问。以获取flag。
> 变量构造的，需要根据具体源代码构造特定的payload。对变量进行绕过赋值。构造特定的payload，进行攻击。等

5. 各种工具系统使用

> 1. 基础
>   msf
>   sqlmap
>   burpsuite
>   ida
>   pwntools
>   kali
>   蚁剑
>   中国菜刀
>   nmap
>   等

> 难点
> 工具各种参数的设置，以及工具的利用方式。
> 输出结果的分析，以及输出结果的利用方式。
> 各种工具的配合使用，以及各种工具的配合方式。

心得体会

经过暑期的训练，对各种漏洞的利用方式，以及利用方式的特点，有了进一步的了解。
各种漏洞的利用方式，以及利用方式的特点，需要进行大量的练习，才能熟练掌握。
暑期的长时间自主学习，锻炼了自己独立思考的能力，以及独立分析的能力。强化了自主学习的能力。
并且训练自我通过互联网等各种资料进行自主学习的能力。
暑期的学习虽然走了很多弯路，甚至有段时间有些漫无目的。不知到应从何学起。
并且暑期的学习，还是存在一些问题，就是对于部分漏洞的利用方式，以及利用方式的特点，还是不够熟悉。
但总体来说还是学习了很多内容。但平时也要定期去反复训练，。加强记忆，以保障不会遗忘曾经学过的内容。
暑期的学习还是非常快乐的，因为能够和志同道合的人一起学习，一起交流，一起讨论，一起学习，一起进步。并且每天都有新的收获。每天的生活都很规律。每天都能看到自己的进步。还是非常有成就感的。
为更好的生活和更好的自己加油努力吧！！
未来一片光明。