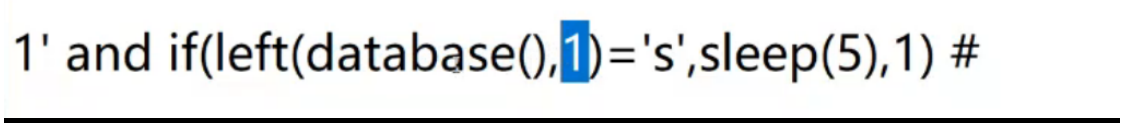
20200630信息安全实训

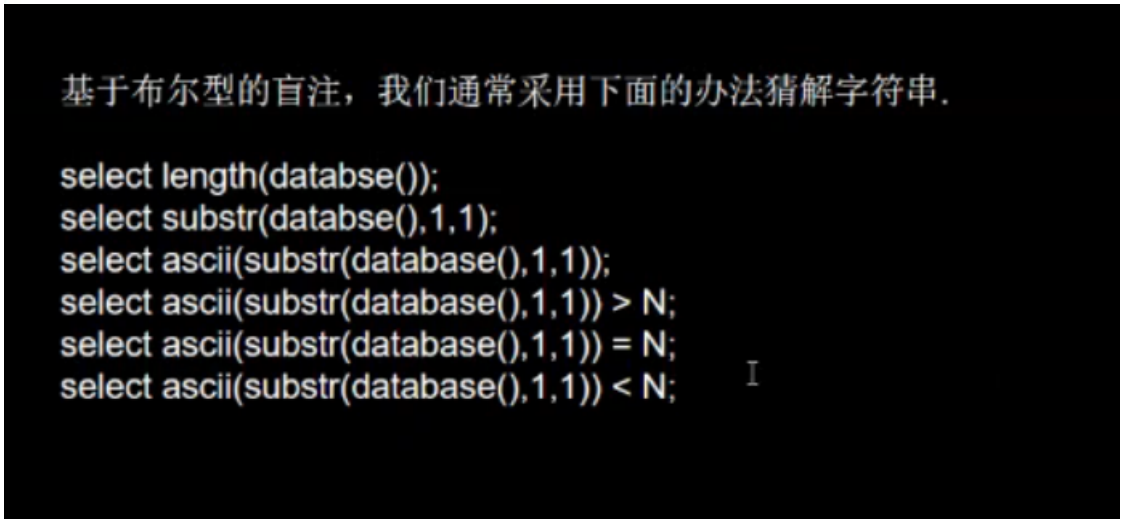
笔记本:	我的第一个笔记本		
创建时间:	2020/6/30 9:02	**更新时间:**	2020/6/30 16:07
作者:	820410740@qq.com		

SQL注入-盲注
无回显的注入
类型：基于时间的 基于布尔的
测试有无sql注入漏洞的时候准确度差
时间盲注 根据服务器的响应时间来判断 网络通畅
sleep() 休眠多长时间后再运行
' and 1=1 # 服务器的响应时间
' and 1=1 and sleep(5)

sqlmap

1.开源程序phpcms
2.站点phpcms 通用型漏洞
3.服务器配置了页面不显示错误信息，sql注入测试 盲注





http头中的注入介绍

Referer 每次请求的来源地址

User-Agent 用户代理

count(*) floor(rand(0)*2) groupby

Sqlmap设置具体SQL注入技术

--technique 参数用来设置具体SQL注入技术。以下列出Sqlmap支持的SQL注入技术。

B: Boolean-based blind 基于布尔的盲注
E: Error-based 报错注入
U: Union query-based Union查询注入
S: Stacked queries 堆叠注入
T: Time-based blind 基于时间的盲注
Q: Inline queries 内联查询注入

例如：sqlmap -u “存在注入点的URL” --technique B --current-db

利用基于布尔的盲注对注入点进行SQL注入探测。