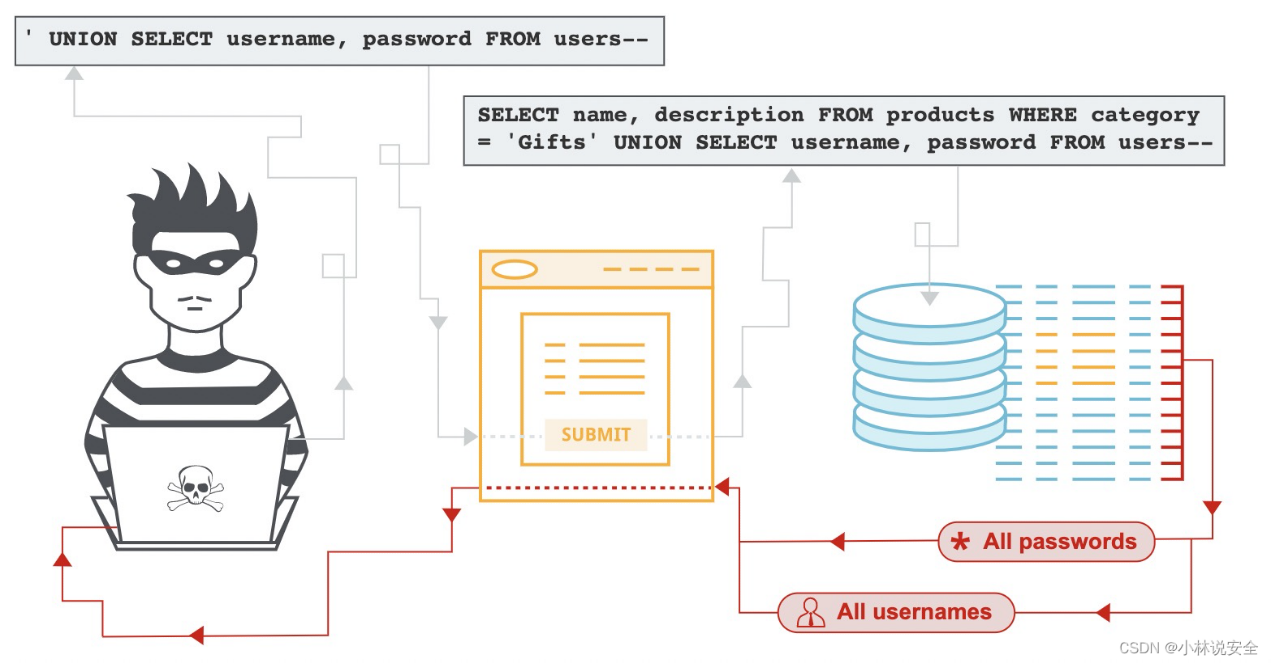
Web攻防-SQL注入&增删改查&HTTP头&UA&XFF&Referer&Cookie&无回显报错&复盘



#知识点：  
1、Web攻防-SQL注入-产生原理&应用因素  
2、Web攻防-SQL注入-各类数据库类型利用  
----------------------------------------------  
1、Web攻防-SQL注入-参数类型\*参数格式  
2、Web攻防-SQL注入-XML&JSON&BASE64等  
3、Web攻防-SQL注入-数字字符搜索等符号绕过  
----------------------------------------------  
1、Web攻防-SQL注入-操作方法&增删改查  
2、Web攻防-SQL注入-HTTP头&UA&Cookie  
3、Web攻防-SQL注入-HTTP头&XFF&Referer  
   
#章节点：(待补充)  
OWTOP10，SQL注入，文件安全（上传,下载,读取,删除,包含等），目录遍历，  
CSRF，SSRF，CRLF，SSTI注入，XML&XXE安全，RCE执行（代码或命令等）  
反序列化，业务逻辑（验证码，接口枚举，支付购买，机制验证，越权，并发等）  
未授权访问，失效访问控制，弱口令安全，第三方组件安全，CORS，JSONP等





演示案例：

* WEB攻防-SQL注入-数据库类型利用
* WEB攻防-SQL注入-参数类型&符号干扰
* WEB攻防-SQL注入-参数格式&参数编码
* WEB攻防-SQL注入-增删改查&无回显报错
* WEB攻防-SQL注入-HTTP头&UA&Cookie
* WEB攻防-SQL注入-HTTP头&XFF&Referer

#数据库知识：  
1、数据库名，表名，列名，数据  
2、自带数据库，数据库用户及权限  
3、数据库敏感函数，默认端口及应用  
4、数据库查询方法（增加删除修改更新）  
   
#SQL注入产生原理：  
代码中执行的SQL语句存在可控变量导致  
   
#影响SQL注入的主要因素：  
1、数据库类型（权限操作）  
2、数据操作方法（增删改查）  
3、参数数据类型（符号干扰）  
4、参数数据格式（加密编码等）  
5、提交数据方式（数据包部分）  
6、有无数据处理（无回显逻辑等）  
   
#常见SQL注入的利用过程：  
1、判断数据库类型  
2、判断参数类型及格式  
3、判断数据格式及提交  
4、判断数据回显及防护  
5、获取数据库名，表名，列名  
5、获取对应数据及尝试其他利用  
   
#黑盒/白盒如何发现SQL注入  
1、盲对所有参数进行测试  
2、整合功能点脑补进行测试  
白盒参考后期代码审计课程  
   
利用过程：  
获取数据库名->表名->列名->数据（一般是关键数据，如管理员）  
   
案例说明：  
在应用中，存在增删改查数据的操作，其中SQL语句结构不一导致注入语句也要针对应用达到兼容执行，另外也需要明白黑盒中功能对应的操作方法；除此之外部分业务应用功能也要做到了解（如接受IP,UA,COOKIE,Referer等头部），并且通过功能分析出对应SQL操作方法。  
   
增删改查大致功能应用：  
select查询：用户查询，新闻查询  
delete删除：用户删除，新闻删除  
update修改：用户修改，新闻修改  
insert增加：用户注册，新闻添加  
   
UA(User-Agent):  
场景1：对UA设备指定显示方案  
场景2：对UA设备进行信息记录  
   
XFF(X-Forwarded-For):  
场景1：限制IP访问功能  
场景2：记录IP访问日志  
   
Cookie:  
场景：开发人员在编写一个根据用户 ID（存储在Cookie中）来查询信息的功能  
   
Referer:  
网站期望登录请求来自于本站页面，如果Referer是其他来源，则拒绝登录。  
   
#实例应用：  
1、增删改查-操作方法注入  
SRC报告-广东工业大学sql注入  
2、HTTP头-cookie注入  
SRC报告-吉林工业职业技术大学sql注入Bypass  
3、HTTP头-XFF注入  
<https://mp.weixin.qq.com/s/CiCxpHbW4IArB2nYSH-12w>  
<https://mp.weixin.qq.com/s/_jj0o7BKm8CGEcn77gvdOg>  
4、加密还原+JSON注入  
<https://mp.weixin.qq.com/s/c3wji_LL_nuiskAKpg89pA>  
5、HTTP头-403绕过  
<https://mp.weixin.qq.com/s/t0VH_9qmb1EuwPGiz3Bbcw>

涉及资源：[资源下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)