QFQ

Pactice / Beginner

Carsten Rose, I-MATH, University of Zurich, 2018

QFQ – Report & Form

- **Report**
  - Pro Webseite können ein oder mehrere Typo3 Content Elemente (ttcontent) vom Typ 'QFQ' angelegt werden.
  - Layout Position: Left / Main / Header / Footer
- **Form**
  - QFQ bringt einen Formular Editor mit, der durch die Typo3 Webseite angezeigt wird.
  - Die Webseite (=Produkt) ist selbst die Entwicklungsumgebung

Report: SQL

- **An einigen wenigen Stellen gibt es Erweiterungen zu SQL.**
  - Variablen in '{{...}}' werden durch QFQ ersetzt, bevor das SQL Statement abgefeuert wird.
  - Das von SQL zurueckgelieferte Ergebnis wird durch QFQ nochmal interpretiert und ggfs. modifiziert.
  - SQL Queries koennen geschachtelt werden.
- **Doc: http://qfq.io > Documentation > Report**
  - https://docs.typo3.org/typo3cms/drafts/github/T3DocumentationStarter/Public-Info-053/Manual.html#report

Report: Variablen

{{<variable name> : <store> : <sanatize> : <escape> : <default>}}

1) **10.sql = SELECT 'hello world'**
2) **10.sql = SELECT 'hello world: {{pageAlias:C}}'**
3) **10.sql = SELECT 'hello world: {{pageAlias:CT}}'**
4) **10.sql = SELECT 'hello world: {{pageAlias:CT:alnumx}}'**
5) **10.sql = SELECT 'hello world: {{pageAlias:CT::m}}'**
6) **10.sql = SELECT 'hello world: {{pageAlias:CFR:::Tuesday}}'**

https://docs.typo3.org/typo3cms/drafts/github/T3DocumentationStarter/Public-Info-053/Manual.html#variable

Report: QFQ = SQL & HTML

10.sql = SELECT p.name FROM Person AS p

RoseBalendraBeceren

**10.sql = SELECT p.name, '
' FROM Person AS p**

Rose
Balendra
Beceren

10.sql = SELECT p.name FROM Person AS p

**10.rend =
**

Rose
Balendra
Beceren

Report: head, row, field, alt

```
10.sql = SELECT '<tr><td>', p.name, '</td></tr>' FROM Person AS p
10.head = <table border="1">
10.tail = </table>

10.sql = SELECT p.name, p.firstName FROM Person AS p
10.head = <table border="1">
10.tail = </table>
10.rbeg = <tr>
10.rend = </tr>
10.fbeg = <td>
10.fend = </td>

10.sql = SELECT p.name FROM Person AS p
                    WHERE p.name LIKE '{{a:C:alnumx}}%'
10.althead = Not found
10.shead = Always shown -
```

Report: Successive,Nested

Nacheinander:

**10.sql = SELECT p.name, '
' FROM Person AS p**

**20.sql = SELECT p.firstName, '
' FROM Person AS p**

Geschachtelt 1:

**10.sql = SELECT p.name, '
' FROM Person AS p**

**10.20.sql = SELECT '-',p.firstName, '
' FROM Person AS p**

Geschachtelt 2:

```
10 {
  sql = SELECT p.name, '<br>' FROM Person AS p
  20.sql = SELECT p.firstName, '<br>' FROM Person AS p
}
```

Report: Column as parameter

Nacheinander via STORE_RECORD

**10.sql = SELECT p.name, '
' FROM Person AS p**

**20.sql = SELECT p.firstName, '({{name:R}})
' FROM Person AS p**

Geschachtelt via STORE_RECORD

**10.sql = SELECT p.name, '
' FROM Person AS p**

**10.20.sql = SELECT p.firstName, '({{name:R}})
' FROM Person AS p**

Geschachtelt via Levelkey:

```
10 {
  sql = SELECT p.name, '<br>', p.id FROM Person AS p
  20.sql = SELECT p.firstName, '<br>' FROM Person AS p WHERE p.id={{id:R}}
}
```

Report: Hide column

```
10 {
  sql = SELECT p.name, '<br>', p.id AS _id FROM Person AS p
  20.sql = SELECT p.firstName, '<br>'
                  FROM Person AS p
                  WHERE p.id={{id:R}}
}
```

Report: Link

```
10.sql = SELECT '10 ', 'p:home' AS _link, '<br>'

20.sql = SELECT '20 ', 'p:home|t:Home' AS _link, '<br>'

30.sql = SELECT '30 ', 'p:home|t:Home|o:HOME' AS _link, '<br>'

40.sql = SELECT '40 ', 'p:home|b' AS _link, '<br>'

50.sql = SELECT '50 ', 'p:home|b|t:Home' AS _link, '<br>'

60.sql = SELECT '60 ', 'p:home|b:btn-success|t:Home' AS _link, '<br>'

70.sql = SELECT '70 ', 'p:home|E' AS _link, '<br>'

80.sql = SELECT '80 ', 'p:home|N|t:Home' AS _link, '<br>'

90.sql = SELECT '90 ', 'p:home|D|t:Home|R' AS _link, '<br>'

100.sql = SELECT '100 ', 'p:home|H|q' AS _link, '<br>'
```

https://docs.typo3.org/typo3cms/drafts/github/T3DocumentationStarter/Public-Info-053/Manual.html#column-link

Report: SIP – protection

SIP: Server ID Pairs

**10.sql = SELECT 'p:{{pageAlias:T}}&v=OMG| **

t:Value={{v:S:::missing}}|s' AS _link

https://example.com/index.php?id=98&s=5a7012db5bbdb

- **Werte bleiben auf dem Server**
  - Keine Manipulation moeglich (?).
- **SIP ist vertrauenswuerdig – kein Sanitizing.**
- **QFQ (und nur QFQ) erstellt die SIPs on the fly.**

Report: List of forms

```
form={{form:SE}}

10 {
  # List of Forms: Do not show this list of forms if there is a form given by SIP.
  sql = SELECT CONCAT('p:{{pageId:T}}&form=form') as _pagen, '#', 'Name', 'Title', 'Table', ''
              FROM (SELECT 1) AS fake WHERE '{{form:SE}}'=''
  head = <table class="table table-hover qfq-table-50">
  tail = </table>
  rbeg = <thead><tr>
  rend = </tr></thead>
  fbeg = <th>
  fend = </th>

  10 {
    # All forms
    sql = SELECT CONCAT('p:{{pageId:T}}&form=form&r=', f.id) as _pagee, f.id, f.name, f.title, f.tableName,
                       CONCAT('form=form&r=', f.id) as _Paged FROM Form AS f ORDER BY f.name
    rbeg = <tr>
    rend = </tr>
    fbeg = <td>
    fend = </td>
  }
}
```

URL: absolute

- **http://example.com/prod/index.php?id=home&form=Person&type=2&sip=5a7012db5bbdb#detail**
- ***Protocol*: http | https**
  - token: ':'
- ***Domain*: example.com**
  - token: '//'
- ***Path/File*: prod/index.php**
  - token: '/'
- ***Parameter*: id=home&form=Person&sip=5a7012db5bbdb**
  - token: '?' , '&'
- ***Anker*: detail**
  - token: '#'

URL: relative

- **Wird kein Protokoll, Domain, Path/File angegeben, impliziert das 'index.php'**
- **'index.php' ohne Protokoll, Domain impliziert 'current location'.**
- **HTML: '?r=123':**
  - http://example.com/prod/index.php?r=123
- **QFQ: 'home&r=123':**
  - http://example.com/prod/index.php?id=home&r=123
- **Wann immer moeglich relative URLs angeben:**
  - transportabel (Code kann an einer anderen Stelle unveraendert benutzt werden).
  - kuerzen – besser lesbar.

Security

- **Parameter manipulation: SIP**
- **Code Injection**
  - URL encode
- **Problematic character: % & ; ( ) < >**
  - Sanatize classes
- **GET parameter max length**
- **Attack detected**
- **Honeypot: *username, password, email***
- **Download**

Typo3

- **Page**
  - Alias: Reiter 'Behaviour'
  - Access: Group
- **Content Element**
  - Type: QFQ
  - Columns: Normal, Left, Right, ~~Border~~
  - Access: Group
  - Language

Browser

- **Webdeveloper Tools: F12**
- **Console**
- **Network (!)**
- **Inspect Element**

Stores

- **F – Form** ***(Default Sanatize: digit)***
- **S – SIP**
- **R – Record**
- **C – Client** ***(Default Sanatize: digit)***
- **T – Typo3**
- **V – Vars**
- **0 – '0' … match always**
- **E – Empty … match always**
- **Y – System**
- **B, P, D,M, L**

Form

- **Primary Table**
  - Record ID – Parameter 'r'
  - r=0: new
  - r>0: edit
- **URL:**
  - Traditional: http://example.com/index.php?id=home&form=Person&r=123
  - QFQ: http://example.com/index.php?id=home&s=5a7012db5bbdb

Form Type

- **Simple Form**
  - Enthaelt nur Felder der Primary Table
- **Advanced Form**
  - Via FormElement.type='Action' werden Non-Primary Records geschrieben.
- ~~**Multi Form**~~ **(noch nicht implentiert)**
- **Delete Form**
  - Loescht primary und dependent Records

Form: Aufbau

- **Formular (1x)**
  - Basic: Name (eindeutig), Titel, Table
  - Access: Parameter, Permission New/Edit, Button
  - Various: Forward
  - ~~Multi~~
- **Formularelemente (mehrere)**
  - Native Element
  - Action Element
  - Container