TYPO3.Flow - Bug # 29488

Status:	Resolved	**Priority:**	Should have
Author:	Carsten Bleicker	**Category:**	Security
Created:	2011-09-05	**Assigned To:**	Bastian Waidelich
Updated:	2011-10-20	**Due date:**	
PHP Version:			
Has patch:			
Complexity:			
Affected Flow version:			
Subject:	AuthenticationManager::authenticate() does not throw Exception for invalid credentials		

Description

if i send empty login data the result of authentication is allways true here.
can somebody reproduce this? exception is also not thrown.
talking about this part:

```
   public function authenticateAction() {

       $authenticated = FALSE;
       try {
           $this->authenticationManager->authenticate();
           $authenticated = TRUE;
       } catch (\TYPO3\FLOW3\Security\Exception\AuthenticationRequiredException $exception) {
           // No Exception is thrown if user sends empty form?
           var_dump($exception);
       }

       /**
        * At this point $authenticated is allways true if user sends empty form?
        */
       var_dump($authenticated);
       die();

       if ($authenticated) {
       ........
   }
```

Associated revisions

Revision d77d2596 - 2011-10-13 23:52 - Bastian Waidelich

[!!!][TASK] Change default authentication strategy

This changes the default authentication strategy from "anyToken"
to "atLeastOneToken" in order to provoke an exception if
authentication fails in the common use case (login with username
and password).

Change-Id: Ia3d15f8e5e900ccc3b5be1b22b668d5ddadad7c8
Resolves: #29488

History

#1 - 2011-10-05 11:50 - Karsten Dambekalns

- Status changed from New to Needs Feedback

Andi, can you shed some light on this?

#2 - 2011-10-05 11:55 - Bastian Waidelich

- Subject changed from authenticationAction allways True? to AuthenticationManager::authenticate() does not throw Exception for invalid credentials

- Assigned To set to Andreas Förthner

- Priority changed from Should have to Must have

I can reproduce this with the default setup.
To fix this you can change the authentication strategy. for instance like this:

```
TYPO3:
  FLOW3:
    security:
      authentication:
        authenticationStrategy: atLeastOneToken
```

But if I get it right, the behavior of the default strategy (anyToken) is not correct.

#3 - 2011-10-05 11:57 - Karsten Dambekalns

This would be "expected" behavior for the anyToken authentication strategy - authenticated doesn't mean authorized. If anonymous authentication is not to be allowed, change the authentication strategy to atLeastOneToken.

But is that what "people" would expect?

#4 - 2011-10-05 12:03 - Bastian Waidelich

Bastian Waidelich wrote:

> *But if I get it right, the behavior of the default strategy (anyToken) is not correct.*

..I didn't get it right obviously. The behavior of anyToken is described with "Authenticate as many tokens as possible but do not require an authenticated token (e.g. for guest users with role Everybody)."

Still, I think we should either change the default strategy or make it easier to check the authentication status.
Currently we'd have to do

```
$activeTokens = $this->securityContext->getAuthenticationTokens();
foreach ($activeTokens as $token) {
    if ($token->isAuthenticated()) {
        // is authenticated
    }
}
```

Another option might be to be able to override the strategy by a parameter in the authenticate() method?

#5 - 2011-10-05 14:22 - Andreas Förthner

As already discussed, the behaviour is correct. But maybe we really should change the default strategy. On the other hand, anyToken ist the strategy with less errors being thown. So it might be a good choice, as it doesn't break something if you do nothing...

#6 - 2011-10-05 14:47 - Bastian Waidelich

Andreas Förthner wrote:

> *On the other hand, anyToken [...] doesn't break something if you do nothing...*

Except for your security if you happen to forget to reconfigure the strategy ;)
I think, the default use case is standard username/password authentication so we should probably have the default configuration "safe" - but we can discuss that again at T3CON!

#7 - 2011-10-12 23:04 - Bastian Waidelich

- Status changed from Needs Feedback to Accepted

- Assigned To changed from Andreas Förthner to Bastian Waidelich

- Priority changed from Must have to Should have

- Target version set to 1230

As discussed at T3CON11 we should change the default strategy from "anyToken" to "atLeastOneToken" as that will fit the most common use case of authenticating via username & password.

#8 - 2011-10-12 23:21 - Mr. Hudson

- Status changed from Accepted to Under Review

Patch set 1 of change Ia3d15f8e5e900ccc3b5be1b22b668d5ddadad7c8 has been pushed to the review server.
It is available at http://review.typo3.org/5750

#9 - 2011-10-13 23:53 - Mr. Hudson

Patch set 2 of change Ia3d15f8e5e900ccc3b5be1b22b668d5ddadad7c8 has been pushed to the review server.
It is available at http://review.typo3.org/5750

#10 - 2011-10-14 00:06 - Bastian Waidelich

- Status changed from Under Review to Resolved

- % Done changed from 0 to 100

Applied in changeset commit:d77d259613775337751115098200e6175adfcb28.

#11 - 2011-10-20 01:37 - Karsten Dambekalns

- Target version changed from 1230 to 1.0.0