Redmine - Defect #37755

Mentioning users with certain characters renders incorrectly

2022-10-06 00:31 - Nicholas Natale

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Marius BĂLTEANU	**% Done:**	0%
Category:	Issues	**Estimated time:**	0.00 hour
Target version:	5.0.5		
Resolution:	Fixed	**Affected version:**	5.0.2

Description

Mentioning users that have apostrophes in their first/last name (possibly other characters too?) causes them to render incorrectly when a note/description is saved.

Example:

```
@someusername
```

Renders as

```
@Paul O&#39;Neil
```

Expected rendering:

```
@Paul O'Neil
```

Other environment information:

- Ruby version: 2.7.6
- Rails version: 6.1.6
- DB: MariaDB 5.5.68

Associated revisions

Revision 21986 - 2022-12-03 14:21 - Marius BĂLTEANU

Fix mentioning users with certain characters renders incorrectly (#37755).

Patch Mizuki ISHIKAWA.

Revision 21988 - 2022-12-04 09:14 - Marius BĂLTEANU

Merge r21986 from trunk to 5.0-stable (#37755).

History

#1 - 2022-10-12 05:37 - Go MAEDA

- Status changed from New to Confirmed

#2 - 2022-12-02 06:32 - Mizuki ISHIKAWA

The following code is causing the problem.

```
# https://github.com/redmine/redmine/blob/df88b9c7ddb485784b1c74c40e7b34675d68f983/app/helpers/application_hel
per.rb#L62-L63
      name = h(principal.name(options[:format]))
      name = "@" + name if options[:mention]
```

- h(principal.name(options[:format])) => ActiveSupport::SafeBuffer object
- "@" => String object

- "@" + name => String object

The concatenation of "" changes the class of the object(ActiveSupport::SafeBuffer => String).
Pre-converting "" to an ActiveSupport::SafeBuffer object by html_safe should prevent the class from being changed.

```
diff --git a/app/helpers/application_helper.rb b/app/helpers/application_helper.rb
index ced1845ebb..ec97845756 100644
--- a/app/helpers/application_helper.rb
+++ b/app/helpers/application_helper.rb
@@ -60,7 +60,7 @@ module ApplicationHelper
     case principal
     when User
       name = h(principal.name(options[:format]))
-      name = "@" + name if options[:mention]
+      name = "@".html_safe + name if options[:mention]
       css_classes = ''
       if principal.active? || (User.current.admin? && principal.logged?)
         url = user_url(principal, :only_path => only_path)
diff --git a/test/helpers/application_helper_test.rb b/test/helpers/application_helper_test.rb
index a5c533a4fb..d34de2b08c 100644
--- a/test/helpers/application_helper_test.rb
+++ b/test/helpers/application_helper_test.rb
@@ -1841,6 +1841,16 @@ class ApplicationHelperTest < Redmine::HelperTest
     assert_equal result, link_to_principal(unknown_principal, :class => 'bar')
   end

+  def test_link_to_principal_should_escape_principal_name
+    user = User.generate!(firstname: "firstname<>'", lastname: 'lastname&"')
+    group = Group.generate!(lastname: "group<>'&")
+
+    assert_include "firstname&lt;&gt;&#39; lastname&amp;&quot;", link_to_principal(user)
+    assert_include "@firstname&lt;&gt;&#39; lastname&amp;&quot;", link_to_principal(user, {mention: true})
+    assert_include "group&lt;&gt;&#39;&amp;", link_to_principal(group)
+    assert_include "&lt;&gt;&#39;&amp;", link_to_principal("<>'&")
+  end
+
   def test_link_to_group_should_return_only_group_name_for_non_admin_users
     User.current = nil
     group = Group.find(10)
```

#3 - 2022-12-03 12:44 - Marius BĂLTEANU

- Target version set to 5.0.5

#4 - 2022-12-03 14:21 - Marius BĂLTEANU

- Status changed from Confirmed to Resolved

- Assignee set to Marius BĂLTEANU

Fix committed, thanks!

#5 - 2022-12-04 09:17 - Marius BĂLTEANU

- Status changed from Resolved to Closed

- Resolution set to Fixed