Redmine - Defect #41930

Redirection after signing in fails when the back_url includes a port number

2024-12-03 16:31 - Kenta Kumojima

Status:	Closed		**Start date:**	
Priority:	Normal		**Due date:**	
Assignee:	Go MAEDA		**% Done:**	0%
Category:	Accounts / authentication		**Estimated time:**	0.00 hour
Target version:	6.0.3			
Resolution:	Fixed		**Affected version:**	6.0.0

Description

If URI contains a port, I cannot redirect to back_url after login.
 	
If back_uri contains port, ApplicationController#validate_back_url raises Addressable::URI::InvalidURIError and returns false.
So, hidden field of back_url is not rendered at '/login'.
The validation method should remove the port before the host.
 	
<pre>   [:scheme, :host, :port].each do |component|
 	
      if uri.send(component).present? && uri.send(component) != request.send(component)
        return false
      end
 	
      uri.send(:"#{component}=", nil) # => raises InvalidURIError
    end</pre>

Related issues:	
Related to Redmine - Defect #31831: Back url parse in validation	**Closed**

Associated revisions

Revision 23465 - 2025-01-28 06:49 - Go MAEDA

Redirection after signing in fails when the back_url includes a port number (#41930).

Patch by Kenta Kumojima (user:kumojima) and Go MAEDA (user:maeda).

Revision 23467 - 2025-01-28 08:49 - Go MAEDA

Merged r23465 from trunk to 6.0-stable (#41930).

Revision 23469 - 2025-01-28 09:24 - Go MAEDA

Simplify URL components omission in ApplicationController#verify_back_url (#41930).

Revision 23470 - 2025-01-28 09:27 - Go MAEDA

Merged r23469 from trunk to 6.0-stable (#41930).

History

#1 - 2025-01-27 03:39 - Go MAEDA

- Related to Defect #31831: Back url parse in validation added

#2 - 2025-01-27 04:12 - Go MAEDA

- Status changed from New to Confirmed

- Target version set to Candidate for next minor release

As reported, I have confirmed the issue where passing a URL containing a port number, such as http://localhost:3000/admin, to the ApplicationController#validate_back_url method results in false being returned.

Inside the validate_back_url method, there is a process that removes the protocol, hostname, and port number from the provided URL. Specifically, the following code is responsible for this:

```
uri = Addressable::URI.parse(back_url)
[:scheme, :host, :port].each do |component|
  if uri.send(component).present? && uri.send(component) != request.send(component)
    return false
  end

  uri.send(:"#{component}=", nil)
end
```

In this code, the protocol, hostname, and port number are removed sequentially from the Addressable::URI object created from the given URL. However, when processing in this order, an exception occurs when attempting to remove the hostname. This happens because removing the hostname leaves the URL in a state where it has a port number but no hostname, resulting in the following exception:

```
Addressable::URI::InvalidURIError: Hostname not supplied: '/admin'
```

As suggested in the proposed patch, this issue can be resolved by removing the port number before removing the hostname. This adjustment ensures that the URL remains valid during the process.

#3 - 2025-01-27 09:47 - Go MAEDA

Here is another solution.

```
diff --git a/app/controllers/application_controller.rb b/app/controllers/application_controller.rb
index a3eaec4bb..9056e1603 100644
--- a/app/controllers/application_controller.rb
+++ b/app/controllers/application_controller.rb
@@ -511,11 +511,10 @@ class ApplicationController < ActionController::Base
         if uri.send(component).present? && uri.send(component) != request.send(component)
           return false
         end
-
-        uri.send(:"#{component}=", nil)
       end
-      # Always ignore basic user:password in the URL
-      uri.userinfo = nil
+
+      # Remove the scheme, user:password, host, and port from the URL
+      uri.omit!(:scheme, :userinfo, :host, :port)
     rescue Addressable::URI::InvalidURIError
       return false
     end
```

#4 - 2025-01-28 00:38 - Go MAEDA

- Target version changed from Candidate for next minor release to 6.0.3

Setting the target version to 6.0.3.

#5 - 2025-01-28 03:03 - Go MAEDA

- File 41930-v2.patch added

- Affected version set to 6.0.0

Here is a new patch. I have updated the code to use the omit! method, as I suggested in #note-3, to remove unnecessary components from the URI object. By using omit! to remove multiple components at once, we no longer need to worry about the order in which the components are removed.

Additionally, the current code has a bug where it throws an exception when a URL contains Basic authentication information (e.g., http://user:password@redmine.example.net) during the uri.send(:"host=") step. This patch also fixes that issue.

#6 - 2025-01-28 06:49 - Go MAEDA

- Status changed from Confirmed to Resolved

- Assignee set to Go MAEDA

- Resolution set to Fixed

Committed the patch in [r23465](r23465). Thank you for your contribution.

#7 - 2025-01-28 06:50 - Go MAEDA

- Subject changed from Cannot redirect to back_url including port after login to Redirection after signing in fails when the back_url includes a port number

#8 - 2025-01-28 08:49 - Go MAEDA

- Status changed from Resolved to Closed

Merged the fix into the 6.0-stable branch in [r23467](#).

#9 - 2025-01-28 09:29 - Go MAEDA

Replaced uri.omit!(:scheme, :userinfo, :host, :port) with uri.omit!(:scheme, :authority) in [r23469](#) (trunk) and [r23470](#) (6.0-stable).

Files

fix_redirect_to_back_url_with_port.patch	2.14 KB	2024-12-03	Kenta Kumojima
41930-v2.patch	2.09 KB	2025-01-28	Go MAEDA