

## Redmine - Feature #21697

### Set secure flag of the session cookie depending on original request

2016-01-12 00:29 - Anonymous

<b>Status:</b> Reopened	<b>Start date:</b>
<b>Priority:</b> Normal	<b>Due date:</b>
<b>Assignee:</b>	<b>% Done:</b> 0%
<b>Category:</b> Security	<b>Estimated time:</b> 0.00 hour
<b>Target version:</b>	
<b>Resolution:</b>	
<b>Description</b>	
<p>The default configuration of redmine sends session cookie open for any connection type. This allows an attacker to steal the session cookie and access one's redmine session.</p> <p>It is possible to secure the cookie by changing the option in application.rb file.</p> <pre>config.session_store :cookie_store, :key =&gt; '_redmine_session', :secure =&gt; true</pre> <p>But this will prevent users from accessing system via plain HTTP protocol in local network.</p> <p>Let Redmine set secure cookie flag depending on request scheme and X-Forwarded-Proto HTTP-header.</p>	
<b>Related issues:</b>	
Related to Redmine - Feature #20935: Set autologin cookie as secure by default... <b>Closed</b>	

#### History

##### #1 - 2016-01-12 00:39 - Go MAEDA

- Status changed from New to Closed
- Resolution set to Duplicate

Fixed by [#20935](#). Please try Redmine 3.2.0.

##### #2 - 2016-01-12 00:40 - Go MAEDA

- Is duplicate of Feature #20935: Set autologin cookie as secure by default when using https added

##### #3 - 2016-01-12 00:44 - Anonymous

The issue [#20935](#) doesn't seem to fix `_redmine_session` cookie.

##### #4 - 2016-01-12 00:45 - Go MAEDA

- Status changed from Closed to Reopened

##### #5 - 2016-01-12 00:46 - Go MAEDA

- Is duplicate of deleted (Feature #20935: Set autologin cookie as secure by default when using https)

##### #6 - 2016-01-12 00:46 - Go MAEDA

- Related to Feature #20935: Set autologin cookie as secure by default when using https added

##### #7 - 2016-01-12 00:47 - Go MAEDA

- Resolution deleted (Duplicate)

##### #9 - 2016-01-12 10:19 - Mahesha Matharage

This issue cannot simulate in the Dev environment.

##### #10 - 2016-01-12 23:53 - Anonymous

#### Steps to simulate task

1. Set up redmine on host A, HTTP-port 80
2. Set up reverse proxy on host B, SSL-port 443
3. Get Redmine page via address <http://A/redmine>
4. Get Redemin page via address <https://B/redmine>

## Desired behaviour

1. Browser receives header Set-Cookie: \_redmine\_session=...-...; path=/redmine/ from domain A
2. Browser receives header Set-Cookie: \_redmine\_session=...-...; path=/redmine/; secure; HttpOnly from domain B

### #11 - 2017-11-30 16:55 - Toshi MARUYAMA

- Description updated

### #12 - 2023-03-03 04:45 - Go MAEDA

You can set secure attribute to the cookie by adding the following line to config/additional\_environments.rb to force access over HTTPS.

```
config.force_ssl = true if Rails.env.production?
```

### #13 - 2023-07-04 17:03 - Popa Marius

Needs to be added to redmine site too

<https://observatory.mozilla.org/analyze/redmine.org>

```
Session cookie set without using the Secure flag or set over HTTP
```