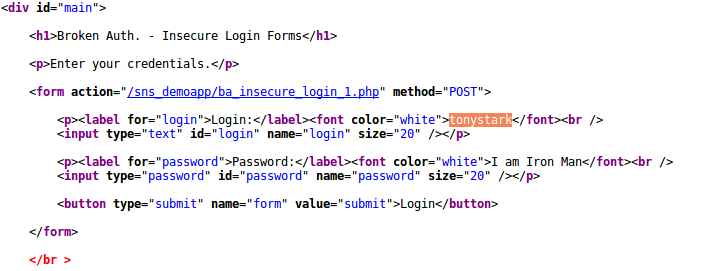
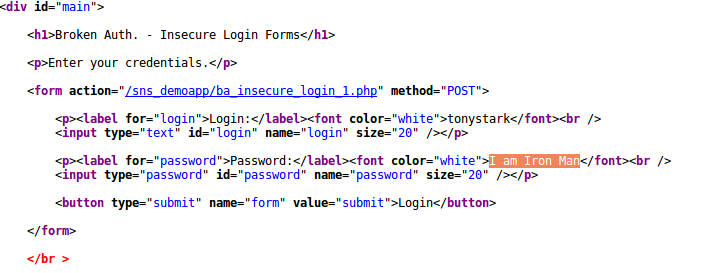
# **A2. Broken Authentication and Session Management**

# **Broken Auth. - Insecure Login Forms**

**Bug:**

1. Right click on page and view source page.
2. We can find that login: tonystark and password: I am Iron Man are by default, so if we input these values, we can successfully login.



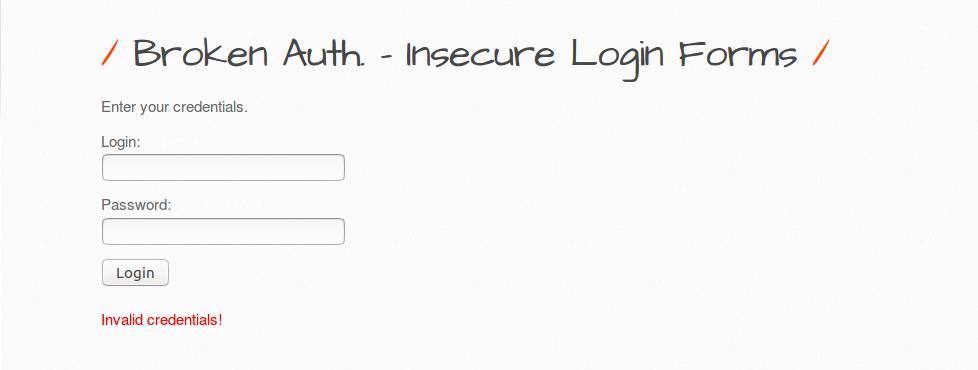






Solution:

Go to source code and remove tonystark and I am Iron Man.



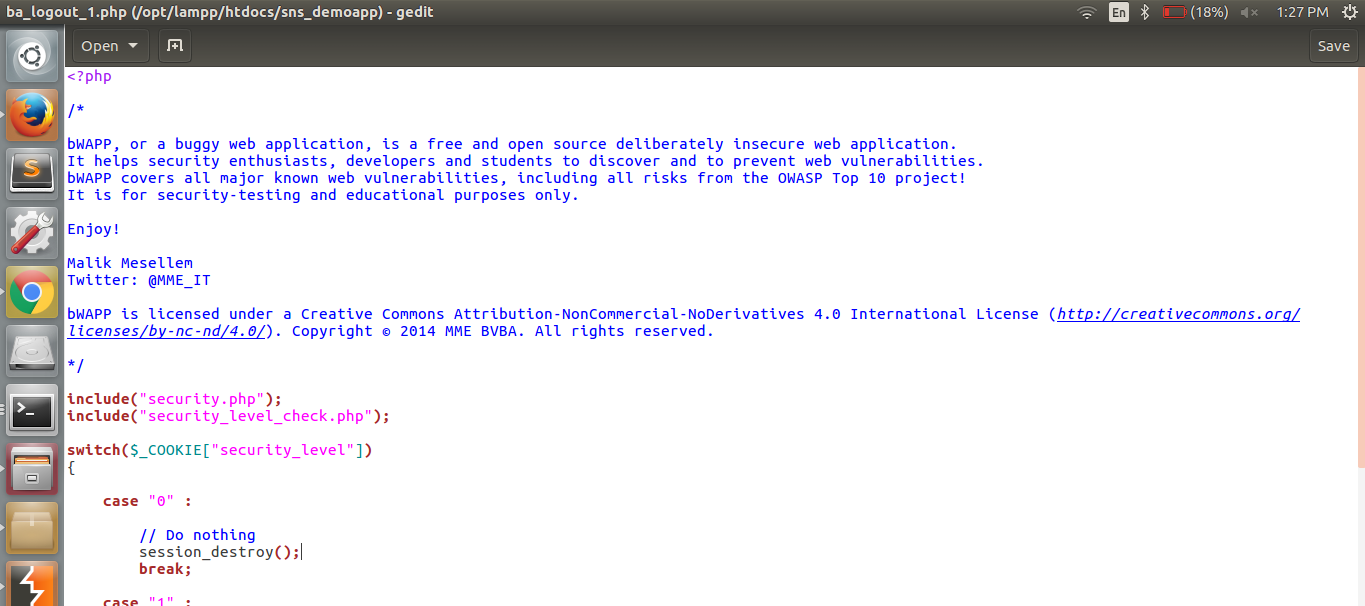
# 

# **Broken Auth. - Logout Management**

BUG: If the user as logout from the page by pressing ‘**here’.** User thinks he has successfully logged out but if some attacker presses back button it will go back to logout page as the session is not terminated.

Solution:

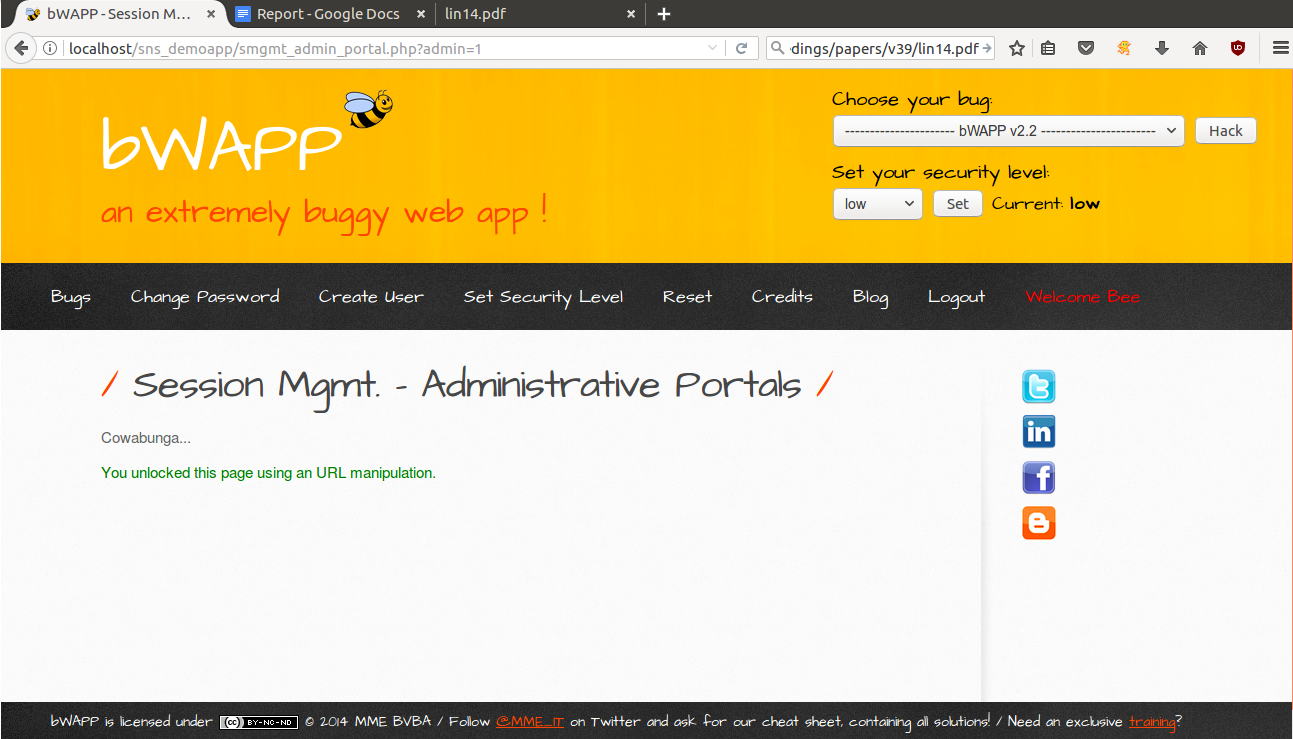
To add session\_expired() in ba\_logout\_1.php so that session gets expired after successful logout.



# 

# **Session Mgmt. - Administrative Portals:**



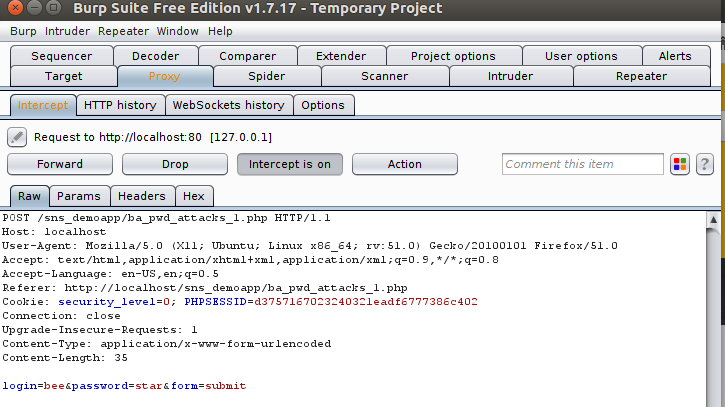


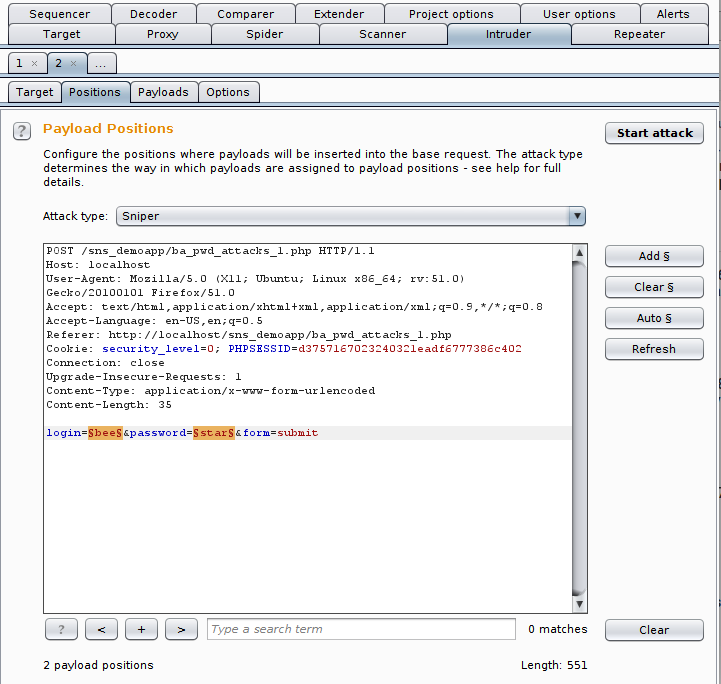
solution: We will make necessary changes in php to avoid this manipulation

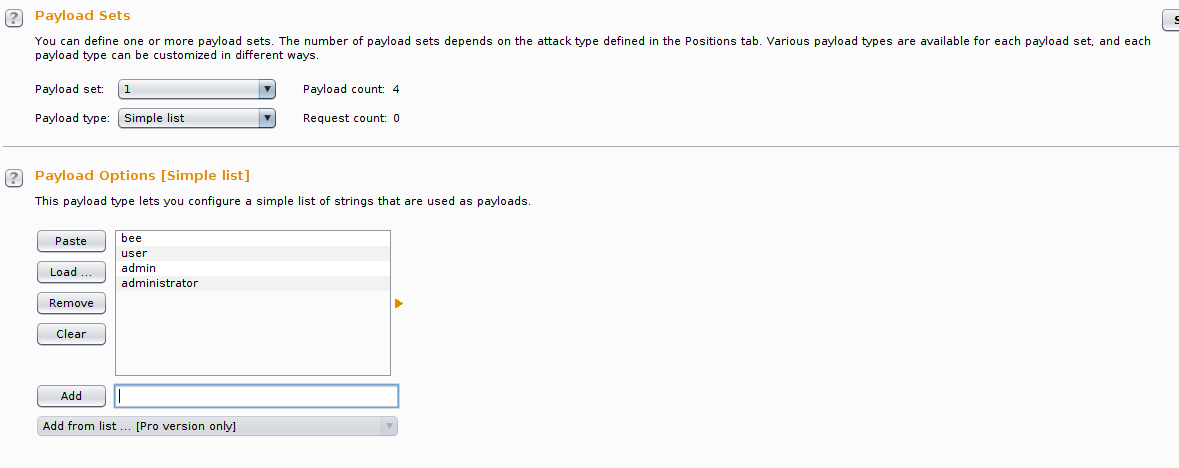


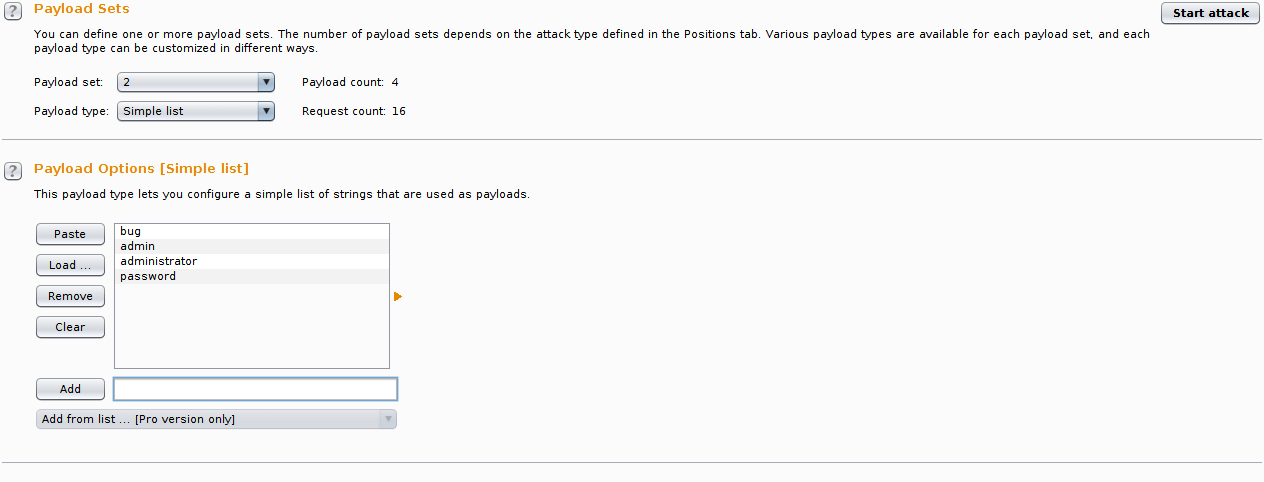
# **Broken Auth. - Password Attacks:**

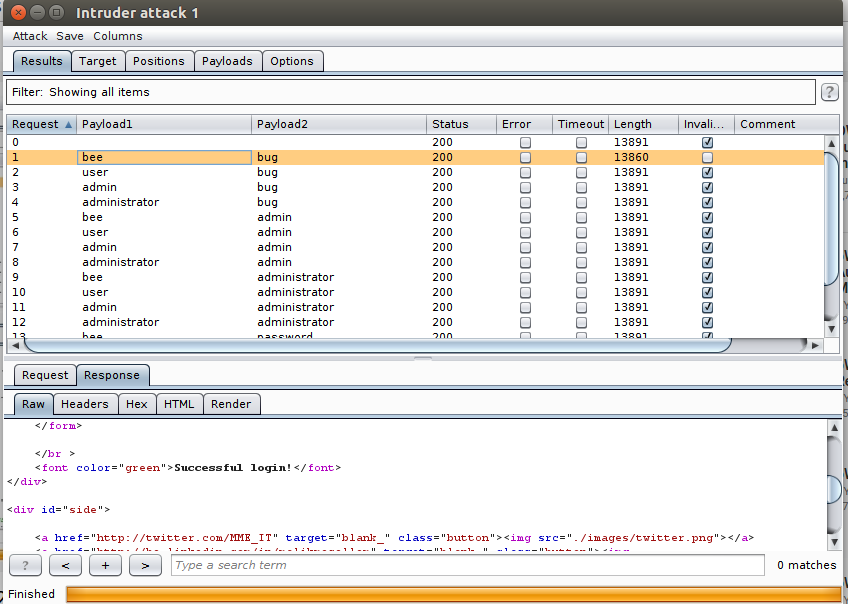


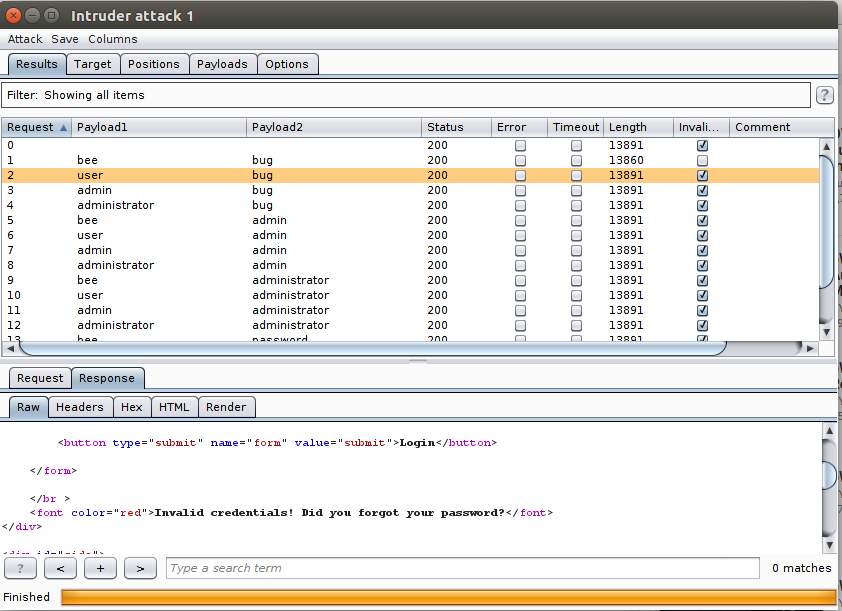


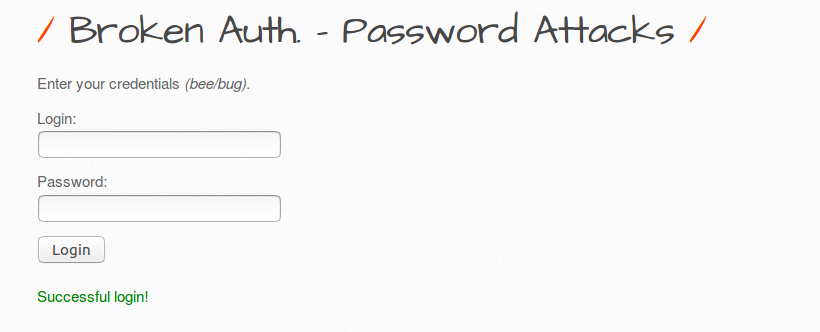












# 

# 

# **A6. Sensitive data exposure**

# **Base64 Encoding (Secret)**

