**6.2 将会话/凭证设置为有效的到期时间（会话超时时间测试）**

|  |  |
| --- | --- |
| 编号 | EdgeGallery Security Compliance Test Case 6-2 |
| Test tool | N/A |
| Test description | 查看是否存在浏览器窗口显示超时后需要重新登录的机制 |
| Configuration Steps | 1. 已知网站的地址 2. Web业务运行正常 3. Web业务存在登录认证模块 4. 一直正确的用户名口令 |
| Step 1 | 使用正常的用户名，口令登录系统 |
| Step 2 | 将浏览器窗口的闲置规定时间（11分钟）增加一分钟 |
| Step 3 | 刷新浏览器，查看是否需要重新登录  备注：也可以登录后台web服务器，查看对应的web.Xml文件中的seesion-timeout参数值，该值表示会话的超时时间。 |
| Test verdict | 会话超时时间不大于10分钟，刷新浏览器之后需要重新登录。 |
|  |  |
|  |  |

**6.4 用户注销时，会话必须无效（注销是会话信息是否清除）**

|  |  |
| --- | --- |
| 编号 | EdgeGallery Security Compliance Test Case 6-4 |
| Test tool | WebScarab |
| Test description | 注销时（logout），会话信息是否清除 |
| Configuration Steps | 1. 已知Web网站地址 2. Web业务正常运行 3. 存在注销功能的页面 |
| Step 1 | 使用正产的用户名，口令登录系统 |
| Step 2 | 开启WebScarab,配置对GET和POST请求进行拦截 |
| Step 3 | 在浏览器中配置代理服务器IP为127.0.0.1，端口为8008 |
| Step 4 | 在Web页面中进行一些操作（比如修改个人信息）， 这些操作都会被WebScarab拦截，不修改，在弹出的WebScarab界面中点击”Accept Changes”  按钮。这样请求就被WebScarab记录下来 |
| Step 5 | 然后在Web页面中点击注销 |
| Step 6 | 点击WebScarab的“Manual Request”TAB页，在Previous Requests的下拉列表框中选择“步骤4”所产生的URL请求，然后点击”Fetch Response” 重新发送“步骤4”的URL 请求 |
| Step 7 | 在WebScarab的Response的“Raw”Tab页中观察返回结果，如果还能够正常完成“步骤4”的操作，则存在安全漏洞 |
| Test verdict | 在WebScarab的Response的“Raw Tab”页中显示“HTTP/101 302 Moved Temporarily”,不能够访问只有登录才能访问的页面，不能完成只有登录才能完成的工作 |
| Remark | 如果存在多个注销功能的页面，要重复测试过程吧所有注销功能的页面测试完 |

**6.1 验证用户身份（注销是会话信息是否清除）**