


Authentication_Change_Password_Finding - Findings Report

Oct 26, 2007 7:07:24 PM

| Classification | Type | Severity | File | Line | CWE ID | SmartTrace |
|----------------|----------------|---|--|------|--------|---|
| Vulnerability | Authentication |  | Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\auth\UserManager.java | 342 | 287 |  |

Description:

The change password process does not require the user to enter his original password. If an attacker has hijacked the victims session or the victim has left his machine unlocked and an attacker has access to his machine with a valid JSPWiki session up, an attacker can change the victims password.

Recommendation:

Consider forcing the user to re-enter their original passwords to prevent attackers who have compromised the users session to also change his password and 1. gain unbound account access and 2. DOS the victim.

```
// Extract values from request stream (cleanse whitespace as needed)
String loginName = request.getParameter( "loginname" );
String password = request.getParameter( "password" );
String wikiname = request.getParameter( "wikiname" );
String fullname = request.getParameter( "fullname" );
String email = request.getParameter( "email" );
loginName = InputValidator.isBlank( loginName ) ? null : loginName;
password = InputValidator.isBlank( password ) ? null : password;
wikiname = InputValidator.isBlank( wikiname ) ? null : wikiname.replaceAll( "\\s", "" );
fullname = InputValidator.isBlank( fullname ) ? null : fullname;
```

| | | | | | | |
|---------------|----------------|---|--|-----|-----|---|
| Vulnerability | Authentication |  | Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\auth\UserManager.java | 341 | 287 |  |
|---------------|----------------|---|--|-----|-----|---|

Description:

The change password process does not require the user to enter his original password. If an attacker has hijacked the victims session or the victim has left his machine unlocked and an attacker has access to his machine with a valid JSPWiki session up, an attacker can change the victims password.

Recommendation:

Consider forcing the user to re-enter their original passwords to prevent attackers who have compromised the users session to also change his password and 1. gain unbound account access and 2. DOS the victim.

```
HttpServletRequest request = context.getHttpRequest();

// Extract values from request stream (cleanse whitespace as needed)
String loginName = request.getParameter( "loginname" );
String password = request.getParameter( "password" );
String wikiname = request.getParameter( "wikiname" );
String fullname = request.getParameter( "fullname" );
String email = request.getParameter( "email" );
loginName = InputValidator.isBlank( loginName ) ? null : loginName;
```

```
password = InputValidator.isBlank( password ) ? null : password;
wikiname = InputValidator.isBlank( wikiname ) ? null : wikiname.replaceAll( "\\s", "" );
```

Vulnerability Authentication



Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\auth\UserManager.java

339

287



Description:

The change password process does not require the user to enter his original password. If an attacker has hijacked the victims session or the victim has left his machine unlocked and an attacker has access to his machine with a valid JSPWiki session up, an attacker can change the victims password.

Recommendation:

Consider forcing the user to re-enter their original passwords to prevent attackers who have compromised the users session to also change his password and 1. gain unbound account access and 2. DOS the victim.

```
// Retrieve the user's profile (may have been previously cached)
UserProfile profile = getUserProfile( context.getWikiSession() );
HttpServletRequest request = context.getHttpRequest();

// Extract values from request stream (cleanse whitespace as needed)
String loginName = request.getParameter( "loginname" );
String password = request.getParameter( "password" );
String wikiname = request.getParameter( "wikiname" );
String fullname = request.getParameter( "fullname" );
String email = request.getParameter( "email" );
loginName = InputValidator.isBlank( loginName ) ? null : loginName;
```

Vulnerability Authentication



Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\auth\UserManager.java

201

287

Description:

The change password process does not require the user to enter his original password. If an attacker has hijacked the victims session or the victim has left his machine unlocked and an attacker has access to his machine with a valid JSPWiki session up, an attacker can change the victims password.

Recommendation:

Consider forcing the user to re-enter their original passwords to prevent attackers who have compromised the users session to also change his password and 1. gain unbound account access and 2. DOS the victim.

```
if ( newProfile )
{
    profile = m_database.newProfile();
    if ( user != null )
    {
        profile.setLoginName( user.getName() );
    }
    if ( !profile.isNew() )
    {
        throw new IllegalStateException(
            "New profile should be marked 'new'. Check your UserProfile implementation." );
    }
}
```

Vulnerability Authentication



Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\auth\UserManager.java

355

287

Description:

The change password process does not require the user to enter his original password. If an attacker has hijacked the victims session or the victim has left his machine unlocked and an attacker has access to his machine with a valid JSPWiki session up, an attacker can change the victims password.

Recommendation:

Consider forcing the user to re-enter their original passwords to prevent attackers who have compromised the users session to also change his password and 1. gain unbound account access and 2. DOS the victim.

```
// A special case if we have container authentication
if ( m_engine.getAuthenticationManager().isContainerAuthenticated() )
{
    // If authenticated, login name is always taken from container
    if ( context.getWikiSession().isAuthenticated() ) {
        loginName = context.getWikiSession().getLoginPrincipal().getName();
    }
}

if ( profile.isNew() )
{
```

Vulnerability Authentication



Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\auth\UserManager.java

188

287

Description:

The change password process does not require the user to enter his original password. If an attacker has hijacked the victims session or the victim has left his machine unlocked and an attacker has access to his machine with a valid JSPWiki session up, an attacker can change the victims password.

Recommendation:

Consider forcing the user to re-enter their original passwords to prevent attackers who have compromised the users session to also change his password and 1. gain unbound account access and 2. DOS the victim.

```
if ( session.isAuthenticated() )
{
    user = session.getUserPrincipal();
    try
    {
        profile = m_database.find( user.getName() );
        newProfile = false;
    }
    catch( NoSuchPrincipalException e )
    {
    }
}
```

Vulnerability Authentication



Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\web-root\JSPWiki.war\UserPreferences.jsp

28

287

Description:

The change password process does not require the user to enter his original password. If an attacker has hijacked the victims session or the victim has left his machine unlocked and an attacker has access to his machine with a valid JSPWiki session up, an attacker can change the victims password.

Recommendation:

Consider forcing the user to re-enter their original passwords to prevent attackers who have compromised the users session to also change his password and 1. gain unbound account access and 2. DOS the victim.

```
// Extract the user profile and action attributes
userManager userManager = wiki.getUserManager();
WikiSession wikiSession = wikiContext.getWikiSession();
// Are we saving the profile?
if( "saveProfile".equals(request.getParameter("action")) )
{
    UserProfile profile = userManager.parseProfile( wikiContext );
    // Validate the profile
    userManager.validateProfile( wikiContext, profile );
}
```