


Findings Report

Classification	Type	Severity	File	Line	CWE ID	SmartTrace
Vulnerability	Validation.Required		Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\attachment\AttachmentServlet.java	414	20	
<div>Description: The attachment servlet uses a "nextpage" parameter to determine where the user is redirected to after the attachment process completes. This nextpage parameter is not validated to ensure that the user is not redirected outside the context of the application. If an attacker can trick a victim into interacting with and posting his malicious "nextpage" parameter, the victim will be redirect to the attacker-controlled site, leading to potential phishing attacks. The victim would see that the original request goes to the appropriate JSPWiki location (http://localhost:8080/JSPWiki/attach) and not realize he was maliciously redirected.</div> <div>Exploit HTTP POST: 1. Note the "nextpage" value contains a value outside the web context of this application and could be that of a malicious location. POST http://localhost:8080/JSPWiki/attach HTTP/1.1 Host: localhost:8080 User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1.8) Gecko/20071008 Firefox/2.0.0.8 Accept: text/xml,application/xml,application/xhtml+xml;text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5 Accept-Language: en-us,en;q=0.5 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 300 Proxy-Connection: keep-alive Referer: http://localhost:8080/JSPWiki/Upload.jsp?page=Main Cookie: JSPWikiAssertedName=127.0.0.1; JSESSIONID=285A5DB7AAE9476B56A653FDCB77C9B7 Content-Type: multipart/form-data; boundary=-----2132026317541759772579111 Content-Length: 813 -----2132026317541759772579111 Content-Disposition: form-data; name="page" Main -----2132026317541759772579111 Content-Disposition: form-data; name="content"; filename="test3" Content-Type: application/octet-stream test -----2132026317541759772579111 Content-Disposition: form-data; name="upload" Upload</div>						

-----2132026317541759772579111

Content-Disposition: form-data; name="action"

upload

-----2132026317541759772579111

Content-Disposition: form-data; name="changenote"

-----2132026317541759772579111

Content-Disposition: form-data; name="nextpage"

<http://www.ouncelabs.com>

-----2132026317541759772579111--

Recommendation:

Validate that the "nextpage" value is that of an acceptable location. For example, maybe it should be confined the host running the JSPWiki site, or even compared to that of list of valid redirection/host locations.

```
{
    try
    {
        String nextPage = upload( req );
        req.getSession().removeAttribute( "msg" );
        res.sendRedirect( nextPage );
    }
    catch( RedirectException e )
    {
        WikiSession session = WikiSession.getWikiSession( m_engine, req );
        session.addMessage( e.getMessage() );
    }
}
```

Vulnerability Validation.Required



Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\attachment\AttachmentServlet.java

493

20



Description:

The attachment servlet uses a "nextpage" parameter to determine where the user is redirected to after the attachment process completes. This nextpage parameter is not validated to ensure that the user is not redirected outside the context of the application. If an attacker can trick a victim into interacting with and posting his malicious "nextpage" parameter, the victim will be redirect to the attacker-controlled site, leading to potential phishing attacks. The victim would see that the original request goes to the appropriate JSPWiki location (<http://localhost:8080/JSPWiki/attach>) and not realize he was maliciously redirected.

Exploit HTTP POST:

1. Note the "nextpage" value contains a value outside the web context of this application and could be that of a malicious location.

POST <http://localhost:8080/JSPWiki/attach> HTTP/1.1

Host: localhost:8080

User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1.8) Gecko/20071008 Firefox/2.0.0.8

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5

Accept-Language: en-us,en;q=0.5

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Proxy-Connection: keep-alive

Referer: <http://localhost:8080/JSPWiki/Upload.jsp?page=Main>

Cookie: JSPWikiAssertedName=127.0.0.1; JSESSIONID=285A5DB7AAE9476B56A653FDCB77C9B7

Content-Type: multipart/form-data; boundary=-----2132026317541759772579111

Content-Length: 813

-----2132026317541759772579111

Content-Disposition: form-data; name="page"

Main
-----2132026317541759772579111
Content-Disposition: form-data; name="content"; filename="test3"
Content-Type: application/octet-stream

test

-----2132026317541759772579111
Content-Disposition: form-data; name="upload"

Upload

-----2132026317541759772579111
Content-Disposition: form-data; name="action"

upload

-----2132026317541759772579111
Content-Disposition: form-data; name="changenote"

-----2132026317541759772579111
Content-Disposition: form-data; name="nextpage"

<http://www.ouncelabs.com>

-----2132026317541759772579111--

Recommendation:

Validate that the "nextpage" value is that of an acceptable location. For example, maybe it should be confined the host running the JSPWiki site, or even compared to that of list of valid redirection/host locations.

```
// Create the context _before_ Multipart operations, otherwise
// strict servlet containers may fail when setting encoding.
WikiContext context = m_engine.createContext( req, WikiContext.ATTACH );
multi = new MultipartRequest( null, // no debugging
                             req.getContentType(),
                             req.getContentLength(),
                             req.getInputStream(),
                             m_tmpDir,
                             Integer.MAX_VALUE,
```

Vulnerability

Validation.Required



Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\attachment\AttachmentServlet.java

299

20



Description:

The attachment servlet uses a "nextpage" parameter to determine where the user is redirected to after the attachment process completes. This nextpage parameter is not validated to ensure that the user is not redirected outside the context of the application. If an attacker can trick a victim into interacting with and posting his malicious "nextpage" parameter, the victim will be redirect to the attacker-controlled site, leading to potential phishing attacks. The victim would see that the original request goes to the appropriate JSPWiki location (<http://localhost:8080/JSPWiki/attach>) and not realize he was maliciously redirected.

Exploit HTTP POST:

1. Note the "nextpage" value contains a value outside the web context of this application and could be that of a malicious location.

POST <http://localhost:8080/JSPWiki/attach> HTTP/1.1

Host: localhost:8080

User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1.8) Gecko/20071008 Firefox/2.0.0.8

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5

Accept-Language: en-us,en;q=0.5

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Proxy-Connection: keep-alive
Referer: <http://localhost:8080/JSPWiki/Upload.jsp?page=Main>
Cookie: JSPWikiAssertedName=127.0.0.1; JSESSIONID=285A5DB7AAE9476B56A653FDCB77C9B7
Content-Type: multipart/form-data; boundary=-----2132026317541759772579111
Content-Length: 813

-----2132026317541759772579111

Content-Disposition: form-data; name="page"

Main

-----2132026317541759772579111

Content-Disposition: form-data; name="content"; filename="test3"

Content-Type: application/octet-stream

test

-----2132026317541759772579111

Content-Disposition: form-data; name="upload"

Upload

-----2132026317541759772579111

Content-Disposition: form-data; name="action"

upload

-----2132026317541759772579111

Content-Disposition: form-data; name="changenote"

-----2132026317541759772579111

Content-Disposition: form-data; name="nextpage"

<http://www.ouncelabs.com>

-----2132026317541759772579111--

Recommendation:

Validate that the "nextpage" value is that of an acceptable location. For example, maybe it should be confined the host running the JSPWiki site, or even compared to that of list of valid redirection/host locations.

```
if(log.isDebugEnabled())
{
    msg = "Attachment "+att.getFileName()+" sent to "+req.getRemoteUser()+" on "+req.getRemoteAddr();
    log.debug( msg );
}
if( nextPage != null ) res.sendRedirect( nextPage );
return;
}
msg = "Attachment '" + page + "', version " + ver +
```

Vulnerability Validation.Required



Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\attachment\AttachmentServlet.java

422

20

Description:

The attachment servlet uses a "nextpage" parameter to determine where the user is redirected to after the attachment process completes. This nextpage parameter is not validated to ensure that the user is not redirected outside the context of the application. If an attacker can trick a victim into interacting with and posting his malicious "nextpage" parameter, the victim will be redirect to the attacker-controlled site, leading to potential phishing attacks. The victim would see that the original request goes to the appropriate JSPWiki location (<http://localhost:8080/JSPWiki/attach>) and not realize he was maliciously redirected.

Exploit HTTP POST:

1. Note the "nextpage" value contains a value outside the web context of this application and could be that of a malicious location.

POST <http://localhost:8080/JSPWiki/attach> HTTP/1.1

Host: localhost:8080

User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1.8) Gecko/20071008 Firefox/2.0.0.8

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5

Accept-Language: en-us,en;q=0.5

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Proxy-Connection: keep-alive

Referer: <http://localhost:8080/JSPWiki/Upload.jsp?page=Main>

Cookie: JSPWikiAssertedName=127.0.0.1; JSESSIONID=285A5DB7AAE9476B56A653FDCB77C9B7

Content-Type: multipart/form-data; boundary=-----2132026317541759772579111

Content-Length: 813

-----2132026317541759772579111

Content-Disposition: form-data; name="page"

Main

-----2132026317541759772579111

Content-Disposition: form-data; name="content"; filename="test3"

Content-Type: application/octet-stream

test

-----2132026317541759772579111

Content-Disposition: form-data; name="upload"

Upload

-----2132026317541759772579111

Content-Disposition: form-data; name="action"

upload

-----2132026317541759772579111

Content-Disposition: form-data; name="changenote"

-----2132026317541759772579111

Content-Disposition: form-data; name="nextpage"

<http://www.ouncelabs.com>

-----2132026317541759772579111--

Recommendation:

Validate that the "nextpage" value is that of an acceptable location. For example, maybe it should be confined the host running the JSPWiki site, or even compared to that of list of valid redirection/host locations.

```
{
    WikiSession session = WikiSession.getWikiSession( m_engine, req );
    session.addMessage( e.getMessage() );

    req.getSession().setAttribute( "msg", e.getMessage() );
    res.sendRedirect( e.getRedirect() );
}
```

```
public void doPut( HttpServletRequest req, HttpServletResponse res )  
    throws IOException, ServletException
```