

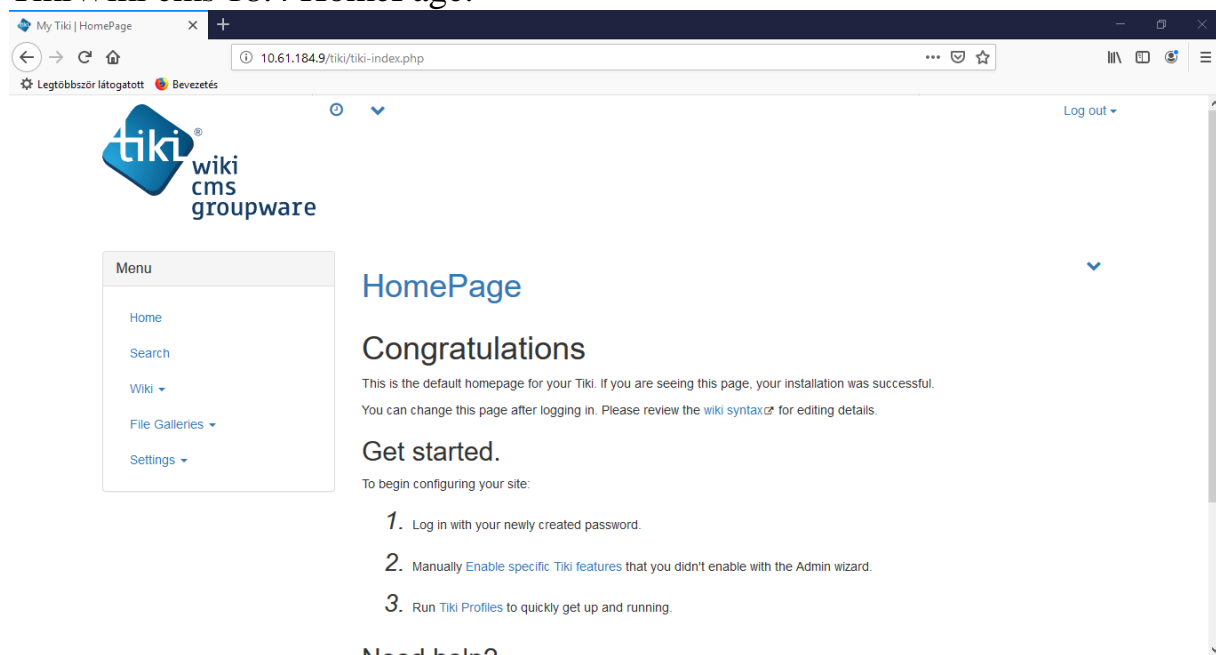
CVE-2019-15314

TikiWiki cms 18.4 Cross Site Scripting [XSS]

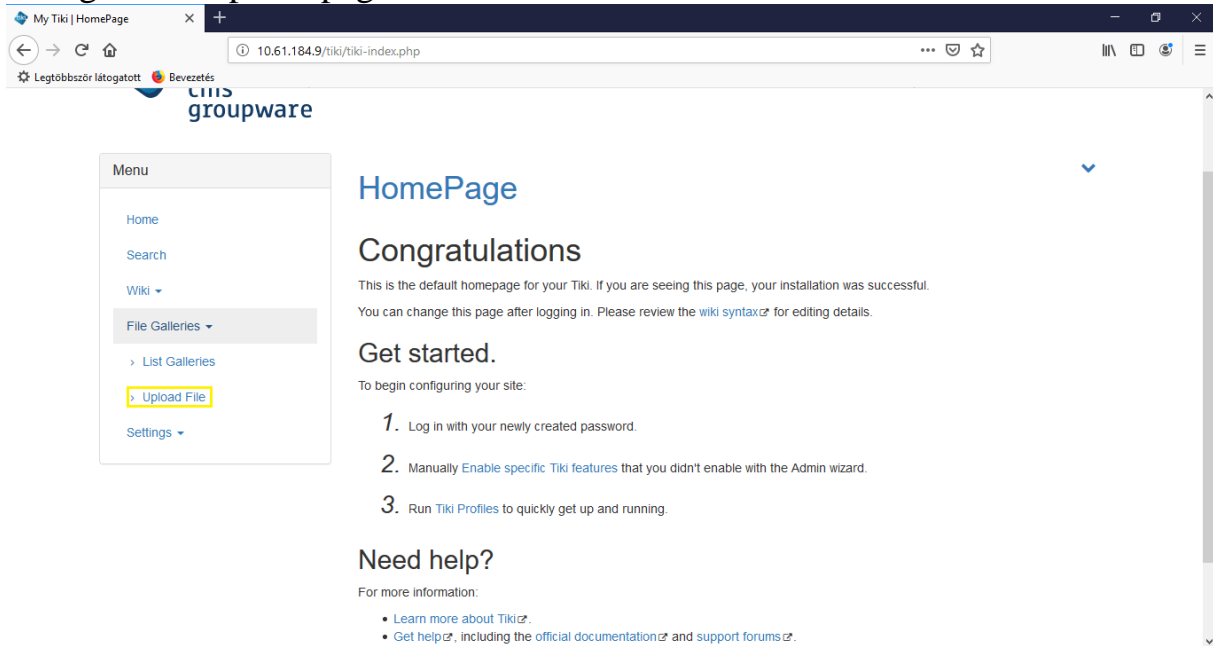
tiki-upload_file.php in Tiki 18.4 allows remote attackers to upload JavaScript code that is executed upon visiting a [tiki/tiki-download_file.php?display&fileId= URI].

File upload and JavaScript code injection.

TikiWiki cms 18.4 HomePage.

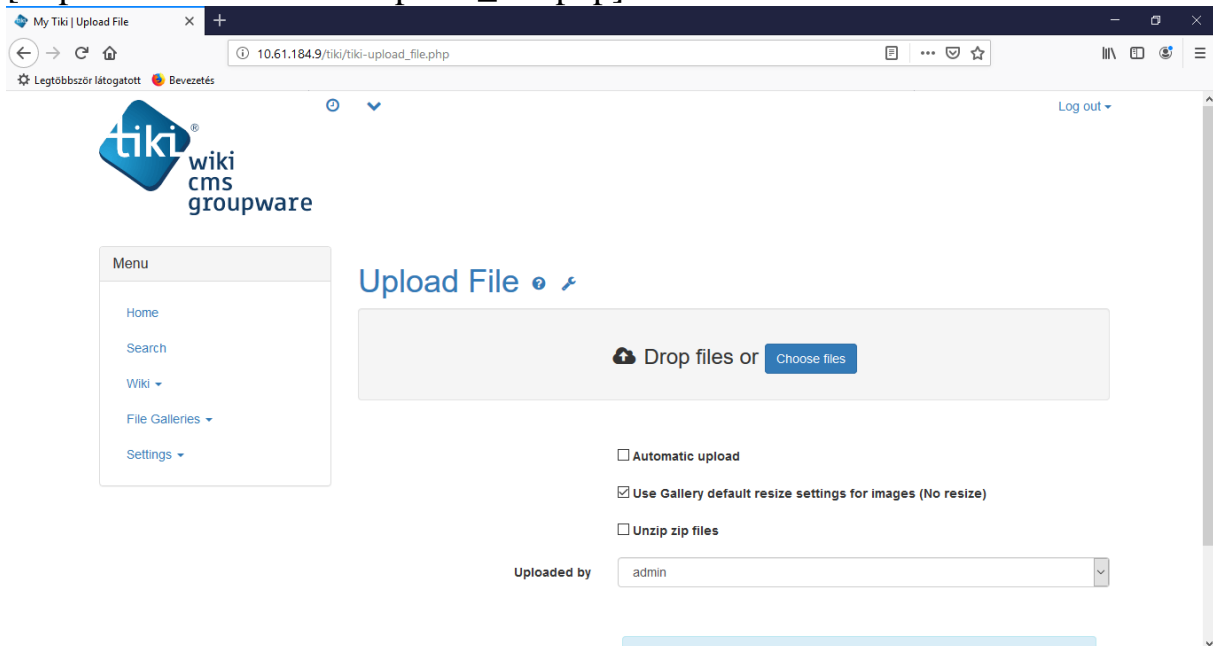


Navigate file upload page.



The screenshot shows the Tiki Wiki CMS groupware homepage. The browser address bar displays "10.61.184.9/tiki-index.php". The page features a "Menu" sidebar on the left with options: Home, Search, Wiki, File Galleries (expanded), List Galleries, Upload File (highlighted with a yellow box), and Settings. The main content area has a "HomePage" heading, followed by "Congratulations" and a message stating: "This is the default homepage for your Tiki. If you are seeing this page, your installation was successful. You can change this page after logging in. Please review the [wiki syntax](#) for editing details." Below this is a "Get started." section with instructions: "To begin configuring your site: 1. Log in with your newly created password. 2. Manually [Enable specific Tiki features](#) that you didn't enable with the Admin wizard. 3. Run [Tiki Profiles](#) to quickly get up and running." A "Need help?" section provides links to "Learn more about Tiki" and "Get help", including the official documentation and support forums.

[http://localhost/tiki/tiki-upload_file.php]



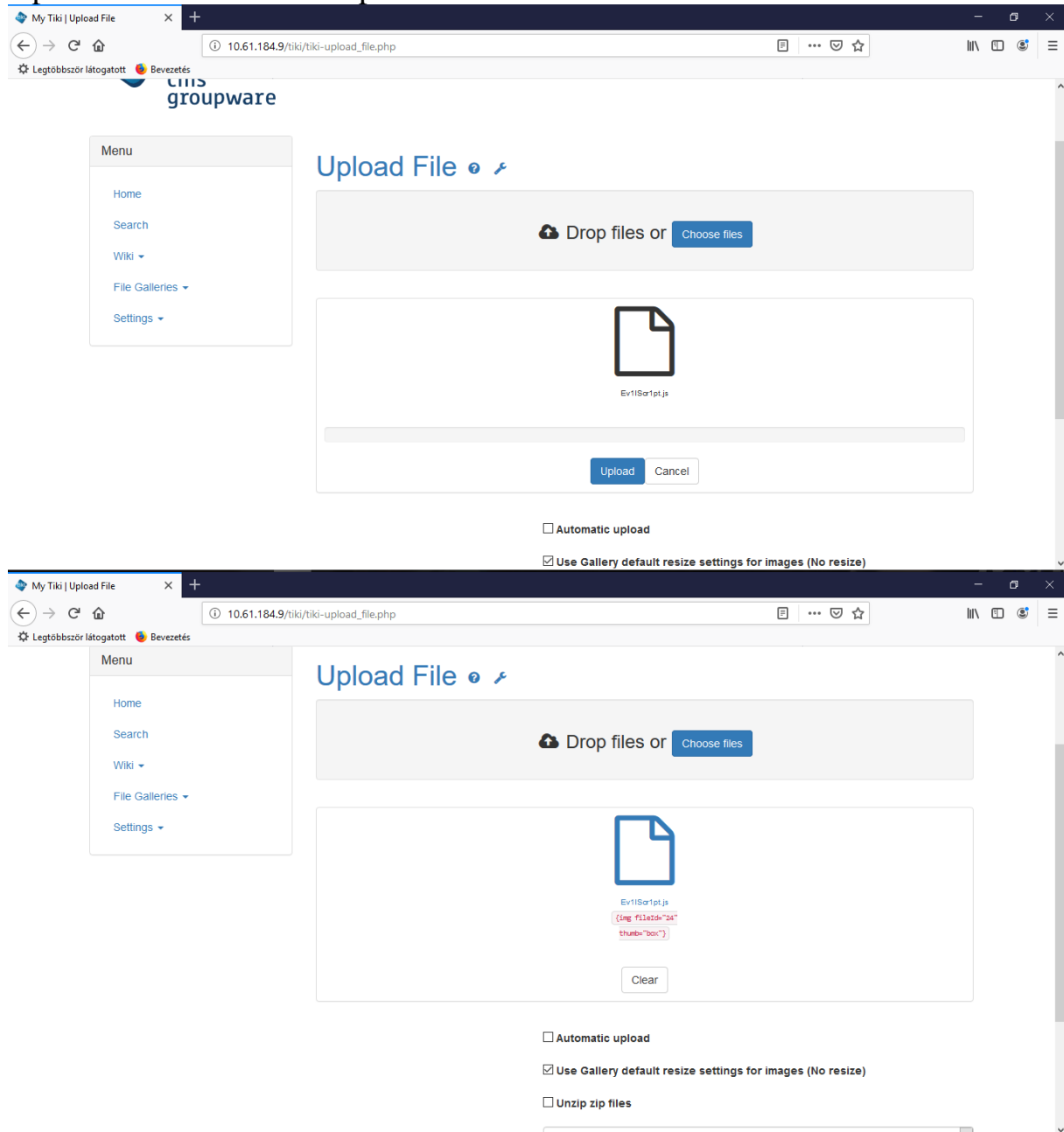
The screenshot shows the Tiki Wiki CMS groupware file upload page. The browser address bar displays "10.61.184.9/tiki-upload_file.php". The page features a "Menu" sidebar on the left with options: Home, Search, Wiki, File Galleries, and Settings. The main content area has an "Upload File" heading. Below the heading is a large gray box with the text "Drop files or" and a "Choose files" button. To the right of this box are three checkboxes: "Automatic upload" (unchecked), "Use Gallery default resize settings for images (No resize)" (checked), and "Unzip zip files" (unchecked). At the bottom, there is a label "Uploaded by" followed by a dropdown menu showing "admin".

[Ev1lScr1pt.js]

```
Ev1lScr1pt.txt x
```

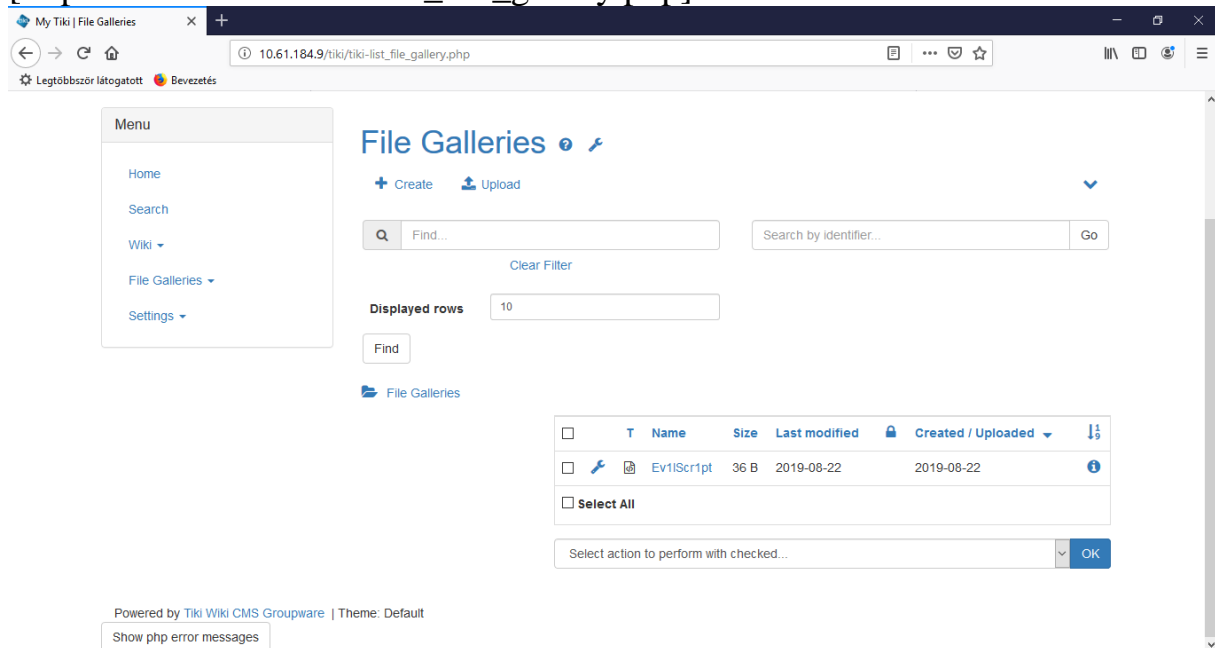
```
1 <script>alert("PWN3D!")</script>
```

Upload malicious JavaScript file.



Running an uploaded file.

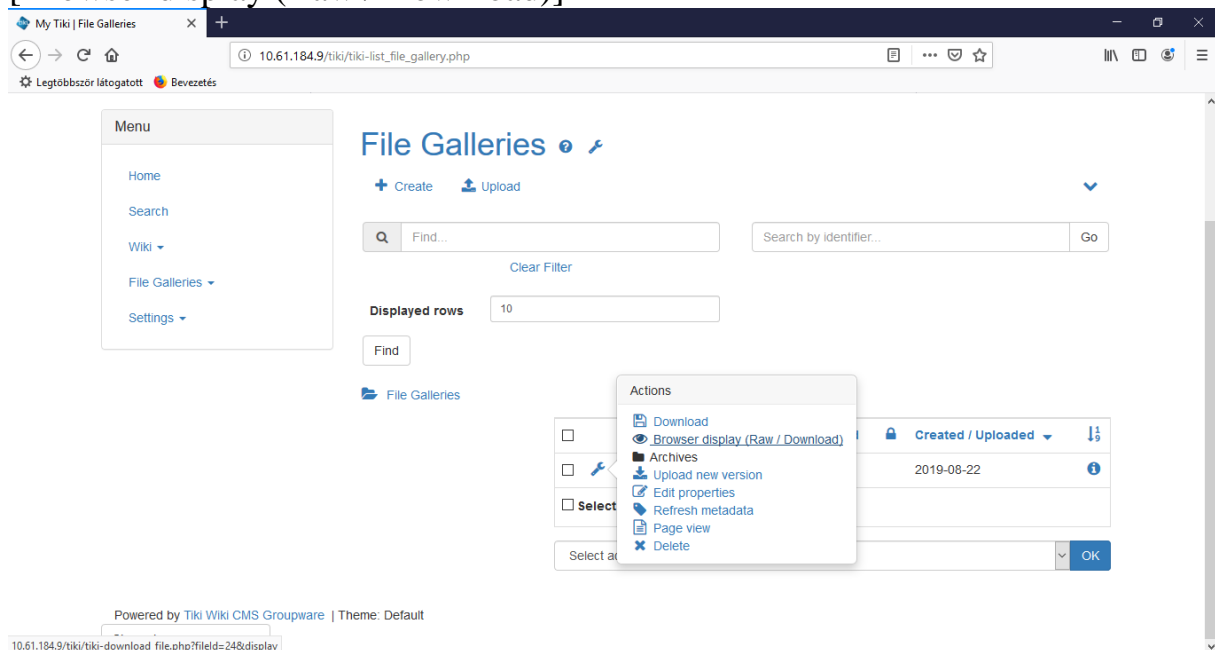
[http://localhost/tiki/tiki-list_file_gallery.php]



The screenshot shows the Tiki File Galleries interface. On the left is a menu with links: Home, Search, Wiki, File Galleries (selected), and Settings. The main area is titled "File Galleries" and includes buttons for "Create" and "Upload". There are search bars for "Find..." and "Search by identifier...", a "Clear Filter" link, and a "Displayed rows" dropdown set to 10. A "Find" button is present. Below the search area is a table of files. The first file is "Ev1Scr1pt" with a size of 36 B, last modified on 2019-08-22, and created/uploaded on 2019-08-22. Below the table is a "Select All" checkbox and a "Select action to perform with checked..." dropdown with an "OK" button. At the bottom, it says "Powered by Tiki Wiki CMS Groupware | Theme: Default" and a "Show php error messages" button.

| <input type="checkbox"/> | T | Name | Size | Last modified | Created / Uploaded | |
|--------------------------|------------|-----------|------|---------------|--------------------|--|
| <input type="checkbox"/> | | Ev1Scr1pt | 36 B | 2019-08-22 | 2019-08-22 | |
| <input type="checkbox"/> | Select All | | | | | |

[Browser display (Raw / Download)]



This screenshot is similar to the previous one, but with the "Actions" menu open for the selected file "Ev1Scr1pt". The menu options are: Download, Browser display (Raw / Download) (highlighted), Archives, Upload new version, Edit properties, Refresh metadata, Page view, and Delete. The rest of the interface remains the same.

| <input type="checkbox"/> | T | Name | Size | Last modified | Created / Uploaded | |
|--------------------------|------------|-----------|------|---------------|--------------------|--|
| <input type="checkbox"/> | | Ev1Scr1pt | 36 B | 2019-08-22 | 2019-08-22 | |
| <input type="checkbox"/> | Select All | | | | | |

[http://localhost/tiki/tiki-download_file.php?fileId=24&display]

