**Malware Removal Report for Ship-Parts Military Boats Website (Task 2)**

**Performed by Julie Haynes**

In March 2019 the following activities were conducted on the <http://www.shipparts.sup> website:

1. Location and removal of malware
2. Removal of LFI vulnerability by application of a secure patch

Details of how these fixes were implemented are included below.

1. **Location and Removal of Malware**

PuTTY was used to connect to the Shipparts website using SSH. I used “cd/” to get to the root directory and then explored all the directories from the root. Using the Linux commands of “pwd”, “find”, and “ls” I was able to eventually locate the following two files:

* “index.php” in the directory /var/www/html
* “cyberO.js” in the directory /var/www/html/libs/scripts

I viewed the contents of “index.php” using PuTTY. It contained a line of code that I suspected might be calling the malware. That line was *<script src= “libs/scripts/cyberO.js”?</script>*. I then used PuTTY to view the “cyberO.js” file and it contained obfuscated code (see example below):

*/\* tweetyfish do u think the ukrainian bozos could do this \*/ var \_0xb390=["\x73\x65\x74\x54\x69\x6D\x65\x6F\x75\x74","\x73\x68\x6F\x77","\x23\x61\x6C\x65\x72\x74","\x66\x61\x64\x65\x49\x6E","\x23\x73\x68\x69\x65\x6C\x64","\x61\x70\x70\x65\x6E\x64","\x62\x6F\x64\x79","\x23\x61\x6C\x65\x72\x74\x33","\x3C\x64\x69\x76\x20\x63\x6C\x61\x73\x73\x3D\x22\x74\x61\x6C\x22\x3E\x57\x68\x79\x20\x64\x69\x64\x20\x79\x6F\x75\x20\x63\x6C\x69\x63\x6B\x20\x74\x68\x61\x74\x20\x62\x75\x74\x74\x6F\x6E\x3F\x20\x20\x59\x6F\x75\x20\x74\x68\x69\x6E\x6B\x20\x73\x6F\x6D\x65\x74\x68\x69\x6E\x67\x20\x69\x73\x20\x73\x61\x66\x65\x20\x62\x65\x63\x61\x75\x73\x65\x20\x69\x74\x20\x3C\x73\x70\x61\x6E\x20\x63\x6C\x61\x73\x73\x3D\x22\x69\x74\x22\x3E\x6C\x6F\x6F\x6B\x73\x3C\x2F\x73\x70\x61\x6E\x3E\x20\x6C\x69\x6B\x65\x20\x61\x20\x73\x65\x63\x75\x72\x69\x74\x79\x20\x64\x69\x61\x6C\x6F\x67\x3F\x20\x20\x59\x6F\x75\x20\x68\x61\x76\x65\x20\x62\x65\x65\x6E\x20\x68\x61\x63\x6B\x65\x64\x21\x3C\x2F\x64\x69\x76\x3E","\x68\x74\x6D\x6C","\x68\x69\x64\x65","\x23\x6D\x73\x67","\x3C\x64\x69\x76\x20\x69\x64\x3D\x22\x73\x68\x69\x65\x6C\x64\x22\x20\x63\x6C\x61\x73\x73\x3D\x22\x70\x66\x69\x78\x65\x64\x20\x74\x30\x20\x6C\x30\x20\x77\x31\x30\x30\x20\x68\x31\x30\x30\x20\x62\x63\x62\x6C\x22\x20\x73\x74\x79\x6C\x65\x3D\x22\x6F\x70\x61\x63\x69\x74\x79\x3A\x2E\x35\x3B\x64\x69\x73\x70\x6C\x61\x79\x3A\x6E\x6F\x6E\x65\x3B\x22\x3E\x3C\x2F\x64\x69\x76\x3E\x0D\x3C\x64\x69\x76\x20\x69\x64\x3D\x22\x61\x6C\x65\x72\x74\x22\x20\x63\x6C\x61\x73\x73\x3D\x22\x64\x66\x72\x20\x66\x72\x76\x61\x6D\x20\x66\x72\x74\x61\x63\x20\x70\x66\x69\x78\x65\x64\x20\x74\x30\x20\x6C\x30\x20\x77\x31\x30\x30\x20\x68\x31\x30\x30\x22\x20\x73\x74\x79\x6C\x65\x3D\x22\x7A\x2D\x69\x6E\x64\x65\x78\x3A\x32\x3B\x64\x69\x73\x70\x6C\x61\x79\x3A\x6E\x6F\x6E\x65\x22\x3E\x0D\x09\x3C\x64\x69\x76\x20\x63\x6C\x61\x73\x73\x3D\x22\x70\x72\x65\x6C\x22\x20\x73\x74\x79\x6C\x65\x3D\x22\x77\x69\x64\x74\x68\x3A\x35\x33\x30\x70\x78\x3B\x22\x3E\x0D\x20\x20\x20\x20\x09\x3C\x69\x6D\x67\x20\x63\x6C\x61\x73\x73\x3D\x22\x77\x31\x30\x30\x22\x20\x73\x72\x63\x3D\x22\x6C\x69\x62\x73\x2F\x69\x6D\x61\x67\x65\x73\x2F\x66\x6C\x61\x73\x68\x2E\x70\x6E\x67\x22\x20\x2F\x3E\x0D\x20\x20\x20\x20\x20\x20\x20\x20\x3C\x64\x69\x76\x20\x69\x64\x3D\x22\x64\x69\x61\x6C\x6F\x67\x22\x20\x63\x6C\x61\x73\x73\x3D\x22\x7A\x70\x31\x30\x20\x7A\x64\x69\x61\x6C\x6F\x67\x22\x3E\x0D\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x3C\x64\x69\x76\x20\x63\x6C\x61\x73\x73\x3D\x22\x70\x61\x62\x73\x20\x62\x30\x20\x72\x30\x20\x77\x31\x30\x30\x20\x74\x61\x72\x20\x70\x6C\x35\x30\x20\x70\x72\x35\x30\x22\x20\x73\x74\x79\x6C\x65\x3D\x22\x62\x6F\x74\x74\x6F\x6D\x3A\x33\x35\x70\x78\x3B\x22\x3E\x0D\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x09\x3C\x64\x69\x76\x20\x63\x6C\x61\x73\x73\x3D\x22\x22\x20\x69\x64\x3D\x22\x6D\x73\x67\x22\x20\x73\x74\x79\x6C\x65\x3D\x22\x6D\x61\x72\x67\x69\x6E\x3A\x30\x70\x78\x20\x30\x70\x78\x22\x3E\x0D\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x09\x3C\x64\x69\x76\x20\x63\x6C\x61\x73\x73\x3D\x22\x62\x74\x32\x20\x68\x73\x20\x6D\x72\x31\x35\x22\x20\x6F\x6E\x63\x6C\x69\x63\x6B\x3D\x22\x6D\x79\x43\x6C\x69\x63\x6B\x32\x28\x29\x3B\x22\x3E\x4C\x61\x74\x65\x72\x3C\x2F\x64\x69\x76\x3E\x0D\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x09\x3C\x64\x69\x76\x20\x63\x6C\x61\x73\x73\x3D\x22\x62\x74\x32\x20\x68\x73\x22\x20\x6F\x6E\x63\x6C\x69\x63\x6B\x3D\x22\x6D\x79\x43\x6C\x69\x63\x6B\x32\x28\x29\x3B\x22\x3E\x44\x6F\x77\x6E\x6C\x6F\x61\x64\x3C\x2F\x64\x69\x76\x3E\x0D\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x09\x3C\x2F\x64\x69\x76\x3E\x0D\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x3C\x2F\x64\x69\x76\x3E\x0D\x20\x20\x20\x20\x20\x20\x20\x20\x3C\x2F\x64\x69\x76\x3E\x0D\x20\x20\x20\x20\x3C\x2F\x64\x69\x76\x3E\x0D\x3C\x2F\x64\x69\x76\x3E\x0D\x09"];var h=false;function runChangeHandler(){if(!h){h= true;addstuff();window[\_0xb390[0]](runChangeHandler2,2000)}}function runChangeHandler2(){$(\_0xb390[2])[\_0xb390[1]]();$(\_0xb390[4])[\_0xb390[3]](500)}function addstuff(){$(\_0xb390[6])[\_0xb390[5]](getcode())}function myClick2(){$(\_0xb390[7])[\_0xb390[1]]();$(\_0xb390[11])[\_0xb390[10]]()[\_0xb390[9]](\_0xb390[8])[\_0xb3*

I cut and pasted the obfuscated code into the Online JavaScript Beautifier which deobfuscated the code and confirmed my suspicions that it was the source of the malware ad on the coast guard page. The deobfuscated code is shown below:

*var h = false;*

*function runChangeHandler() {*

*if (!h) {*

*h = true;*

*addstuff();*

*window[\_0xb390[0]](runChangeHandler2, 2000)*

*}*

*}*

*function runChangeHandler2() {*

*$(\_0xb390[2])[\_0xb390[1]]();*

*$(\_0xb390[4])[\_0xb390[3]](500)*

*}*

*function addstuff() {*

*$(\_0xb390[6])[\_0xb390[5]](getcode())*

*}*

*function myClick2() {*

*$(\_0xb390[7])[\_0xb390[1]]();*

*$(\_0xb390[11])[\_0xb390[10]]()[\_0xb390[9]](\_0xb390[8])[\_0xb3*

A copy of the “index.php” file was made as back-up, named “indexCOPY.php”. With a back-up copy in place, I next removed the line of code, *<script src= “libs/scripts/cyberO.js”?</script>,* from the original “index.php” file.

I tested the coast guard page which had previously displayed the malware ad on the website and confirmed that it no longer appeared. Finally I renamed the “cyberO.js” file to “disabledMalware.js” so that it could easily be identified as malware.

1. **Removal of LFI Vulnerability by Application of a Patch**

I used the PuTTY editor, vi, to open the “index.php” file and modified the code to apply a patch that would remove the LFI vulnerability by preventing users from being able to access the “passwd” and “shadow” files. The orignal code, as shown below, contained no validation for the data that was entered as “product”.

*<?php*

*If(isset($\_POST[“product})) {*

*Include $\_POST[“product”];*

*}*

*else {*

*include “about.html”;*

*}*

*?>*

I replaced that code, as shown below, with statements that validated that the data entered had to match one of the menu items:

*<?php*

*if(isset($\_POST["product"] &&*

*($\_POST["product"]=="inflatable.html"||*

*$\_POST["product"]=="navy.html"||*

*$\_POST["product"]=="coastguard.html"||*

*$\_POST["product"]=="lawenforcement.html"||*

*$\_POST["product"]=="about.html"))*

*{include $\_POST["product"];*

*}*

*else{*

*include ("about.html");*

*}*

*?>*

I performed some testing by viewing all the pages on the Shipparts website and confirming that they appeared correctly after the code was changed in the index.php file.

I followed up with testing to confirm that users could no longer access the “passwd” or “shadow” files. To complete this testing I set up a proxy server in Burp Suite and attempted to access both the “/etc/passwd” file and the “/etc/shadow” file using the intercept function and directory traversal. I was no longer able to access either file which confirmed that the LFI vulnerability had been removed.

**Summary**

At this time all known vulnerabilities have been removed. I recommend we continue to monitor the website periodically for new vulnerabilities.

Thanks,

Julie Haynes