**Security Review of Ship-Parts Military Boats Website (Task 1)**

In March 2019 an initial review of the <http://www.shipparts.sup> website was performed. Initial findings indicate at least three issues:

1. Malware Infection
2. Local File Inclusion Risk
3. Outdated Password Standards

These issues provide potential avenues of vulnerability and should be remedied immediately. Recommendations are included at the end of the report.

1. **Malware Infection**

A quick review of each page revealed that the **Coast Guard Boats** page contains the following pop-up. One of the first indicators that this pop-up is not from Adobe can be detected by the button labels. The pop-up uses the **Later** and **Download** labels for the buttons. Traditionally Adobe uses **Remind Me Later** and **Install**. Most Adobe pop-ups also contain a black background and different color scheme.



After the user clicks on the **Later** button to exit the pop-up, the following message appears, clearly indicating malware.



1. **Local File Inclusion**

Burp Suite was used to set up a proxy. The Intercept was set on to catch the request and reply. When the website’s **Show Info** button for any of the menu items was clicked, the request displayed in the proxy revealed that the menu items are displayed in html as “**product = *menu item****”*. Using the repeater function and directory traversal, after just a few tries I was able to modify this request and retrieve both the **passwd** and **shadow** files (see below)

**Passwd File Contents:**

root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin

adm:x:3:4:adm:/var/adm:/sbin/nologin

lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

sync:x:5:0:sync:/sbin:/bin/sync

shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

halt:x:7:0:halt:/sbin:/sbin/halt

mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin

operator:x:11:0:operator:/root:/sbin/nologin

games:x:12:100:games:/usr/games:/sbin/nologin

gopher:x:13:30:gopher:/var/gopher:/sbin/nologin

ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin

nobody:x:99:99:Nobody:/:/sbin/nologin

rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin

ntp:x:38:38::/etc/ntp:/sbin/nologin

saslauth:x:499:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin

mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin

smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin

rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin

nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin

sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin

dbus:x:81:81:System message bus:/:/sbin/nologin

ec2-user:x:500:500:EC2 Default User:/home/ec2-user:/bin/bash

apache:x:48:48:Apache:/var/www:/sbin/nologin

webmaster:x:501:502::/home/webmaster:/bin/bash

**Shadow File Contents**

root:\*LOCK\*:14600::::::

bin:\*:16323:0:99999:7:::

daemon:\*:16323:0:99999:7:::

adm:\*:16323:0:99999:7:::

lp:\*:16323:0:99999:7:::

sync:\*:16323:0:99999:7:::

shutdown:\*:16323:0:99999:7:::

halt:\*:16323:0:99999:7:::

mail:\*:16323:0:99999:7:::

uucp:\*:16323:0:99999:7:::

operator:\*:16323:0:99999:7:::

games:\*:16323:0:99999:7:::

gopher:\*:16323:0:99999:7:::

ftp:\*:16323:0:99999:7:::

nobody:\*:16323:0:99999:7:::

rpc:!!:17155:0:99999:7:::

ntp:!!:17155::::::

saslauth:!!:17155::::::

mailnull:!!:17155::::::

smmsp:!!:17155::::::

rpcuser:!!:17155::::::

nfsnobody:!!:17155::::::

sshd:!!:17155::::::

dbus:!!:17155::::::

ec2-user:!!:17188:0:99999:7:::

apache:!!:17188::::::

webmaster:$1$jcjajX05$A4P8JqsbnBkcVl.dPyDLG0:17188:0:99999:7:::

1. **Outdated Password Standards**

Both an outdated hashing algorithm and a weak webmaster password are issues for this website. The hashing algorithm appears to be MD5 ($1 prefix) as evidenced by the webmaster’s hashed password (webmaster:$1$jcjajX05$A4P8JqsbnBkcVl.dPyDLG0:17188:0:99999:7::). MD5 is considered an older outdated hasing algorithm.

The webmaster’s hashed password was copied to a .txt file titled **Webmaster.txt**. The Windows Command Prompt was used to run the textfile containing the hashed password through John the Ripper. No special rules were required and the password was cracked on the first try using the command **John webmaster.txt** which revealed that the password was **Wolverine**. This password does not meet today’s complexity standards for passwords.

**Recommendations**

1. Remove malware.
2. Revise html code to remove LFI vulnerability.
3. Replace hashing algorithm with an updated version.
4. Require all users including webmaster to adopt a higher complexity password standard that includes upper/lower case characters, numbers, and/or special characters.

Thanks,

Julie Haynes