To whom it may concern,

The following is a detailed report on the vulnerabilities found when gathering data on the 'shipparts.sup' website:

Burp Suite was used as an HTTP proxy to access and alter the POST method product variable to display both the 'passwd' and 'shadow' files and their information. This vulnerability currently leaves the shipparts.sup site open to LFI (Local File Inclusion) exploits.

Not only were these files easily accessible, but through use of the 'John the Ripper' (JtR) application, I was able to extract the webmaster's hashed password from the displayed shadow file, and decode the password.

The password is: Wolverine

Here is the hashed password: 1jcjajX05$A4P8JqsbnBkcVl.dPyDLG0