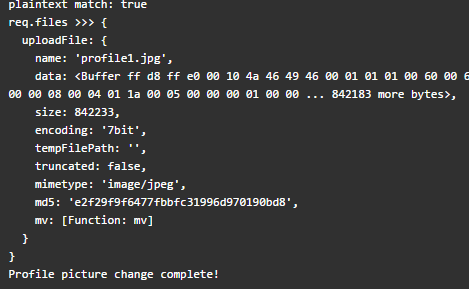
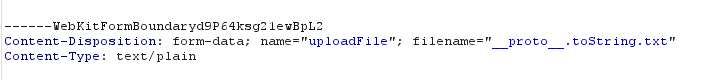
## OWASP 09 – Using Components with Known Vulnerabilities

### Walkthrough – Shopping App

The npm module that was added for OWASP 06 that allowed for file uploading, if the correct versions is installed, has the flaw when a setting is enabled called parseNested. When this is set to true, it is possible to cause a pollution of the string operator. If a POST request is sent with the name of the file being \_\_proto\_\_.toString, it can lead to the high jacking and pollution of operators. It does not have to be \_\_proto\_\_.toString specifically, this can be used with any operation that has \_\_proto\_\_ at the start.

Burp suite community edition or another software capable of sending POST requests will be required.

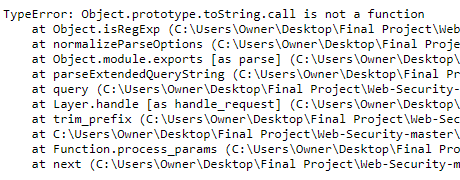
1. Launch Burp suite
   1. Use temporary project
   2. Use Burp defaults
2. Select the Proxy tab
   1. Choose Open Browser
   2. Leave intercept off for the moment
3. On Burp suite browser go to localhost:3000
4. Login to any profile or create a new one
5. Navigate to the view profile page
6. Upload any regular image
7. Observe the console for the details of the file
8. On Burp suite, turn intercept on
9. Select a file to upload
   1. For simplicity select the file \_\_proto\_\_.toString.txt to upload
10. After pressing the upload button, observe the POST request on Burp suite



* 1. At the Content-Disposition line, change the name to equal “\_\_proto\_\_.toString”



1. Then use the Forward button on Burp suite to send the POST request (it may need 2 presses)
2. Now the method, Object.prototype.toString has been polluted because a something that is not a function has been placed into it.
3. Every request sent to the application will now result in a 500 error



\*Note: The application uses EJS, because of this it is possible to create a reverse shell by polluting using \_\_proto\_\_.outputFunctionName. However, researching and implementing the current state of the vulnerability took far longer than anticipated due to this a consistent process for this was not developed before the end of this iteration and will need to be implemented in the next\*

### Exercises – Shopping App

1. Locate the express-fileUpload module and modify the processNested function to avoid processing anything starting with \_\_proto\_\_
2. Optional: Update the Shopping Application to only take in files for images such as .png or .jpeg