“.jpg” but because %0d%0a are newline characters it is saved as zseano.html. Don’t forget that often filenames are reflected on the page and you can smuggle XSS characters in the filename (some *developers may think users can’t save files with < > “ characters in them*).

```
------WebKitFormBoundarySrtFN30pCNmqmNz2
Content-Disposition: form-data; name="file"; filename="58832_300x300.jpg<svg onload=confirm()>"
Content-Type: image/jpeg

ÿØÿà
```

What is the developer checking for exactly and how are they handling it? Are they trusting any of our input? For example if I provide it with:

```
------WebKitFormBoundaryAxbOlwnrQnLjU1j9
Content-Disposition: form-data; name="imageupload"; filename="zseano.jpg"
Content-Type: text/html
```

Does the code see “.jpg” and think “Image extension, must be ok!” but trust my content-type and reflect it as Content-Type:text/html? Or does it set content-type based on the file extension? What happens if you provide it with NO file extension (or file name!), will it default to the content-type or file extension?

```
------WebKitFormBoundaryAxbOlwnrQnLjU1j9
Content-Disposition: form-data; name="imageupload"; filename="zseano."
Content-Type: text/html

------WebKitFormBoundaryAxbOlwnrQnLjU1j9
Content-Disposition: form-data; name="imageupload"; filename=".html"
Content-Type: image/png
<html>HTML code!</html>
```

It is all about providing it with malformed input & seeing how much of that they trust. Perhaps they aren’t even doing checks on the file extension and they are instead