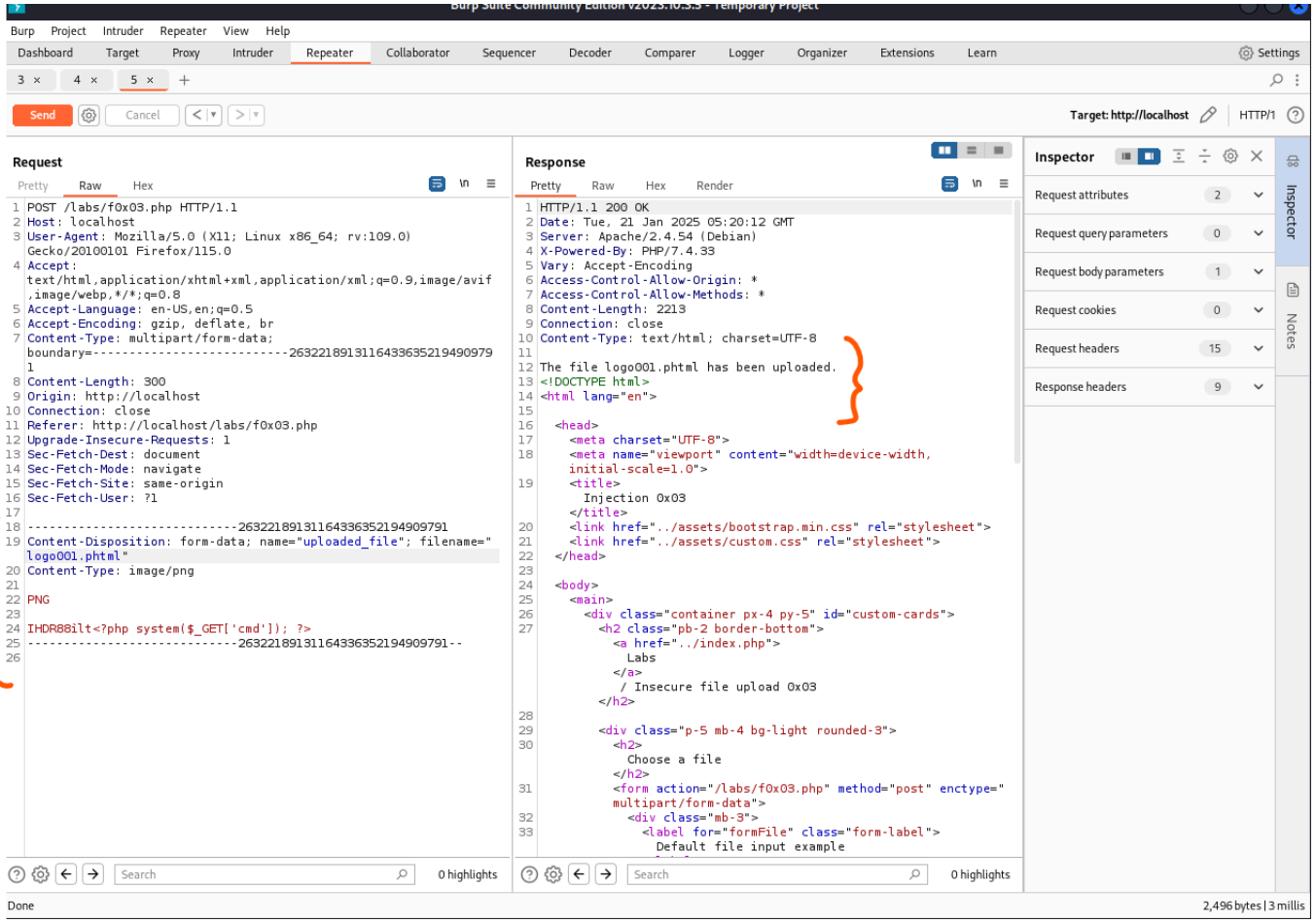
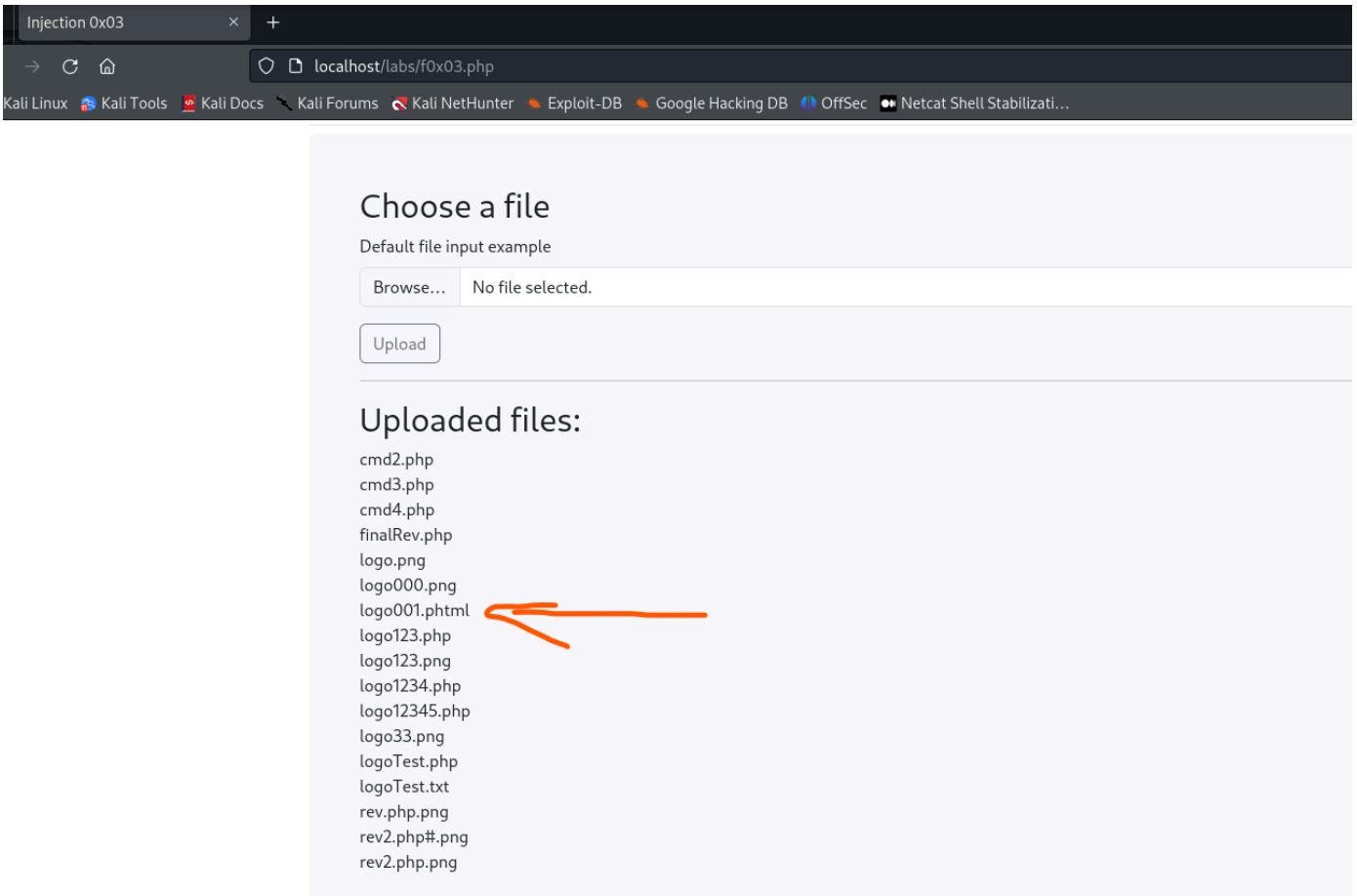
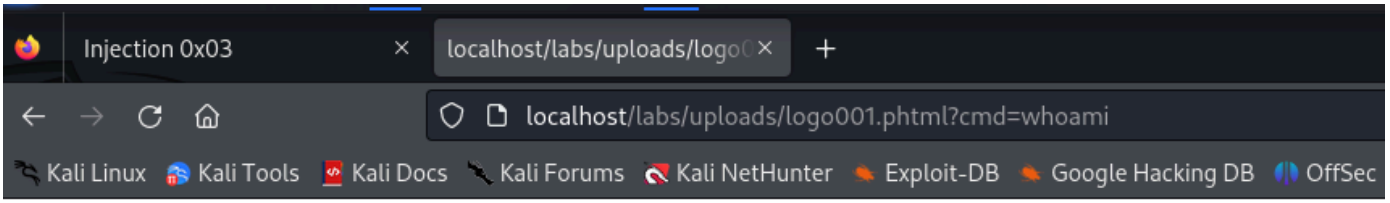
16 - Insecure File Upload - Challenge Walkthrough

Methodology

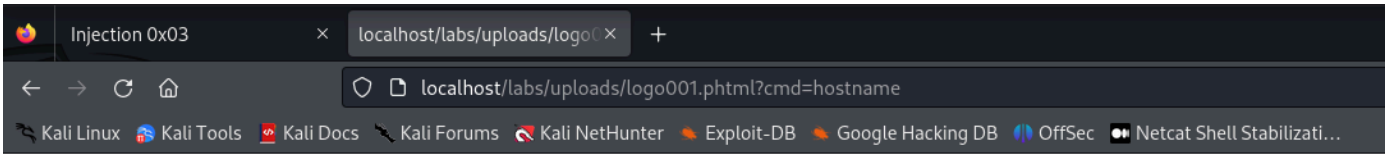
- PHP Server. .php .php3 .php4 .php5 .php7 # Less known PHP extensions .pht .phps .phar .phpt .pgif .phtml .phtm .inc.
- ASP Server. ...
- JSP : .jsp, .jspx, .jsw, .jsv, .jspf, .wss, .do, .actions.
- Perl: .pl, .pm, .cgi, .lib.
- Coldfusion: .cfm, .cfml, .cfc, .dbm.
- Node.js: .js, .json, .node.





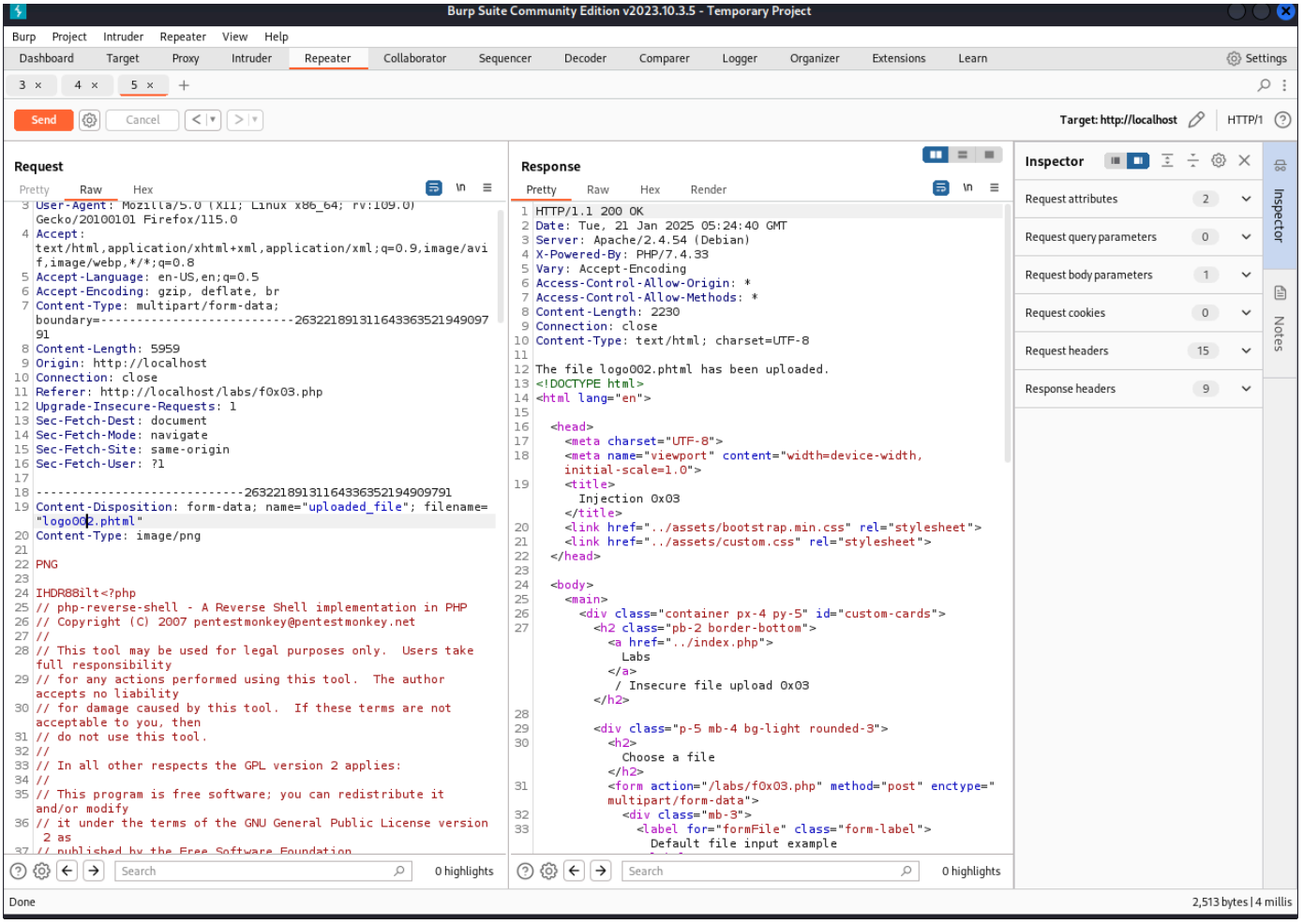


PNG IHDR88l t www-data

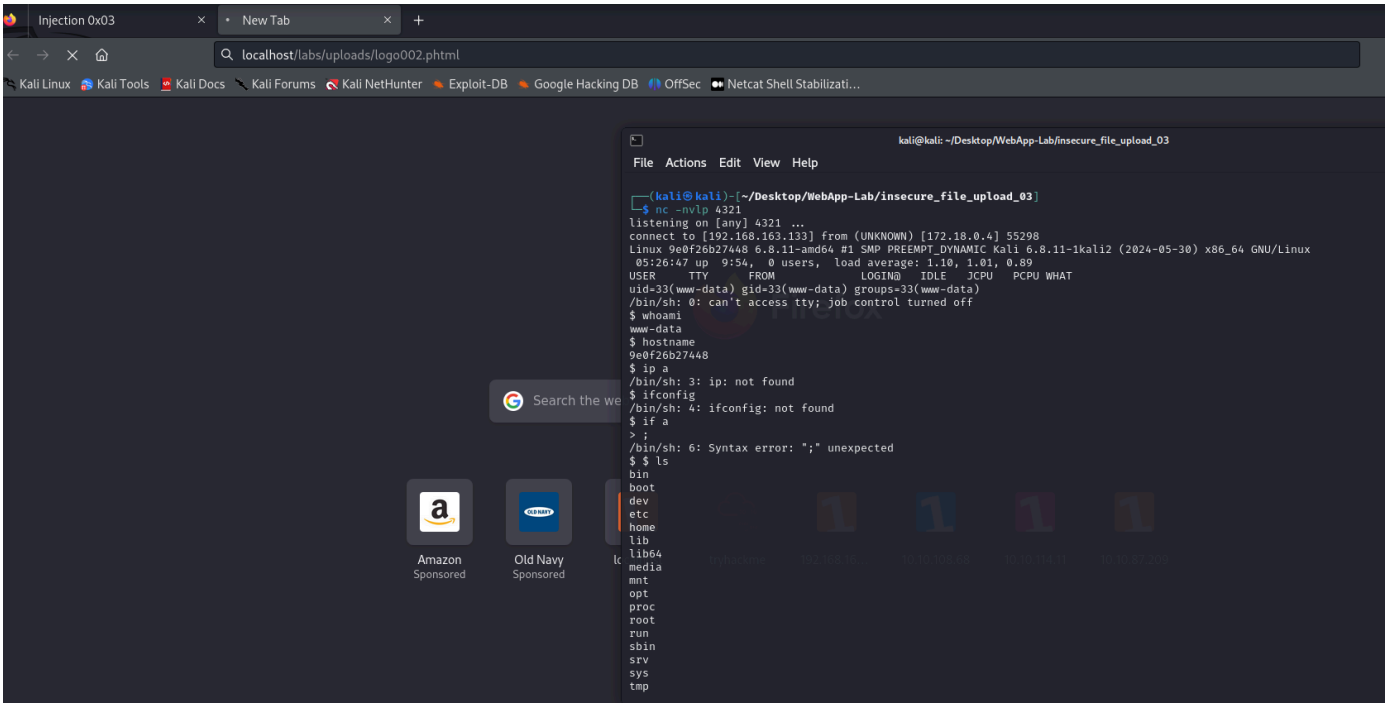


PNG IHDR88l t 9e0f26b27448

Lets try rev shell.



Same as previous lab, but using a different file extension. Looks like the website is indeed using a block list to filter file type rather than an allow list. Otherwise, this would not be possible.



Voila!

We are in the right mindset here. This is a solid methodology for testing insecure file uploading vulnerabilities.

And, it is good to know how to properly test for it.