Bypass File Filters

Different systems encode data in different ways. When you have a request that traverses multiple systems, these differences sometimes open opportunities for attack.
In Juice Shop's /ftp/ directory, there are several files visible, but the system won't let you download all of them.
In this lab, you'll look at ways to get around those limits.

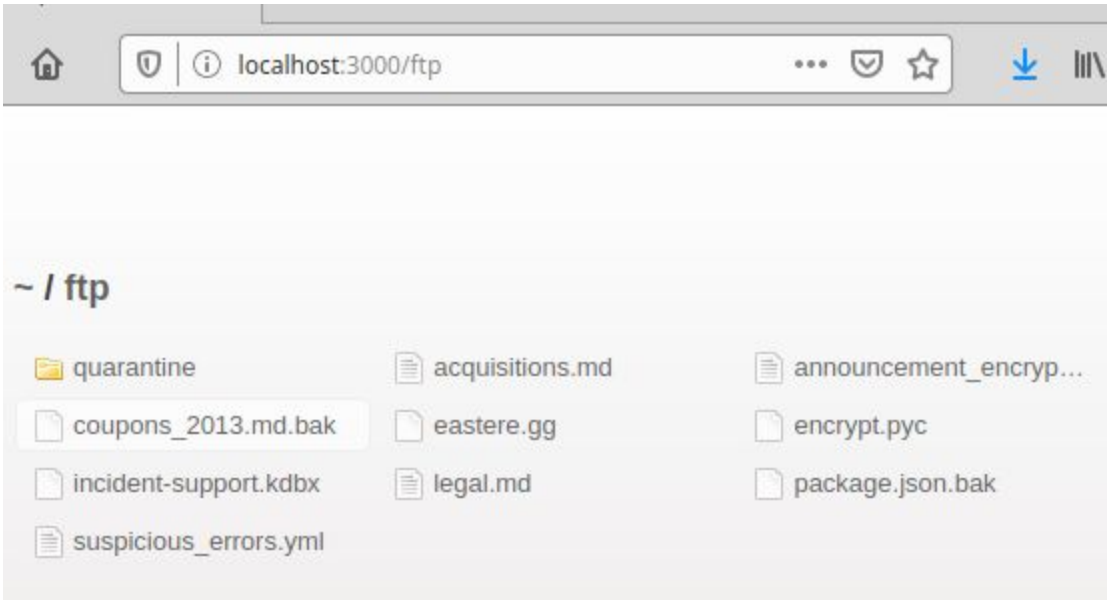
Ideas

Look at the error messages you get when you try to get a file it won't let you have.
What kinds of files are you allowed to get?
How might the server be checking file types?
Might there be more than one system involved? Maybe the server process (which checks the rules) and the operating system (which is where the files come from) don't interpret strings the same way...

Walk-Thru

Make sure you have Firefox set to use your Burp Suite as a proxy, and that the Proxy > Intercept pane says "Intercept is off"

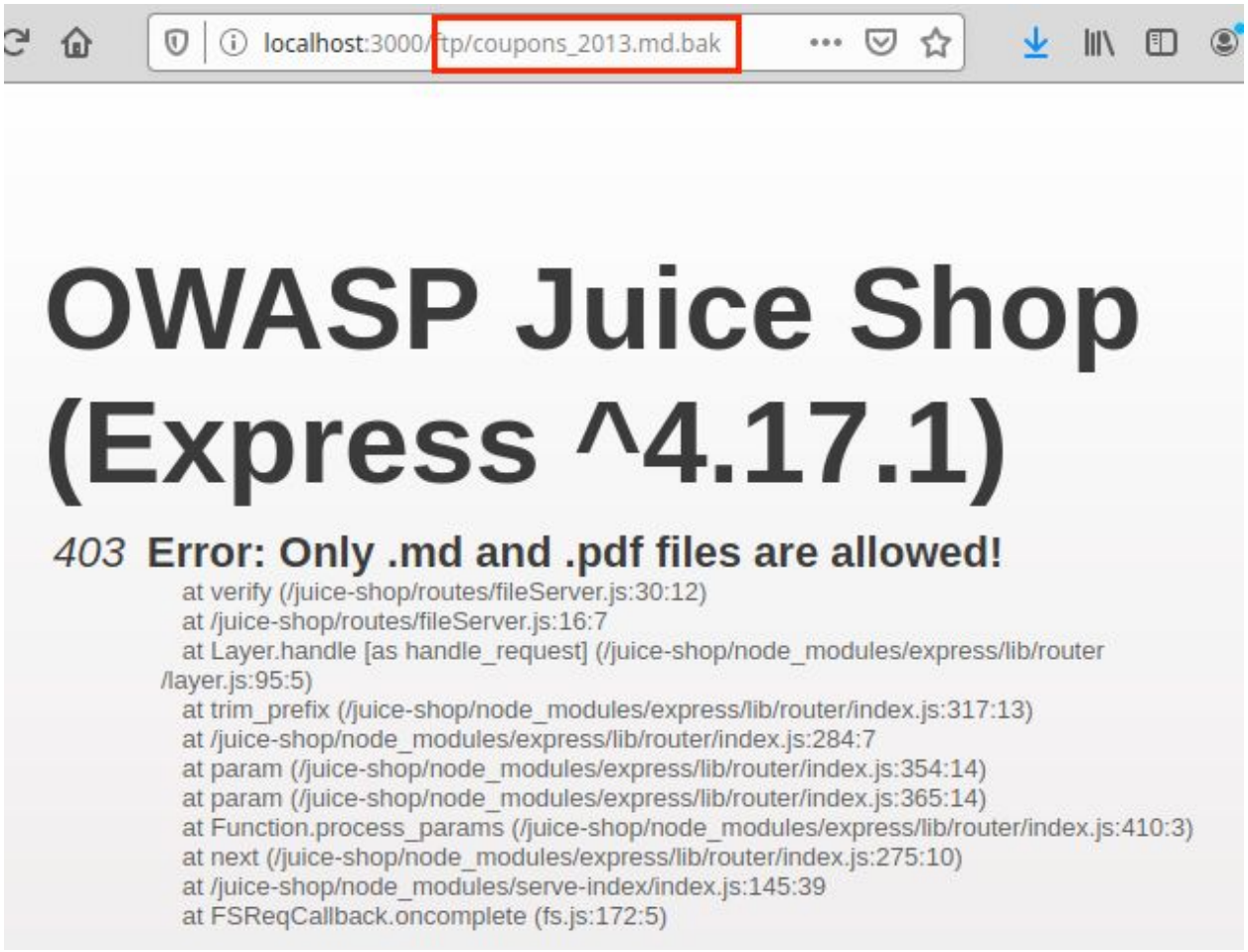
1. View the /ftp/ directory of your Juice Shop installation. Click on each file and pay attention to which ones you can download, which ones you cannot, and what the error messages tell you.



Start at http://localhost:3000/ftp

Remember: the # in a URL indicates the end of what the server sees, and the start of information used only by the browser. This URL should not have a # in it, because we're talking only to the server for this lab.

2. Notice that the error message says "only .md and .pdf files are allowed" to be downloaded.



Example: coupons_2013.md.bak is not allowed

3. You need to send a request that (in one interpretation) ends with ".md" or ".pdf" and also (in another interpretation) is the filename of the file you want.

The OS is probably written in a C-like language and probably uses the null byte to indicate "end of string". The server is probably looking at the whole string it receives in the HTTP request.

Find in Burp Proxy History a request for the file "coupons_2013.md.bak" and send it to Repeater.

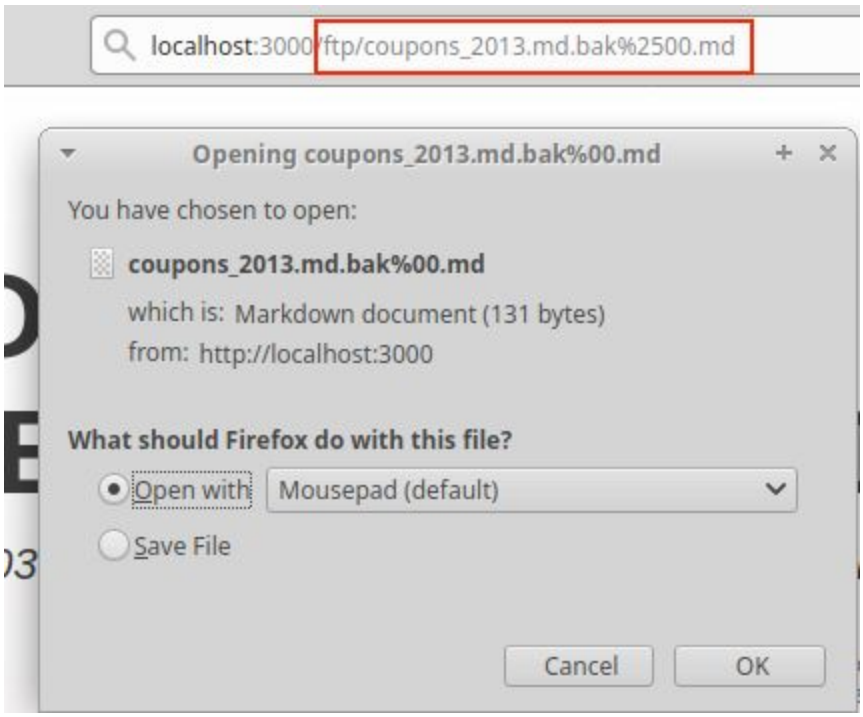
4. Adding a null byte to the end of the actual filename, followed by a file extension that is "allowed" may get past the filter and then access the file.

5. Remember that non-printable characters must be encoded in a URL.

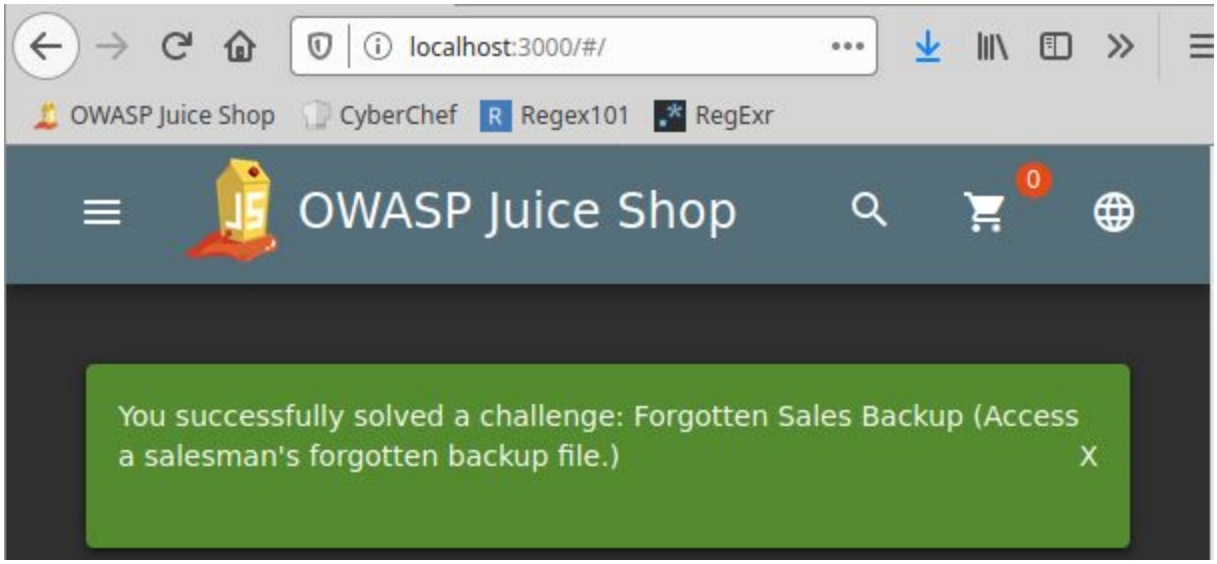
6. Change the filename to `coupons_2013.md.bak%00.md` and send it.
(Remember that %00 is a URL-encoded null byte, meaning "end of string" to C programs)
`http://localhost:3000/ftp/coupons_2013.md.bak%00.md`

7. Notice that the request still fails. Why? Because the web server is decoding the %00 into an actual null byte before the PHP gets to see it. This one needs to be double-encoded, so that the percent character is restored by the web server before the application sees it.
%25 is a URL-encoded percent sign

`http://localhost:3000/ftp/coupons_2013.md.bak%2500.md`



8. Re-load the Juice Shop homepage and receive your well-deserved recognition.



9. If you have time now, do this again with the file "eastere.gg" and see if you can solve the additional challenge inside that file.