Apache have many vulnerabilities like XSS, RCE, etc..

we talk abaut RCE

errors during file upload

Content_type
Content-disposition } headers to exploit XSS
Content-length

* ognl expression to exploit

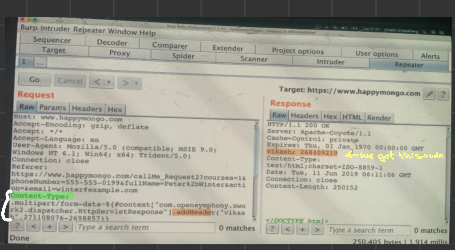
* content_type : $(#_='multipart/form-data')

How to identify structs RCE vuln.

① web application should base on java
↳ identify using weppalyzer

② if you get structs error, index.action, anything.do
anything.out, anything.action, anything.java
any.pm, anything.bat, any.sh, any.bson, any.el

*steps: ① spider
② look for ? in links.
③ send to repeater
④ see picture →



* exploitation

> python exploit.py url "cmd"

or

jexBoss tool on github