Sql injection,Cross site scripting
Tool: D-TECT
Command:
cd D-TECT
python d-tect.py

CORS
Tool: Corstest
Command:
cd Corstest
python corstest.py filename
(filename:text file containing domains)

XMAS
Tool :Nmap
Command:
Nmap –sX –p- -Pn 192.168.18.132 or simply do nmap scanning

Broken ACL
Command:
curl -X POST http://192.168.35.86:3000/api/url/ -H 'Content-Type: application/x-www-form-urlencoded' -d 'url=https%3A%2F%2Fscotch.io%2Ftutorials%2Fuse-expressjs-to-get-url-and-post-parameters&undefined='

Bad authentication
Command:
curl -I URL
(check
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN or deny
X-XSS-Protection: 1; mode=block)
Check for single failure message in login form(invalid password)
Check for SSL certificate
Check for captcha