- Create errors to find information disclosure: non-existing paths, invalid datatypes,…

- Target > Site Map > Engagement tools > Find comments / Discover content

- Intruder: interesting files and directories + sitemap.xml, crossdomain.xml

- Use TRACE-method to find out if special access is given to local IP-Address (X-Custom-IP-Authorization: 127.0.0.1), then add the custom header to requests using Proxy > Options > Match and Replace

- Sourcetree: “wget -r” to download the whole git repository => right click on file => Log Selected…

\_ Standardfehlerseiten

\_ Stack-Traces

\_ Sever banner: Apache version

\_ Information in der Browser-Konsole

\_ /actuator, /systemconfig

\_ /actuator/{env, configprops, heapdump, info, logfile, loggers, metrics, scheduledtasks, sessions, shutdown, threaddump}