Матрица
Отчет

Web1: изучив статью https://insafety.org/lfi.php , отредактировав данную ссылку получили флаг (nto{P6t9_T77v6RsA1}).

Web2: сперва мы декомпилировали jar file с помощью приложения JD-GUI, нашли изначальный код, запустив приложение. Отредактировав ссылку данную в задание, добавив в нее часть ссылки из статьи https://www.veracode.com/blog/secure-development/spring-view-manipulation-vulnerability , удалив файл password.txt, который был дан в изначальном коде и задали новое значение password, после чего нашли флаг (nto{abobovichasdfas})

Web3: прочитав статьи https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection#jinja2 , https://portswigger.net/web-security/server-side-template-injection ,https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection/jinja2-ssti , https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection , отредактировав ссылку данную в задании получили флаг (nto{Ht1P_sM088Lin6_88Ti})