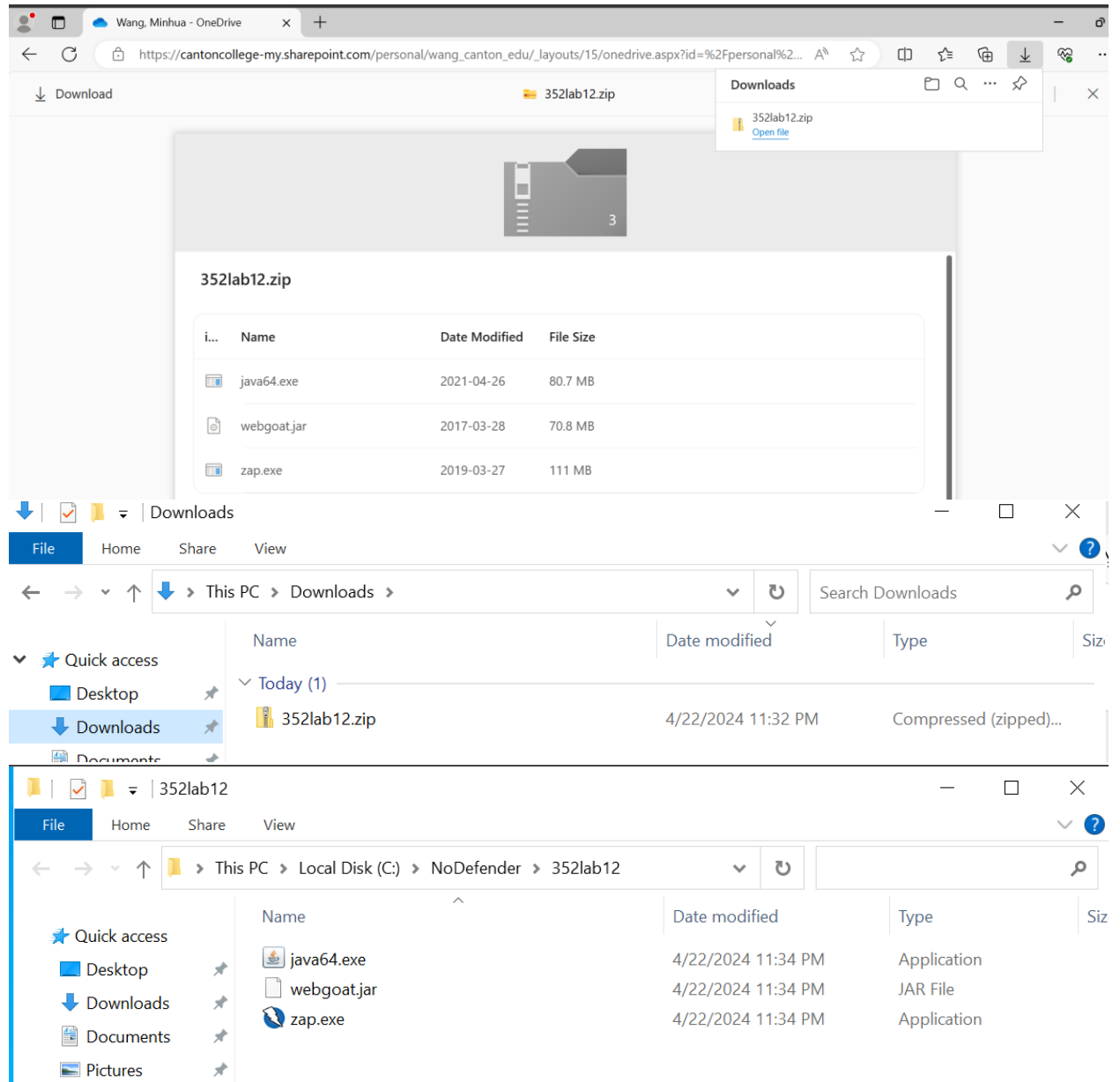
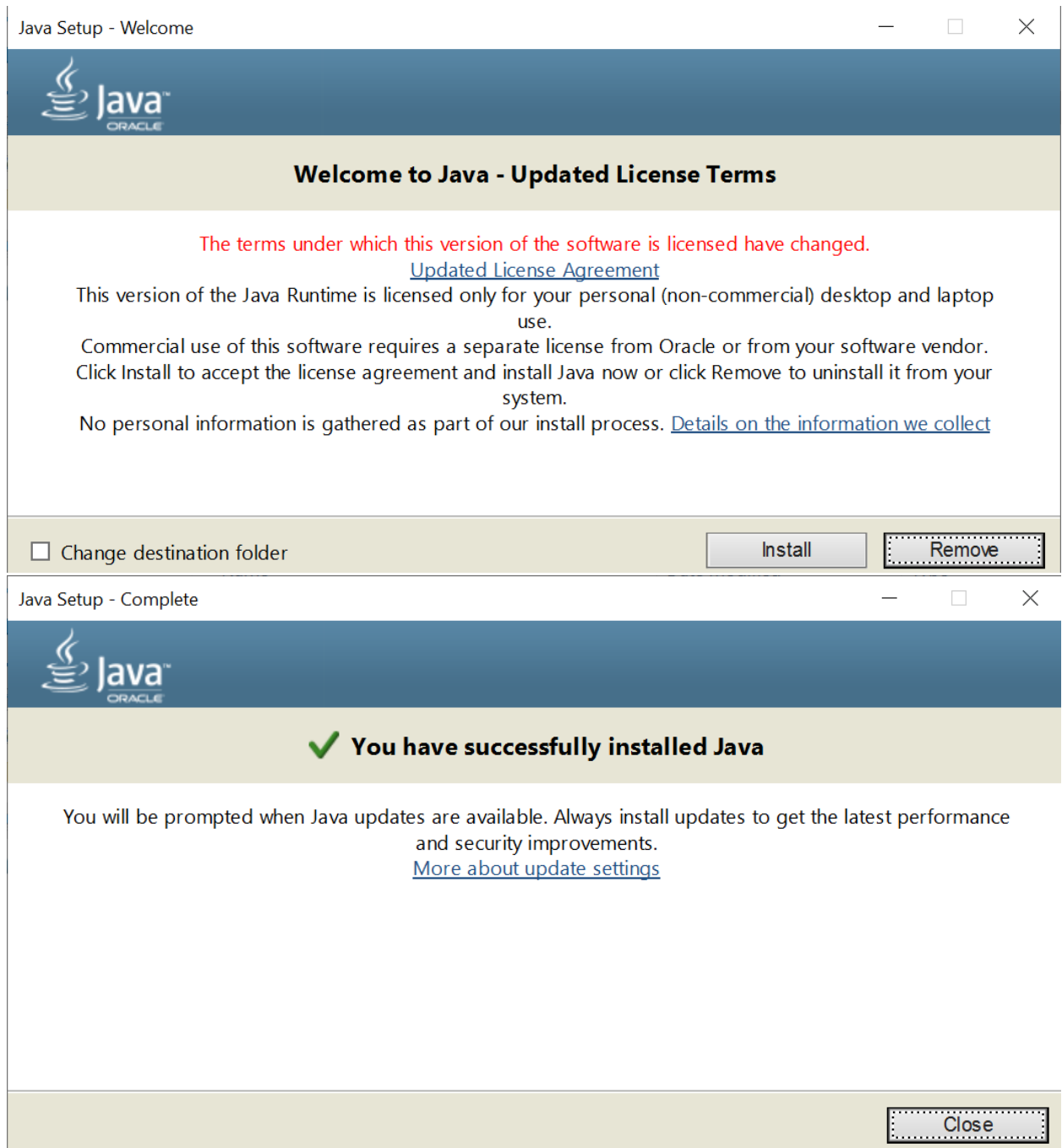


CYBR 352 Week 12 Lab

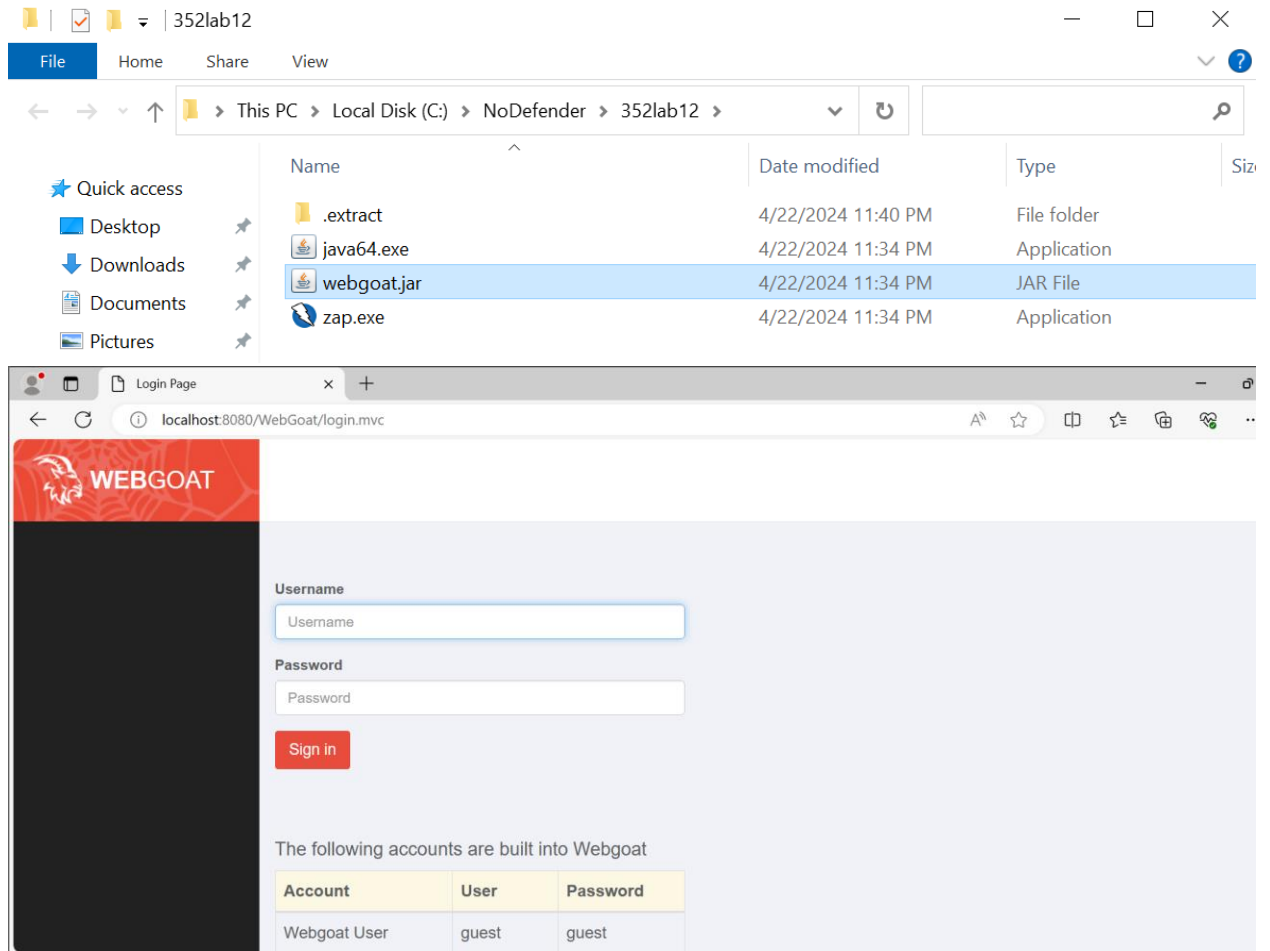
- Download 352lab12.zip file and extract it to the 352lab12 folder in the NoDefender folder.



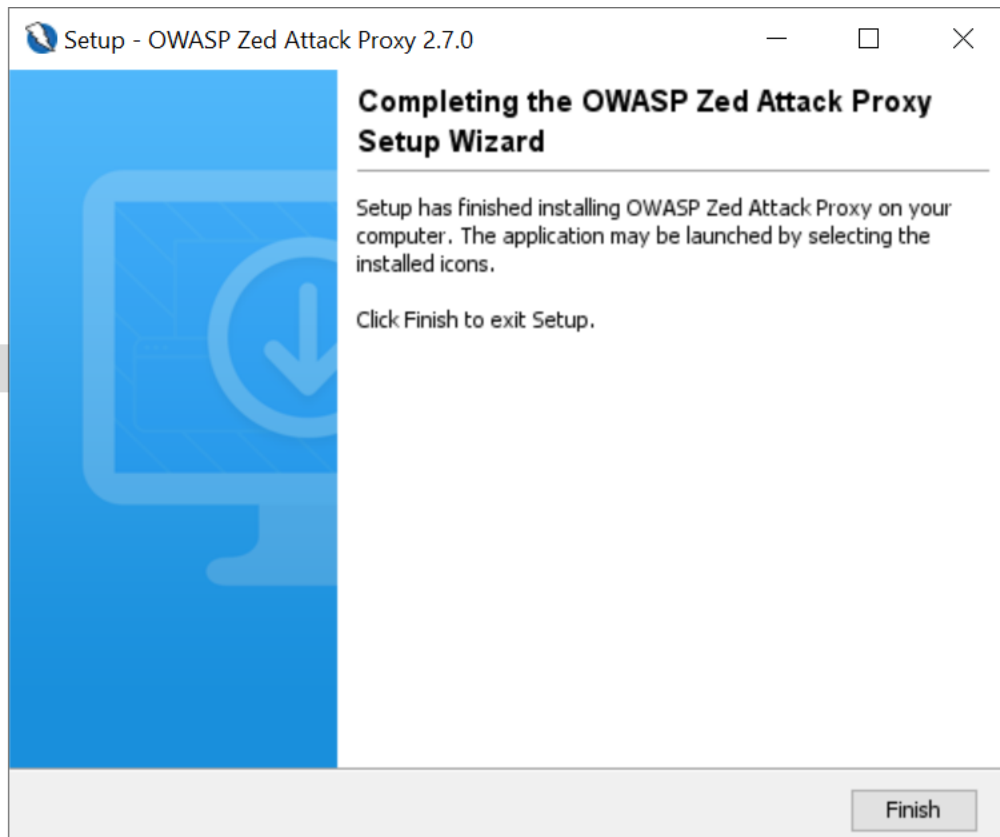
- Install 64-bit Java with java64.exe file

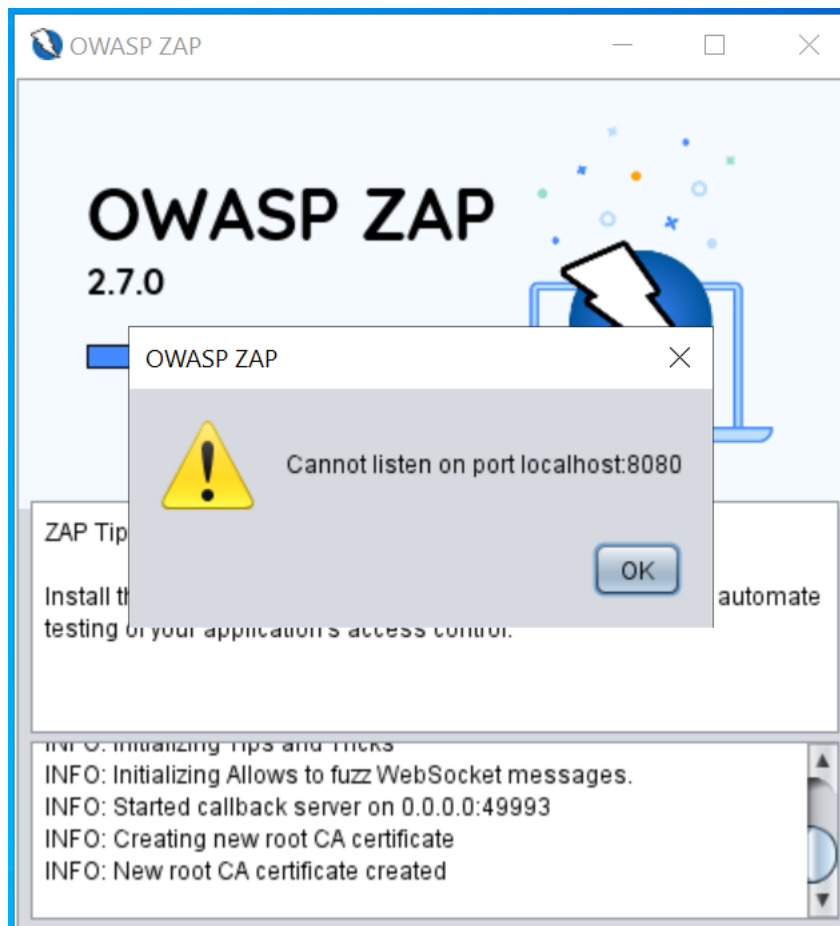


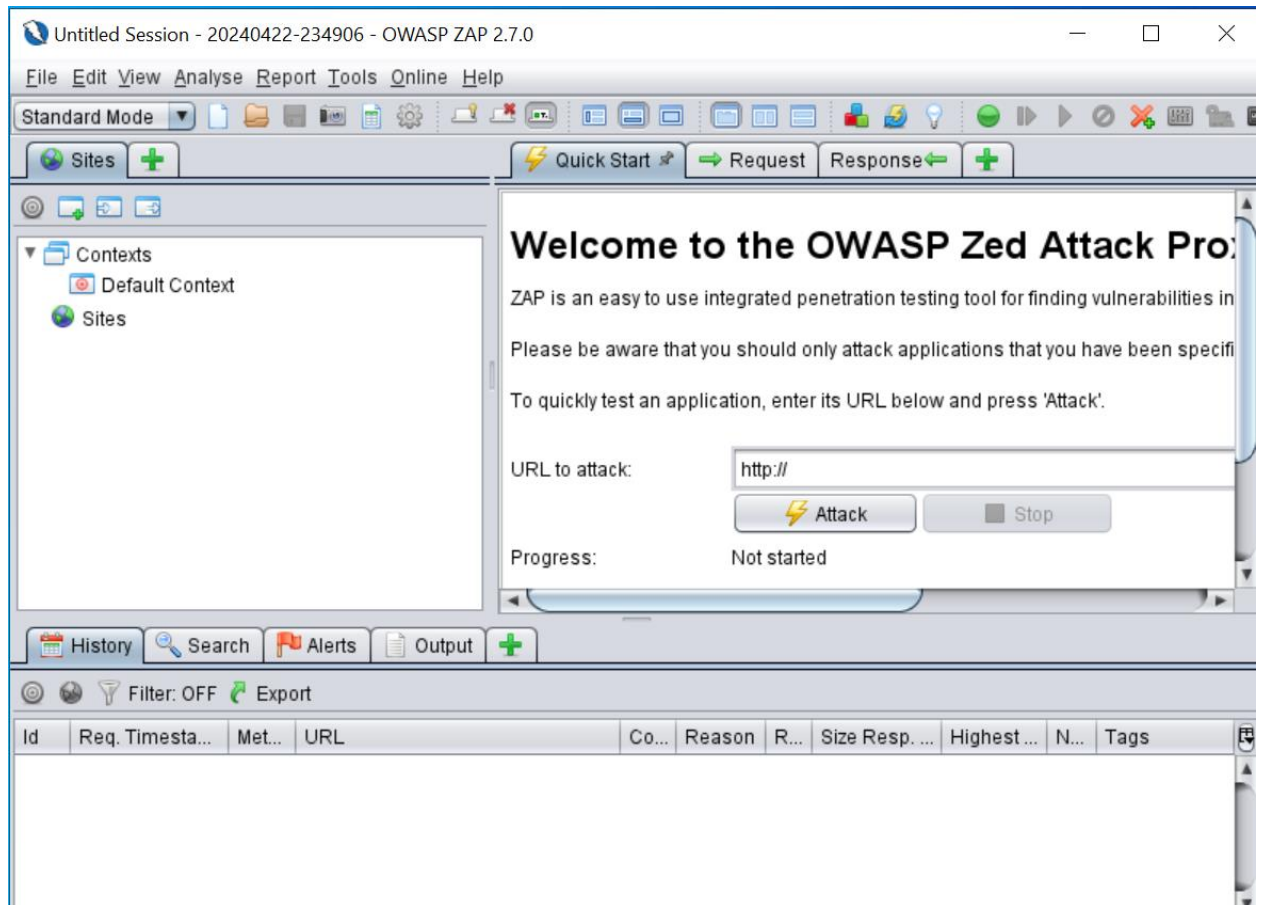
- Open webgoat.jar to run WebGoat and test it by accessing <http://localhost:8080/WebGoat>

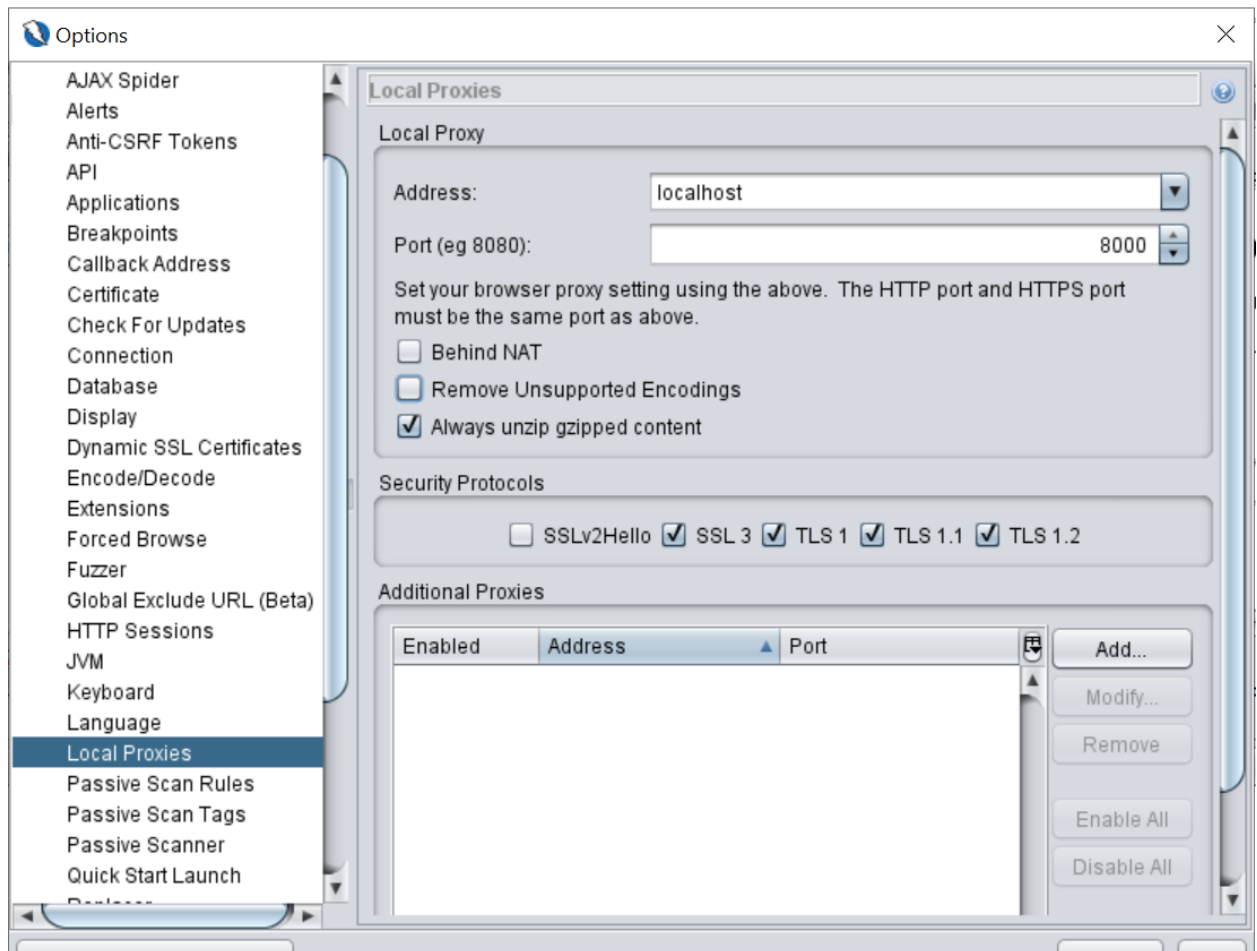


- Install ZAP with zap.exe file, run ZAP, and set its Local Proxies to port number 800 under Tools

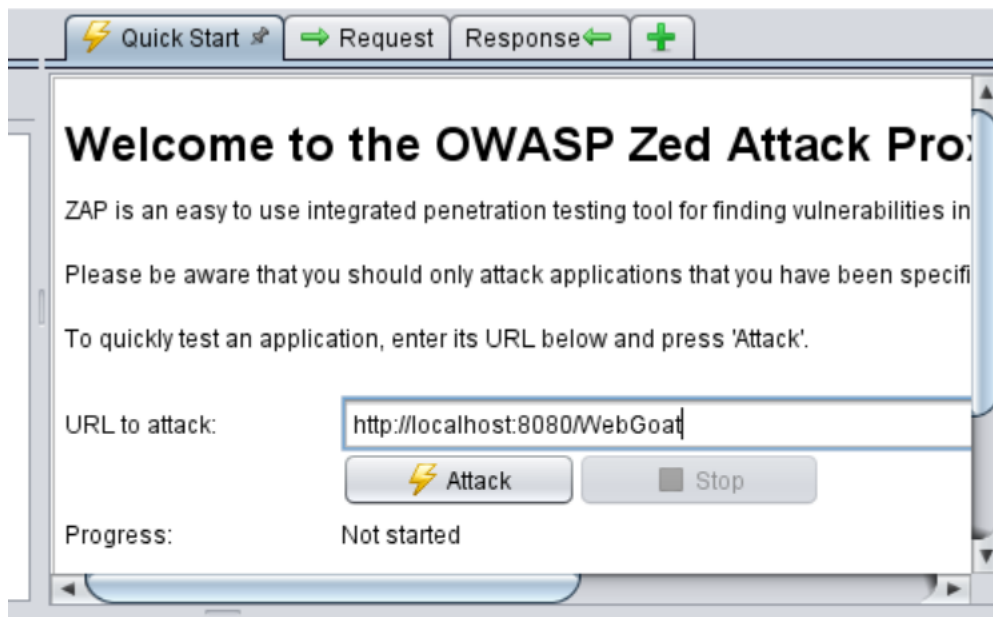


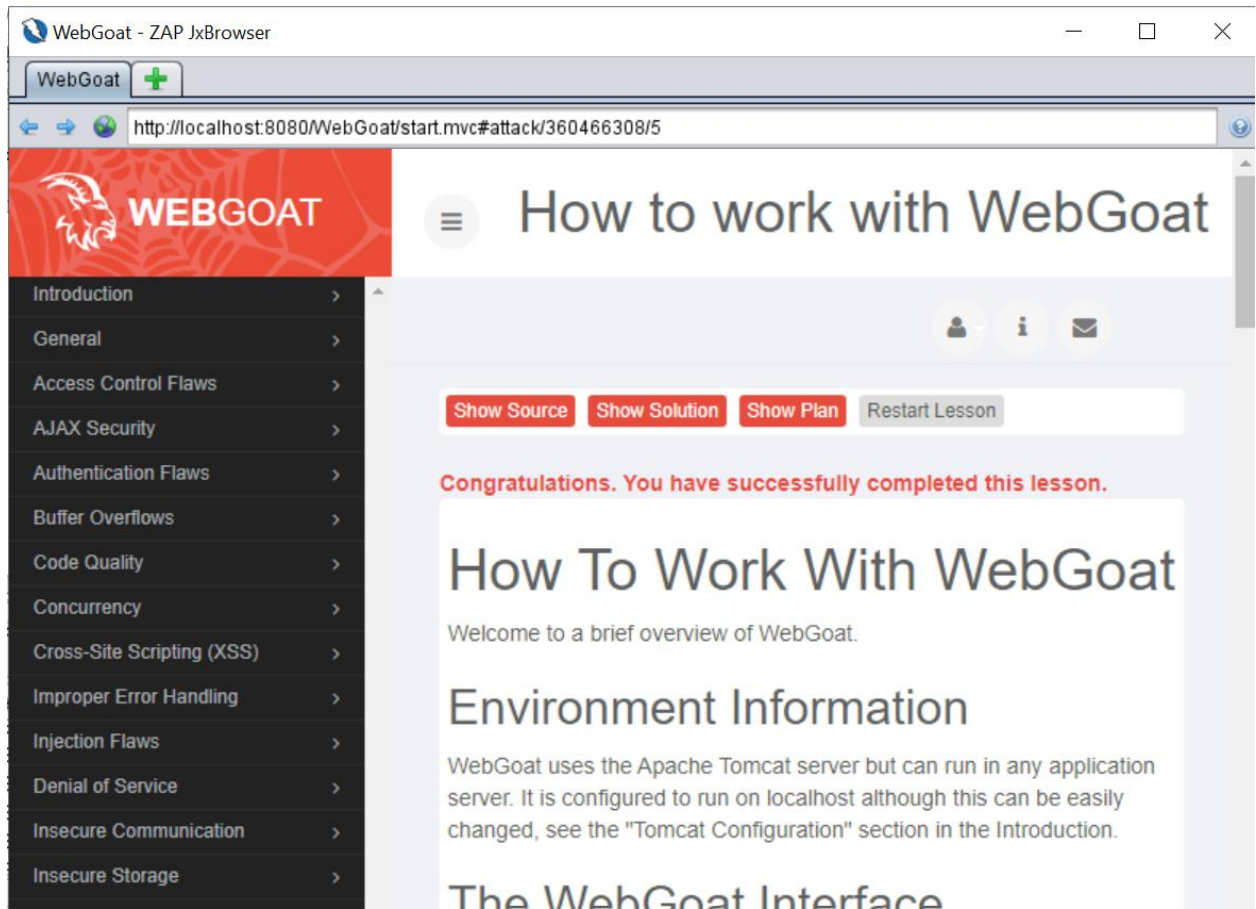






- In ZAP, set URL to Attack as <http://localhost:8080/WebGoat>, and launch JxBrowser to access the same URL





- Complete the WebGoat lesson Web Service SAX injection

WebGoat - ZAP JxBrowser

WebGoat +

http://localhost:8080/WebGoat/start.mvc#attack/360466308/5

- Denial of Service >
- Insecure Communication >
- Insecure Storage >
- Malicious Execution >
- Parameter Tampering >
- Session Management Flaws >
- Web Services >
- Create a SOAP Request
- WSDL Scanning
- Web Service SAX Injection ☒
- Web Service SQL Injection
- Admin Functions >
- Challenge >

In this exercise, try to change the password for a user other than 101.
Please change your password:

```
<?xml version='1.0' encoding='UTF-8'?>
<wsns0:Envelope
  xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
  xmlns:xsd='http://www.w3.org/2001/XMLSchema'
  xmlns:wsns0='http://schemas.xmlsoap.org/soap/envelope/'
  xmlns:wsns1='http://lessons.webgoat.owasp.org'>
  <wsns0:Body>
    <wsns1:changePassword>
      <id xsi:type='xsd:int'>101</id>
      <password xsi:type='xsd:string'>newpassword</password><i
    </wsns1:changePassword>
  </wsns0:Body>
</wsns0:Envelope>
```

You have changed the password for userid 102 to
'notforyoutoknow'

Cookies / Parameters