OpenSSL Signature Example

Generate the Private Key

```
openssl genrsa -out privkey.pem 1024
```

Generate the Pubic Key from the Private Key

```
openssl rsa -in privkey.pem -outform PEM -pubout -out pubkey.pem
```

Inspect the Public Key to find the Modulus.

```
openssl rsa –pubin –in pubkey.pem –text –noout
```

Insert the Modulus into a text file in hex without a delimiter

```
nano modulus.txt
```

Sign a digest of the modulus with the Private Key and SHA256

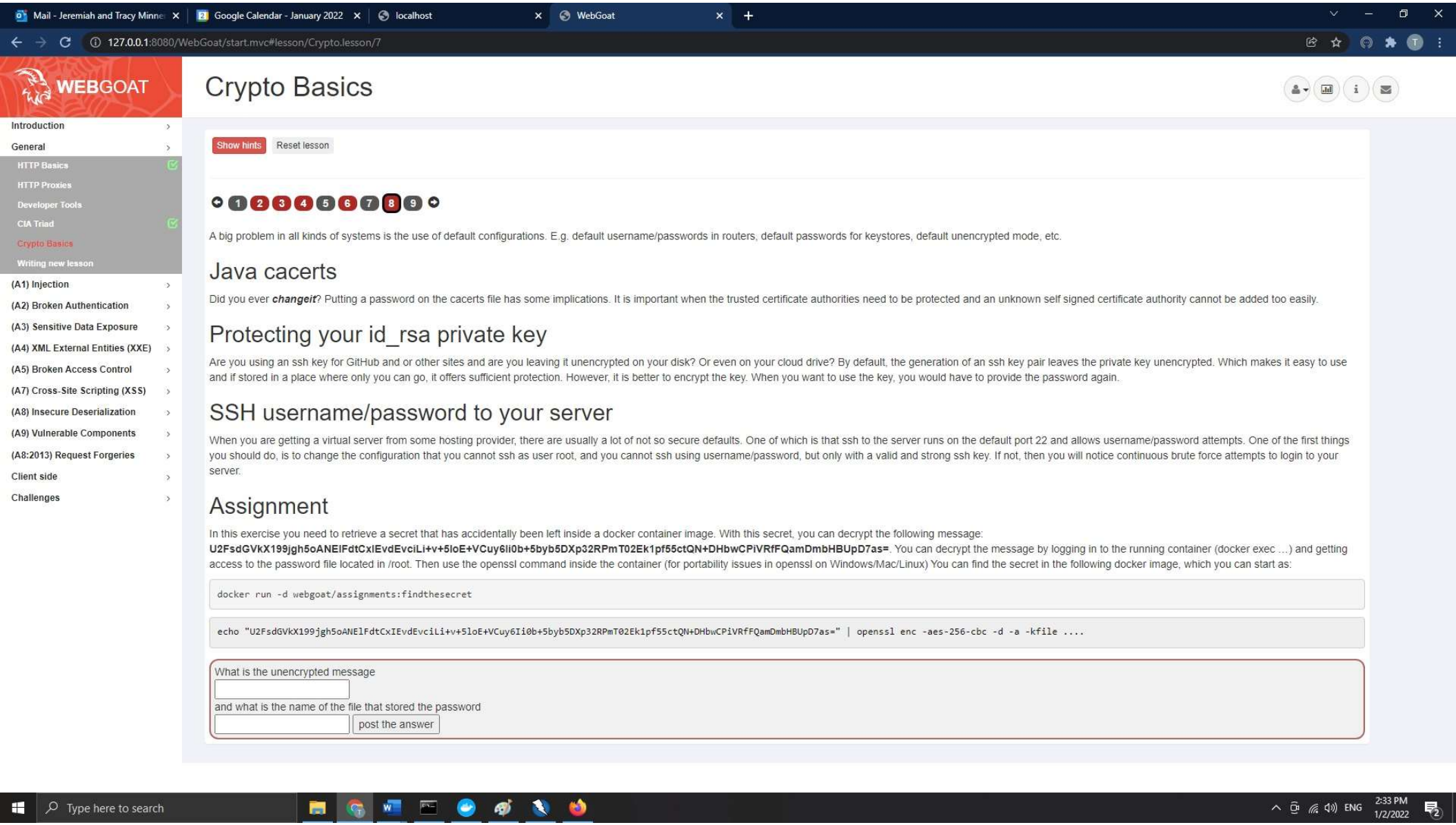
```
openssl dgst –sha256 –sign privkey.pem –out signature.bin modulus.txt
```

Convert the signature to base64 so you can see it (not required)

```
openssl base64 –in signature.bin –out signature.base64
```

Verify the signature using the Public Key, the Signature (in binary), and the modulus.txt file

```
openssl dgst –sha256 –verify pubkey.pem –signature signature.bin modulus.txt
```


Mail - Jeremiah and Tracy Minner
Google Calendar - January 2022
localhost
WebGoat
127.0.0.1:8080/WebGoat/start.mvc#lesson/Crypto.lesson/7
WEBGOAT
Introduction
General
HTTP Basics
HTTP Proxies
Developer Tools
CIA Triad
Crypto Basics
Writing new lesson
(A1) Injection
(A2) Broken Authentication
(A3) Sensitive Data Exposure
(A4) XML External Entities (XXE)
(A5) Broken Access Control
(A7) Cross-Site Scripting (XSS)
(A8) Insecure Deserialization
(A9) Vulnerable Components
(A8:2013) Request Forgeries
Client side
Challenges
Crypto Basics
Show hints
Reset lesson
1 2 3 4 5 6 7 8 9
A big problem in all kinds of systems is the use of default configurations. E.g. default username/passwords in routers, default passwords for keystores, default unencrypted mode, etc.
Java cacerts
Did you ever changeit? Putting a password on the cacerts file has some implications. It is important when the trusted certificate authorities need to be protected and an unknown self signed certificate authority cannot be added too easily.
Protecting your id_rsa private key
Are you using an ssh key for GitHub and or other sites and are you leaving it unencrypted on your disk? Or even on your cloud drive? By default, the generation of an ssh key pair leaves the private key unencrypted. Which makes it easy to use and if stored in a place where only you can go, it offers sufficient protection. However, it is better to encrypt the key. When you want to use the key, you would have to provide the password again.
SSH username/password to your server
When you are getting a virtual server from some hosting provider, there are usually a lot of not so secure defaults. One of which is that ssh to the server runs on the default port 22 and allows username/password attempts. One of the first things you should do, is to change the configuration that you cannot ssh as user root, and you cannot ssh using username/password, but only with a valid and strong ssh key. If not, then you will notice continuous brute force attempts to login to your server.
Assignment
In this exercise you need to retrieve a secret that has accidentally been left inside a docker container image. With this secret, you can decrypt the following message:
U2FsdGVkX199jgh5oANElFdtCxIEvdEvciLi+v+5loE+VCuy6Ii0b+5byb5DXp32RPmT02Ek1pf55ctQN+DHbwCPiVRfFQamDmbHBUpD7as=. You can decrypt the message by logging in to the running container (docker exec ...) and getting access to the password file located in /root. Then use the openssl command inside the container (for portability issues in openssl on Windows/Mac/Linux) You can find the secret in the following docker image, which you can start as:
docker run -d webgoat/assignments:findthesecret
echo "U2FsdGVkX199jgh5oANElFdtCxIEvdEvciLi+v+5loE+VCuy6Ii0b+5byb5DXp32RPmT02Ek1pf55ctQN+DHbwCPiVRfFQamDmbHBUpD7as=" | openssl enc -aes-256-cbc -d -a -kfile ....
What is the unencrypted message
and what is the name of the file that stored the password
post the answer
Type here to search
ENG
2:33 PM
1/2/2022

Lesson 8 Assignment is beyond the scope of Security+

However…there are two methods of attacking the problem, one is to open up a docker with user 0 privileges (0 = root). Then you can get straight to the secret folder.

The other method is to take advantage of the fact that you have access to CMD prompts outside of the docker. So, you can cp the /etc/passwd folder from the running container to the local machine, change the permissions from 1000:1000 to 0:0 (root) for webgoat and the cp the file back into the container. Then just start up the container as webgoat (using the container ID that is either the numbers that show up when you start the original container or the noun_name that is listed in the docker dashboard. Once you are in the container as webgoat you have root permissions and can continue with the assignment.