| Juiceshop Walkthrough Diploma in CSF  Year 3 Apr 2022 (Semester 5) | Week 2 |
| --- | --- |
| Practical |
| Premium Paywall | |

**OBJECTIVES**

* OWASP vulnerabilities: Sensitive Data Exposure -> Cryptographic Failures

A03:2017->A02:2021

**Prerequisite**

* ZAP
* Openssl

**Challenge – Premium Paywall**

* Unlock Premium Challenge to access exclusive content.
* Premium Paywall - Difficulty: 6/6 stars

**Step 1**

We need to inspect the html source of the premium paywall row in the scoreboard page on the juice shop website. You will be able to see a comment that is encrypted.

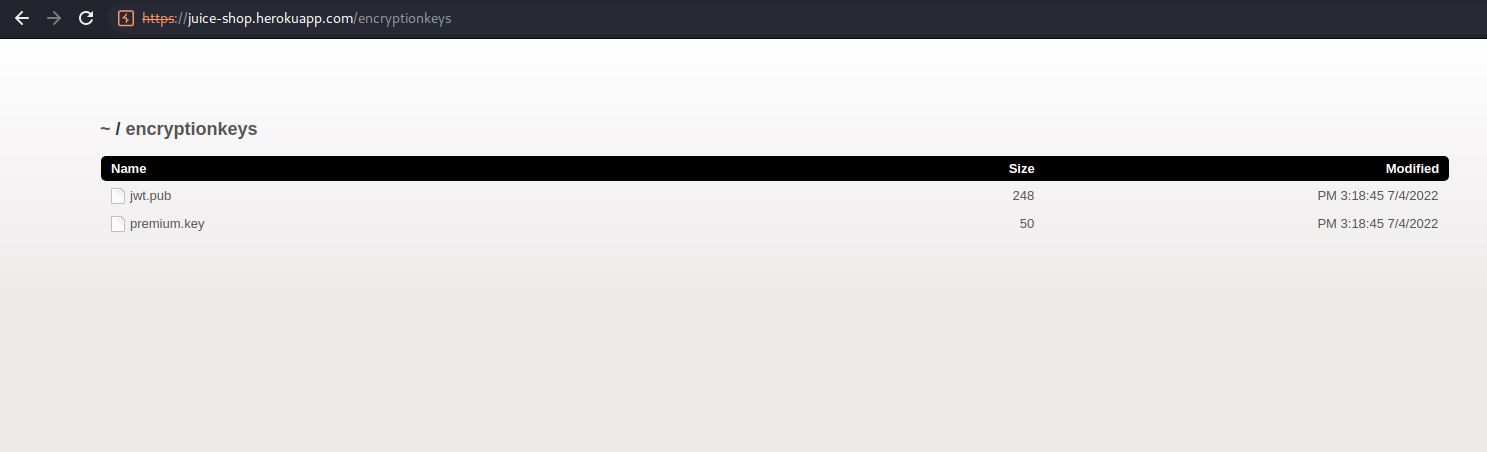


**Step 2**

From the hints on for the juice shop challenges we are able to identify that this is a cipher text that came out of an AES encryption in the cipher block chaining. Next we will need to get the key and initialization vector (IV). We will need to run a forced browsing directory attack by using OWASP Zap and running a dictionary with it.

**Step 3**

After running the attack we manage to discover a directory which is ~/encryptionkeys



**Step 4**

Open up the premium.key file we will find information about the encryption key as well as the IV

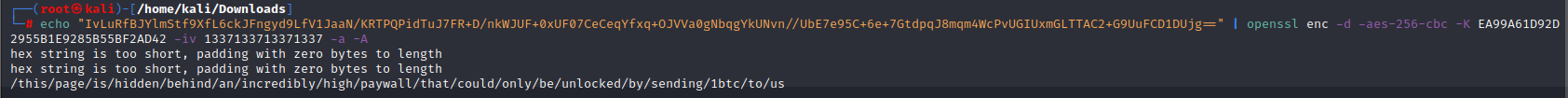
**Step 5**

We will need to decrypt the cipher text by using openssl.

* echo "IvLuRfBJYlmStf9XfL6ckJFngyd9LfV1JaaN/KRTPQPidTuJ7FR+D/nkWJUF+0xUF07CeCeqYfxq+OJVVa0gNbqgYkUNvn//UbE7e95C+6e+7GtdpqJ8mqm4WcPvUGIUxmGLTTAC2+G9UuFCD1DUjg==" | openssl enc -d -aes-256-cbc -K EA99A61D92D2955B1E9285B55BF2AD42 -iv 1337133713371337 -a -A

The result of the plaintext will be:

/this/page/is/hidden/behind/an/incredibly/high/paywall/that/could/only/be/unlocked/by/sending/1btc/to/us



**Step 6**

To solve the challenge, we will need to add the result of the plaintext to our url.

**~ End of Challenge ~**