**Second DEPI CTF Writeup**

---

---

\*\*1. Executive Summary\*\*

This section provides a brief overview of the findings from the penetration test, including key vulnerabilities identified and their potential impact on the organization's security posture.

---

\*\*2. Scope\*\*

Details the systems, networks, and applications that were tested during the engagement. This includes IP addresses, domains, and any specific applications that were in scope.

[Second DEPI CTF: Go Through The Basics (depi-ctfs.vercel.app)](https://depi-ctfs.vercel.app/)

A screenshot of a computer

Description automatically generated

* [depi-ctfs.vercel.app/robots.txt](https://depi-ctfs.vercel.app/robots.txt)
* [Second DEPI CTF: Go Through The Basics (depi-ctfs.vercel.app)](https://depi-ctfs.vercel.app/devLogin)
* https://depi-ctfs.vercel.app/home/

A screenshot of a phone

Description automatically generated

A screenshot of a computer

Description automatically generated

---

\*\*3. Methodology\*\*

Outlines the testing techniques and tools used throughout the penetration testing process. This may include manual testing, automated tools, social engineering tactics, and any specific frameworks or standards followed (e.g., OWASP, NIST).

A black and white dotted background

Description automatically generated

Here is comminate

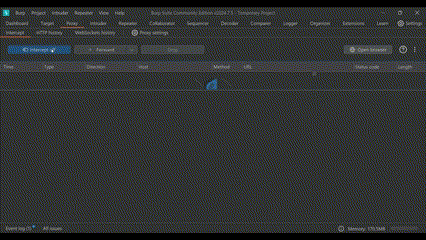
 <!-- TODO: REMOVE BEFORE PRODUCTION - Only the "Admin" can log in without a password.

             [Hacker Note] Only the "Admin" can comment it out.

             I love creating backdoors by injecting vulnerable code or simulating it.

             The only ingredients you need to access my masterpiece are in this list: ["a", "d", "m", "i", "n", "A", "D", "M", "I", "N", "'", "-", " "]. -->

username=admin'-- '&password=' 🡺 SQL Injection



anther

|  |
| --- |
|  |
| <!-- You did it—congratulations! By the way, it wasn’t SQL injection; I just like making the passwords on the machines I hack look like vulnerabilities. And yes, my backdoor was just a simulation that won’t be detected by some vulnerability scanners. Ready for the next challenge? -->  Code javascript : in an online complier like: https://www.programiz.com/javascript/online-compiler/  A screen shot of a computer screen  Description automatically generatedHere’s a snapshot of the future—use it wisely. You will find a PCAP file along the way. I always love to play with the \*\*\* protocol; it’s an easy protocol and very suitable for beginners to understand any manipulation in it. So, it’s now obvious that you will need to look for malformed packets. When the moment arrives, use your SSL key to unlock the secret door: \*\*\*\*\*\*\*\*. It’s a shame they wouldn’t let me reveal it here, but don’t worry—I’ve hidden it within the captured packets. Trace the HTTP stream to retrieve it. Enjoy the challenge! === Session Ended. Please Run the code again === |
|  |

<https://www.linkedin.com/in/ahmed-hesham-78b957319/>

A close-up of a resume

Description automatically generated

<https://www.linkedin.com/in/ahmed-hesham-78b957319/overlay/1723504722934/single-media-viewer?type=DOCUMENT&profileId=ACoAAFDDxJsBukcDQY5pJ4Tk6mX9vQLpBchxqoY&lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base%3BQgGFpBbHRQmV2EhA4JVBlQ%3D%3D>

Now after downloaded file “Elliot Alderson.docx.pdf”   
Try slack all to see anything is hidden liked that

A screenshot of a computer

Description automatically generatedNow we can copy for hidden line :  
“ The file is encrypted with one of the most famous symmetric encryption algorithms, using a robust key size, and the password is EVerYTHING!$CONNECTeD ”

Try used [Metadat For Elliot Alderson.docx.pdf (exif.tools)](https://exif.tools/upload.php)

A screenshot of a computer

Description automatically generated

<https://depi-ctfs.vercel.app/home/Mr_Robot_CV.docx>

A screenshot of a computer

Description automatically generated

The is file when open we find this message

A screenshot of a computer

Description automatically generated  
A screenshot of a computer error message

Description automatically generated

Used strange to fine file name up normal so used unzip or in windows used tar -xf name.zip

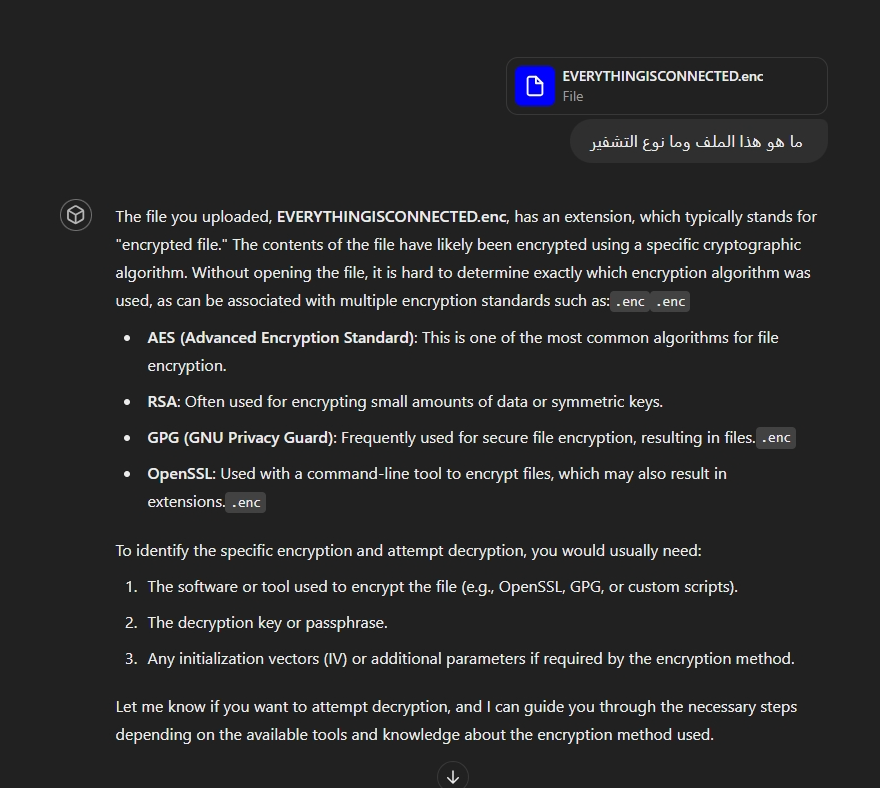
A screenshot of a computer program

Description automatically generated

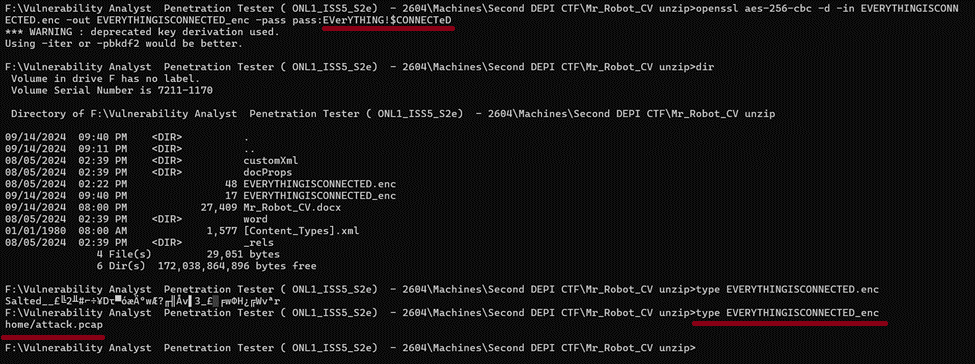
A screen shot of a computer

Description automatically generated

Now

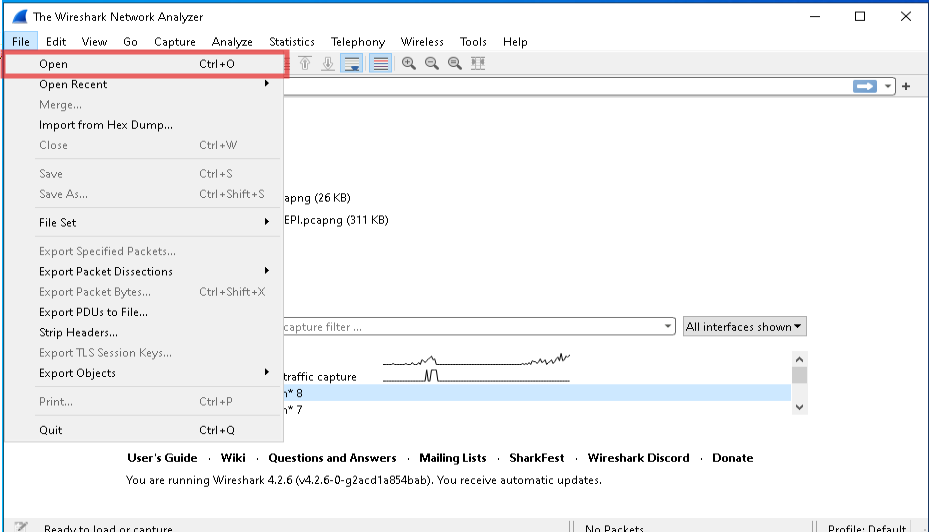


A screenshot of a computer

Description automatically generated  
openssl aes-256-cbc -d -in EVERYTHINGISCONNECTED.enc -out EVERYTHINGISCONNECTED\_enc -pass pass: EVerYTHING!$CONNECTeD  


Go to this URL <https://depi-ctfs.vercel.app/home/attack.pcap> after that we fine download file name “attack.pcap”

Can we open and analysis in Wireshark



A screenshot of a computer

Description automatically generated

---

\*\*4. Vulnerabilities Discovered\*\*

Provides a detailed list of all vulnerabilities identified during the penetration test. Each vulnerability should be described along with its potential impact, including screenshots or evidence where applicable.

---

\*\*5. Risk Assessment\*\*

Evaluates the severity and potential impact of each identified vulnerability. This section should categorize the vulnerabilities (e.g., Critical, High, Medium, Low) and provide an overall risk score for the organization’s security posture.

---

\*\*6. Recommendations\*\*

Offers actionable recommendations for mitigating or fixing the identified vulnerabilities. This section should be detailed, providing steps or guidance on how to address each issue.

---

\*\*7. Methods and Techniques\*\*

Provides a comprehensive account of all methods and techniques attempted during the penetration test, including both successful and unsuccessful attempts. This section helps demonstrate the thoroughness of the testing process.

---

\*\*8. Conclusion\*\*

Summarizes the overall security posture of the organization based on the findings from the penetration test. This section should also include recommended next steps for improving security.

---

\*\*9. Appendices\*\*

Includes supporting data such as raw test results, logs, scripts used, and any other relevant documentation that supports the findings and recommendations presented in the report.

---

This structure will help you create a thorough and professional penetration testing report. If you need further assistance in detailing any specific section, feel free to ask!