



# [Suninatas 21] Write-Up

작성자	윤지원
분석 일자	2024.05.09
작성 일자	2024.05.09
분석 대상	monitor.jpg
문서 버전	2.0
작성자 E-mail	<a href="mailto:yoonjw0827@gmail.com">yoonjw0827@gmail.com</a>

0. 목차

1. 문제 .....3

2. 분석 도구 .....3

3. 환경 .....3


4. Write-Up.....4

5. Flag.....7

6. 별도 첨부 .....8

7. Reference .....9

1. 문제

URL	<a href="http://suninatas.com/challenge/web21/web21.asp">http://suninatas.com/challenge/web21/web21.asp</a>
문제 내용	What is a Solution Key? Is it a Puzzle?
문제 파일	<div>  </div> <div>monitor.jpg</div>
문제 유형	jpg 파일 분석
난이도	1.5 / 5

2. 분석 도구

도구명	다운로드 링크	Version
HxD	<a href="https://mh-nexus.de/en/downloads.php?product=HxD20">https://mh-nexus.de/en/downloads.php?product=HxD20</a>	2.5.0.0

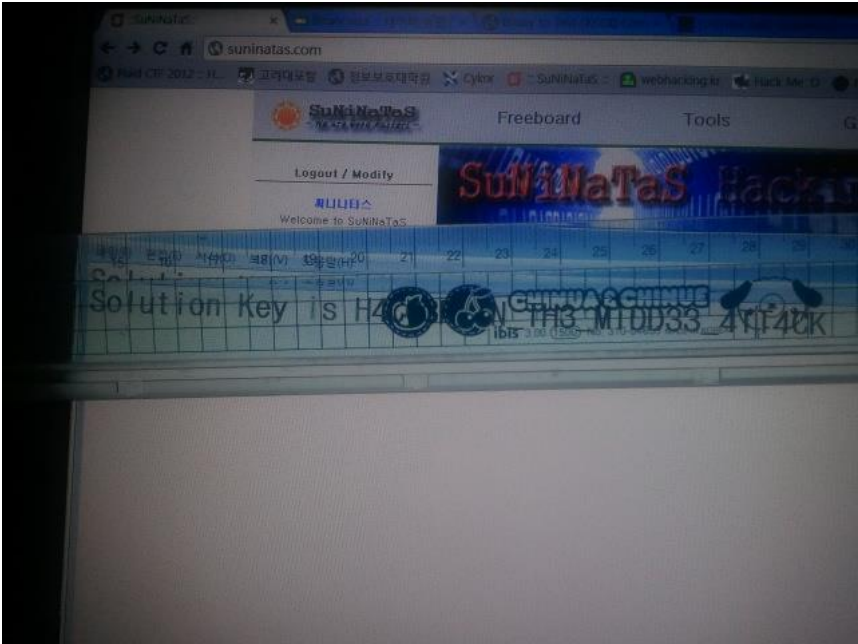
3. 환경

OS
Windows 11 64-bit

# 4. Write-Up

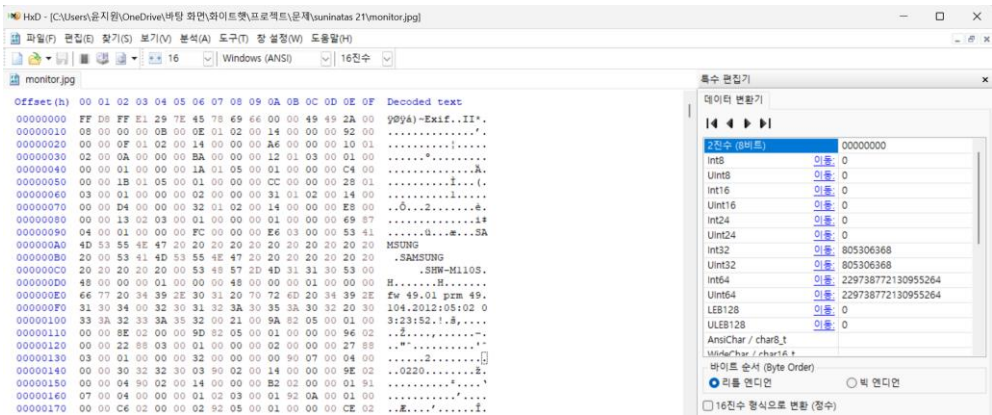
파일명	monitor.jpg
용량	1.40MB
SHA256	0376e7e8fb37ef10bb5ed22fcea654931dcc0244e05d6a4e77a3ba236d8f8308
Timestamp	2012-05-02 03:23:00

가장 먼저 문제 파일을 압축 풀면 monitor.jpg 파일이 하나 들어있다.



[사진 1] monitor.jpg 파일

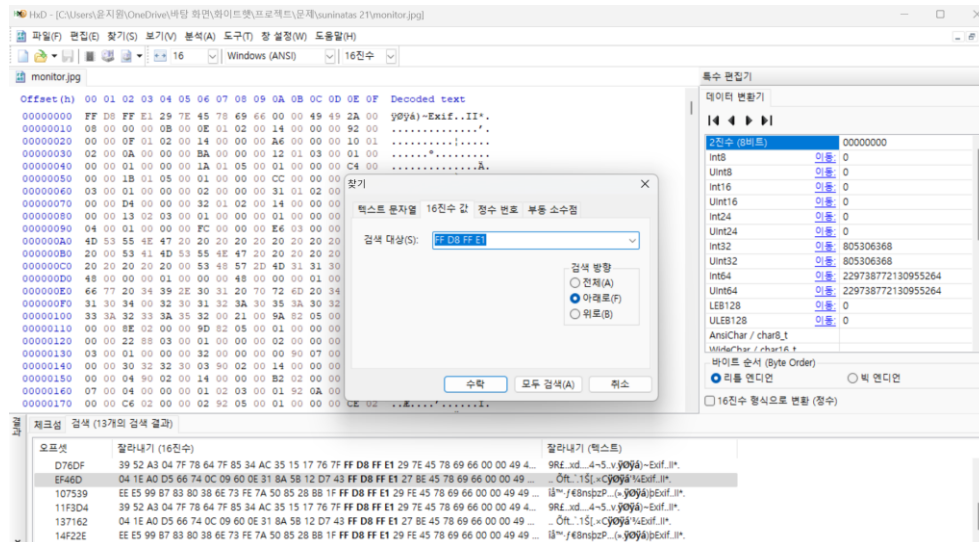
이 파일에 적혀있는 문구는 Solution Key is H4\*\*\*\*\*N\_TH3\_MIDD33\_4TT4CK이기 때문에 이 문구가 바로 이 문제의 flag 값이라고 생각하였다. 따라서 저기 가려져 있는 부분을 알아내는 것을 이 문제의 해결법으로 추정했다. 일반적으로 jpg 파일 분석할 때 사진의 바이트 정보를 파악하여 어떻게 구성되어 있는지를 살펴보기 때문에, HxD에 문제 파일을 넣어 보기로 했다.



[사진 2] HxD에 monitor.jpg 파일을 넣어본 모습



## [WHS-2] .iso

Jpg 파일을 HxD로 넣으면 FF D8 FF E1로 시작하는 것을 볼 수 있는데, 이는 파일 포맷 별로 가지고 있는 고유한 시그니처이다. 이를 통해 파일 포맷들을 구별할 수 있다. 조금 더 내려보니 FF D8 FF E1로 시작하는 부분을 하나 더 발견할 수 있었다. 그래서 이 이미지 파일에 또다른 이미지 파일이 숨겨져 있을 것이라고 생각하여 찾기를 통해 FF D8 FF E1을 검색해보았다.



[사진 3] FF D8 FF E1을 찾기 도구를 통해 찾는 모습

찾기 도구를 통해 jpg 파일의 시그니처를 검색해보니 총 13개의 부분이 검색되었다. 그 중 하나의 시그니처를 골라서 그 부분으로부터 다음 시그니처 부분 이전까지 드래그하여 선택하였다. 이 부분이 또다른 이미지 파일일 것이라고 생각하여 이를 생성하기 위해 '파일 - 지정된 부분만 저장하기' 버튼을 눌러보았다. 그러나 아무 파일 확장자도 안 붙이고 그냥 monitor2라고만 저장하면 파일이 열리지 않았다. 따라서 monitor2.jpg라고 확장자까지 붙여서 저장해보았다.

	monitor	유형: JPG 파일	찍은 날짜: 2012-05-02 오전 3:23 크기: 1.40MB
	monitor2	유형: JPG 파일	찍은 날짜: 2012-05-02 오전 3:25 크기: 96.1KB

[사진 4] monitor2.jpg가 저장된 모습

이렇게 저장하면 숨겨져 있던 jpg 파일이 제대로 저장된 것을 확인할 수 있었다. monitor2.jpg 파일을 열어보면 다음과 같은 이미지가 나온다.

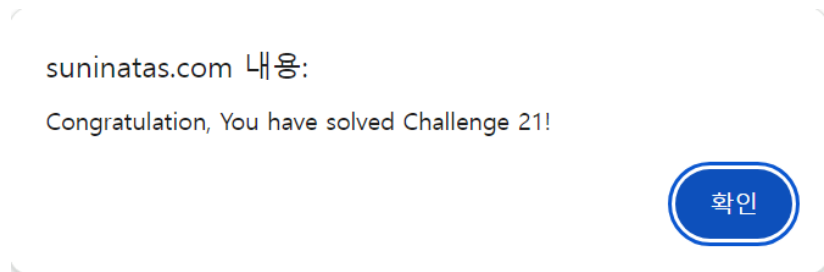


[사진 5] monitor2.jpg 파일

monitor1.jpg에서 가려졌던 key가 여기서는 보이는 것을 확인할 수 있다. 따라서 문구를 조합해보면 다음과 같다.

**Solution Key is H4CC3R\_IN\_TH3\_MIDD33\_4TT4CK**

해당 key를 Auth에 입력하면 다음과 같은 메시지가 출력된다.



[사진 6] 21번 문제를 성공적으로 해결했다는 메시지

## 5. Flag

H4CC3R\_IN\_TH3\_MIDD33\_4TT4CK

## 6. 별도 첨부



## 7. Reference

- [URL]