코드큐어 11주차 write-up

202321316 이승훈

1. WEB 1

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

이런 문제가 있다. 이 문제에서텍스트, 영수증, 폰트, 대수학이(가) 표시된 사진

자동 생성된 설명

이런 그림을 참고해서, 결과값이 result가 나오게 하는것이다.

거기서 나는 aadmin까지 예측함.

하지만 i 가 in으로 바뀌는 것을 못 봄

In을 i로 치환하면, aadmi 이다.

Aad는 또 a로 바뀐다고 했으니.

값은 ami가 된다.

거기서 하나 까먹은게 있는데, 2번재에서 2개를 가져오고, 4번째에서 6개까지 가져온다.

총 5개를 가져온다.

aadmin에서 admin을 가져오기 때문에, ami가 되는것이다.

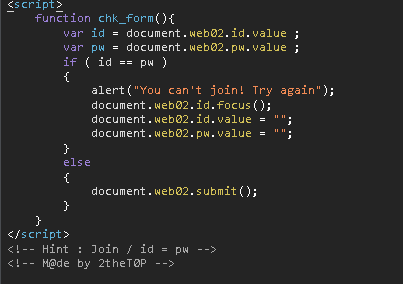
나한테는 조금 까다로웠음.(나만 그랬나?)

1. WEB -2

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

이런 문제가 있는데, F12를 눌러서 web02.asp 라는 파일에 들어가보면,



뭔 이런 코드가 있다. Id와 pw가 같으면 못들어간다는 그런 내용인데, 거기서 바로 콘솔창에 들어가서 해도 된다. (까먹음….)

근데 주석에 보면 아이디와 pw가 같아야 한다고 되어있는데, 분명 같으면 못들어간다고 했음.

(뭐 어떻게 하라고….)

우리는 burp를 이용해서 할껀데, intercept 를 이용해서 할것이다.

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

짜잔. 이런 화면이 떳는데, 아까 개발자 도구에서 주석 내용에서 id=pw가 되야한다고 했는데,

이게 그 내용이다!!

그때 몇주전에 우리가 코드큐어 사이트를 해킹 같은 걸 했을대, 게시글을 접근할수 없는 곳에 올리는 그런거를 했었다.

그 원리를 이용해서 맨 아래의 id와 pw를 같게 한다음에 forward를 눌러서 authkey를 얻는다.

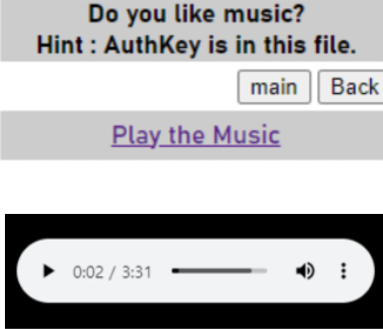
텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

헿헿헿헿헿헿헿헿헿헿헿헿헿헿~~~

1. FORENSIC-15

내가 조금은 귀찮아 하는 포렌식이 나왔는데, 한번 풀어보도록 하자



키가 이 파일속에 있다고 한다.

실제로 이 파일을 받아서 속성에 들어가보면 무슨 이상한 영어 문자가 나온다.

(분명 이 노래와 상관없는 영어 문자가 나온다…)

텍스트, 스크린샷, 폰트이(가) 표시된 사진

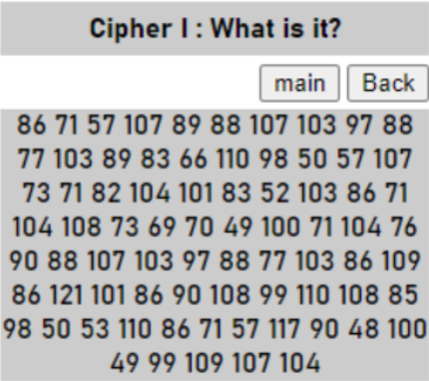
자동 생성된 설명

(아니 솔직히 참여 음악가, 앨범 음악가가 나비이고, 지휘자도 분명히 나비일것인데, 뜬금없이

GoodjobMetaTagSearch 가 나온다.

이게 바로 그 키이다!!!

1. FORENSIC-18



오잉? 뭐지 할수도 있겠지만 공대를 나왔거나 다니고 있다면 아스키코드라는 것을 한번에 알아차릴수 있다.

이를 해독하면, VG9kYXkgaXMgYSBnb29kIGRheS4gVGhlIEF1dGhLZXkgaXMgVmVyeVZlcnlUb25nVG9uZ0d1cmkh

가 나오는데, 그게 답일리는 없으니 또 해독한다.

Today is a good day. The AuthKey is VeryVeryTongTongGuri!

히히히히히히히히히히히히히

답이 VeryVeryTongTongGuri! 이거라네…

이게 답임.