|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | |
|  | |  | |
| CTF 문제 풀이 보고서  *CTF문제 1회차* | | | |
| 2019-11-14 |  | |  |
|  |  | | 권원준 |

목차

[Senegal-Quiz1 2](#_Toc24645367)

[South Africa-Quiz2 2](#_Toc24645368)

CTF 문제 풀이 보고서

CTF문제 1회차

# Senegal-Quiz1

▶인터넷 상의 서버를 통해 데이터 저장, 네트워크, 콘텐츠 사용 등 IT 관련 서비스를 자신의 컴퓨터가 아닌 다른 컴퓨터로 사용할 수 있는 컴퓨팅 환경이란?

정답: 클라우드 컴퓨팅 → BASE64 Encoding: 7YG065287Jqw65Oc7Lu07ZOo7YyF

# South Africa-Quiz2

▶바이러스, 웜 등 시스템에 해를 입히거나 시스템을 방해하기 위해 설계된 악성 소프트웨어

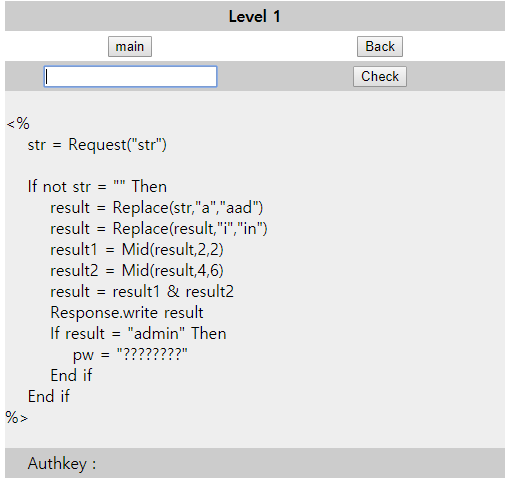
정답: 멀웨어 → BASE64 Encoding: 66mA7Juo7Ja0

# Finland-Quiz3

▶ ????은 2010년 6월에 발견된 웜 바이러스이다. 마이크로소프트 윈도를 통해 감염되어, 지멘스 산업의 소프트웨어 및 장비를 공격한다. 이 웜이 산업시설을 공격하는 최초의 악성 소프트웨어는 아니지만, 산업시설을 감시하고 파괴하는 악성 소프트웨어로는 최초인 악성코드의 이름은 무엇인가?

정답: 스턱스넷 → BASE64 Encoding: 7Iqk7YSx7Iqk64S3

# Poland-Find the password



우선 이 문제는 웹언어인 ASP를 통해 작성되어 있는데 구현이 간단한 장점이 있다. 코드를 보자.

먼저 str에 “str”이라는 문자열을 요청한다.

if문을 통해 str변수가 공백이 아니라면 다음 코드를 실행한다.

Replace는 치환하는 함수로서 ‘Replace(문자열, 치환될 문자열, 치환할 문자열)’의 형식으로 사용한다. Replace(str, “a”, “aad”)는 str에 있는 a문자열을 aad로 치환한다는 함수이다. 그리고 치환 값을 result라는 변수에 넣어준다.

위와 같이 다시 result의 값에서 i를 in으로 치환해 return에 넣어준다.

Mid는 문자열의 일부를 가져오는 함수인데 ‘Mid(문자열, 시작위치, 가져올 개수)’의 형식으로 사용한다. Mid(result, 2, 2)는 result의 2번째 위치에서 2개의 문자를 가져와 result1에 넣는다.

Mid(result, 4, 6)은 result의 4번째 위치에서 6개의 문자를 가져와 result2에 넣는다.

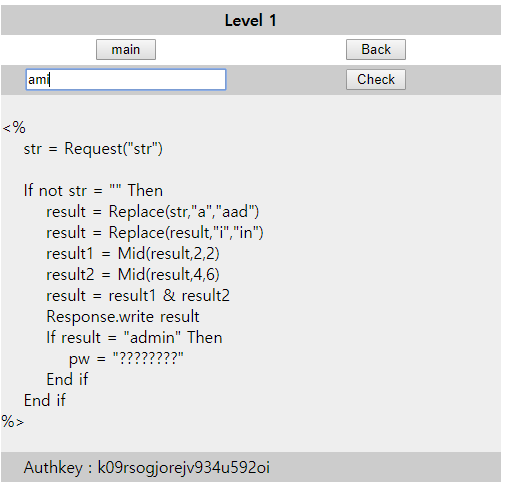
다시 result에 result1과 result2를 합쳐 넣어준다.

Response.write()함수는 문자열을 출력하기 위해서 사용한다. Response.write result를 통해 result를 출력한다.

If문을 통해 만약 result가 “admin”이라면 pw가 나타난다.

Str에 ami를 요청한다면 ami -> aadmi -> aadmin , result1 = ad, result2 = min, resut = admin

Result가 admin이 나오므로 pw가 나타난다.



정답: ami → BASE64 Encoding: YW1p

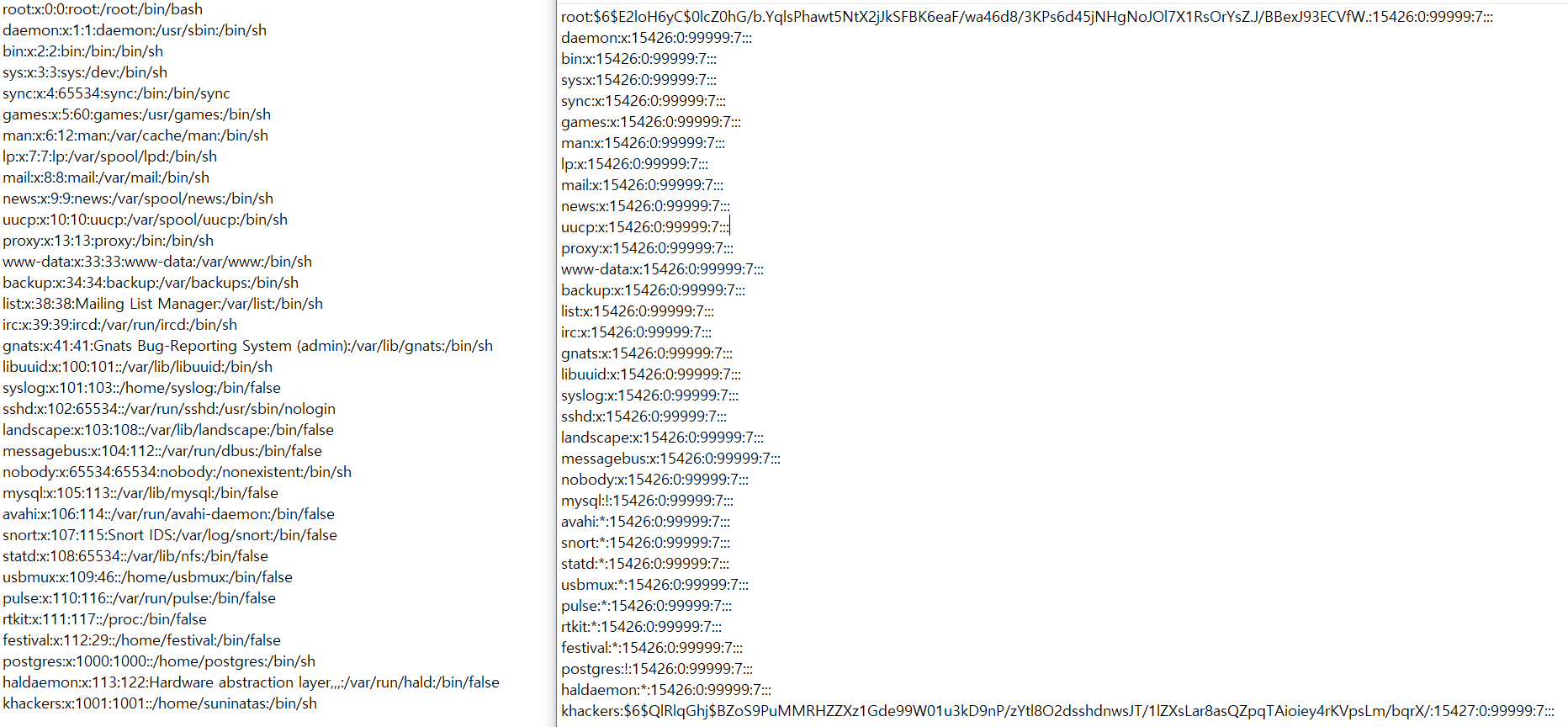
# Philippines-Do you know password?

▶Find the khackers linux password?

Linux 패스워드를 알아내는 것이므로 우선 우분투 환경이라는 것을 알 수 있다. 첨부된 파일을 보자.



Passwd와 shadow라는 두 파일이 있는데 작성된 형식이 우분투 환경에서 쓰이는 것 같다.



먼저 비밀번호는 사용자 계정 정보에 담겨 있을 것 같아 사용자 정보가 어떤 식으로 저장되어 있는지 확인했다.

**-사용자 정보**  시스템 관리자가 사용자 계정을 만들 때마다 해당 사용자와 관련된 정보를 /etc/passwd파일에 저장함. 시스템을 이용하는데 필요한 기본 정보들이 담겨 있다. 구분자 ‘:’를 사용해 7개의 필드로 구분한다.

예시) root:x:0:0:root:/root:/bin/bash

1. root: 사용자 계정, 로그인 이름
2. x: 사용자의 패스워드
3. 0: 사용자 ID로 특정 사용자를 나타내는 숫자로 된
4. root: 사용자 관련 기타 정보(코멘트, 공지사항)
5. /root: 로그인에 성공한 후에 사용자가 위치할 홈 디렉토리 명
6. /bin/bash: 명령어를 처리하는 쉘의 종류를 지정

**-패스워드 암호화**

/etc/shadow 파일에 각 사용자 계정에 대한 패스워드가 암호화 되어 있음

khackers:$6$QlRlqGhj$BZoS9PuMMRHZZXz1Gde99W01u3kD9nP/zYtl8O2dsshdnwsJT/1lZXsLar8asQZpqTAioiey4rKVpsLm/bqrX/:15427:0:99999:7:::

$6$QlRlqGhj$BZoS9PuMMRHZZXz1Gde99W01u3kD9nP/zYtl8O2dsshdnwsJT/1lZXsLar8asQZpqTAioiey4rKVpsLm/bqrX/:

위 부분이 암호화된 패스워드이며 $hashid $salt $hash value

$6은 SHA512, $1: MD5, $2: blowfish, $5: SHA256

$QlRlqGhj은 salt값

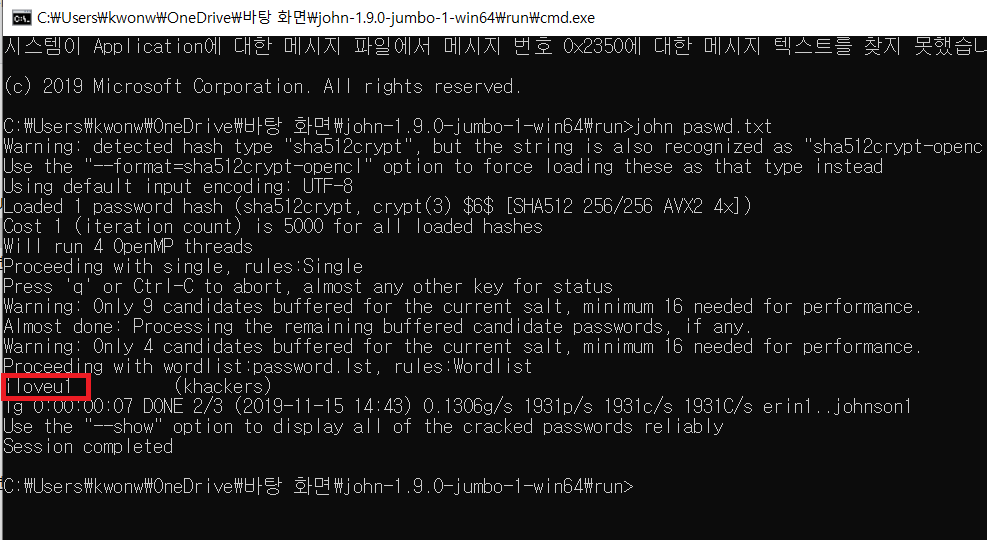
$BZoS9PuMMRHZZXz1Gde99W01u3kD9nP은 salt값 + 사용자 입력 패스워드

출처: <https://eunguru.tistory.com/88>

Shadow의 암호화된 영역을 해독하기 위해 크랙 툴인 john the ripper를 사용했다.

다운로드 받은 john the ripper툴 안의 run파일안에 해독하고자 하는 부분을 텍스트 파일형태로 넣어준다.

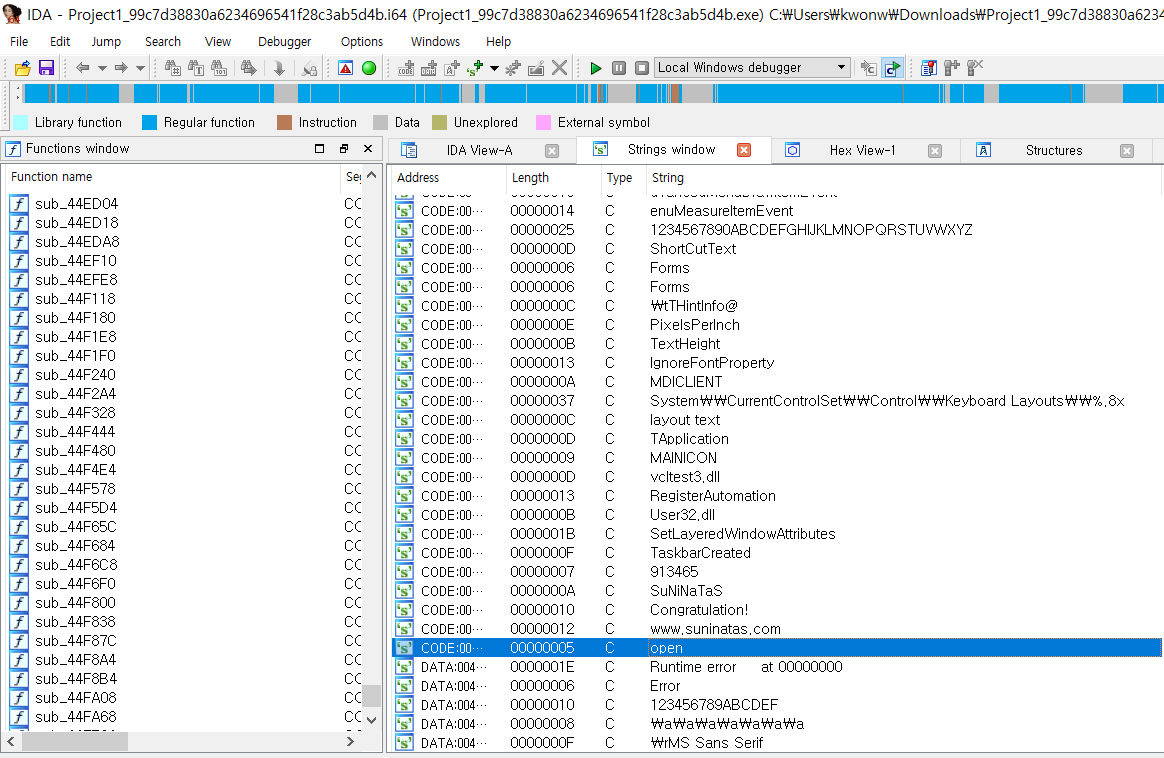
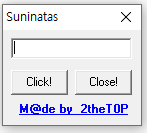
그 뒤 층에 해당 경로로 명령어 john 텍스트파일명.txt를 입력해준다면 아래와 같이 결과가 나온다.



Password는 ilove1이다.

정답: iloveu1 → BASE64 Encoding: aWxvdmV1MQ==

# Newzealand-Find The Flag



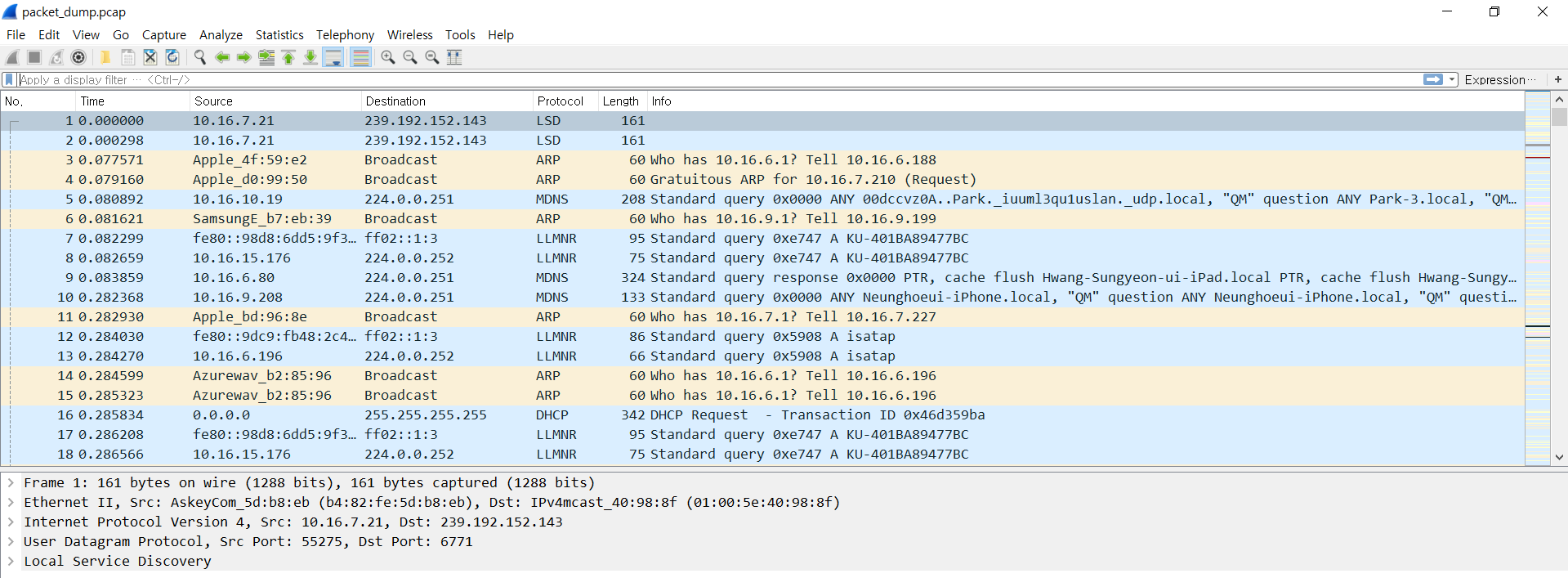
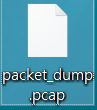
Flag값을 찾는 리버싱 문제이다. 우선 리버싱 툴인 IDA를 통해 파일을 열어보았다.

String.window에서 스트링 값들을 확인한 결과 suninatas와 congratulation!의 위에 있는 숫자가 암호 같아 base64인코딩 결과 정답이다.

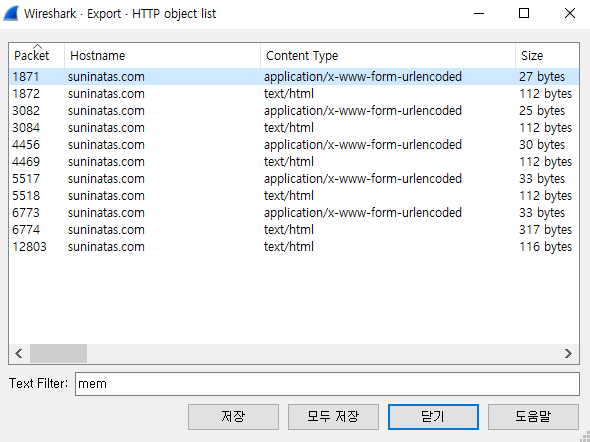
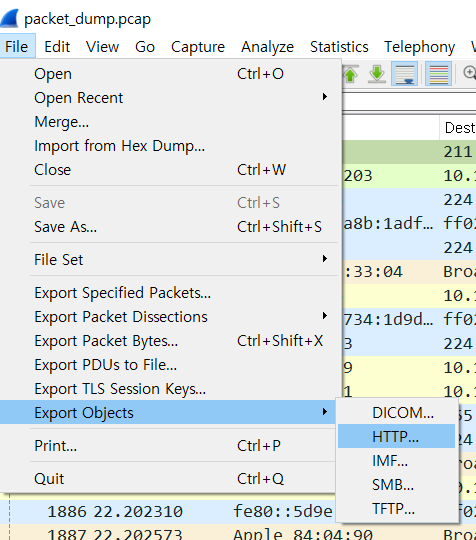
정답: 913465 → BASE64 Encoding: OTEzNDY1

# Turkey-Can you use Wireshark?

▶ Can you find the password for a member of SuNiNaTaS.com?



pcap파일은 많은 네트워크 툴에서 캡쳐 된 네트워크 데이터를 저장하는데 사용된다. 이러한 pcap파일형식은 Wireshark, TcpDump/WinDump, snort등의 네트워크 툴을 이용한다. 위 화면은 Wireshark를 이용해 packet\_dump파일을 연 화면이다.



suNiNaTaS.com이라는 페이지에서 멤버의 비밀번호를 찾아내려면 로그인 서버와 클라이언트 사이에 데이터를 주고 받는 통신 프로토콜인 http를 찾는다. 그 중 file형식 중 mem이라는 파일들이 보이는데 member의 정보가 들어있다. 그리고 이 content Type들은 HTTP프로토콜의 전송 메소드 중 POST메소드의 content Type들이다.

1. application/x-www-form-urlencoded
2. text/plain
3. multipart/form-data

위 content Type중 1번 형식에서 BODY에 key와 value쌍으로 데이터가 들어있다.

5개의 항목을 찾아보면 value값으로 pw는 5개를 찾을 수 있는데 suninatas, blackkey, sharkpass0, =sharkpass01, =SharkPass01이다.

모두 시도한 결과 =SharkPass01이 정답이었다.

정답: =SharkPass01→ BASE64 Encoding: PVNoYXJrUGFzczAx