

# SCP CTF 2020

---

2020.09.22 Crypto & Web

# Challenges

START

100

FOR A+

200

Can you login?

200

# START

---

정보보호학과 여러분들은 이 암호문을  
배운 적이 있습니다!  
가장 오래되었으며 가장 간단한 암호문 중  
하나인 이 암호문을 해독하세요!

MESSAGE : WKLV\_LV\_D\_FDHVDU\_FLSKHU

flag형식 : scpCTF{MESSAGE}

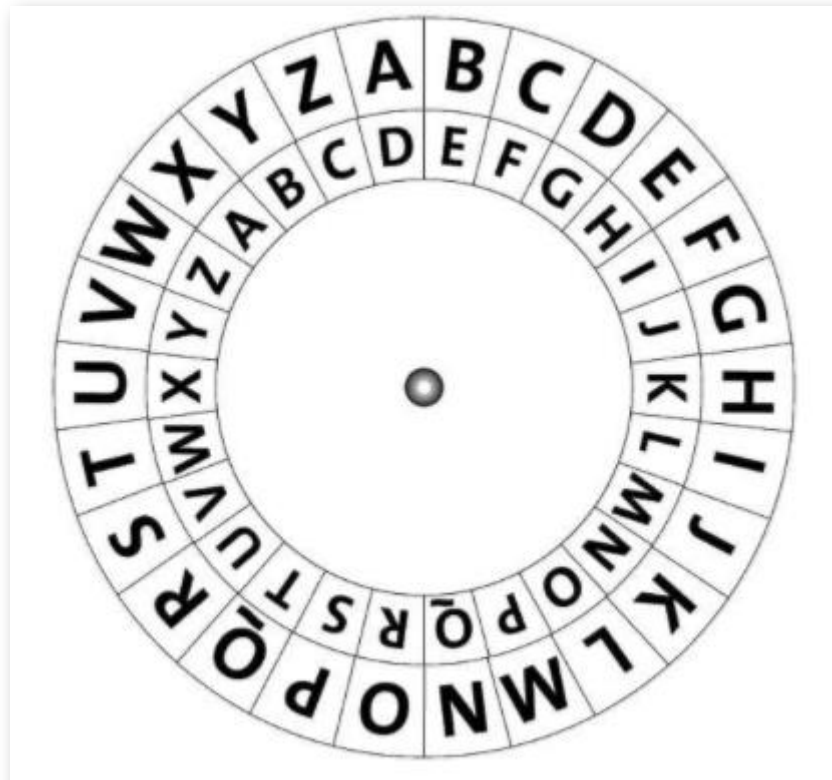
START

100

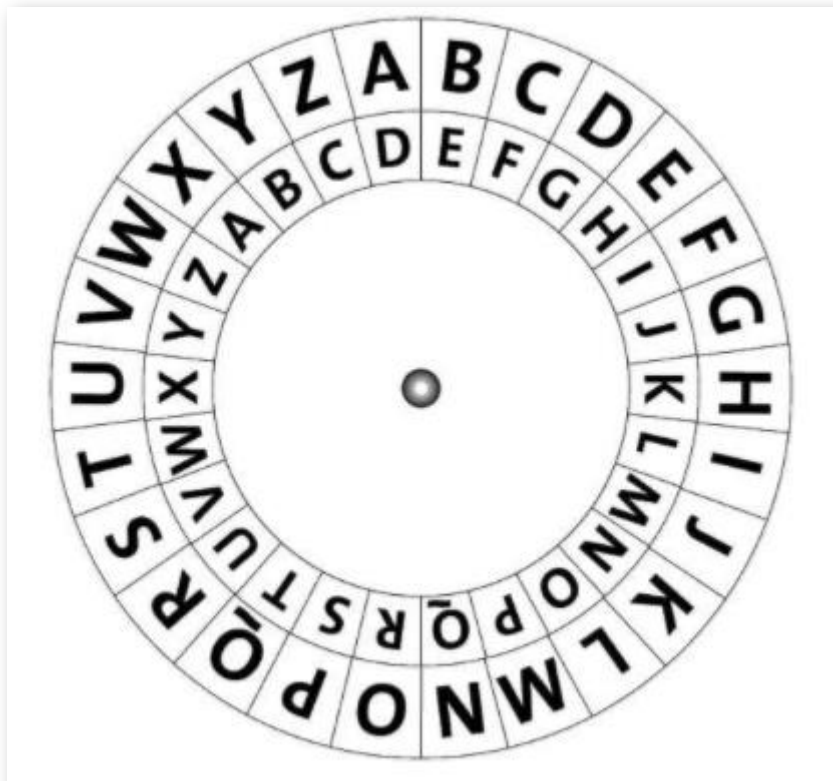
Can you login?

200

# START



# START

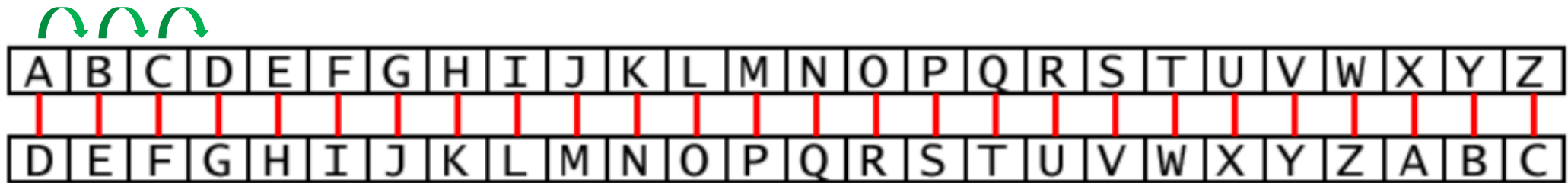


## 시저 암호 (Caesar Cipher)

각각의 알파벳을 정해진 규칙에 따라 치환하여  
사용하는 암호화 방식

# START

WKLV\_LV\_D\_FDHVDU\_FLSKHU



# START

WKLV\_LV\_D\_FDHVDU\_FLSKHU

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

# START

## 적분의 수학 이야기

🏠 Home

📁 수학과 암호

📁 소수와 인수분

### 카이사르 암호 변환기

카이사르 암호 방식으로 평문을 암호화하거나, 암호문을 해독할 수 있습니다.

WKLV LV D FDHVDU FLSKHU

암호화

복호화

this\_is\_a\_caesar\_cipher



# START

---

정보보호학과 여러분들은 이 암호문을  
배운 적이 있습니다!  
가장 오래되었으며 가장 간단한 암호문 중  
하나인 이 암호문을 해독하세요!

MESSAGE : WKLV\_LV\_D\_FDHVDU\_FLSKHU

flag형식 : scpCTF{MESSAGE}

START

100

Can you login?

200

# Challenges

START

100

FOR A+

200

Can you login?

200

# FOR A+

---

공개키 암호 알고리즘의 하나인  
RSA 암호문을 해독하실 수 있으신 가요?  
이걸 푼다면 당신은 정보보호학개론 A+!!

flag형식 : scpCTF{MESSAGE}

RSA.txt

scpCTF{...}

Submit

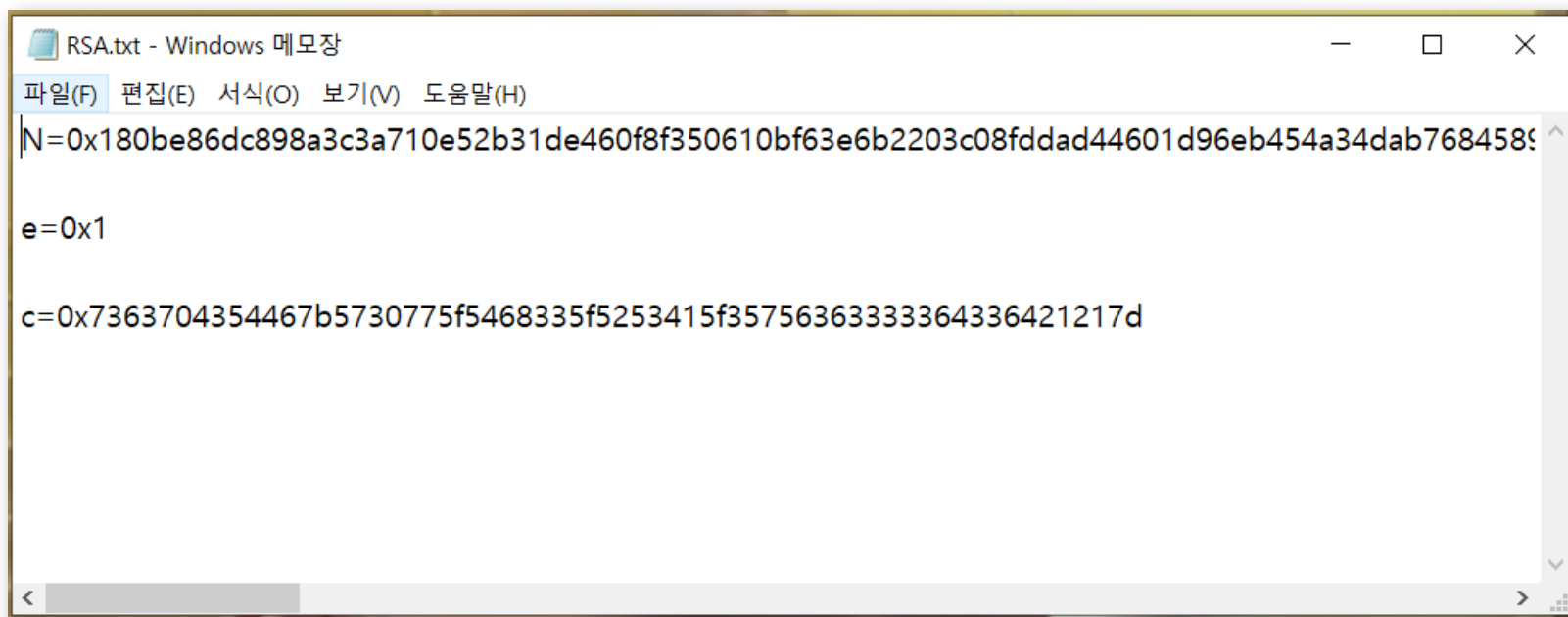
CUTE CAT

100

Can you login?

200

# FOR A+



```
RSA.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
N=0x180be86dc898a3c3a710e52b31de460f8f350610bf63e6b2203c08fddad44601d96eb454a34dab7684589
e=0x1
c=0x7363704354467b5730775f5468335f5253415f3575636333364336421217d
```

FOR A+



# FOR A+



## RSA (Rivest Shamir Adleman)

공개키 암호 알고리즘의 하나이며  
평문과 암호문 모두 숫자로 나타낸다.

512, 1024, 2048, 4096 등의 다양한 버전이 존재한다.

# FOR A+

암호화  $C = M^e \bmod n$

복호화  $M = C^d \bmod n$

$C$  = 암호문  $M$  = 평문  $e$  = 공개키  $d$  = 개인키

# FOR A+

step1. 두개의 큰 소수  $p, q$ 를 선정한다.(예시에서는 작은 수로 한다.)

(ex :  $p=11, q=13$ )

step2.  $p-1, q-1$ 과 각각 서로소인 정수  $e$ 를 찾는다.

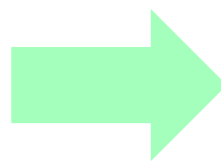
(ex :  $p=11, q=13, e=7$ )

step3.  $ed$ 를  $(p-1)(q-1)$ 로 나눈 나머지가 1이 되도록 하는  $d$ 를 찾는다.

(ex :  $p=11, q=13, e=7, d=103$ )

step4.  $N=pq$ 를 계산 후  $(N,e)$ 는 공개키로  $(N,d)$ 는 개인키로 가진다.

(ex :  $p=11, q=13, e=7, d=103, N=143$ )



**복잡하다!!!!**



# FOR A+



```
*RSA복호화.py - C:/Users/jin36/OneDrive/바탕 화면/CTF/JBUCTF/Crypto_qoqokim/RSA/RSA복호화.py ...
File Edit Format Run Options Window Help
N=0x180be86dc898a3c3a710e52b31de460f8f350610bf63e6b2203c08fddad44601d96eb4!

e=0x1

c=0x7363704354467b5730775f5468335f5253415f35756363333364336421217d

plainText= hex(pow(c,e,N))
plainText= plainText.replace('0x', '')

plainText= bytes.fromhex(plainText).decode('utf-8')

print (plainText)
```

# FOR A+

```
*RSA복호화.py - C:/Users/jin36/OneDrive/바탕 화면/CTF/JBUCTF/Crypto_qoqokim/RSA/RSA복호화.py ...
File Edit Format Run Options Window Help
N=0x180be86dc898a3c3a710e52b31de460f8f350610bf63e6b2203c08fddad44601d96eb4!
e=0x1
c=0x7363704354467b5730775f5468335f5253415f35756363333364336421217d
plainText= hex(pow(c,e,N)) (c^e)%N
plainText= plainText.replace('0x', '')
plainText= bytes.fromhex(plainText).decode('utf-8')
print (plainText)
```

# FOR A+

```
*RSA복호화.py - C:/Users/jin36/OneDrive/바탕 화면/CTF/JBUCTF/Crypto_qoqokim/RSA/RSA복호화.py ...
File Edit Format Run Options Window Help
N=0x180be86dc898a3c3a710e52b31de460f8f350610bf63e6b2203c08fddad44601d96eb4!
e=0x1
c=0x7363704354467b5730775f5468335f5253415f35756363333364336421217d

plainText= hex(pow(c,e,N))
plainText= plainText.replace('0x', '')
plainText= bytes.fromhex(plainText).decode('utf-8')
print (plainText)
```

숫자가 너무 길기 때문에  
0x 를 띄어쓰기로 바꾸어야 한다!

# FOR A+

```
*RSA복호화.py - C:/Users/jin36/OneDrive/바탕 화면/CTF/JBUCTF/Crypto_qoqokim/RSA/RSA복호화.py ...
File Edit Format Run Options Window Help
N=0x180be86dc898a3c3a710e52b31de460f8f350610bf63e6b2203c08fddad44601d96eb4!
e=0x1
c=0x7363704354467b5730775f5468335f5253415f35756363333364336421217d

plainText= hex(pow(c,e,N))
plainText= plainText.replace('0x', '')
plainText= bytes.fromhex(plainText).decode('utf-8')
print (plainText)
```

16진수를 문자열로 읽기 위해  
fromhex() 사용

# FOR A+

```
= RESTART: C:/Users/jin36/OneDrive  
y  
scpCTF{W0w_Th3_RSA_5ucc33d3d!!}
```

# FOR A+

왜 N, E, C 만으로 복호화를 할 수 있을까?

평문 M 을 암호화  
한 게 C라고 했을 때 ←

$$C = M^e \pmod N$$

$$C' = C \times r^e \pmod N$$

$$(C')^d = (C \times r^e)^d = (M^e \times r^e)^d = M^{e \times d} \times r^{e \times d} = M \times r$$

# FOR A+

---

공개키 암호 알고리즘의 하나인  
RSA 암호문을 해독하실 수 있으신 가요?  
이걸 푼다면 당신은 정보보호학개론 A+!!

flag형식 : scpCTF{MESSAGE}

RSA.txt

scpCTF{W0w\_Th3\_RSA\_5ucc33d3d!!}

Submit

START

100

Can you login?

200

# Challenges

START

100

FOR A+

200

Can you login?

200



# Can you login?

---

플래그를 확인하기 위해선

로그인이 필수입니다!!

이 문제에 도전하고 있는 당신...!

혹시 로그인에 성공하실 수 있으신가요??!

URL

scpCTF{...}

Submit

CUTE CAT

100

Can you login?

200

# Can you login?

로그인 화면

로그인 페이지

127.0.0.1/login\_h.php

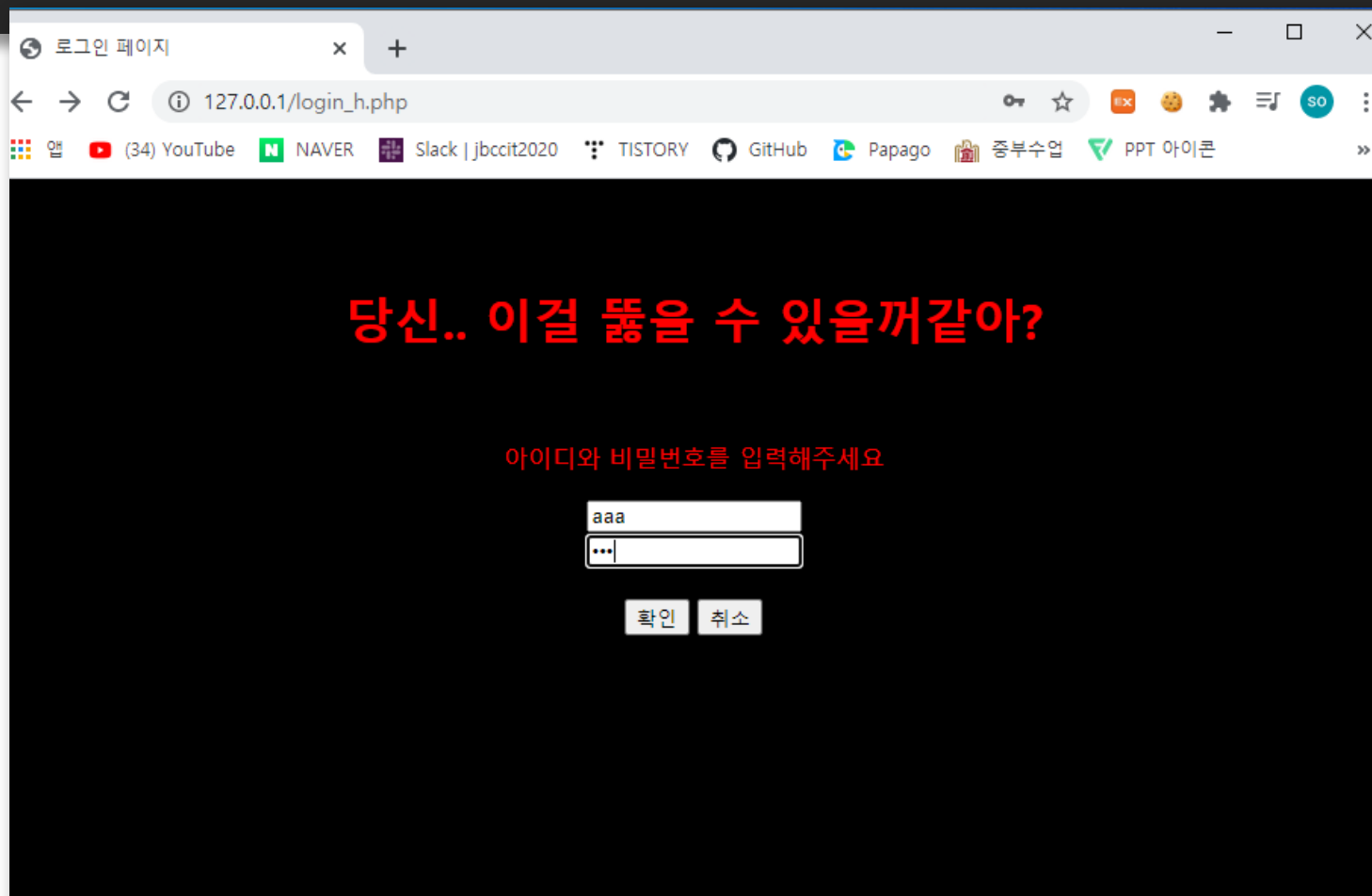
당신.. 이걸 뚫을 수 있을까같아?

아이디와 비밀번호를 입력해주세요

확인 취소

# Can you login?

잘못된 로그인 시도



The screenshot shows a web browser window with the title '로그인 페이지' (Login Page) and the address bar displaying '127.0.0.1/login\_h.php'. The browser's toolbar includes navigation buttons, a search bar, and various extension icons. The main content area has a black background with red text that reads '당신.. 이걸 뚫을 수 있을꺼같아?' (You.. I think you can break this?). Below this, a smaller red text prompt says '아이디와 비밀번호를 입력해주세요' (Please enter your ID and password). There are two input fields: the first contains 'aaa' and the second is empty with a password mask icon. At the bottom, there are two buttons labeled '확인' (Confirm) and '취소' (Cancel).

로그인 페이지

127.0.0.1/login\_h.php

당신.. 이걸 뚫을 수 있을꺼같아?

아이디와 비밀번호를 입력해주세요

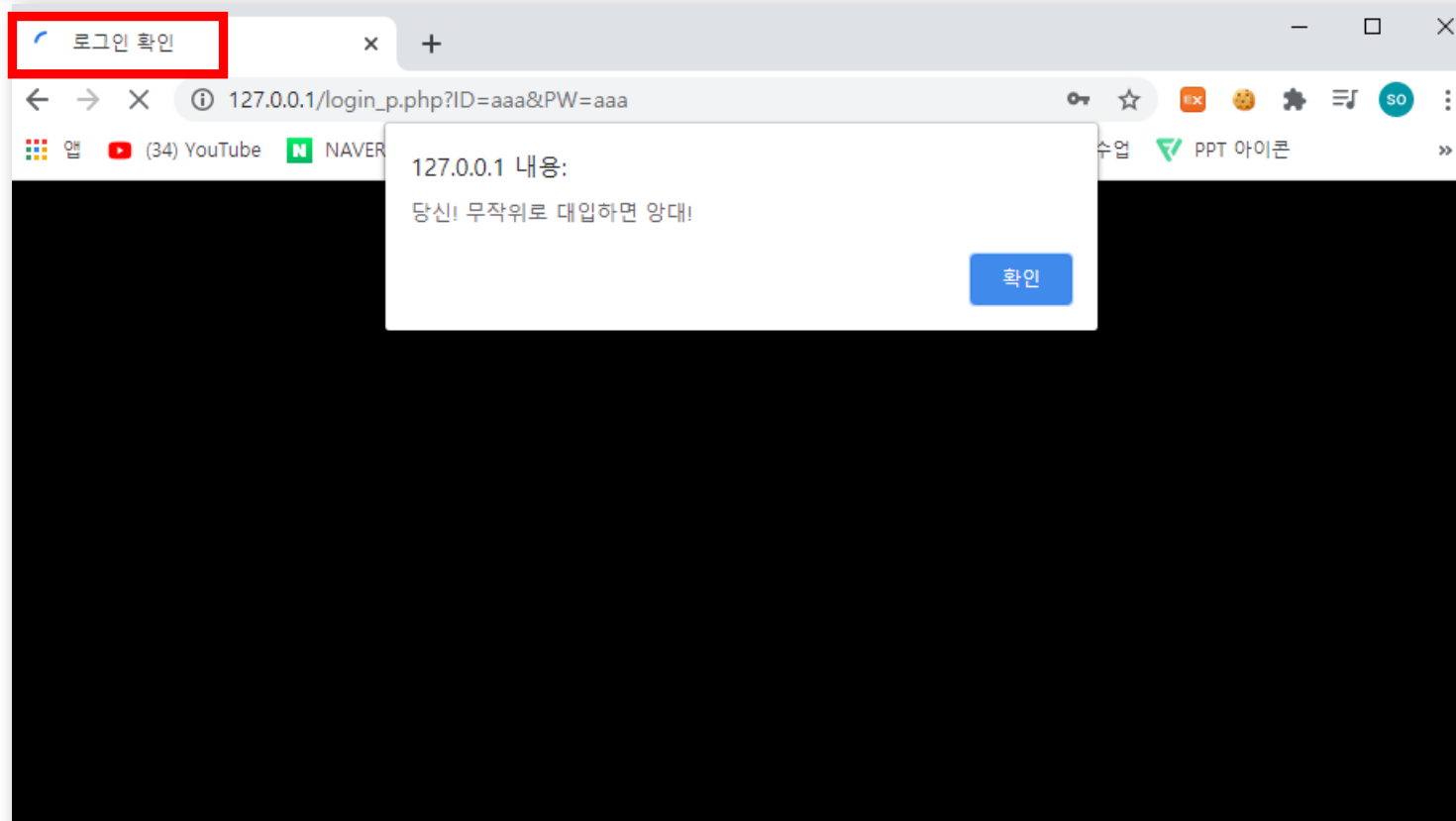
aaa

...

확인 취소

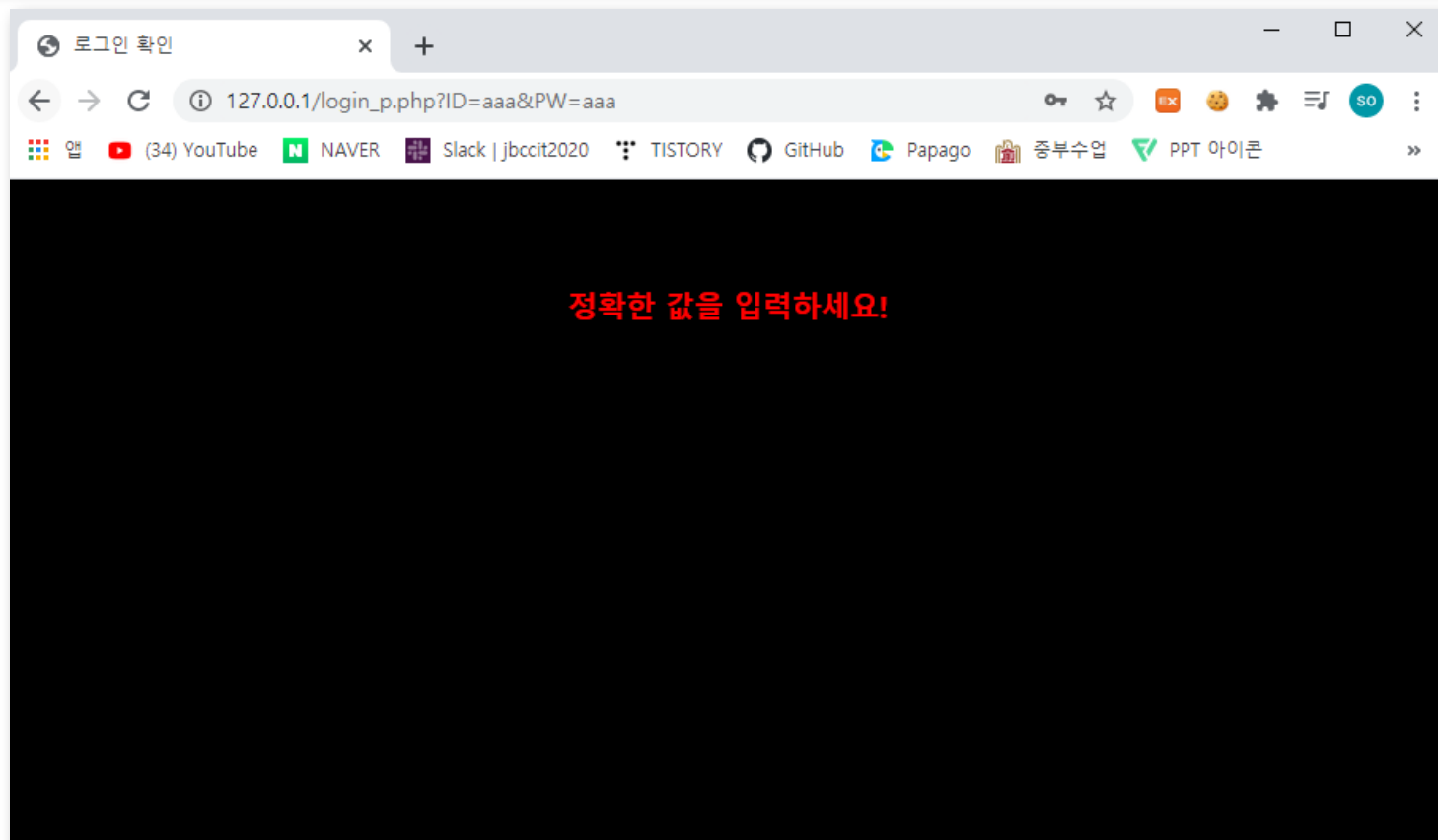
# Can you login?

잘못된 로그인 시도



# Can you login?

잘못된 로그인 시도



# Can you login?

The screenshot shows a web browser window with the title '로그인 페이지' (Login Page). The address bar displays '127.0.0.1/login\_h.php'. The browser's toolbar includes navigation buttons, a star icon, and several extension icons. The main content area has a black background with red text that reads '당신.. 이걸 뚫을 수 있을꺼같아?' (You.. I think you can break this?). Below this, a smaller red text prompt says '아이디와 비밀번호를 입력해주세요' (Please enter your ID and password). There are two white input fields for text entry. At the bottom, there are two buttons: '확인' (Confirm) and '취소' (Cancel).

로그인 페이지

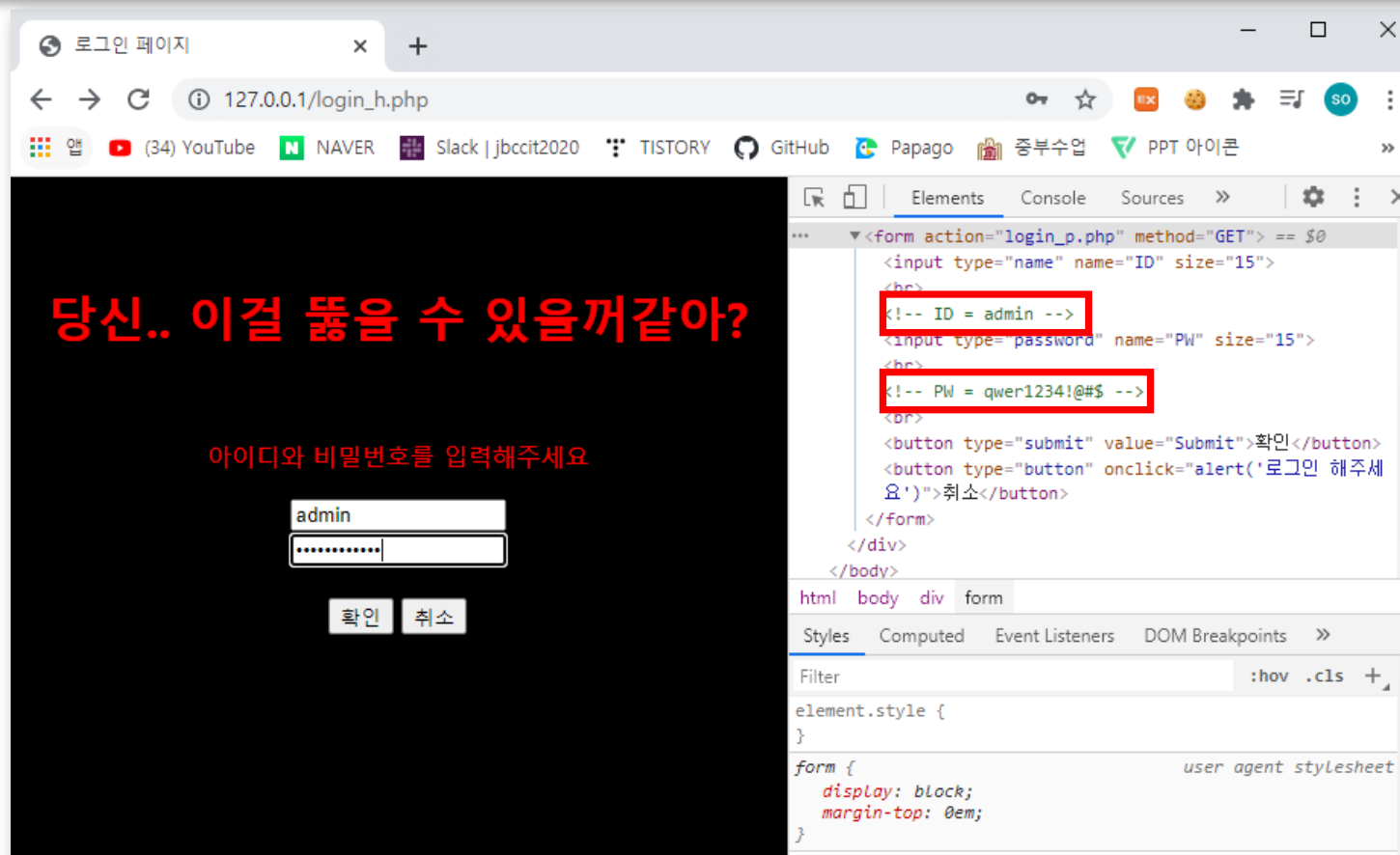
127.0.0.1/login\_h.php

당신.. 이걸 뚫을 수 있을꺼같아?

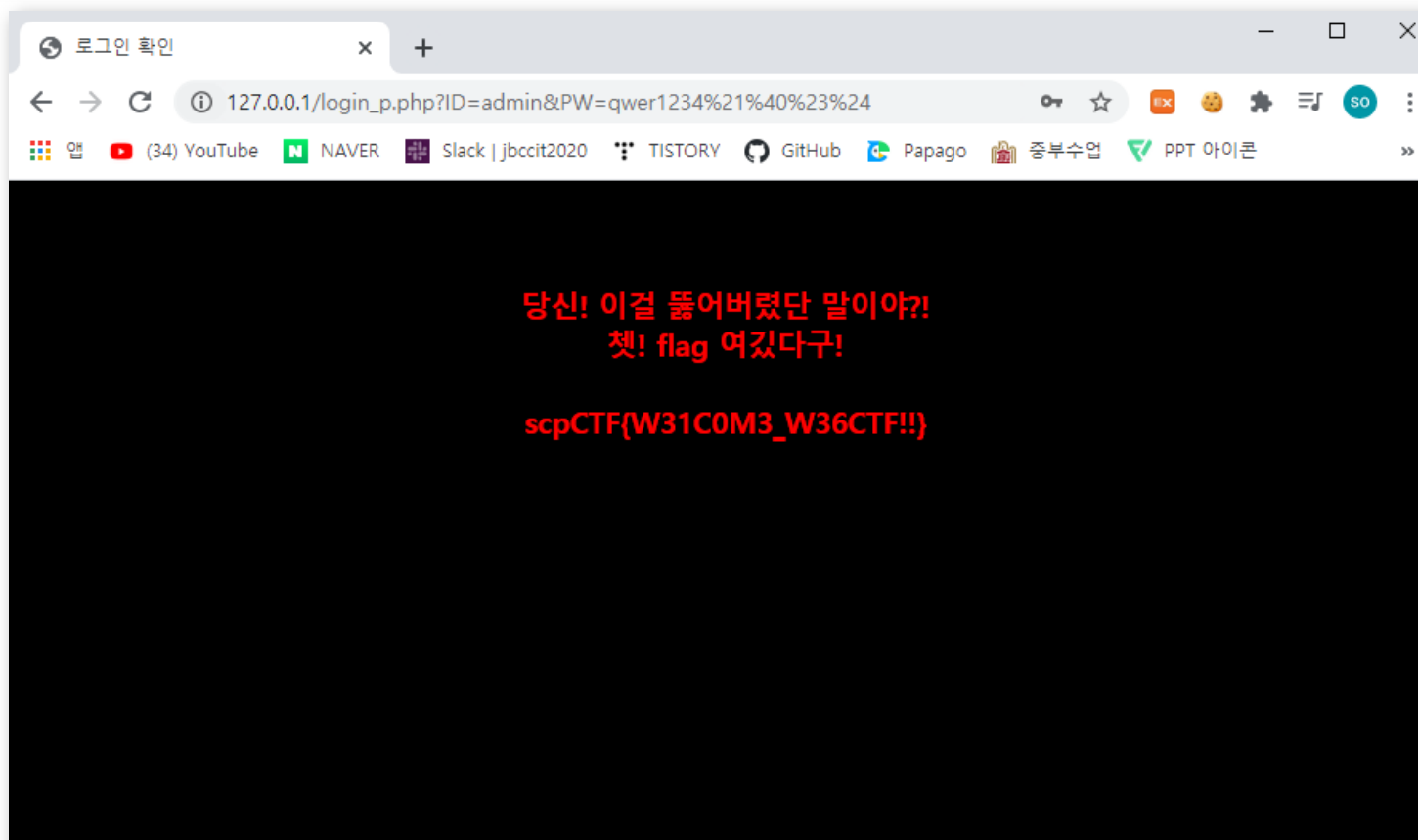
아이디와 비밀번호를 입력해주세요

확인 취소

# Can you login?



# Can you login?





# Can you login?

---

플래그를 확인하기 위해선

로그인이 필수입니다!!

이 문제에 도전하고 있는 당신...!

혹시 로그인에 성공하실 수 있으신가요??!

URL

scpCTF{W31C0M3\_W36CTF}

Submit

CUTE CAT

100

Can you login?

200

# Challenges

START

100

FOR A+

200

Can you login?

200

# Thank you

---

2020.09.22 Crypto & Web