브루트 포스 공격

2024-01-10 IT정보공학과 이진규

TABLE OF CONTENTS

목차

01 브루트 포스 공격

무차별 암호 대입 공격

특정 정보(주로 패스워드)를 알아내기 위한 공격

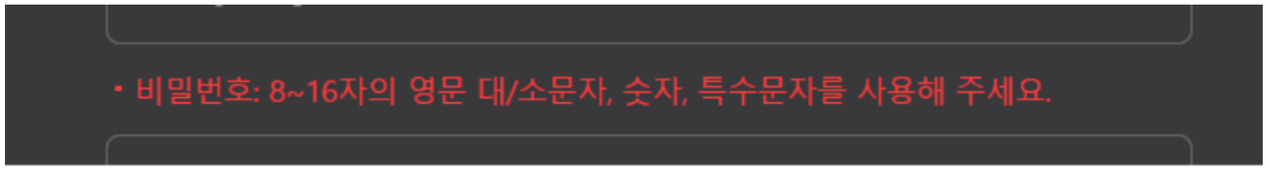
비밀번호, 암호화 키, PIN 번호 등 무작위의 값을 계속 입력

조합 가능한 모든 문자열을 하나씩 대입해 보는 방식

02 정보 수집

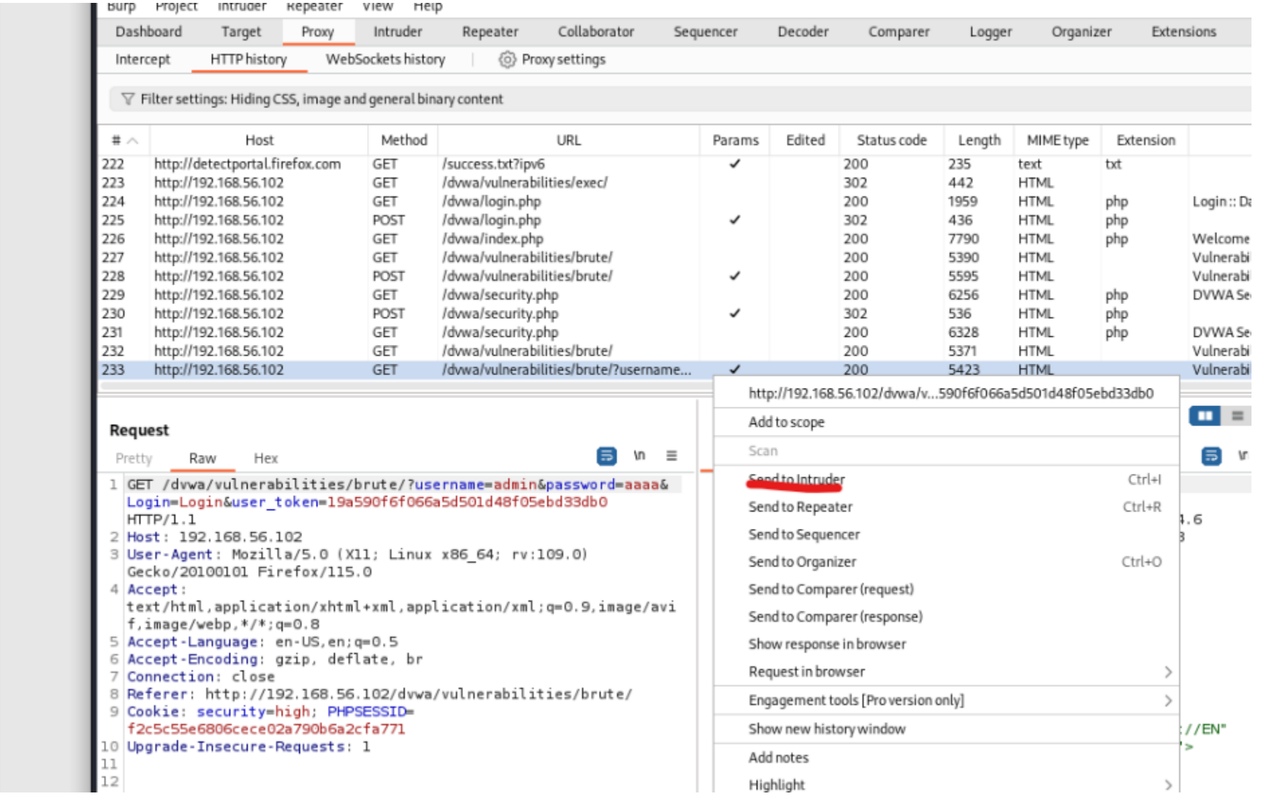
비밀번호 길이 제한 여부

특수문자 사용 여부



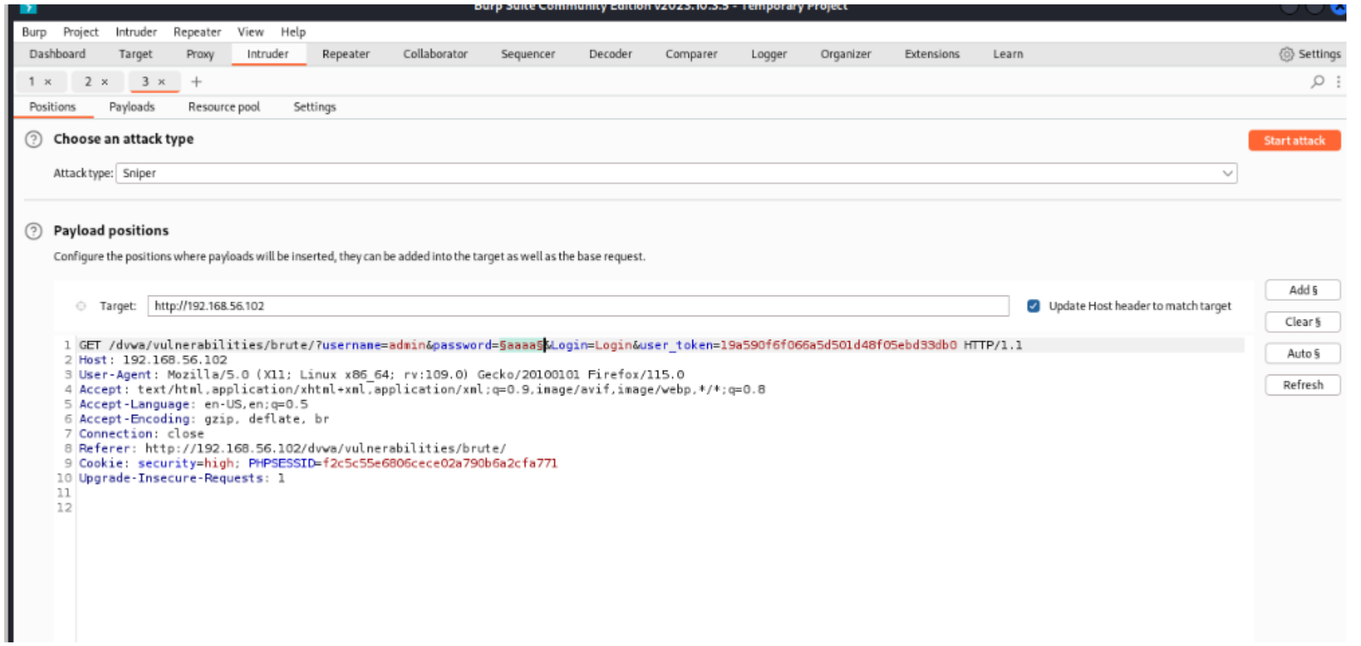
03 실습

로그인 시도 시 발생하는 http 요청

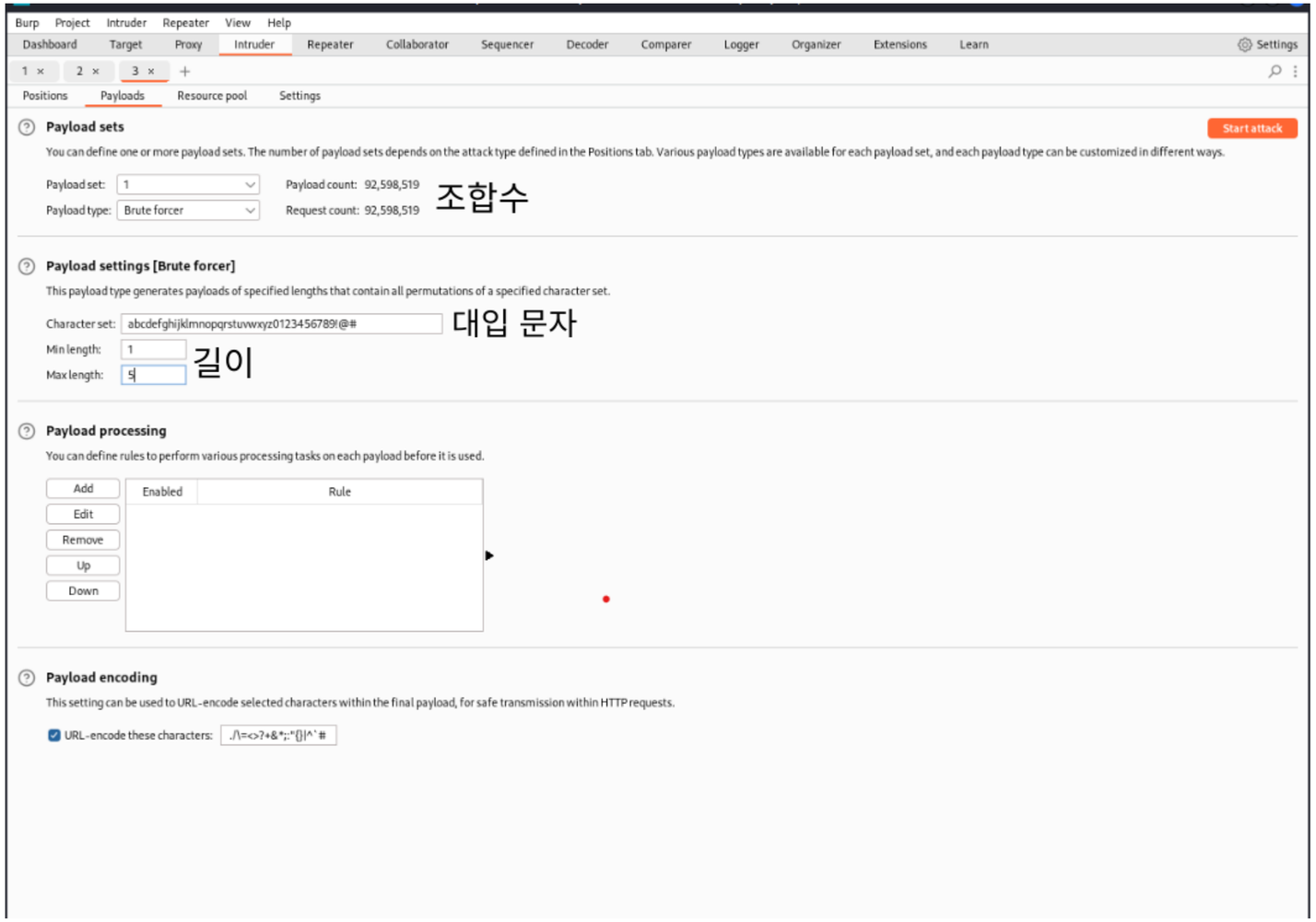


03 실습

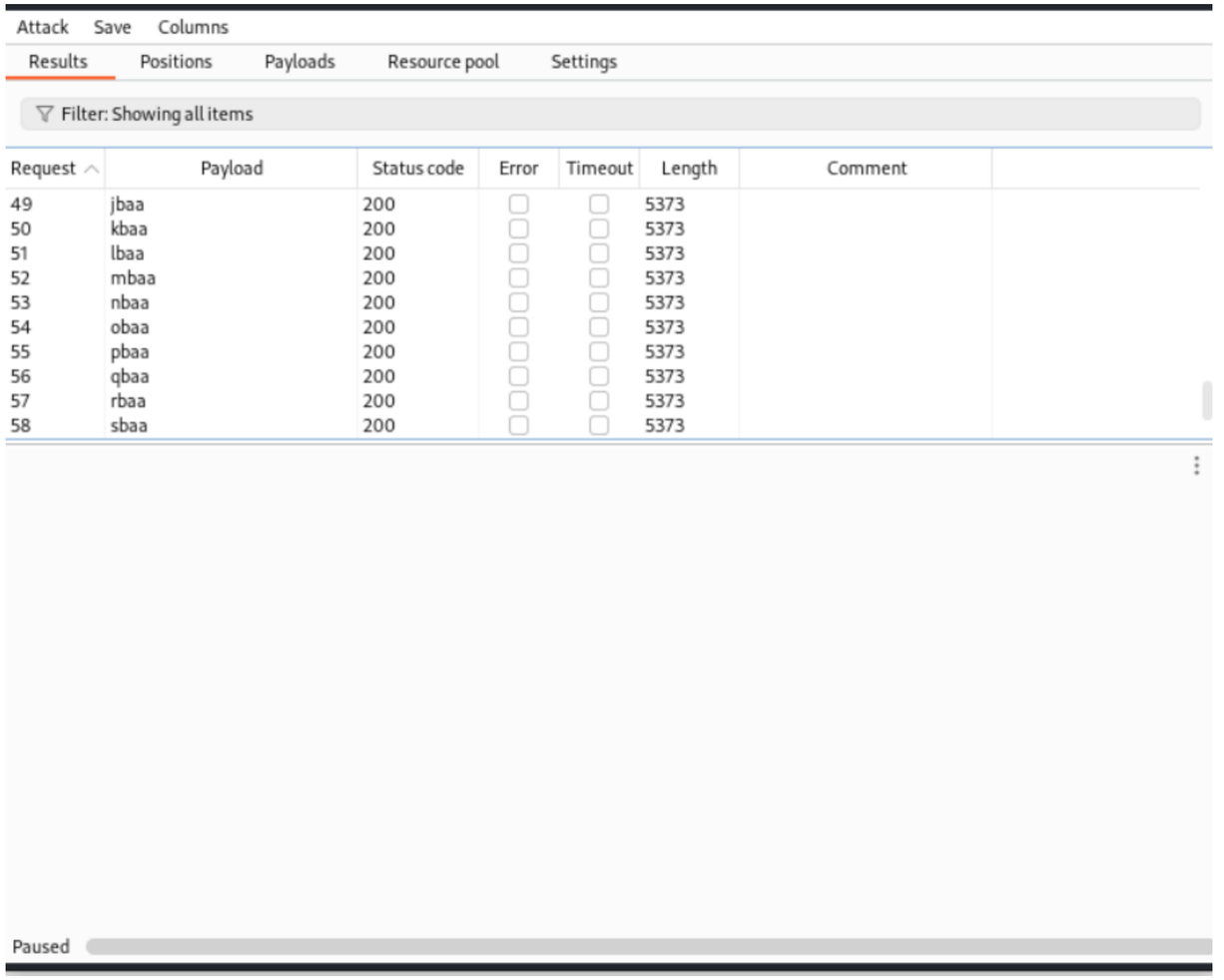
데이터를 전송 할 부분 지정



03 실습


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 × 2 × 3 × +
Positions Payloads Resource pool Settings
Payload sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 92,598,519
Payload type: Brute forcer
Request count: 92,598,519
조합수
Payload settings [Brute forcer]
This payload type generates payloads of specified lengths that contain all permutations of a specified character set.
Character set: abcdefghijklmnopqrstuvwxyz0123456789!@#
대입 문자
Min length: 1
Max length: 5
길이
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`#

03 실습


Attack
Save
Columns
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items
Request
Payload
Status code
Error
Timeout
Length
Comment
49 jbaa 200 5373
50 kbaa 200 5373
51 lbaa 200 5373
52 mbaa 200 5373
53 nbaa 200 5373
54 obaa 200 5373
55 pbaa 200 5373
56 qbaa 200 5373
57 rbaa 200 5373
58 sbaa 200 5373
Paused

04 대응방안

길고 복잡한 암호 사용

'password'

문자

문자 + 숫자 + 특수기호 14 + 3 + 1

04 대응방안

sleep

딜레이를 걸어 공격 지연

3초 지연

```
}
else {
    sleep( 3 );
    echo "<pre><br />password incorrect.</pre>";
}
```

0 ~ 4초 랜덤 지연

```
}
else {
    sleep( rand( 0, 4 ) );
    echo "<pre><br />password incorrect.</pre>";
}
```

04 대응방안

locking

일정 시간동안 로그인 시도 제한

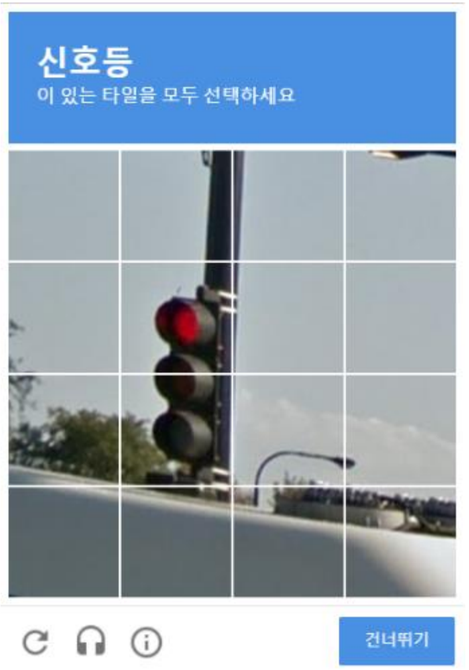
Alternative, the account has been locked because of too many failed logins.
If this is the case, **please try again in 15 minutes**.

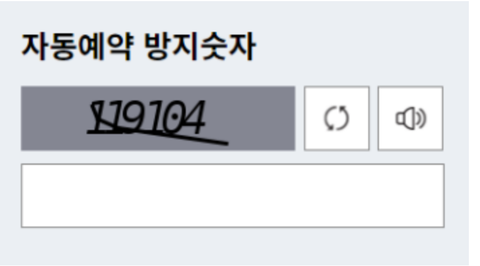
부작용 - 고의적인 사용제한

04 대응방안

CAPTCHA

자동화하기 어려운 글자나 그림으로
로그인 시도 주체 확인





04 대응방안

서로 다른 사이트 다른 암호 사용 **크리덴셜 스터핑**

다중 인증 시큐어 코딩의 중요성

감사합니다