

브루트 포스 공격

목차

01 브루트 포스 공격 개념

02 정보 수집

03 실습

04 대응방안

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

• 비밀번호: 8~16자의 영문 대/소문자, 숫자, 특수문자를 사용해 주세요.

03 실습

로그인 시도 시 발생하는 http 요청

The screenshot displays the Burp Suite interface. The top menu bar includes 'burp', 'Project', 'Intruder', 'Repeater', 'View', and 'Help'. Below this is a toolbar with tabs for 'Dashboard', 'Target', 'Proxy' (selected), 'Intruder', 'Repeater', 'Collaborator', 'Sequencer', 'Decoder', 'Comparer', 'Logger', 'Organizer', and 'Extensions'. Under the 'Proxy' tab, there are sub-tabs for 'Intercept', 'HTTP history' (selected), 'WebSockets history', and 'Proxy settings'. A filter settings bar indicates 'Hiding CSS, image and general binary content'. The main table lists HTTP history entries with columns: #, Host, Method, URL, Params, Edited, Status code, Length, MIME type, Extension, and a description. Entry #233 is selected, showing a GET request to 'http://192.168.56.102/dvwa/vulnerabilities/brute/?username=admin&password=aaaa&Login=Login&user_token=19a590f6f066a5d501d48f05ebd33db0'. Below the table, the 'Request' tab is active, showing the raw HTTP request details. A context menu is open over the request, with options like 'Send to Intruder', 'Send to Repeater', 'Send to Sequencer', 'Send to Organizer', 'Send to Comparer (request)', 'Send to Comparer (response)', 'Show response in browser', 'Request in browser', 'Engagement tools [Pro version only]', 'Show new history window', 'Add notes', and 'Highlight'. The 'Send to Intruder' option is highlighted.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	
222	http://detectportal.firefox.com	GET	/success.txt?ip=6	✓		200	235	text	txt	
223	http://192.168.56.102	GET	/dvwa/vulnerabilities/exec/			302	442	HTML		
224	http://192.168.56.102	GET	/dvwa/login.php			200	1959	HTML	php	Login :: D
225	http://192.168.56.102	POST	/dvwa/login.php	✓		302	436	HTML	php	
226	http://192.168.56.102	GET	/dvwa/index.php			200	7790	HTML	php	Welcome
227	http://192.168.56.102	GET	/dvwa/vulnerabilities/brute/			200	5390	HTML		Vulnerabi
228	http://192.168.56.102	POST	/dvwa/vulnerabilities/brute/	✓		200	5595	HTML		Vulnerabi
229	http://192.168.56.102	GET	/dvwa/security.php			200	6256	HTML	php	DVWA Se
230	http://192.168.56.102	POST	/dvwa/security.php	✓		302	536	HTML	php	
231	http://192.168.56.102	GET	/dvwa/security.php			200	6328	HTML	php	DVWA Se
232	http://192.168.56.102	GET	/dvwa/vulnerabilities/brute/			200	5371	HTML		Vulnerabi
233	http://192.168.56.102	GET	/dvwa/vulnerabilities/brute/?username=...	✓		200	5423	HTML		Vulnerabi

Request

Pretty Raw Hex

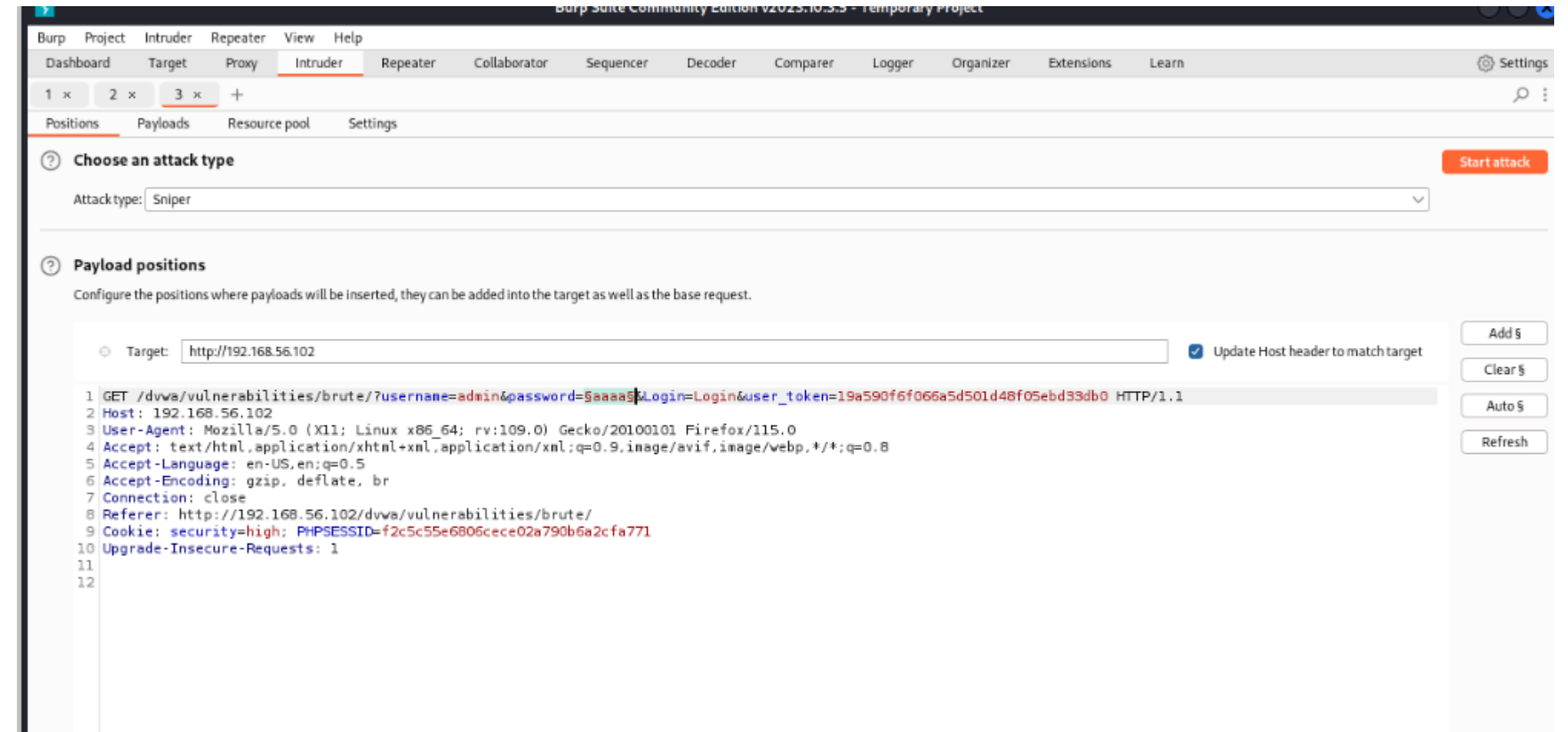
```
1 GET /dvwa/vulnerabilities/brute/?username=admin&password=aaaa&
  Login=Login&user_token=19a590f6f066a5d501d48f05ebd33db0
  HTTP/1.1
2 Host: 192.168.56.102
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
  f,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://192.168.56.102/dvwa/vulnerabilities/brute/
9 Cookie: security=high; PHPSESSID=
  f2c5c55e6806cece02a790b6a2cfa771
10 Upgrade-Insecure-Requests: 1
11
12
```

Context Menu Options:

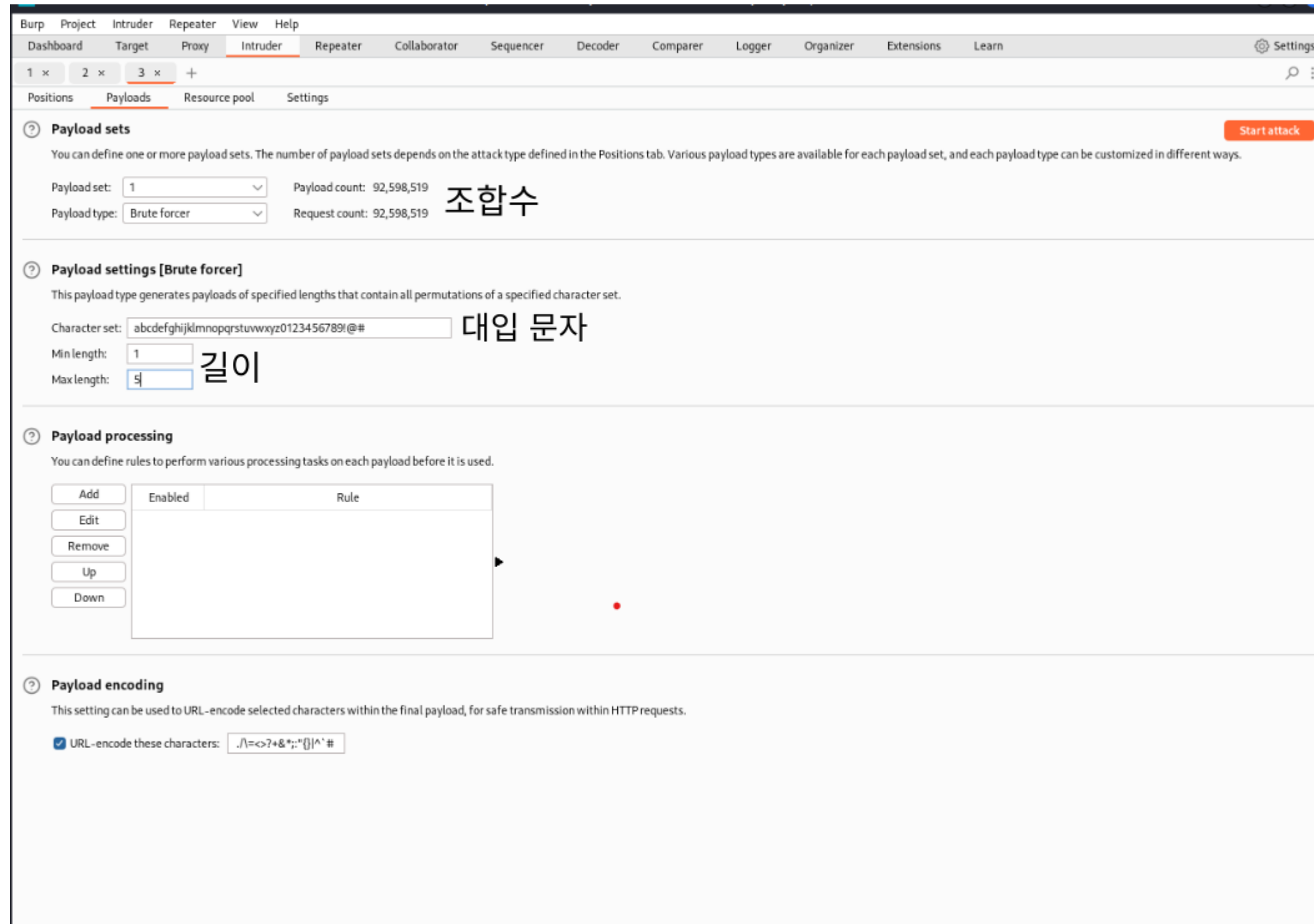
- http://192.168.56.102/dvwa/v...590f6f066a5d501d48f05ebd33db0
- Add to scope
- Scan
- Send to Intruder (Ctrl+I)
- Send to Repeater (Ctrl+R)
- Send to Sequencer
- Send to Organizer (Ctrl+O)
- Send to Comparer (request)
- Send to Comparer (response)
- Show response in browser
- Request in browser
- Engagement tools [Pro version only]
- Show new history window
- Add notes
- Highlight

03 실습

데이터를 전송 할 부분 지정



03 실습



03 실습

AttackSaveColumns

ResultsPositionsPayloadsResource poolSettings

▼ Filter: Showing all items

Request ^	Payload	Status code	Error	Timeout	Length	Comment	
49	jbaa	200	<input type="checkbox"/>	<input type="checkbox"/>	5373		
50	kbaa	200	<input type="checkbox"/>	<input type="checkbox"/>	5373		
51	lbaa	200	<input type="checkbox"/>	<input type="checkbox"/>	5373		
52	mbaa	200	<input type="checkbox"/>	<input type="checkbox"/>	5373		
53	nbaa	200	<input type="checkbox"/>	<input type="checkbox"/>	5373		
54	obaa	200	<input type="checkbox"/>	<input type="checkbox"/>	5373		
55	pbaa	200	<input type="checkbox"/>	<input type="checkbox"/>	5373		
56	qbaa	200	<input type="checkbox"/>	<input type="checkbox"/>	5373		
57	rbaa	200	<input type="checkbox"/>	<input type="checkbox"/>	5373		
58	sbaa	200	<input type="checkbox"/>	<input type="checkbox"/>	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.

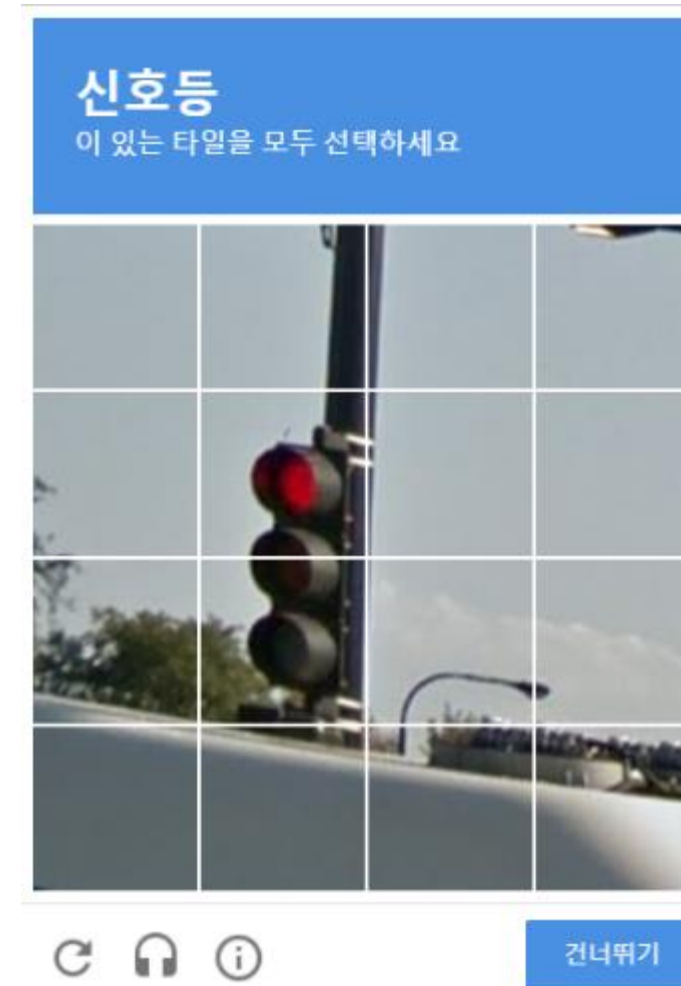


부작용 - 고의적인 사용제한

04 대응방안

CAPTCHA

자동화하기 어려운 글자나 그림으로
로그인 시도 주체 확인



NAVER

PC방 등 공용PC라면 QR코드 로그인도 안전해요 >

ID 로그인 | (1) 일회용 번호 | QR코드

아이디(로그인 전용 아이디), 비밀번호 또는 자동입력 방지 문자를 잘못 입력했습니다. 입력하신 내용을 다시 확인해주세요.

아이디: BCG

비밀번호

점

제품명	가격	개수	총 합
낙지 (0.5kg)	700	4	2800
숙취 꽃게	900	7	6300
파전 부침가루	600	1	600

해당 영수증은 가상으로 제작된 것으로 실제 영수증 사진이 아닙니다.

구매한 낙지 하나는 몇 kg 입니까?

정답을 입력해주세요

☐ 로그인 상태 유지 ☒ IP보안

로그인

[비밀번호 찾기](#) | [아이디 찾기](#) | [회원가입](#)

자동예약 방지숫자

04 대응방안

서로 다른 사이트 다른 암호 사용

크리덴셜 스테핑

다중 인증

시큐어 코딩의 중요성

감사합니다
