



# [WHS][웹해킹 원리] 33반 김신아(9502)

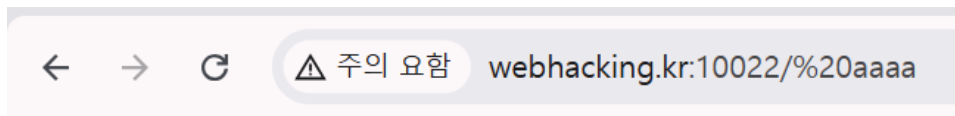
## 🔥 자주 등장하는 HTTP 오류 코드 요약

상태코드	이름	설명
400	Bad Request	요청 형식이 잘못됨 (문법 오류 등)
401	Unauthorized	인증이 필요함 (로그인 안됨)
403	Forbidden	접근 거부 (인증해도 안 됨)
404	Not Found	요청한 자원이 없음
405	Method Not Allowed	지원되지 않는 HTTP 메소드 사용
408	Request Timeout	요청 시간이 너무 김
409	Conflict	요청 충돌 발생 (주로 PUT/POST 시)
410	Gone	자원이 영구히 사라짐
413	Payload Too Large	업로드 용량이 너무 큼
414	URI Too Long	URL 길이가 너무 김
418	I'm a teapot 🍵	이스터에그 코드 (실제 사용은 거의 X)
429	Too Many Requests	요청 너무 많음 (Rate Limit)

### HTTP 오류 코드 종류 조사

우선 404 Error부터 시도해주었습니다.

#### 1. 404 Error



## 404 Error!

your key : KEY{23c0b3a9ccc44b72f17a99eadb351d2f}

404 에러란?

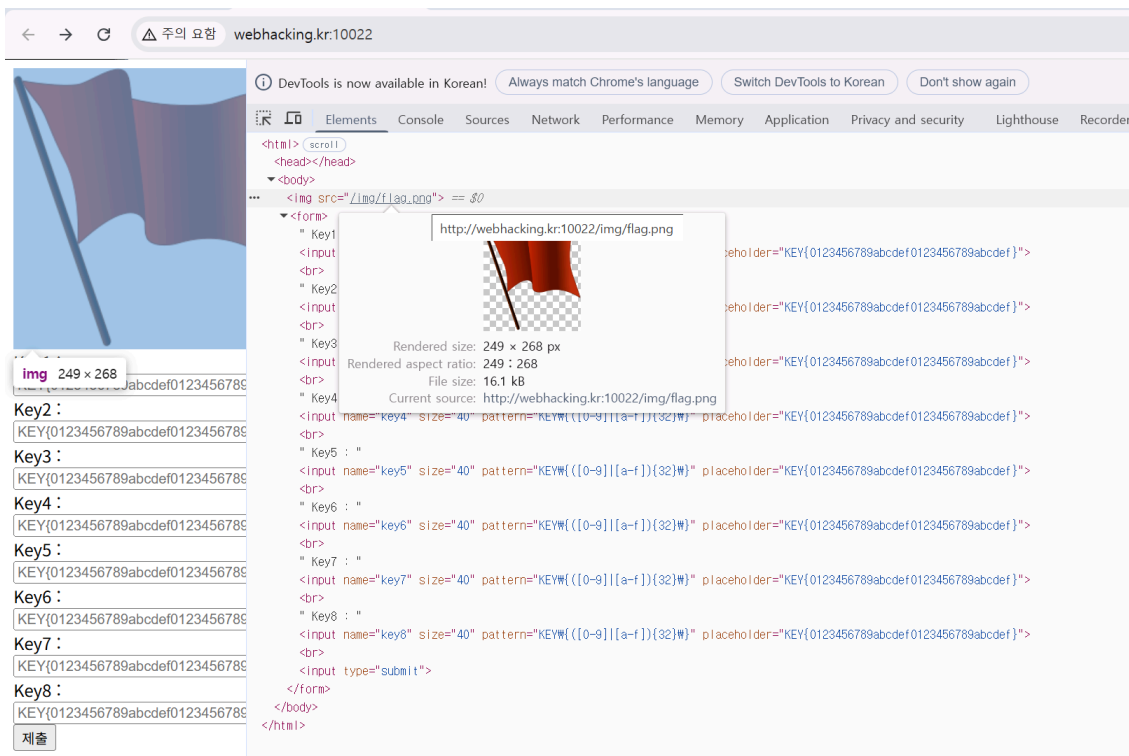
- 요청한 페이지를 찾을 수 없음을 의미하는 HTTP 표준 응답 코드
- 클라이언트가 올바른 요청을 보냈지만 서버가 요청한 페이지를 찾을 수 없을 때 발생한다

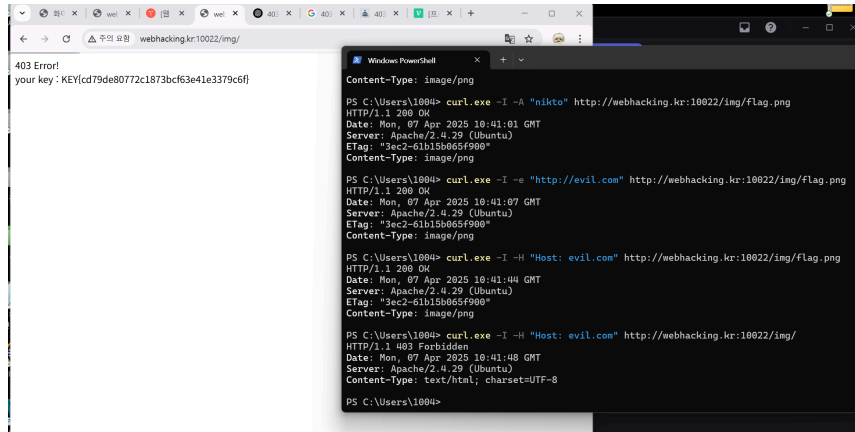
→ 주소창에 올바른 주소가 아닌 이상하게 변경하여 404 에러 발생시킴



KEY{23c0b3a9ccc44b72f17a99eadb351d2f}

## 2. 403 Error





403 에러란?

- "Forbidden"이라는 HTTP 상태 코드, 요청한 리소스에 액세스할 권한이 없음을 의미
- 서버가 요청을 이해했지만 권한 부족으로 인해 액세스를 거부한 경우에 발생

→ <http://webhacking.kr:10022/> 에서 시도해보았지만 플래그를 발견하지 못하여 깃발 이미지 <http://webhacking.kr:10022/img/flag.png>로 시도

→ `curl.exe -I -A "nikto"`

: User-Agent가 Nikto여도 정상 응답

→ `curl.exe -I -e "http://evil.com"`

: Referer가 evil.com인데도 OK

→ `curl.exe -I -H "Host: evil.com"`

: Host 헤더 변조했지만 정상 응답

→ `curl.exe -I -H "Host: evil.com" http://webhacking.kr:10022/img/`

: img/ 디렉토리에 Host 헤더가 evil.com일 때만 차단 발생



KEY{cd79de80772c1873bcf63e41e3379c6f}

[ 디렉토리([/img/](#))에 접근할 때만 Host 필터링이 적용 ]

### 3. 405 Error

```
Windows PowerShell
Content-Type: text/html; charset=UTF-8

PS C:\Users\1004> curl.exe -I -A "sqlmap" http://webhacking.kr:10022/
HTTP/1.1 200 OK
Date: Mon, 07 Apr 2025 10:28:21 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Type: text/html; charset=UTF-8

PS C:\Users\1004> curl.exe -I -A "evil-bot" http://webhacking.kr:10022/
HTTP/1.1 200 OK
Date: Mon, 07 Apr 2025 10:28:43 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Type: text/html; charset=UTF-8

PS C:\Users\1004> curl.exe -I -e "http://evil.com" http://webhacking.kr:10022/
HTTP/1.1 200 OK
Date: Mon, 07 Apr 2025 10:29:02 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Type: text/html; charset=UTF-8

PS C:\Users\1004> curl.exe -I -H "Host: evil.com" http://webhacking.kr:10022/
HTTP/1.1 200 OK
Date: Mon, 07 Apr 2025 10:29:07 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Type: text/html; charset=UTF-8

PS C:\Users\1004> curl.exe -X TRACE http://webhacking.kr:10022/
405 Error!<br>
your key : KEY{e5602408f2037c05bbbb0995fec6bc58}
PS C:\Users\1004>
```

405 에러란?

- 하이퍼텍스트 전송 프로토콜(HTTP)의 응답 상태 코드
- 클라이언트가 요청한 메서드가 서버에서 허용되지 않을 때 발생

→ -A "sqlmap"

: 보안 스캐너 UA에도 차단 안 함

→ -A "evil-bot"

: 봇 탐지 없이 정상 응답

→ -e "http://evil.com"

: Referer 필터 없음

→ -H "Host: evil.com"

: Host 필터도 없음 ( /img/ 와 다름)

→ -X TRACE

: HTTP 표준 메서드, 원래 보안상 비활성화 되지만 Key 추출됨

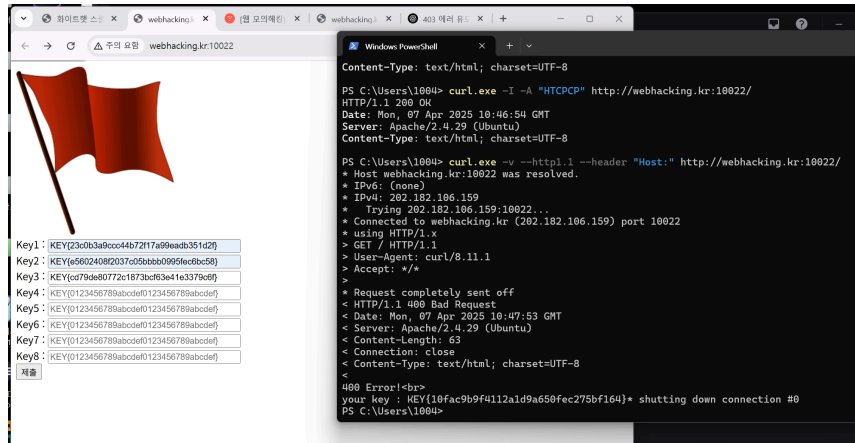


KEY{e5602408f2037c05bbbb0995fec6bc58}

[ TRACE 요청을 허용하되, 그에 대해 405와 함께 KEY를 노출하도록 이루어짐 ]

#### 4. 414 Error





400에러란?

- HTTP 프로토콜의 응답 상태 코드, 클라이언트가 잘못된 요청을 했음을 의미
- 잘못된 요청으로 문법상 오류가 있어서 서버가 요청사항을 이하지 못하는 경우 발생

→ curl.exe -I -A "HTTCCPCP"

: User-Agent 장난감 문자열, 서버는 무시하고 응답

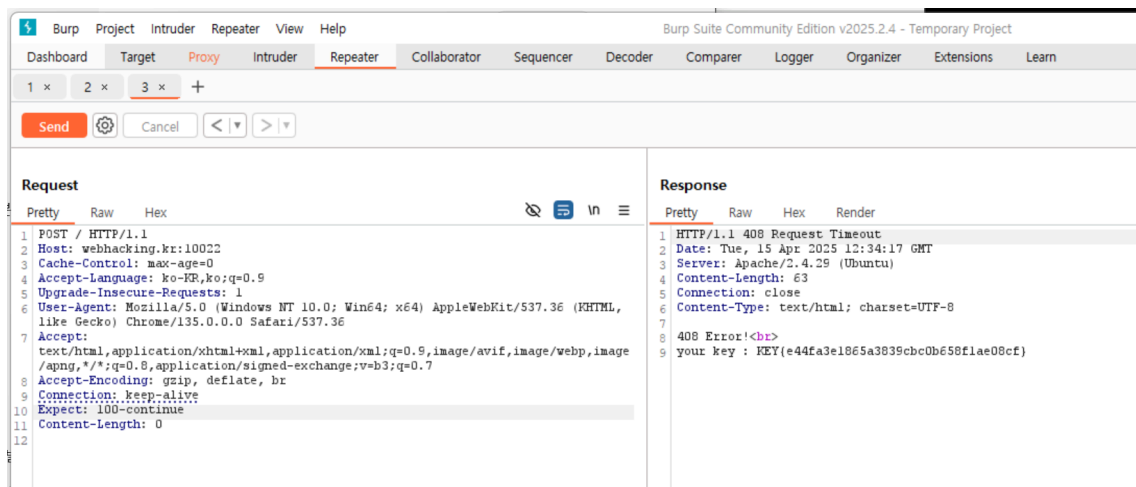
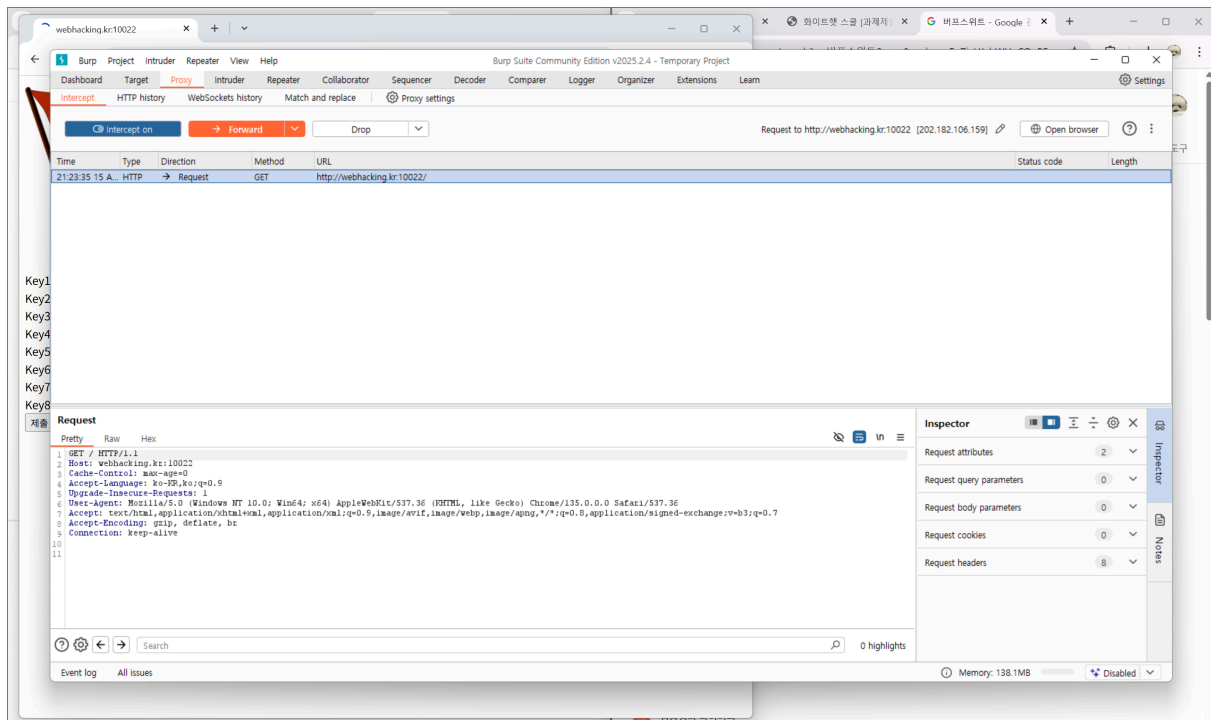
→ curl.exe -v --http1.1 --header "Host:"

: 헤더를 빈 값으로 보냈기 때문에, 서버는 이를 잘못된 요청으로 판단하고 400 에러 발생



KEY{10fac9b9f4112a1d9a650fec275bf164}

## 6. 408 Error



## 408 에러란?

- HTTP 응답 상태 코드, 클라이언트가 서버에 요청을 보냈지만, 일정 시간 내에 서버가 해당 요청을 처리하지 못했음을 의미
- 네트워크 연결 문제나 서버의 응답 지연으로 인해 발생

→ Burp Suite를 사용

→

Expect: 100-continue 는 클라이언트가 "본문 보내기 전에 확인받겠다"는 뜻

→ 서버는 이를 받고 기다리다가 본문도 없고 딜레이도 없어서 Timeout 처리

→ 전송 속도 제어 없이 보내어 타임아웃 유도 성공



KEY{e44fa3e1865a3839cbc0b658f1ae08cf}

## 7. 최종 플래그

---

Your score : 6  
FLAG is WHS{aprilFoolsDay}