웹해킹

기초 기법

보고서

4XX 에러 발생 유도

Name : 조민혁

Class Number : 5

Phone Number : 010-4923-2198

목 차

1. 풀이 과정

1-1. 400 Error 및 Key 확인

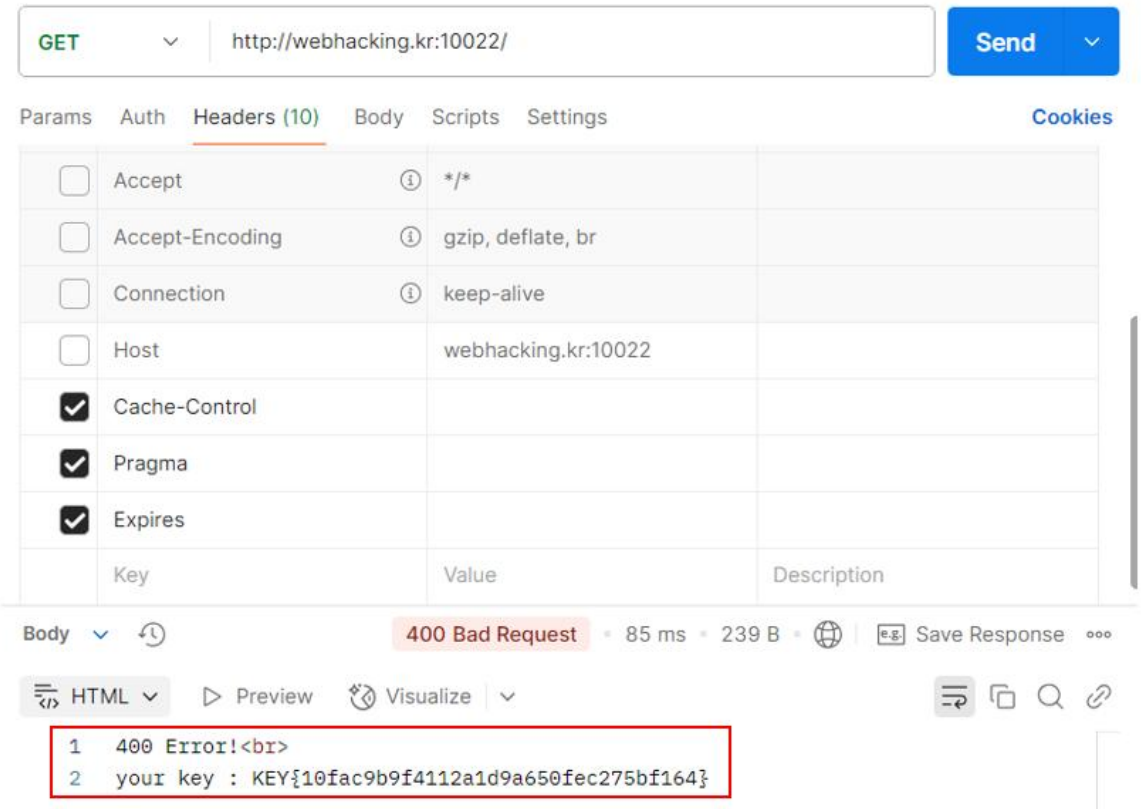

그림 1. 400 Error 및 Key

400 Error란 Bad Request로 클라이언트가 서버에 문법적으로 잘못된 요청을 하거나 형식 오류가 발생할 경우 발생한다. 이에 따라 Postman을 이용하여 HTTP 헤더에서 Cache-Control과 Pragma, Expires에 공백으로 요청해보았다. 그에 따라 그림 1과 같이 400 Error와 Key를 획득할 수 있었다.

1-2. 403 Error 및 Key 확인

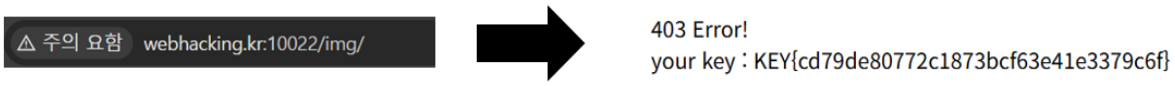

그림 2. 403 Error 및 Key

403 Error는 인증은 되었으나 권한이 없어서 발생하는 오류이다. 즉, 권한 문제로 인해 해당 리소스에 접근하지 못하는 것을 말한다. 이에 따라 URL을 “webhacking.kr:10022/img”를 입력해보았다. 그 결과 그림 2와 같이 403 Error와 Key 값을 확인할 수 있었다.

1-3. 404 Error 및 Key 확인

그림 3. 404 Error 및 Key

404 Error는 클라이언트가 요청한 자원이 존재하지 않을 경우 발생하는 경우이다. 이에 따라 URL에 유효하지 않은 요청을 “webhacking.kr:10022/qwer” 처럼 보내 보았다. 그 결과 그림 3과 같이 404 Error와 Key 값을 확인할 수 있었다.

1-4. 405 Error 및 Key 확인

```
minhyuk@minhyuk:~/WhiteHatSchool/Web_Hacking$ curl -X DELETE  http://webhacking.kr:10022/index.html
405 Error!<br>
your key : KEY{e5602408f2037c05bbbb0995fec6bc58}minhyuk@minhyuk:~/WhiteHatSchool/Web_Hacking$
```

그림 4. 405 Error 및 Key

405 Error는 요청이 허용되지 않은 메소드일 경우 반환한다. 이에 따라 curl을 이용하여 그림 4와 같이 유효하지 않은 URL에 DELETE를 해보니 405 Error와 key값을 확인할 수 있었다.

1-5. 412 Error 및 Key 확인

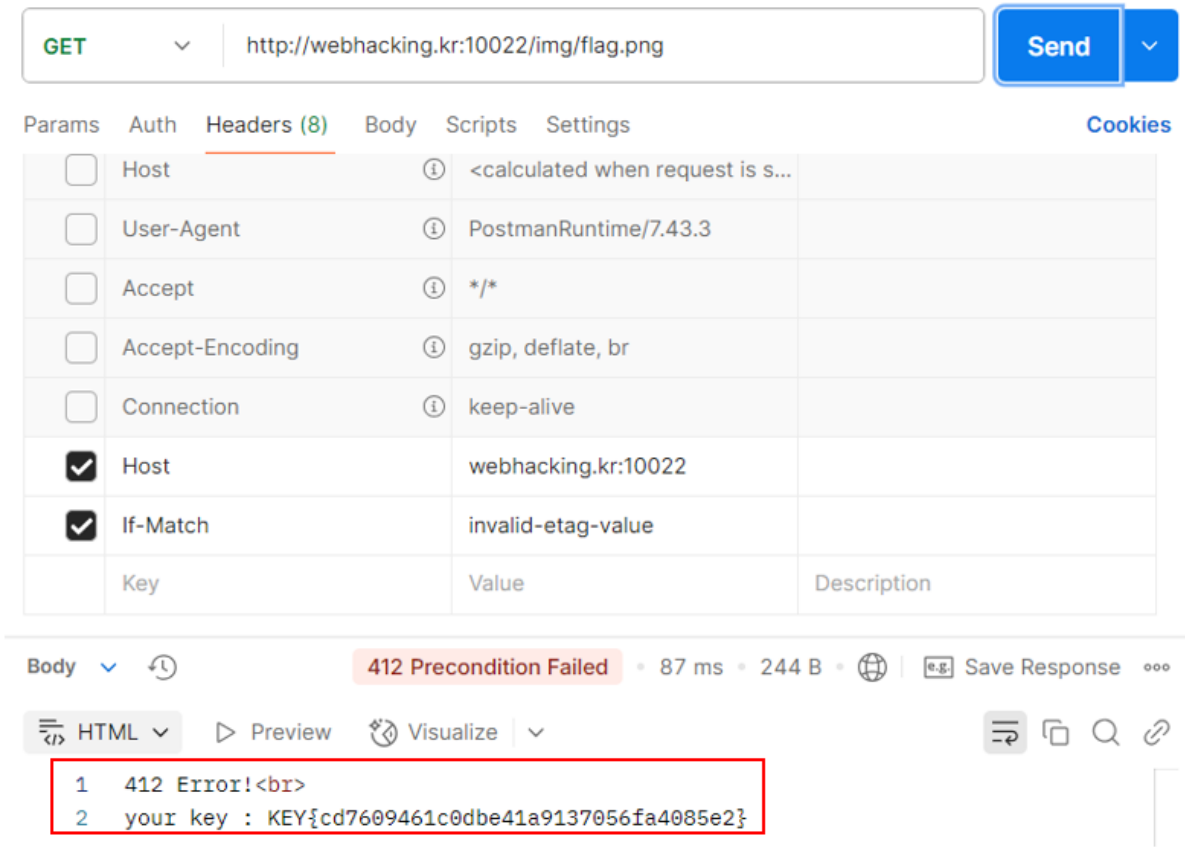

그림 5. 412 Error 및 Key

412 Error의 경우 eTag가 유효하지 않은 값일 경우 반환된다. 이에 따라 Postman을 이용하여 헤더에 If-match: invalid-etag-value를 입력하여 전송해본 결과 그림 5와 같이 412 Error 및 Key

값을 확인할 수 있었다.

1-6. 414 Error 및 Key 확인

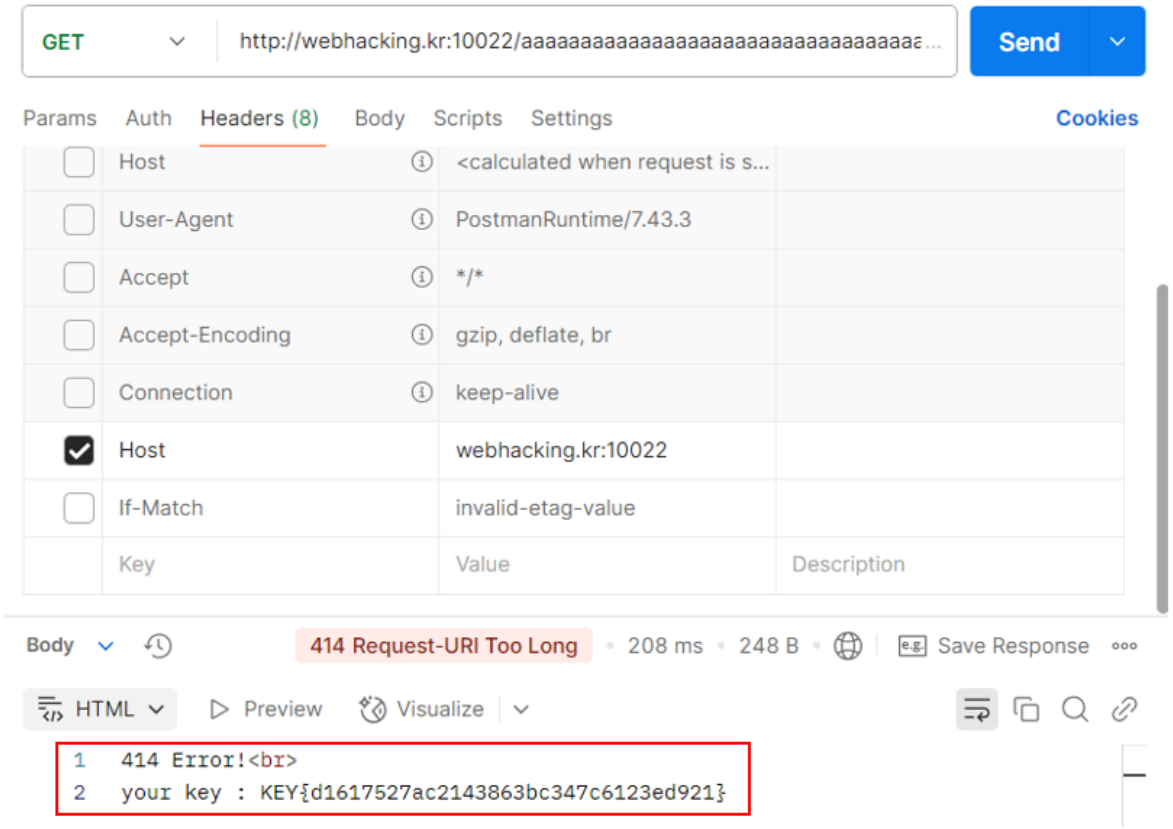

그림 6. 414 Error 및 Key

414 Error는 요청 URI의 크기가 서버가 처리하는 최대 크기를 초과할 경우 발생하는 에러다. 이에 따라 Apache 서버는 8192 바이트까지 처리할 수 있기에 최대 URI 크기를 처리 가능 바이트보다 크게 하였다. 그 결과 그림 6과 같이 414 Error 및 Key 값을 확인할 수 있었다.

1-7. 417 Error 및 Key 확인

```
minhyuk@minhyuk:~/WhiteHatSchool/Web_Hacking$ curl -v http://webhacking.kr:10022/ \
     -H "Expect: nonsense-expectation"
*   Trying 202.182.106.159:10022...
* Connected to webhacking.kr (202.182.106.159) port 10022 (#0)
> GET / HTTP/1.1
> Host: webhacking.kr:10022
> User-Agent: curl/7.81.0
> Accept: */*
> Expect: nonsense-expectation
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 417 Expectation Failed
< Date: Tue, 15 Apr 2025 14:25:31 GMT
< Server: Apache/2.4.29 (Ubuntu)
< Content-Length: 63
< Content-Type: text/html; charset=UTF-8
<
417 Error!<br>
* Connection #0 to host webhacking.kr left intact
your key : KEY{ed2dd6cb38fe6a4a10e46d22d20047e6}minhyuk@minhyuk:~/WhiteHatSchool/Web_Hacking$
```

그림 7. 417 Error 및 Key

417 Error의 경우 HTTP 요청 시 Expect 값을 통해 서버가 Expect 값을 반환하지 않으면 그에 따라 발생하는 반환 에러 코드다. 이에 따라 Expect 값을 유효하지 않은 값으로 설정하여 서버로 요청하였다. 그 결과 그림 7과 같이 417 Error 와 Key 값을 확인할 수 있었다.

2. FLAG 확인

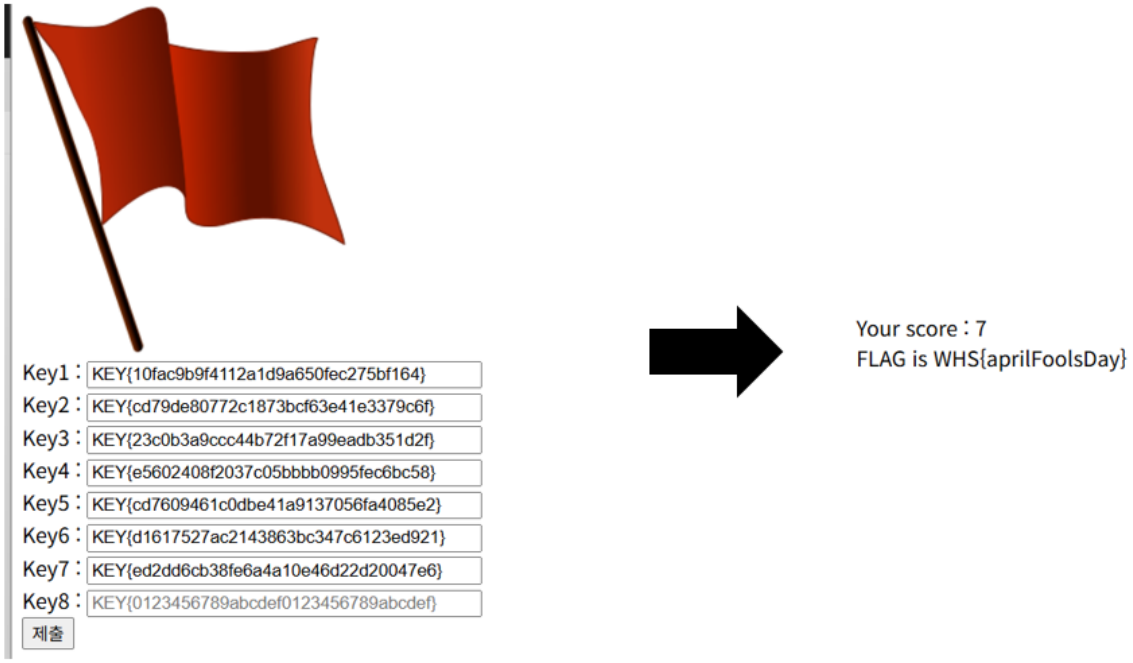

그림 8. Key 값 입력 및 FLAG 확인

Key값 8개 중 7개를 확인할 수 있었기에 이를 webhacking.kr:10022에 Key 입력 폼에 입력하여 FLAG를 확인하였다. 그 결과 그림 8과 같이 Score와 WHS{} 형식의 플래그 값이 WHS{apirlFoolsDay} 인 것을 확인할 수 있었다.