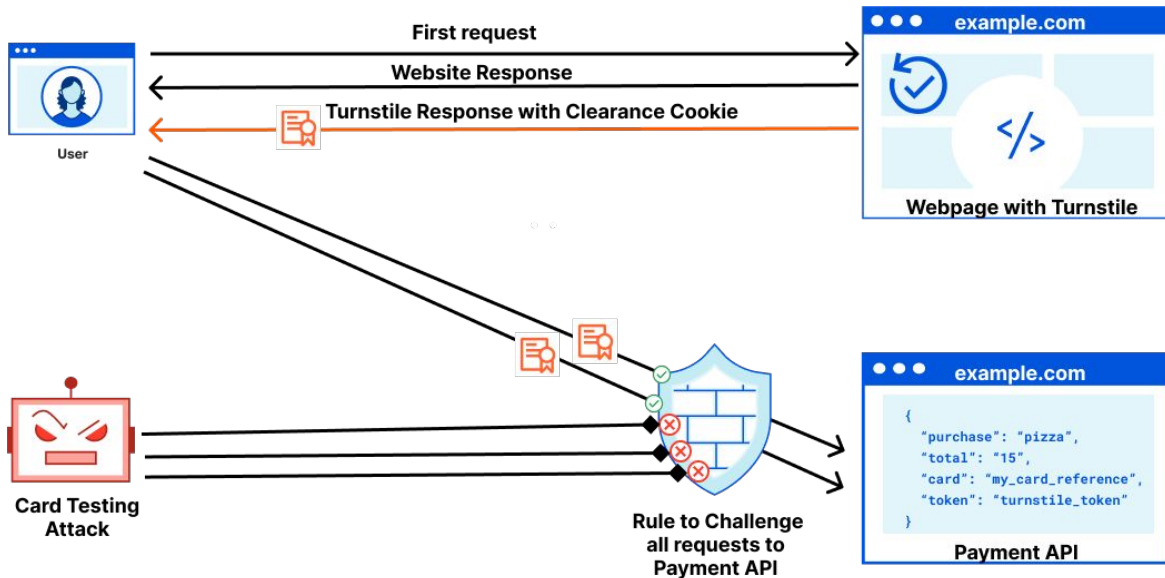CLOUDFLARE

1 - Turnstile now issues clearance cookies
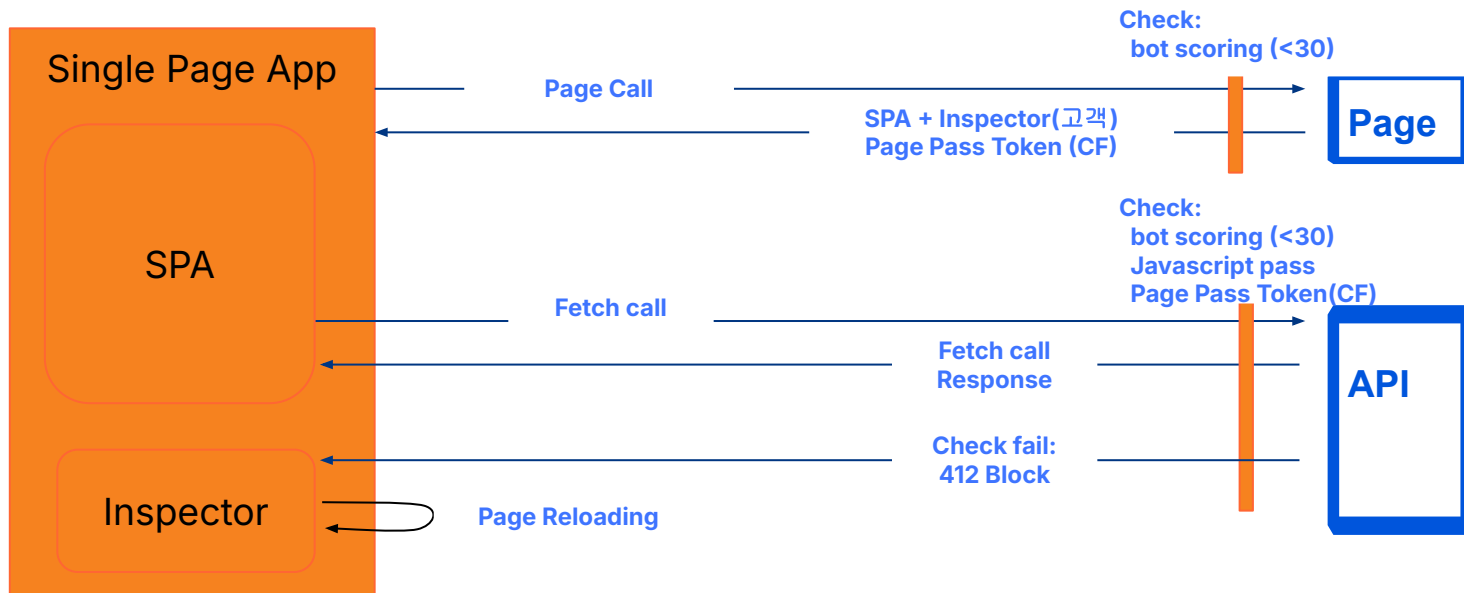
Turnstile required:

- AJAX requests
- XML HTTP requests
- Fetch requests
- Single Page Applications
- Embedded iFrames

https://gcp.stephenkim.site/demo.html

First request
Website Response
Turnstile Response with Clearance Cookie

User

example.com
Webpage with Turnstile

Card Testing Attack

Rule to Challenge all requests to Payment API

example.com
```
{
    "purchase": "pizza",
    "total": "15",
    "card": "my_card_reference",
    "token": "turnstile_token"
}
```
Payment API

2- API에 대한 Challenge Case

SPA 페이지 호출 시 봇체크와 패스 후 Pass Token발행, API호출 시 Pass Token유효성과 봇체크 후
정상 요청에 대해서만 응답 처리하고, 패스 실패 시 412 응답, SPA 와 함께 로드된 Inspector 에서 412
응답 시 SPA 리로드 처리

Single Page App

SPA

Inspector

Check:
bot scoring (<30)

Page Call

SPA + Inspector(고객)
Page Pass Token (CF)

Page

Check:
bot scoring (<30)
Javascript pass
Page Pass Token(CF)

Fetch call

Fetch call
Response

API

Check fail:
412 Block

Page Reloading

Demo URL: https://gcp.stephenkim.site/demo.html **(Id/Pass: admin/admin),** 챌린지 시**(412**
응답코드**) Inspector Page Reload**

WAF Custom Rules

SPA 페이지 호출 시 봇체크와 패스 후 Pass Token발행, API호출 시 Pass Token유효성과 봇체크 후 정상 요청에 대해서만 응답 처리하고, 패스 실패 시 412 응답, SPA 와 함께 로드된 Inspector 에서 412 응답 시 SPA 리로드 처리

Rule name (required)

```
protect login page
```
Give your rule a descriptive name.

Use expression builder

```
(
  (http.host eq "node.abcapp24.club" and http.request.uri.path contains "/login" ) and
  (cf.bot_management.score <= 99   )
)
```

Then take action...

Choose action

```
Interactive Challenge          ▼
```

Rule name (required)

```
verify bot score
```
Give your rule a descriptive name.

Use expression builder

```
(
  (http.host eq "node.abcapp24.club" and http.request.uri.path contains "/api/")
  and  (
   cf.bot_management.score < 30
   )
```

Then take action...

Choose action	With response type	With response code
Block ▼	Custom Text ▼	413

Blocks matching requests and stops evaluating other rules

Rule name (required)

```
verify token
```
Give your rule a descriptive name.

Use expression builder

```
   (http.host eq "node.abcapp24.club" and http.request.uri.path contains "/api/")
   and (
    not is_timed_hmac_valid_v0(
     "testkeysample",
     concat(http.request.cookies["__cf_bm"][0],http.request.cookies["__CF_TOKEN__"][0]),
     86400, http.request.timestamp.sec,0)
```

Then take action...

Choose action	With response type	With response code
Block ▼	Custom Text ▼	412

Rule name (required)

```
Duplicate of verify js passed
```
Give your rule a descriptive name.

Use expression builder

```
(
  (http.host eq "node.abcapp24.club" and http.request.uri.path contains "/api/")
  and  (
   not cf.bot_management.js_detection.passed
   )
```

Warning: Please ensure your rule expression only captures traffic from devices that have already submitted a JavaScript Detection response. Learn more ⬚

Then take action...

Choose action	With response type	With response code
Block ▼	Custom Text ▼	414

모듈 별 구현 기능