CH12, 13

안전(safe) 메소드와 멱등(Idempotent) 메소드

> Search forms that are idempotent should use the GET method

멱등(idempotent) 메소드

서버에 동일한 요청을 여러 번 했을 때의 효과와 요청을 한 번만 했을 때의 효과가 동일한메소드

- OPTIONS, GET, HEAD, PUT, DELETE

안전(safe)메소드

타겟 리소스에 요청을 했을 때, 서버의 상태 변경이 일어나지 않는 메소드. 읽기 전용 메소드.

- OPTIONS, GET, HEAD
- 그러나 강제사항이 아니므로...

2005년

> 따라서 GET 요청을 사용해 데이터를 서버로 전송할 수는 있지만 상태를 바꾸는 작업을 해서는 안된다. 많은 웹 개발자는 2005년에 구글 웹 엑셀레이터가 일반에 공개됐을 때 시행착오를 통해 이 사실을 힘들게 깨달았다. 이 애플리케이션은 각 페이지에서 링크된 내용을 모두 미리 가져왔는데, GET 요청은 안전하므로 이 작업을 HTTP 내에서 하는 것은 아무런 문제가 없었다. 하지만 많은 웹 개발자들은 HTTP 관례를 무시하고 '항목 삭제' 또는 '쇼핑 카트에 추가' 같은 간단한 링크를 자신들의 애플리케이션에 추가했고, 이로써 걷잡을 수 없는 혼란이 야기됐다.
>
> 그 중 한 기업은 모든 페이지 내용이 계속해서 삭제되는 것을 보고 구글 웹 엑셀레이터의 컨텐츠 관리 시스템이 반복적으로 악의적인 공격을 받고 있다고 생각했다. 하지만 그들은 나중에 비로소 검색 엔진 봇이(역자 주 : 구글, 야후 같은 검색 엔진은 자체 봇을 활용해 임의의 웹 페이지를 이동하며 한 페이지에 연결된 링크를 모두 클릭해 웹 페이지 정보를 수집한다. 여기서는 이런 검색 엔진 봇이 페이지 내 링크를 클릭하는 과정에서 데이터가 삭제된 것이다) 관리 페이지의 URL을 눌렀다는 사실과 모든 삭제 링크를 크롤링하고 있었다는 사실을 깨달았다.

2016년

김신입 1k
9달 전

#361058 Q&A

구글 봇이라는 놈이 자꾸 운영하는 사이트 게시물을 삭제합니다 ㅋㅋ

게시판 글에 글이 몇개 없어져서 apache access 로그를 살펴보고있는데요...

66.249.79.180 - - [17/Nov/2016:18:08:18 +0900] "GET /test/board_delete?no=7 HTTP/1.1" 200 261 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"

실습 시간

CSRF 이야기

~~CSRF - Cross-site request forgery~~
~~사이트간 요청 위조~~

~~어떻게 사이트간 요청 위조가 일어날까?~~
~~실제 코드 샤례~~
~~주의사항 HTTPS, HSTS~~
~~나쁜 HS~~

Form Validation 코드 상으로 살펴보기

https://github.com/django/django/blob/master/django/forms/forms.py#L178
https://github.com/django/django/blob/master/django/forms/forms.py#L170
https://github.com/django/django/blob/master/django/forms/forms.py#L362

모델폼일 때,
https://github.com/django/django/blob/master/django/forms/models.py#L380

Widgets

장고 어드민 위젯도 참고할만 한 자료
django/widgets.py at master · django/django · GitHub

템플릿 이야기

DIRS 로 정의된 순서대로 찾는다.
loaders 를 보면, app 안의 templates 디렉토리부터 템플릿을 찾는다. 만약에 같은 이름을 사용할 경우, 템플릿 상속시 오류가 발생할 가능성이 있다.

경험담: templates 폴더 내에 base.html를 만들어 넣어두었는데, 다른 개발자가 app을 추가하면서 거기 templates에 base.html을 넣어버려서 장애가 발생한 적이 있다.

Django debug toolbar

템플릿의 성능 측정을 위해서 시각 패널에 대해서 이야기를 해보겠습니다.
https://github.com/jazzband/django-debug-toolbar/blob/master/debug_toolbar/panels/timer.py

N+1 Query

~~N+1 쿼리는 쿼리 1번으로 N건을 가져왔는데, 관련 컬럼 데이터를 얻기 위해 추가적으로 쿼리를 N번 수행하는 경우를 말합니다.~~
~~나쁜 H.J~~

```
class Job(models.Model):
    name = models.CharField('직업명', max_length=32)

class User(models.Model):
    MALE, FEMALE = 'MALE', 'FEMALE'
    GENDER_CHOICES = ((MALE, 'male'),
                      (FEMALE, 'female'))
    name = models.CharField('이름', max_length=128)
    gender = models.CharField('성별', choices=GENDER_CHOICES, blank=True)
    job = models.ForeignKey(Job, verbose_name='직업')
```

```
<ul>
  {% for user in users %}
  <li>{{ user.job.name }}</li>
  {% endfor %}
<ul>
```

어떻게 알 수 있나?

1) Django debug toolbar w/ Django debug panel
2) https://github.com/jmcarp/nplusone
[잔소리] 오픈소스 문서는 업데이트가 제대로 안되어있을 수도 있다. 코드를 직접 보는 게 나을 수도.
3) New Relic 같은 APM (Application Performance Monitoring)

어떻게 고칠 수 있나?

~~select*related()* 혹은 *prefetch*related()를 써봅니다.~~

참고문서

멱등법칙 - 위키백과, 우리 모두의 백과사전

RFC 7231 - Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content

OKKY - 구글 봇이라는 놈이 자꾸 운영하는 사이트 게시물을 삭제합니다 ㅋㅋ

프로 제이쿼리 완벽 마스터: 최고의 웹+앱 개발자를 위한 필수 선택 - Adam Freeman - Google 도서

35.11. resource — Resource usage information — Python 3.6.2 documentation

Python 3 Module of the Week — PyMOTW 3

django 쿼리셋 수정을 통한 웹서비스 성능 개선 - select_related, prefetch_related · 초보몽키의 개발 공부로그