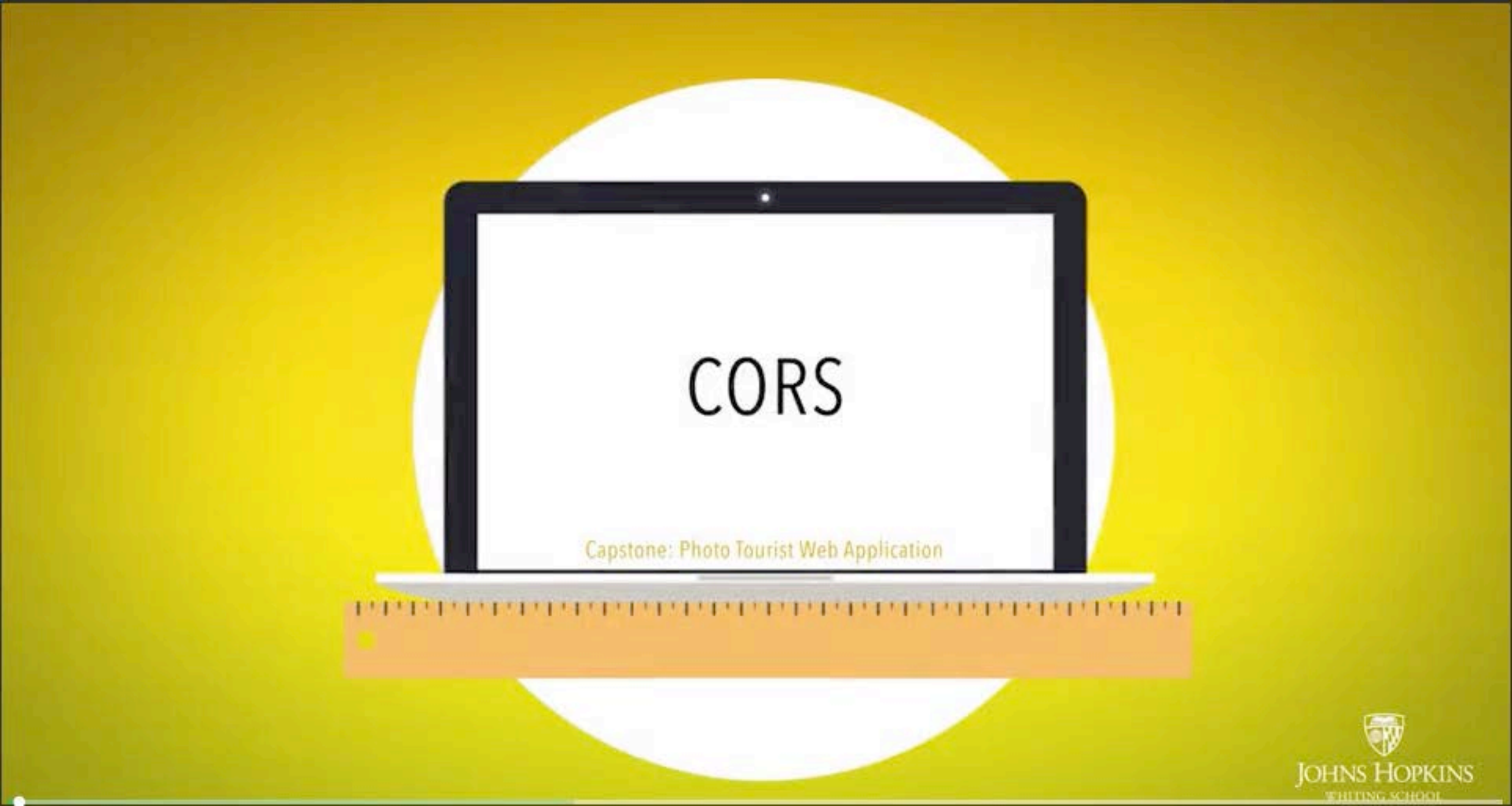
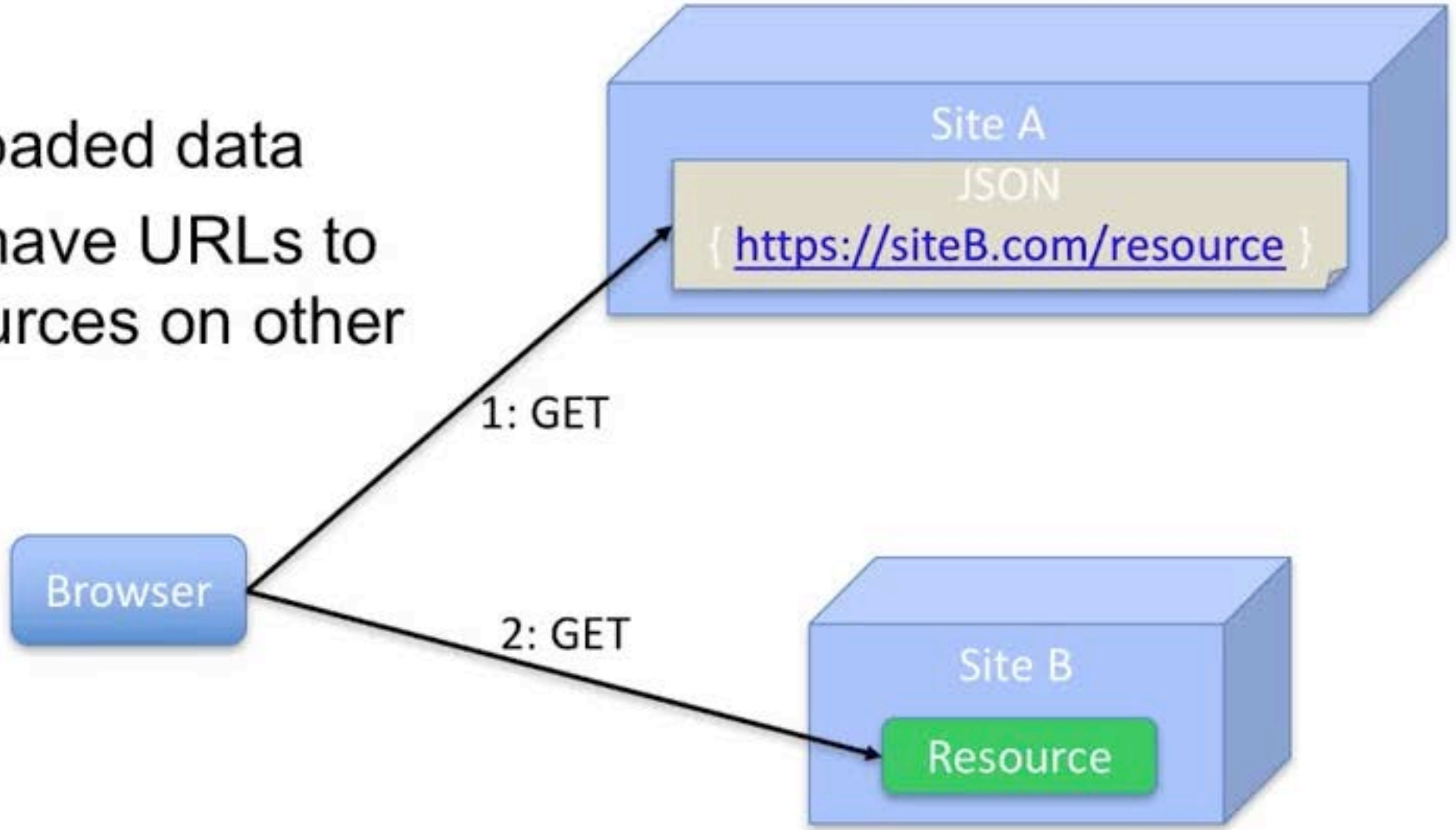

CORS
Capstone: Photo Tourist Web Application
JOHNS HOPKINS
WHITING SCHOOL

In this lecture, we will discuss…

- ✧ Same-Origin Policy
- ✧ Cross-Origin Resource Sharing (CORS)
- ✧ API Server Support Requirements

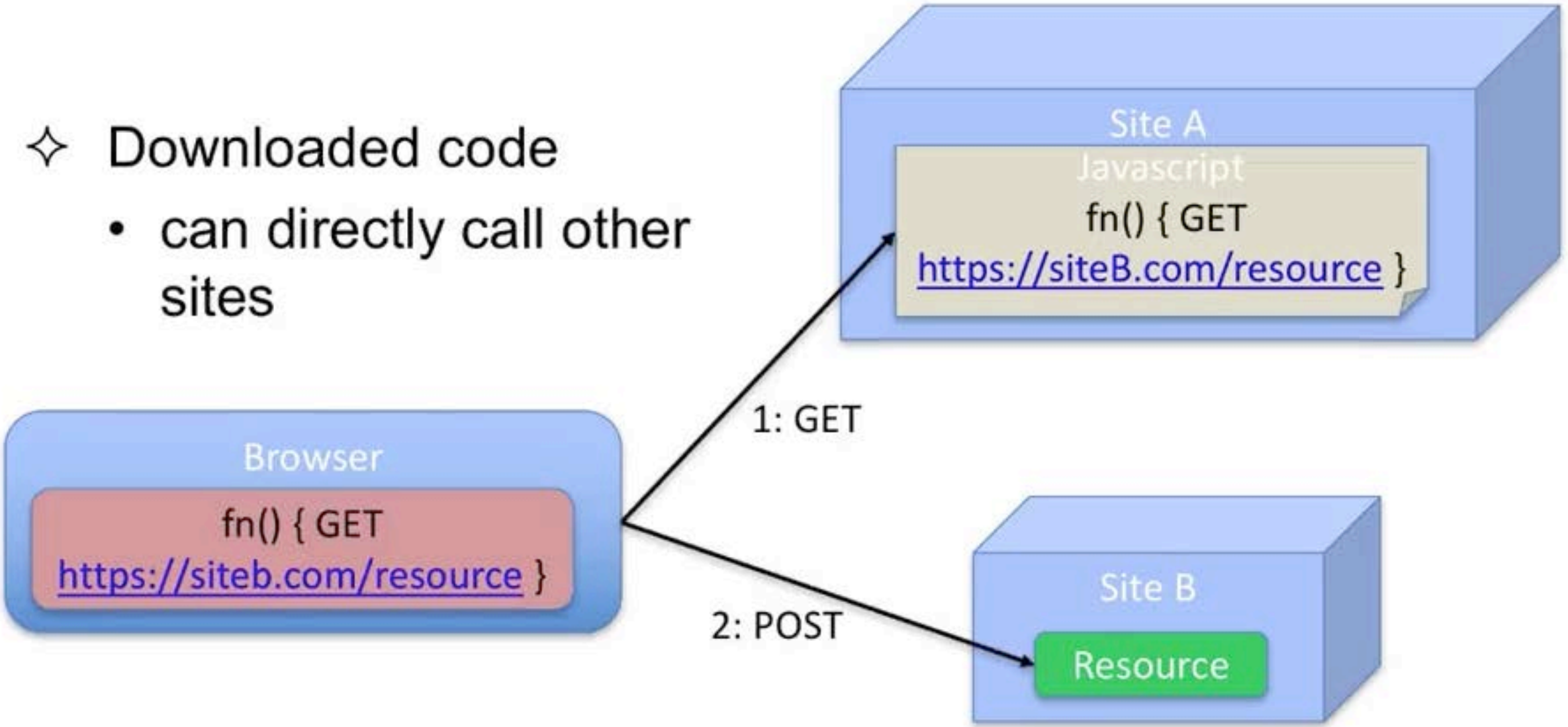
Data Scenario

- Downloaded data
  - can have URLs to resources on other sites



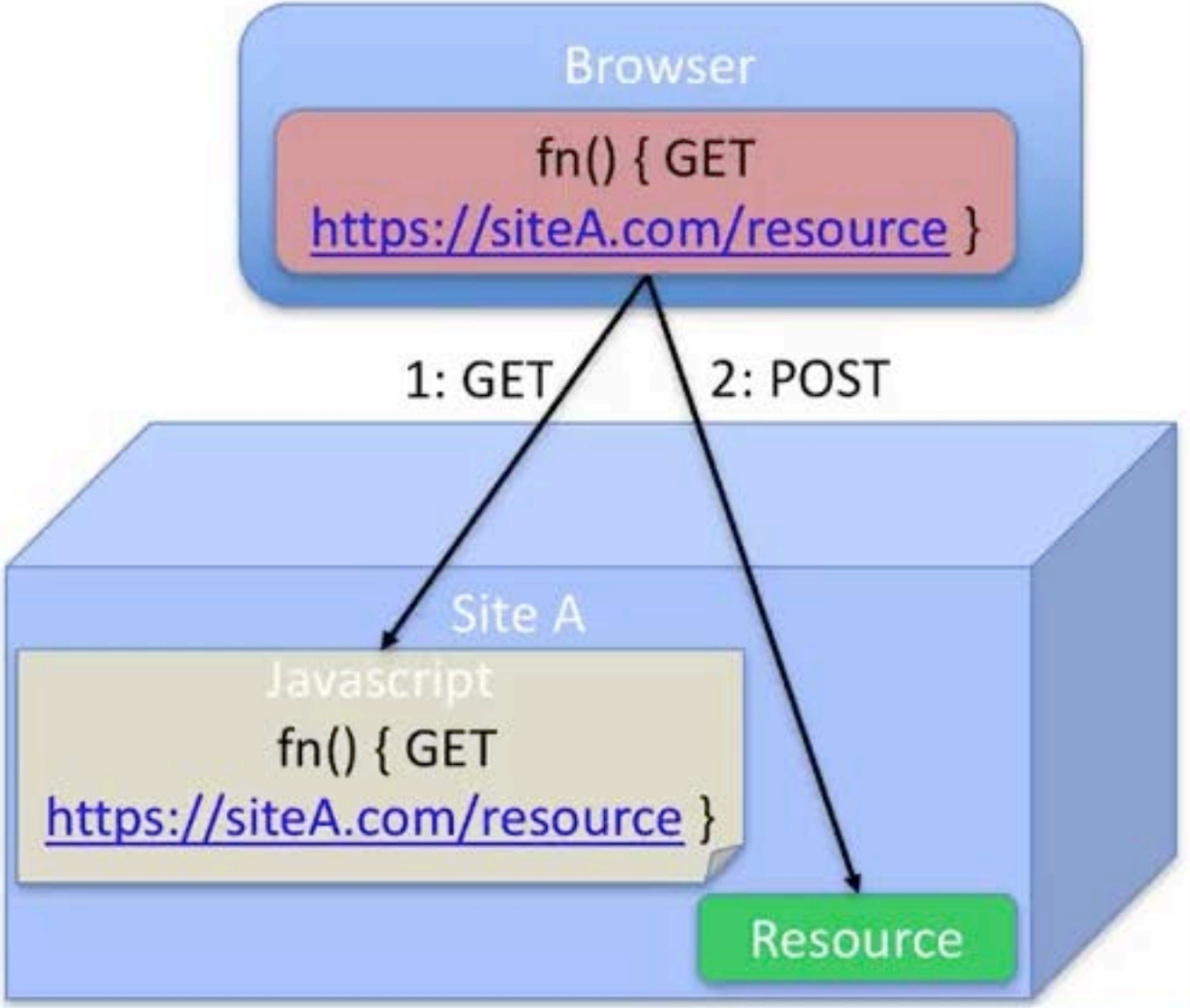
Code Scenario

- ✧ Downloaded code
  - can directly call other sites



Same-Origin Policy

- Browsers execute downloaded code within limits
- One limit is “Same Origin” Policy
  - Downloaded code may not make destructive (non-GET) calls to sites they do not originate from



Scenario

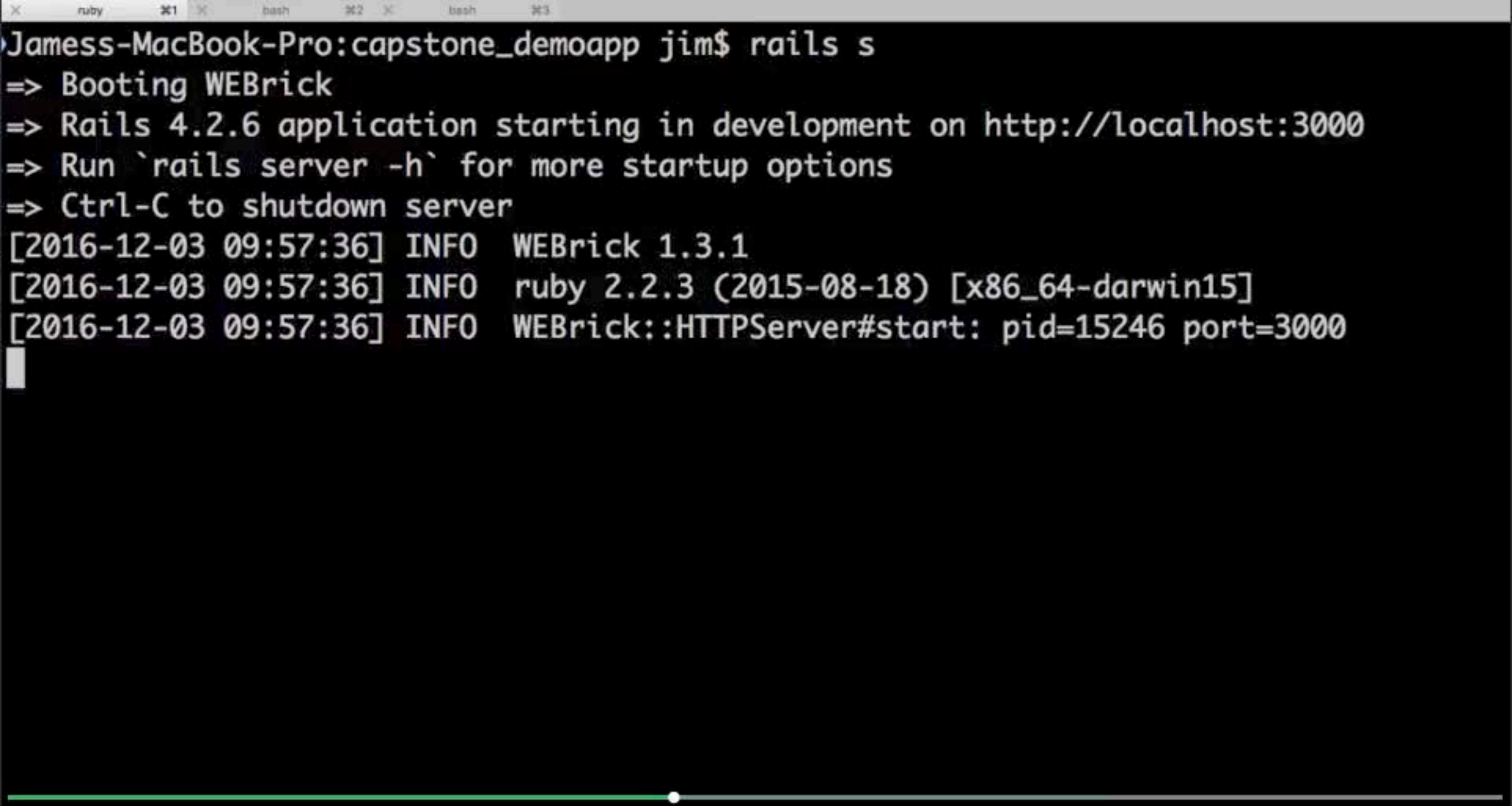
- ✧ Harm?
  - Code from sneeky.com posts to your Amazon account
- ✧ Trust?
  - Amazon deploys multiple UI faces to different sites
  - Sneeky.com is a trusted partner of Amazon that sells shoes

Cross-Origin Resource Sharing (CORS)

- Browser, executing code downloaded from SiteA
  - sends “Origin” header listing SiteA with initial GET
- Server will respond with
  - List of methods allowed
  - List of headers allowed
  - Whether authenticated access is allowed
  - How long the answer is good for
  - The origin the answer applies to
- Browser is the one doing the enforcement

```
<- "GET /api/foos HTTP/1.1\r\n
Origin: http://siteA.com\r\n
...
Host: http://siteB.com\r\n\r\n"
```

```
-> "HTTP/1.1 200 OK \r\n"
...
-> "Access-Control-Allow-Origin: http://siteA.com\r\n"
-> "Access-Control-Allow-Methods:
                    GET, POST, PUT, DELETE, OPTIONS\r\n"
-> "Access-Control-Expose-Headers: \r\n"
-> "Access-Control-Max-Age: 1728000\r\n"
-> "Access-Control-Allow-Credentials: true\r\n"
```


ruby ⌘1
bash ⌘2
bash ⌘3
Jamess-MacBook-Pro:capstone_demoapp jim$ rails s
=> Booting WEBrick
=> Rails 4.2.6 application starting in development on http://localhost:3000
=> Run `rails server -h` for more startup options
=> Ctrl-C to shutdown server
[2016-12-03 09:57:36] INFO WEBrick 1.3.1
[2016-12-03 09:57:36] INFO ruby 2.2.3 (2015-08-18) [x86_64-darwin15]
[2016-12-03 09:57:36] INFO WEBrick::HTTPServer#start: pid=15246 port=3000

```
Jamess-MacBook-Pro:capstone_demoapp jim$ rails c
Running via Spring preloader in process 15316
Loading development environment (Rails 4.2.6)
(reverse-i-search)`': 
```

```
Jamess-MacBook-Pro:capstone_demoapp jim$ rails c
Running via Spring preloader in process 15316
Loading development environment (Rails 4.2.6)
irb(main):001:0> url="http://localhost:3000/api/foos"
=> "http://localhost:3000/api/foos"
irb(main):002:0>
```

```
Jamess-MacBook-Pro:capstone_demoapp jim$ rails c
Running via Spring preloader in process 15316
Loading development environment (Rails 4.2.6)
irb(main):001:0> url="http://localhost:3000/api/foos"
=> "http://localhost:3000/api/foos"
irb(main):002:0> response=HTTParty.get(url, :headers=>{"Origin"=>"http://siteB.com"}, debug_output:$stdout); nil

opening connection to localhost:3000...
opened
<- "GET /api/foos HTTP/1.1\r\nOrigin: http://siteB.com\r\nConnection: close\r\nHost: localhost:3000\r\n\r\n"
-> "HTTP/1.1 200 OK \r\n"
-> "X-Frame-Options: SAMEORIGIN\r\n"
-> "X-Xss-Protection: 1; mode=block\r\n"
-> "X-Content-Type-Options: nosniff\r\n"
-> "Content-Type: application/json; charset=utf-8\r\n"
-> "Etag: W/\"6886a762f1fa286a1ded5191422bbb29\"\r\n"
-> "Cache-Control: max-age=0, private, must-revalidate\r\n"
-> "X-Request-Id: a2d41c15-35d1-454e-b2d9-98dc5331a862\r\n"
-> "X-Runtime: 0.006043\r\n"
-> "Server: WEBrick/1.3.1 (Ruby/2.2.3/2015-08-18)\r\n"
-> "Date: Sat, 03 Dec 2016 14:59:40 GMT\r\n"
-> "Content-Length: 436\r\n"
-> "Connection: close\r\n"
-> "\r\n"
reading 436 bytes...
-> "[{\"id\":2,\"name\":\"test1\",\"created_at\":\"2016-12-03T04:37:08.068Z\",\"updated_at\":\"2016-12-03T04:37:
08.068Z\",\"url\":\"http://localhost:3000/api/foos/2\"},{\"id\":3,\"name\":\"test2\",\"created_at\":\"2016-12-03
T04:37:08.153Z\",\"updated_at\":\"2016-12-03T04:37:08.153Z\",\"url\":\"http://localhost:3000/api/foos/3\"},{\"id
\":4,\"name\":\"test3\",\"created_at\":\"2016-12-03T04:37:08.155Z\",\"updated_at\":\"2016-12-03T04:37:08.155Z\",
\"url\":\"http://localhost:3000/api/foos/4\"}]"
read 436 bytes
Conn close
=> nil
```

```
Jamess-MacBook-Pro:capstone_demoapp jim$ rails c
Running via Spring preloader in process 15316
Loading development environment (Rails 4.2.6)
irb(main):001:0> url="http://localhost:3000/api/foos"
=> "http://localhost:3000/api/foos"
irb(main):002:0> response=HTTParty.get(url, :headers=>{"Origin"=>"http://siteB.com"}, debug_output:$stdout); nil

opening connection to localhost:3000...
opened
<- "GET /api/foos HTTP/1.1\r\nOrigin: http://siteB.com\r\nConnection: close\r\nHost: localhost:3000\r\n\r\n"
-> "HTTP/1.1 200 OK \r\n"
-> "X-Frame-Options: SAMEORIGIN\r\n"
-> "X-Xss-Protection: 1; mode=block\r\n"
-> "X-Content-Type-Options: nosniff\r\n"
-> "Content-Type: application/json; charset=utf-8\r\n"
-> "Etag: W/\"6886a762f1fa286a1ded5191422bbb29\"\r\n"
-> "Cache-Control: max-age=0, private, must-revalidate\r\n"
-> "X-Request-Id: a2d41c15-35d1-454e-b2d9-98dc5331a862\r\n"
-> "X-Runtime: 0.006043\r\n"
-> "Server: WEBrick/1.3.1 (Ruby/2.2.3/2015-08-18)\r\n"
-> "Date: Sat, 03 Dec 2016 14:59:40 GMT\r\n"
-> "Content-Length: 436\r\n"
-> "Connection: close\r\n"
-> "\r\n"
reading 436 bytes...
-> "[{\"id\":2,\"name\":\"test1\",\"created_at\":\"2016-12-03T04:37:08.068Z\",\"updated_at\":\"2016-12-03T04:37:
08.068Z\",\"url\":\"http://localhost:3000/api/foos/2\"},{\"id\":3,\"name\":\"test2\",\"created_at\":\"2016-12-03
T04:37:08.153Z\",\"updated_at\":\"2016-12-03T04:37:08.153Z\",\"url\":\"http://localhost:3000/api/foos/3\"},{\"id
\":4,\"name\":\"test3\",\"created_at\":\"2016-12-03T04:37:08.155Z\",\"updated_at\":\"2016-12-03T04:37:08.155Z\",
\"url\":\"http://localhost:3000/api/foos/4\"}]"
read 436 bytes
Conn close
=> nil
```

```
Mac:capstone_demoapp$ vi Gemfile
```

```
#
source 'https://rubygems.org'

gem 'rails', '4.2.6'
gem 'rails-api', '~>0.4', '>=0.4.0'
gem 'rack-cors', '~>0.4', '>=0.4.0', :require => 'rack/cors'

gem 'jbuilder', '~> 2.0', '>=2.6.0'

group :development do
  gem 'spring', '~>2.0', '>=2.0.0'
end

group :development, :test do
  gem 'tzinfo-data', :platforms=>[:mingw, :mswin, :x64_mingw, :jruby]
  gem 'httparty', '~>0.14', '>=0.14.0'

  gem 'rspec-rails', '~> 3.5', '>=3.5.2'
end

gem 'pg', '~>0.19', '>=0.19.0'
gem 'mongoid', '~>5.1', '>=5.1.5'
```

```
#
source 'https://rubygems.org'

gem 'rails', '4.2.6'
gem 'rails-api', '~>0.4', '>=0.4.0'
gem 'rack-cors', '~>0.4', '>=0.4.0', :require => 'rack/cors'

gem 'jbuilder', '~> 2.0', '>=2.6.0'

group :development do
  gem 'spring', '~>2.0', '>=2.0.0'
end

group :development, :test do
  gem 'tzinfo-data', :platforms=>[:mingw, :mswin, :x64_mingw, :jruby]
  gem 'httparty', '~>0.14', '>=0.14.0'

  gem 'rspec-rails', '~> 3.5', '>=3.5.2'
end

gem 'pg', '~>0.19', '>=0.19.0'
gem 'mongoid', '~>5.1', '>=5.1.5'
```

```
Mac:capstone_demoapp$ vi Gemfile
Mac:capstone_demoapp$ bundle
```

```
Using nokogiri 1.6.8.1
Using rack-test 0.6.3
Using mime-types 3.1
Using mongo 2.3.1
Using sprockets 3.7.0
Using httparty 0.14.0
Using rspec-core 3.5.4
Using rspec-expectations 3.5.0
Using rspec-mocks 3.5.0
Using activesupport 4.2.6
Using loofah 2.0.3
Using mail 2.6.4
Using rails-deprecated_sanitizer 1.0.3
Using globalid 0.3.7
Using activemodel 4.2.6
Using jbuilder 2.6.0
Using spring 2.0.0
Using rails-html-sanitizer 1.0.3
Using rails-dom-testing 1.0.7
Using activejob 4.2.6
Using activerecord 4.2.6
Using mongoid 5.1.5
Using actionview 4.2.6
Using actionpack 4.2.6
Using actionmailer 4.2.6
Using railties 4.2.6
Using sprockets-rails 3.2.0
Using rails-api 0.4.0
Using rspec-rails 3.5.2
Using rails 4.2.6
Bundle complete! 10 Gemfile dependencies, 53 gems now installed.
Gems in the group production were not installed.
Use `bundle show [gemname]` to see where a bundled gem is installed.
```

```
Mac:capstone_demoapp$ vi config/application.rb
```

```ruby
require File.expand_path('../boot', __FILE__)

require "rails"
# Pick the frameworks you want:
require "active_model/railtie"
require "active_job/railtie"
require "active_record/railtie"
require "action_controller/railtie"
require "action_mailer/railtie"
require "action_view/railtie"
require "sprockets/railtie"
# require "rails/test_unit/railtie"

# Require the gems listed in Gemfile, including any gems
# you've limited to :test, :development, or :production.
Bundler.require(*Rails.groups)

module Myapp
  class Application < Rails::Application
    # Settings in config/environments/* take precedence over those specified here.
    # Application configuration should go into files in config/initializers
    # -- all .rb files in that directory are automatically loaded.

    # Set Time.zone default to the specified zone and make Active Record auto-convert to this zone.
    # Run "rake -D time" for a list of tasks for finding time zone names. Default is UTC.
    # config.time_zone = 'Central Time (US & Canada)'

    # The default locale is :en and all translations from config/locales/*.rb,yml are auto loaded.
    # config.i18n.load_path += Dir[Rails.root.join('my', 'locales', '*.{rb,yml}').to_s]
    # config.i18n.default_locale = :de

    Mongoid.load!('./config/mongoid.yml')
    #which default ORM are we using with scaffold
```

```
19  class Application < Rails::Application
20    # Settings in config/environments/* take precedence over those specified here.
21    # Application configuration should go into files in config/initializers
22    # -- all .rb files in that directory are automatically loaded.
23
24    # Set Time.zone default to the specified zone and make Active Record auto-convert to this zone.
25    # Run "rake -D time" for a list of tasks for finding time zone names. Default is UTC.
26    # config.time_zone = 'Central Time (US & Canada)'
27
28    # The default locale is :en and all translations from config/locales/*.rb,yml are auto loaded.
29    # config.i18n.load_path += Dir[Rails.root.join('my', 'locales', '*.{rb,yml}').to_s]
30    # config.i18n.default_locale = :de
31
32    Mongoid.load!('./config/mongoid.yml')
33    #which default ORM are we using with scaffold
34    #add  --orm mongoid, or active_record
35    #    to rails generate cmd line to be specific
36    config.generators {|g| g.orm :active_record}
37    #config.generators {|g| g.orm :mongoid}
38
39  config.middleware.insert_before 0, "Rack::Cors" do
40    allow do
41      origins '*'
42
43      resource '/api/*',
44        :headers => :any,
45        :methods => [:get, :post, :put, :delete, :options]
46    end
47  end
```

```
20    # Settings in config/environments/* take precedence over those specified here.
21    # Application configuration should go into files in config/initializers
22    # -- all .rb files in that directory are automatically loaded.
23
24    # Set Time.zone default to the specified zone and make Active Record auto-convert to this zone.
25    # Run "rake -D time" for a list of tasks for finding time zone names. Default is UTC.
26    # config.time_zone = 'Central Time (US & Canada)'
27
28    # The default locale is :en and all translations from config/locales/*.rb,yml are auto loaded.
29    # config.i18n.load_path += Dir[Rails.root.join('my', 'locales', '*.{rb,yml}').to_s]
30    # config.i18n.default_locale = :de
31
32    Mongoid.load!('./config/mongoid.yml')
33    #which default ORM are we using with scaffold
34    #add  --orm mongoid, or active_record
35    #    to rails generate cmd line to be specific
36    config.generators {|g| g.orm :active_record}
37    #config.generators {|g| g.orm :mongoid}
38
39    config.middleware.insert_before 0, "Rack::Cors" do
40      allow do
41        origins '*'
42
43        resource '/api/*',
44          :headers => :any,
45          :methods => [:get, :post, :put, :delete, :options]
46      end
47    end
48
```

```
20      # Settings in config/environments/* take precedence over those specified here.
21      # Application configuration should go into files in config/initializers
22      # -- all .rb files in that directory are automatically loaded.
23
24      # Set Time.zone default to the specified zone and make Active Record auto-convert to this zone.
25      # Run "rake -D time" for a list of tasks for finding time zone names. Default is UTC.
26      # config.time_zone = 'Central Time (US & Canada)'
27
28      # The default locale is :en and all translations from config/locales/*.rb,yml are auto loaded.
29      # config.i18n.load_path += Dir[Rails.root.join('my', 'locales', '*.{rb,yml}').to_s]
30      # config.i18n.default_locale = :de
31
32      Mongoid.load!('./config/mongoid.yml')
33      #which default ORM are we using with scaffold
34      #add  --orm mongoid, or active_record
35      #    to rails generate cmd line to be specific
36      config.generators {|g| g.orm :active_record}
37      #config.generators {|g| g.orm :mongoid}
38
39      config.middleware.insert_before 0, "Rack::Cors" do
40        allow do
41          origins 'siteB.com'
42
43          resource '/api/*',
44            :headers => :any,
45            :methods => [:get, :post, :put, :delete, :options]
46        end
47      end
48
```

```
Jamess-MacBook-Pro:capstone_demoapp jim$ rails s
=> Booting WEBrick
=> Rails 4.2.6 application starting in development on http://localhost:3000
=> Run `rails server -h` for more startup options
=> Ctrl-C to shutdown server
[2016-12-03 10:23:36] INFO  WEBrick 1.3.1
[2016-12-03 10:23:36] INFO  ruby 2.2.3 (2015-08-18) [x86_64-darwin15]
[2016-12-03 10:23:36] INFO  WEBrick::HTTPServer#start: pid=15707 port=3000
```

```
irb(main):004:0> response=HTTParty.get(url, :headers=>{"Origin"=>"http://siteB.com"}, debug_output:$stdout); nil
```

```
irb(main):004:0> response=HTTParty.get(url, :headers=>{"Origin"=>"http://siteB.com"}, debug_output:$stdout); nil
opening connection to localhost:3000...
opened
<- "GET /api/foos HTTP/1.1\r\nOrigin: http://siteB.com\r\nConnection: close\r\nHost: localhost:3000\r\n\r\n"
-> "HTTP/1.1 200 OK \r\n"
-> "X-Frame-Options: SAMEORIGIN\r\n"
-> "X-Xss-Protection: 1; mode=block\r\n"
-> "X-Content-Type-Options: nosniff\r\n"
-> "Content-Type: application/json; charset=utf-8\r\n"
-> "Etag: W/\"6886a762f1fa286a1ded5191422bbb29\"\r\n"
-> "Cache-Control: max-age=0, private, must-revalidate\r\n"
-> "X-Request-Id: 12d2c35c-1d9f-4a9a-99e3-8486420b61ec\r\n"
-> "X-Runtime: 0.141814\r\n"
-> "Access-Control-Allow-Origin: http://siteB.com\r\n"
-> "Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS\r\n"
-> "Access-Control-Expose-Headers: \r\n"
-> "Access-Control-Max-Age: 1728000\r\n"
-> "Access-Control-Allow-Credentials: true\r\n"
-> "Vary: Origin\r\n"
-> "Server: WEBrick/1.3.1 (Ruby/2.2.3/2015-08-18)\r\n"
-> "Date: Sat, 03 Dec 2016 15:23:46 GMT\r\n"
-> "Content-Length: 436\r\n"
-> "Connection: close\r\n"
-> "\r\n"
reading 436 bytes...
-> "[{\"id\":2,\"name\":\"test1\",\"created_at\":\"2016-12-03T04:37:08.068Z\",\"updated_at\":\"2016-12-03T04:37:
08.068Z\",\"url\":\"http://localhost:3000/api/foos/2\"},{\"id\":3,\"name\":\"test2\",\"created_at\":\"2016-12-03
T04:37:08.153Z\",\"updated_at\":\"2016-12-03T04:37:08.153Z\",\"url\":\"http://localhost:3000/api/foos/3\"},{\"id
\":4,\"name\":\"test3\",\"created_at\":\"2016-12-03T04:37:08.155Z\",\"updated_at\":\"2016-12-03T04:37:08.155Z\",
\"url\":\"http://localhost:3000/api/foos/4\"}]"
read 436 bytes
Conn close
=> nil
```

```
irb(main):004:0> response=HTTParty.get(url, :headers=>{"Origin"=>"http://siteB.com"}, debug_output:$stdout); nil
opening connection to localhost:3000...
opened
<- "GET /api/foos HTTP/1.1\r\nOrigin: http://siteB.com\r\nConnection: close\r\nHost: localhost:3000\r\n\r\n"
-> "HTTP/1.1 200 OK \r\n"
-> "X-Frame-Options: SAMEORIGIN\r\n"
-> "X-Xss-Protection: 1; mode=block\r\n"
-> "X-Content-Type-Options: nosniff\r\n"
-> "Content-Type: application/json; charset=utf-8\r\n"
-> "Etag: W/\"6886a762f1fa286a1ded5191422bbb29\"\r\n"
-> "Cache-Control: max-age=0, private, must-revalidate\r\n"
-> "X-Request-Id: 12d2c35c-1d9f-4a9a-99e3-8486420b61ec\r\n"
-> "X-Runtime: 0.141814\r\n"
-> "Access-Control-Allow-Origin: http://siteB.com\r\n"
-> "Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS\r\n"
-> "Access-Control-Expose-Headers: \r\n"
-> "Access-Control-Max-Age: 1728000\r\n"
-> "Access-Control-Allow-Credentials: true\r\n"
-> "Vary: Origin\r\n"
-> "Server: WEBrick/1.3.1 (Ruby/2.2.3/2015-08-18)\r\n"
-> "Date: Sat, 03 Dec 2016 15:23:46 GMT\r\n"
-> "Content-Length: 436\r\n"
-> "Connection: close\r\n"
-> "\r\n"
reading 436 bytes...
-> "[{\"id\":2,\"name\":\"test1\",\"created_at\":\"2016-12-03T04:37:08.068Z\",\"updated_at\":\"2016-12-03T04:37:
08.068Z\",\"url\":\"http://localhost:3000/api/foos/2\"},{\"id\":3,\"name\":\"test2\",\"created_at\":\"2016-12-03
T04:37:08.153Z\",\"updated_at\":\"2016-12-03T04:37:08.153Z\",\"url\":\"http://localhost:3000/api/foos/3\"},{\"id
\":4,\"name\":\"test3\",\"created_at\":\"2016-12-03T04:37:08.155Z\",\"updated_at\":\"2016-12-03T04:37:08.155Z\",
\"url\":\"http://localhost:3000/api/foos/4\"}]"
read 436 bytes
Conn close
=> nil
```

```
irb(main):005:0> response=HTTParty.get(url, :headers=>{"Origin"=>"http://siteC.com"}, debug_output:$stdout); nil

opening connection to localhost:3000...
opened
<- "GET /api/foos HTTP/1.1\r\nOrigin: http://siteC.com\r\nConnection: close\r\nHost: localhost:3000\r\n\r\n"
-> "HTTP/1.1 200 OK \r\n"
-> "X-Frame-Options: SAMEORIGIN\r\n"
-> "X-Xss-Protection: 1; mode=block\r\n"
-> "X-Content-Type-Options: nosniff\r\n"
-> "Content-Type: application/json; charset=utf-8\r\n"
-> "Etag: W/\"6886a762f1fa286a1ded5191422bbb29\"\r\n"
-> "Cache-Control: max-age=0, private, must-revalidate\r\n"
-> "X-Request-Id: e8801840-ca0e-44d6-a27d-6abcf95be5db\r\n"
-> "X-Runtime: 0.005957\r\n"
-> "Vary: Origin\r\n"
-> "Server: WEBrick/1.3.1 (Ruby/2.2.3/2015-08-18)\r\n"
-> "Date: Sat, 03 Dec 2016 15:24:04 GMT\r\n"
-> "Content-Length: 436\r\n"
-> "Connection: close\r\n"
-> "\r\n"
reading 436 bytes...
-> "[{\"id\":2,\"name\":\"test1\",\"created_at\":\"2016-12-03T04:37:08.068Z\",\"updated_at\":\"2016-12-03T04:37:
08.068Z\",\"url\":\"http://localhost:3000/api/foos/2\"},{\"id\":3,\"name\":\"test2\",\"created_at\":\"2016-12-03
T04:37:08.153Z\",\"updated_at\":\"2016-12-03T04:37:08.153Z\",\"url\":\"http://localhost:3000/api/foos/3\"},{\"id
\":4,\"name\":\"test3\",\"created_at\":\"2016-12-03T04:37:08.155Z\",\"updated_at\":\"2016-12-03T04:37:08.155Z\",
\"url\":\"http://localhost:3000/api/foos/4\"}]"
read 436 bytes
Conn close
=> nil
irb(main):006:0>
```

```
Jamess-MacBook-Pro:capstone_demoapp jim$ rails s
=> Booting WEBrick
=> Rails 4.2.6 application starting in development on http://localhost:3000
=> Run `rails server -h` for more startup options
=> Ctrl-C to shutdown server
[2016-12-03 10:23:36] INFO  WEBrick 1.3.1
[2016-12-03 10:23:36] INFO  ruby 2.2.3 (2015-08-18) [x86_64-darwin15]
[2016-12-03 10:23:36] INFO  WEBrick::HTTPServer#start: pid=15707 port=3000


Started GET "/api/foos" for ::1 at 2016-12-03 10:23:45 -0500
  ActiveRecord::SchemaMigration Load (0.3ms)  SELECT "schema_migrations".* FROM "schema_migrations"
Processing by FoosController#index as JSON
  Foo Load (0.3ms)  SELECT "foos".* FROM "foos"
  Rendered foos/_foo.json.jbuilder (0.7ms)
  Rendered foos/_foo.json.jbuilder (0.2ms)
  Rendered foos/_foo.json.jbuilder (0.2ms)
  Rendered foos/index.json.jbuilder (10.4ms)
Completed 200 OK in 17ms (Views: 13.9ms | ActiveRecord: 2.0ms)


Started GET "/api/foos" for ::1 at 2016-12-03 10:24:04 -0500
Processing by FoosController#index as JSON
  Foo Load (0.2ms)  SELECT "foos".* FROM "foos"
  Rendered foos/_foo.json.jbuilder (0.3ms)
  Rendered foos/_foo.json.jbuilder (0.2ms)
  Rendered foos/_foo.json.jbuilder (0.2ms)
  Rendered foos/index.json.jbuilder (2.8ms)
Completed 200 OK in 4ms (Views: 3.6ms | ActiveRecord: 0.2ms)
```

```
=> Run `rails server -h` for more startup options
=> Ctrl-C to shutdown server
[2016-12-03 10:23:36] INFO  WEBrick 1.3.1
[2016-12-03 10:23:36] INFO  ruby 2.2.3 (2015-08-18) [x86_64-darwin15]
[2016-12-03 10:23:36] INFO  WEBrick::HTTPServer#start: pid=15707 port=3000


Started GET "/api/foos" for ::1 at 2016-12-03 10:23:45 -0500
  ActiveRecord::SchemaMigration Load (0.3ms)  SELECT "schema_migrations".* FROM "schema_migrations"
Processing by FoosController#index as JSON
  Foo Load (0.3ms)  SELECT "foos".* FROM "foos"
  Rendered foos/_foo.json.jbuilder (0.7ms)
  Rendered foos/_foo.json.jbuilder (0.2ms)
  Rendered foos/_foo.json.jbuilder (0.2ms)
  Rendered foos/index.json.jbuilder (10.4ms)
Completed 200 OK in 17ms (Views: 13.9ms | ActiveRecord: 2.0ms)


Started GET "/api/foos" for ::1 at 2016-12-03 10:24:04 -0500
Processing by FoosController#index as JSON
  Foo Load (0.2ms)  SELECT "foos".* FROM "foos"
  Rendered foos/_foo.json.jbuilder (0.3ms)
  Rendered foos/_foo.json.jbuilder (0.2ms)
  Rendered foos/_foo.json.jbuilder (0.2ms)
  Rendered foos/index.json.jbuilder (2.8ms)
Completed 200 OK in 4ms (Views: 3.6ms | ActiveRecord: 0.2ms)
^C[2016-12-03 10:24:52] INFO  going to shutdown ...
[2016-12-03 10:24:52] INFO  WEBrick::HTTPServer#start done.
Exiting
```

```ruby
    # Set Time.zone default to the specified zone and make Active Record auto-convert to this zone.
    # Run "rake -D time" for a list of tasks for finding time zone names. Default is UTC.
    # config.time_zone = 'Central Time (US & Canada)'

    # The default locale is :en and all translations from config/locales/*.rb,yml are auto loaded.
    # config.i18n.load_path += Dir[Rails.root.join('my', 'locales', '*.{rb,yml}').to_s]
    # config.i18n.default_locale = :de

    Mongoid.load!('./config/mongoid.yml')
    #which default ORM are we using with scaffold
    #add  --orm mongoid, or active_record
    #    to rails generate cmd line to be specific
    config.generators {|g| g.orm :active_record}
    #config.generators {|g| g.orm :mongoid}

    config.middleware.insert_before 0, "Rack::Cors" do
      allow do
        origins 'SiteB.com'

        resource '/api/*',
          :headers => :any,
          :methods => [:get, :post, :put, :delete, :options]
      end
    end

    # Do not swallow errors in after_commit/after_rollback callbacks.
    config.active_record.raise_in_transactional_callbacks = true
  end
end
```

```
24      # Set Time.zone default to the specified zone and make Active Record auto-convert to this zone.
25      # Run "rake -D time" for a list of tasks for finding time zone names. Default is UTC.
26      # config.time_zone = 'Central Time (US & Canada)'
27
28      # The default locale is :en and all translations from config/locales/*.rb,yml are auto loaded.
29      # config.i18n.load_path += Dir[Rails.root.join('my', 'locales', '*.{rb,yml}').to_s]
30      # config.i18n.default_locale = :de
31
32      Mongoid.load!('./config/mongoid.yml')
33      #which default ORM are we using with scaffold
34      #add  --orm mongoid, or active_record
35      #    to rails generate cmd line to be specific
36      config.generators {|g| g.orm :active_record}
37      #config.generators {|g| g.orm :mongoid}
38
39      config.middleware.insert_before 0, "Rack::Cors" do
40        allow do
41          origins '*'
42
43          resource '/api/*',
44            :headers => :any,
45            :methods => [:get, :post, :put, :delete, :options]
46        end
47      end
48
49      # Do not swallow errors in after_commit/after_rollback callbacks.
50      config.active_record.raise_in_transactional_callbacks = true
51    end
52  end
```

```
Jamess-MacBook-Pro:capstone_demoapp jim$
```

```
Jamess-MacBook-Pro:capstone_demoapp jim$ rails s
=> Booting WEBrick
=> Rails 4.2.6 application starting in development on http://localhost:3000
=> Run `rails server -h` for more startup options
=> Ctrl-C to shutdown server
[2016-12-03 10:25:37] INFO  WEBrick 1.3.1
[2016-12-03 10:25:37] INFO  ruby 2.2.3 (2015-08-18) [x86_64-darwin15]
[2016-12-03 10:25:37] INFO  WEBrick::HTTPServer#start: pid=15791 port=3000
```

```
irb(main):006:0> response=HTTParty.get(url, :headers=>{"Origin"=>"http://siteC.com"}, debug_output:$stdout); nil
opening connection to localhost:3000...
opened
<- "GET /api/foos HTTP/1.1\r\nOrigin: http://siteC.com\r\nConnection: close\r\nHost: localhost:3000\r\n\r\n"
-> "HTTP/1.1 200 OK \r\n"
-> "X-Frame-Options: SAMEORIGIN\r\n"
-> "X-Xss-Protection: 1; mode=block\r\n"
-> "X-Content-Type-Options: nosniff\r\n"
-> "Content-Type: application/json; charset=utf-8\r\n"
-> "Etag: W/\"6886a762f1fa286a1ded5191422bbb29\"\r\n"
-> "Cache-Control: max-age=0, private, must-revalidate\r\n"
-> "X-Request-Id: 1dffe501-cc18-4954-bb7f-41896db909b3\r\n"
-> "X-Runtime: 0.142804\r\n"
-> "Access-Control-Allow-Origin: http://siteC.com\r\n"
-> "Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS\r\n"
-> "Access-Control-Expose-Headers: \r\n"
-> "Access-Control-Max-Age: 1728000\r\n"
-> "Access-Control-Allow-Credentials: true\r\n"
-> "Vary: Origin\r\n"
-> "Server: WEBrick/1.3.1 (Ruby/2.2.3/2015-08-18)\r\n"
-> "Date: Sat, 03 Dec 2016 15:25:42 GMT\r\n"
-> "Content-Length: 436\r\n"
-> "Connection: close\r\n"
-> "\r\n"
reading 436 bytes...
-> "[{\"id\":2,\"name\":\"test1\",\"created_at\":\"2016-12-03T04:37:08.068Z\",\"updated_at\":\"2016-12-03T04:37:
08.068Z\",\"url\":\"http://localhost:3000/api/foos/2\"},{\"id\":3,\"name\":\"test2\",\"created_at\":\"2016-12-03
T04:37:08.153Z\",\"updated_at\":\"2016-12-03T04:37:08.153Z\",\"url\":\"http://localhost:3000/api/foos/3\"},{\"id
\":4,\"name\":\"test3\",\"created_at\":\"2016-12-03T04:37:08.155Z\",\"updated_at\":\"2016-12-03T04:37:08.155Z\",
\"url\":\"http://localhost:3000/api/foos/4\"}]"
read 436 bytes
Conn close
=> nil
```

```
irb(main):006:0> response=HTTParty.get(url, :headers=>{"Origin"=>"http://siteC.com"}, debug_output:$stdout); nil
opening connection to localhost:3000...
opened
<- "GET /api/foos HTTP/1.1\r\nOrigin: http://siteC.com\r\nConnection: close\r\nHost: localhost:3000\r\n\r\n"
-> "HTTP/1.1 200 OK \r\n"
-> "X-Frame-Options: SAMEORIGIN\r\n"
-> "X-Xss-Protection: 1; mode=block\r\n"
-> "X-Content-Type-Options: nosniff\r\n"
-> "Content-Type: application/json; charset=utf-8\r\n"
-> "Etag: W/\"6886a762f1fa286a1ded5191422bbb29\"\r\n"
-> "Cache-Control: max-age=0, private, must-revalidate\r\n"
-> "X-Request-Id: 1dffe501-cc18-4954-bb7f-41896db909b3\r\n"
-> "X-Runtime: 0.142804\r\n"
-> "Access-Control-Allow-Origin: http://siteC.com\r\n"
-> "Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS\r\n"
-> "Access-Control-Expose-Headers: \r\n"
-> "Access-Control-Max-Age: 1728000\r\n"
-> "Access-Control-Allow-Credentials: true\r\n"
-> "Vary: Origin\r\n"
-> "Server: WEBrick/1.3.1 (Ruby/2.2.3/2015-08-18)\r\n"
-> "Date: Sat, 03 Dec 2016 15:25:42 GMT\r\n"
-> "Content-Length: 436\r\n"
-> "Connection: close\r\n"
-> "\r\n"
reading 436 bytes...
-> "[{\"id\":2,\"name\":\"test1\",\"created_at\":\"2016-12-03T04:37:08.068Z\",\"updated_at\":\"2016-12-03T04:37:
08.068Z\",\"url\":\"http://localhost:3000/api/foos/2\"},{\"id\":3,\"name\":\"test2\",\"created_at\":\"2016-12-03
T04:37:08.153Z\",\"updated_at\":\"2016-12-03T04:37:08.153Z\",\"url\":\"http://localhost:3000/api/foos/3\"},{\"id
\":4,\"name\":\"test3\",\"created_at\":\"2016-12-03T04:37:08.155Z\",\"updated_at\":\"2016-12-03T04:37:08.155Z\",
\"url\":\"http://localhost:3000/api/foos/4\"}]"
read 436 bytes
Conn close
=> nil
```

Summary

- APIs and UI code may be deployed independently
- Presents an origin security risk to browsers
- APIs must support browser headers for CORS to work

What's Next?

- Configuring Alternate Servers