4 ActionController::Parameters .each returns an unsafe hash

Share:

TIMELINE

abuisman submitted a report to Ruby on Rails. Nov 24th (5 years ago)

Rails 5.1.4

The goal of `ActionController::Parameters`'s `permit` method (strong parameters) is to prevent accidental trust in the parameters sent by the client. We can therefore not simply create a hash of all the parameters in the params without permitting them first. When we really want to do this there is the method `to_unsafe_h`, indicating the importance of controlling when an unsafe hash is returned. However, when we use `.each` on our parameters object, an unsafe hash is returned that includes all the keys and their values in a new hash:

Code 644 Bytes Wrap lines Copy Download

```
params = ActionController::Parameters.new(city: 'Nijmegen', country: 'Netherlands', language: 'Dutch')

params.to_h

# ActionController::UnfilteredParameters: unable to convert unpermitted parameters to hash
# from ...lib/ruby/gems/2.4.0/gems/actionpack-5.1.4/lib/action_controller/metal/strong_parameters.rb:265:in `to_h'

params.permit(:city)
=> <ActionController::Parameters {"city"=>"Nijmegen"} permitted: true>

params.permit(:city).to_h
=> {"city"=>"Nijmegen"}

params.to_unsafe_h
=> {"city"=>"Nijmegen", "country"=>"Netherlands", "language"=>"Dutch"}

params.each {}
=> {"city"=>"Nijmegen", "country"=>"Netherlands", "language"=>"Dutch"}
```

This behaviour is extra strange when contraste with how `select` works:

Code 141 Bytes Wrap lines Copy Download

```
params.select { true }
=> <ActionController::Parameters {"city"=>"Nijmegen", "country"=>"Netherlands", "language"=>"Dutch"} permitted: false>
```

Here you can see that select returns an instance of `ActionController::Parameters` that has `permitted: false`

Impact

An attacker could find out about the accidental use of each in working with parameters in a controller and use this knowledge to send additional (more than provided in a form) parameters along and in this way circumvent authorisation checks.

Code 210 Bytes Wrap lines Copy Download

```
# controller:

def update
  # Attacker has included the parameter: `{ is_admin: true }`
  User.update(clean_up_params)
end

def clean_up_params

  params.each { |k, v|  SomeModel.check(v) if k == :name }
end
```

The example (admittedly simplified) above shows a possible scenario where a developer builds a method to do something with each param in a seperate method after which he might expect his parameters to adhere to normal working `permitted: true/false`. Slightly unexpected behaviour that could cause security issues.

Biggest threat would seem to be to opensource projects where attackers can survey the project's code.

rafaelfranca Ruby on Rails staff posted a comment. Dec 5th (5 years ago)

Thank you for the report. Our team will investigate the issue and we will return back in a few days.

In meantime we ask you to not disclose this issue with anyone until we fully discard it as a security issue.

rafaelfranca Ruby on Rails staff added weakness "SQL Injection" and removed weakness "Cross-site Scripting (XSS) - Generic". Updated Feb 28th (5 years ago)

rafaelfranca Ruby on Rails staff updated the severity from High (7.1) to Medium (6.5). Dec 5th (5 years ago)

lasagna removed weakness "SQL Injection". May 13th (3 years ago)

jack_mccracken changed the status to Triaged. May 13th (3 years ago)

2 attachments:
F827234: 0001-5.2-backport-ActionController-StrongParameters-Retur.patch
F827235: 0001-6.0-ActionController-StrongParameters-Return-self-when-c.patch

tenderlove Ruby on Rails staff closed the report and changed the status to ⚭ **Resolved**. May 18th (3 years ago)

Shipped

The Internet Bug Bounty rewarded abuisman with a **$500** bounty. May 18th (3 years ago)

tenderlove Ruby on Rails staff requested to disclose this report. May 18th (3 years ago)

abuisman agreed to disclose this report. May 18th (3 years ago)

Hi @rafaelfranca, @jack_mccracken and @tenderlove,

Thanks a lot for handling my report. I don't think abuse of this is very likely either, but small incremental fixes make the security go round.

Thanks for the bounty as well! I wasn't expecting anything, so it is a very nice and welcome surprise.

Kind regards,

Achilleas Buisman

This report has been disclosed. May 18th (3 years ago)