The Boy Who Cried GitHub

James Magahern

April 9, 2012

About GitHub

- GitHub.com runs on Ruby on Rails
- Ruby on Rails is open source
- Ruby on Rails's source repository is hosted on... GitHub!

Vulnerability

- Russian developer opens ticket about a vulnerability he found.
- Vulnerability had to do with a special permissions attribute.
- If the developer does not specify this attribute in a configuration file, a hacker could potentially assign it himself using a malformed POST request.

Ticket Closed?

homakov opened this issue a month ago

Mass assignment vulnerability - how to force dev. define attr_accesible?

No one is assigned | No milestone

Those who don't know methods attr_accesible / protected - check that article out http://enlightsolutions.com/articles/whats-new-in-edge-scoped-mass-assignment-in-rails-3-1

Let's view at typical situation - middle level rails developer builds website for customer, w/o any special protections in model(Yeah! they don't write it! I have asked few my friends - they dont!)
Next, people use this website but if any of them has an idea that developer didnt specify "attr_accesible" - hacker can just add an http field in params, e.g. we have pursue's name edition. POST request at pursues#update

id = 333 (target's pursues id)
pursue['name'] = 'my purses name'
pursue['user_id'] = 412(hacker id)

if code is scaffolded than likely we got Pursue.find(params[:id]).update_attributes(params[:pursue]) in the controller. And that is what I worry about.

After execution that POST we got hacker owning target's pursue!

I don't mean that it is Rails problem, of course not. But let's get it real(Getting Real ok) - most of developers are middle/junior level and most of them don't write important but not very neccessary things: tests, role checks etc including topic - attr_accesible

how to avoid injections ? What should Rails framework do to force people to keep their rails websites safe? Making attr_accesible necessary field in model? What do you think guys.

Closed

105 comments

Labels

STFU N00B!

- Ticket was closed multiple times by other project maintainers.
- Homakov tried multiple times to get his point across.
- Project maintainers said it's not a Rails problem, that it's the developer's responsibility to secure his/her own code.

A little fun...


homakov opened this issue in 1001 years
I'm Bender from Future.
No one is assigned
Hey. Where is a suicide booth?
from 3012 with love
You should check it ... #5228

GitHub, Y U SO OPEN?

- GitHub bug?
- Issue was closed... again.
- Project watchers just laugh at issue.
- Everybody forgets about it...

Told ya so

wow how come I commit in master? O_o

homakov authored a month ago 1 parent 4d391a4f

Showing 1 changed file with 3 additions and 0 deletions.

\+ hacked

hacked

```
...  ...  @@ -0,0 +1,3 @@
       1  +another showcase of rails apps vunlerability.
       2  +Github pwned. again :(
       3  +will you pay me for security audit?
```

Noo! Not Reddit!

- Homakov commits to master branch of the Ruby on Rails project.
- Had the power to delete the entire history of projects such as jQuery, Node.js, Reddit, and Redis.


I found an exploit using
attr_accessible
Better commit to Rails master
quickmeme.com

Aftermath

- GitHub apologizes for how it handled how white hat hackers should disclose important security vulnerabilities.
- GitHub authors an official document about how these issues should be handled in the future.

What We Learned

- You can't trust an individual user of a popular framework to take proper security precautions themselves (even GitHub, apparently).
- Improperly designed default settings can be dangerous.
- If a white-hat Russian hacker tells you about an important security vulnerability, you should probably listen!

References

- http://blog.mhartl.com/2008/09/21/mass-assignment-in-rails-applications/
- http://www.extremetech.com/computing/120981-github-hacked-millions-of-projects-at-risk-of-being-modified-or-deleted
- http://homakov.blogspot.com/2012/03/how-to.html
- http://www.zdnet.com/blog/security/how-github-handled-getting-hacked/10473
- https://github.com/blog/1069-responsible-disclosure-policy