Bug Bounty Hunting on Steroids

@anshuman_bh @_devalias @mhmdiaa

The Team

Anshuman Bhartiya

@anshuman_bh

Security Engineer, Bug Bounty Hunter

Automate all the things!!

All things as code!!

Mohammed Diaa

@mhmdiaa

Developer, Bug Hunter

Never send a human to do a machine's job

Glenn 'devalias' Grant

@_devalias

Hacker, Polyglot Developer, Bounty Hunter, #SecDevOpsInTheCloudCyber™ enthusiast...

Penetration Tester and Offensive Capability Development at TSS

TSS
DISCREET | NICHE | TAILORED

@anshuman_bh @_devalias @mhmdiaa

Agenda

- Problem?
- Current Situation
- Target: Ellingson Mineral Corporation
- Introducing BountyMachine
- Lessons Learned
- Conclusion

Problem?

- Not all hacking is fun. A lot of manual repetitive work.
- Building everything from scratch is a bad idea..
- How do we scale across thousands of targets?
- Things change all the time, we need continuous monitoring

Current Situation

Redundancy Between Tools

Not invented here / anti unix philosophy is prevalent

@anshuman_bh @_devalias @mhmdiaa

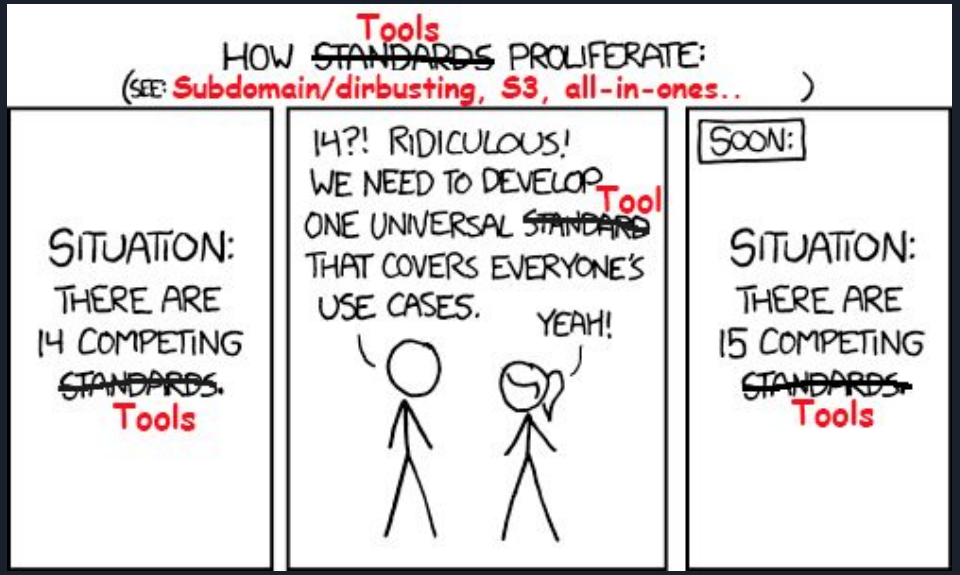
An unmaintained tool is born

ToolA released: does a few things

ToolB released: handles some missing bits, but fails in other areas

Maintainers (often a single point of failure) move on to something new..

Back to square one!



https://xkcd.com/927/

shouldn’t

You can’t build everything from scratch

Lack of Reliable Tool Comparisons

You don’t know the right tool for the job unless you try all of them.. and there are a lot...

The situation is improving!

The Bug Hunter's Methodology by Jason Haddix (@jhaddix)

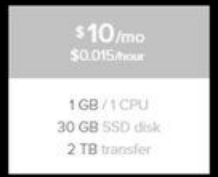
https://github.com/jhaddix/tbhm

Thanks, Jason! You're awesome \m/

Sub Bruting

1,136,964 LINE SUBDOMAIN DICTIONARY (ALL.TXT)

Tool	Time to run	Threads	Found
subbrute time ./subbrute.py -c 100 all.txt $TARGET.com | tee subbrute.output	errored	100	0
gobuster time gobuster -m dns -u $TARGET.com -t 100 -w all.txt	21m15.857s	100	87
massdns time ./subbrute.py /root/work/bin/all.txt $TARGET.com | ./bin/massdns -r resolvers.txt -t A -a -o -w massdns_output.txt -	1m24.167	n/a	213
dns-parallel-prober time python dns-queue.py $TARGET.com 100 $TARGET_outputfile -i /root/work/bin/all.txt	42m2.868s	100	43
blacksheepwall time ./blacksheepwall_linux_amd64 -clean -dictionary /root/work/bin/all.txt -domain $TARGET.com	256m9.385s	100	61



Poor Interoperability

Many tools just don’t play nicely with each other

ReconJSON

- JSON-based recon tool data output standard
- Increase interoperability between tools
- Enable a unix-philosophy recon tooling digital utopia!

Join the discussion:

https://github.com/ReconJSON/ReconJSON

Scaling & Reliability

Learning from the dev side of the tech world

@anshuman_bh @_devalias @mhmdiaa

Scaling & Reliability

- Vertical scaling
  - More server, more money, more problems
- Horizontal scaling
  - Flexible, fault tolerant, cheaper
- Learn from the tech giants
  - Great architectures and tools to leverage

Practical Research Environment

There are tons of assets that you can hack legally

@anshuman_bh @_devalias @mhmdiaa

I just want to hack things...

Wouldn't it be nice to have:

- An organized database with all the assets that are legal to hack
  - Stick to the scope
- A supporting platform that collects data about these assets
  - Fast feedback loop
- A way to easily explore the asset data
  - Locate targets and #HackAllTheThings™

It’s all about identifying assets

What you don’t know about, you can’t protect

Unmaintained assets cause breaches

Which of the OWASP Top 10 Caused the World's Biggest Data Breaches?

Guy Podjarny

10 May, 2017

https://snyk.io/blog/owasp-top-10-breaches

Unmaintained assets cause breaches

A9-Using Components with Known Vulnerabilities	**12/50 breaches**	24%
A5-Security Misconfiguration	**10/50 breaches**	20%

Real-time inventory of target assets

Ephemeral assets, they said.

It will be fine, they said.

@anshuman_bh @_devalias @mhmdiaa

Attack surface is always evolving

Code changes

Bugs/regressions

New code

Backups

New assets

Hosts

Cloud services

Subdomains

Target


ELLINGSON MINERAL CORPORATION
YES, WE ARE A CORPORATION. OUR PRODUCT IS THAT OF CURIOSITY.
IN BUSINESS SINCE THE MID-1990S

What we know...


github.com/ellingsoncorp
EMC
ELLINGSON MINERAL COMPANY
DNS
ellingsoncorp.com

Let’s start the demo...

Introducing BountyMachine

@anshuman_bh @_devalias @mhmdiaa

Technologies

Golang

https://golang.org/

@anshuman_bh @_devalias @mhmdiaa

Docker

https://www.docker.com

Kubernetes

https://kubernetes.io/

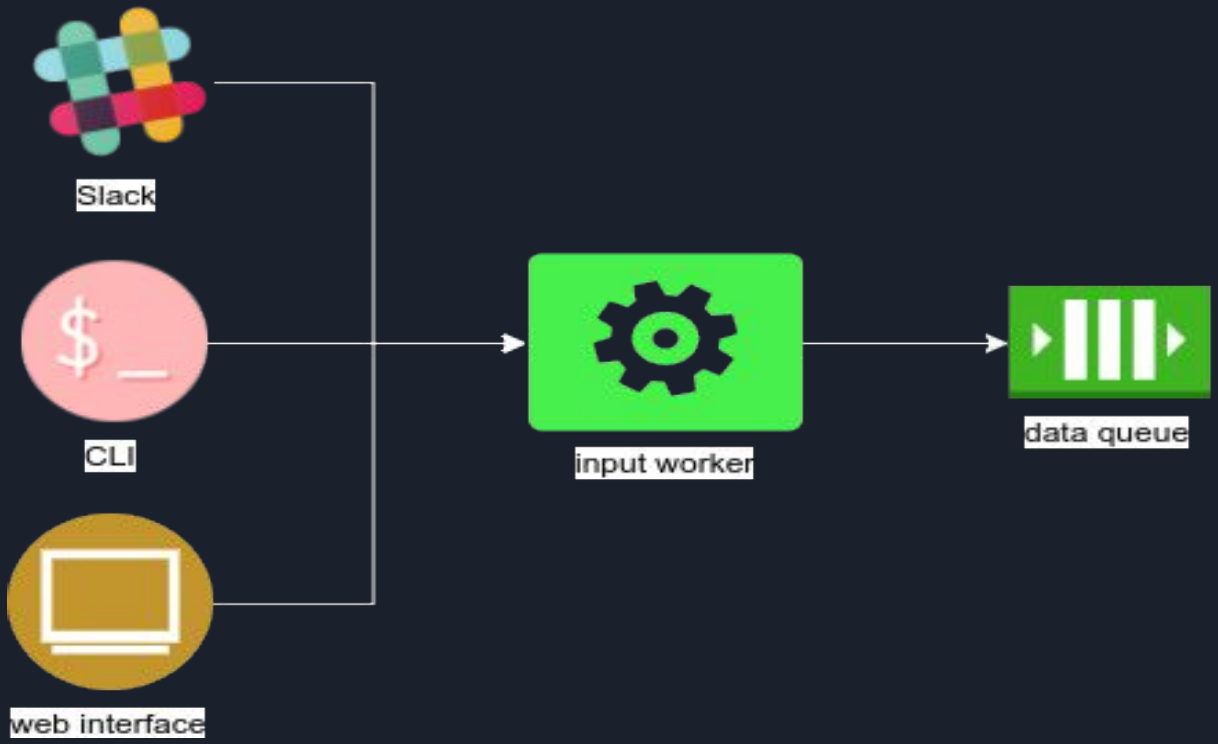
Argo

https://argoproj.github.io/argo

@anshuman_bh @_devalias @mhmdiaa

Architecture

It starts with a target

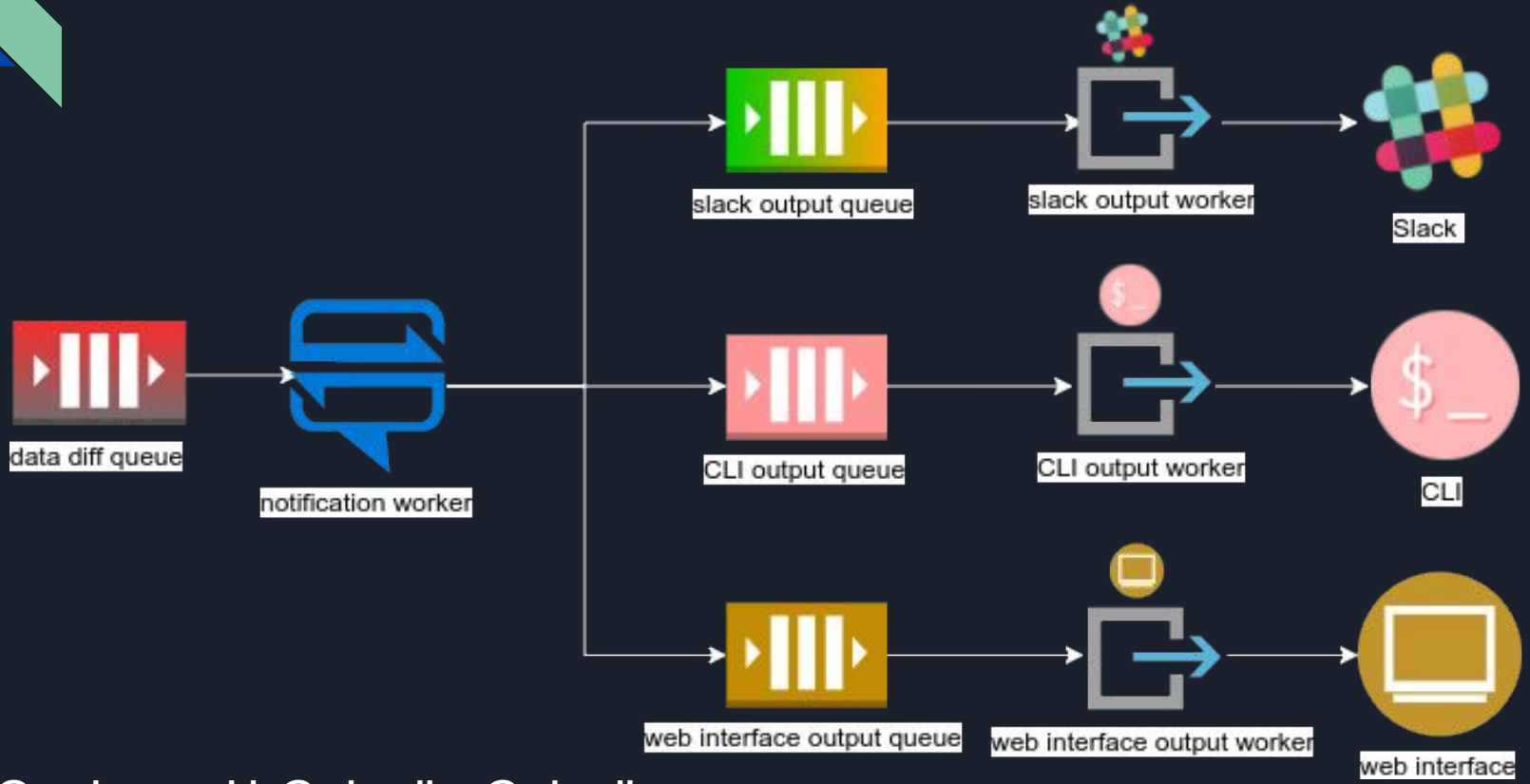


Everything is managed by queues

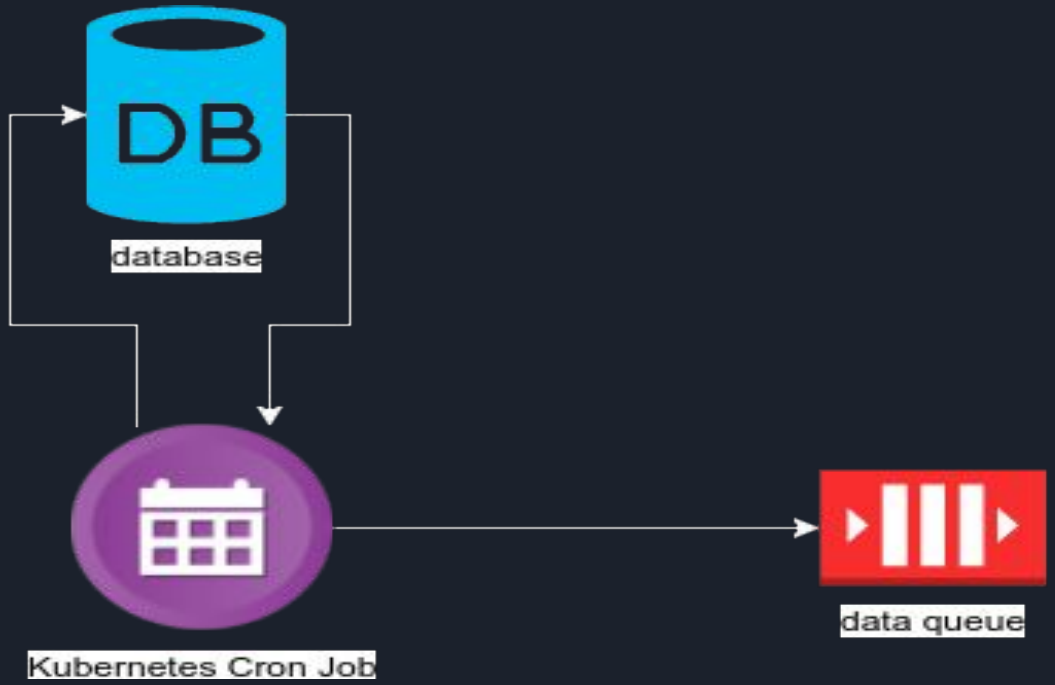
The output of a workflow can be passed to another

New results are identified by a diff worker

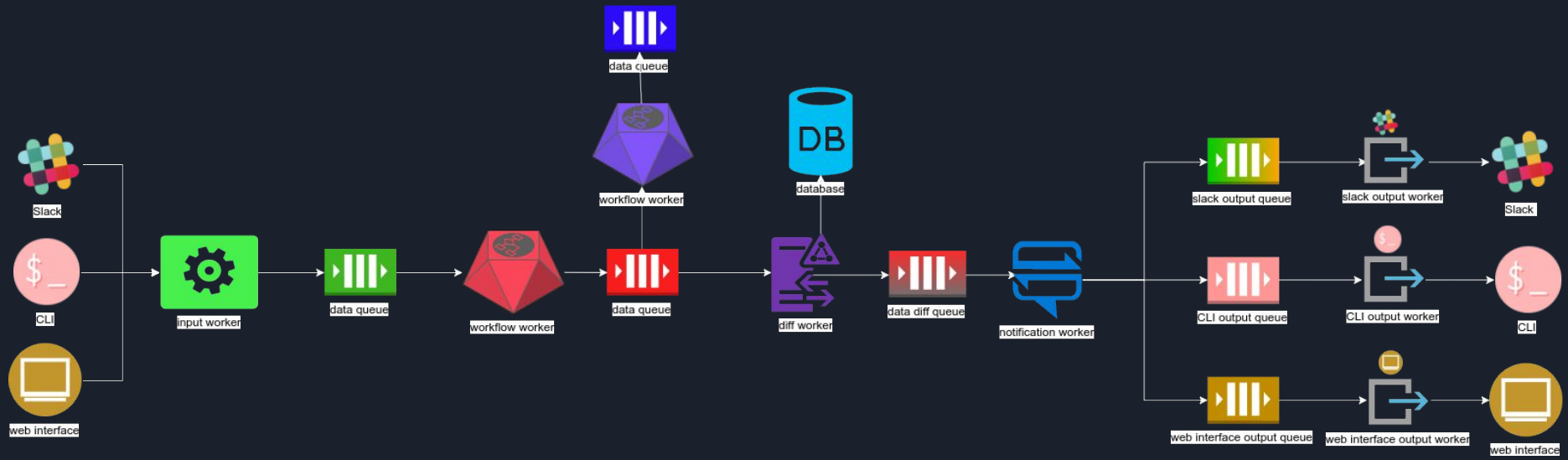
Notifications only include new results



The monitoring worker re-checks things as scheduled



To sum up...



@anshuman_bh @_devalias @mhmdiaa

Lessons Learned

@anshuman_bh @_devalias @mhmdiaa

Geographic Limitations

World Domination Headquarters

Communication

@anshuman_bh @_devalias @mhmdiaa

Dealing with conflicts

- Check your ego
- **Communicate openly, honestly and thoroughly!**
- Stay open to new suggestions
- Delegate responsibilities
- Be flexible
- Code/data trumps assumptions

Technology

@anshuman_bh @_devalias @mhmdiaa

Technology

- Keep an open mind
- Explore what is out there
- Dig deep, understand how the underlying tech works
- Sometimes what you want doesn’t quite exist yet.. and that’s ok
- ‘Simple’ problems sometimes take a while to solve well

MVP? JIT!

MVP? JIT!

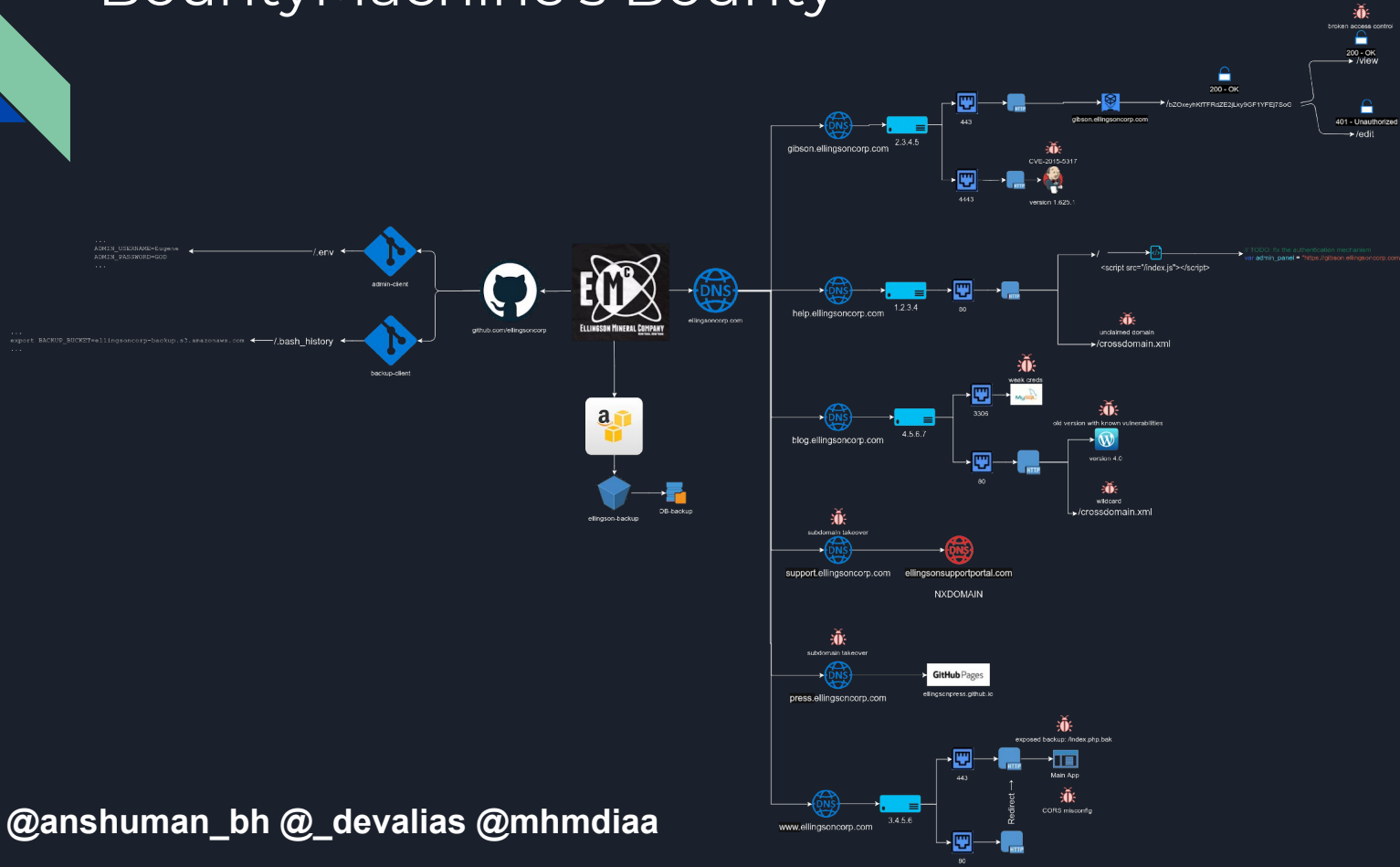
- Plan at the macro level
- Handle intricate details Just In Time (JIT)
- Backlog anything not needed now
- Move fast and (hopefully don’t) break (too many) things
- Done is better than perfect

About that demo...

Remember Ellingson Mineral Corp?

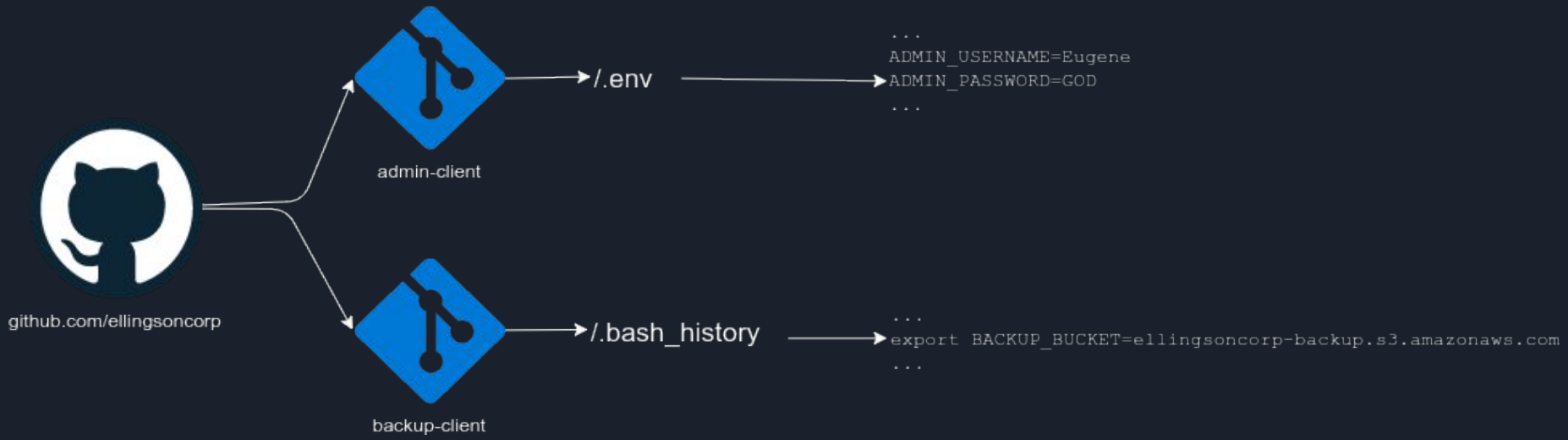
We started with...

BountyMachine’s Bounty



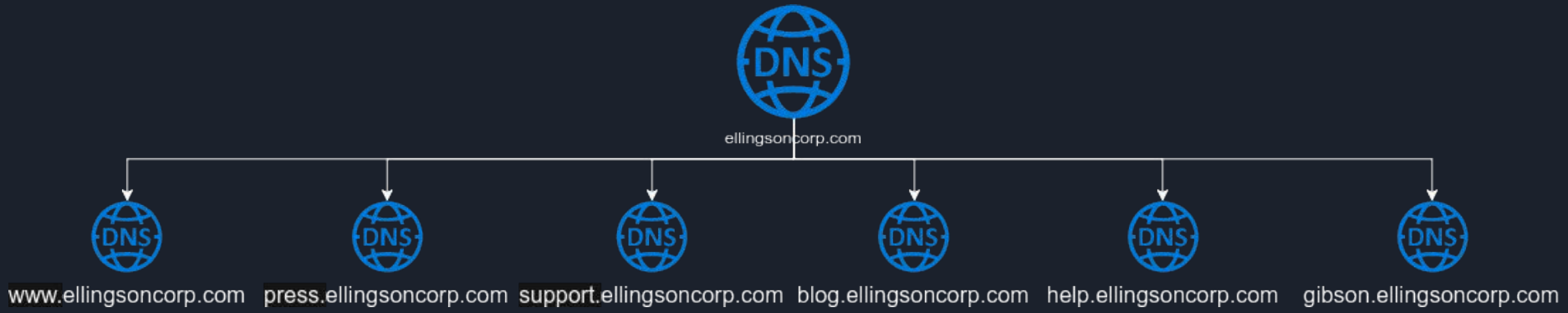
@anshuman_bh @_devalias @mhmdiaa

GitHub

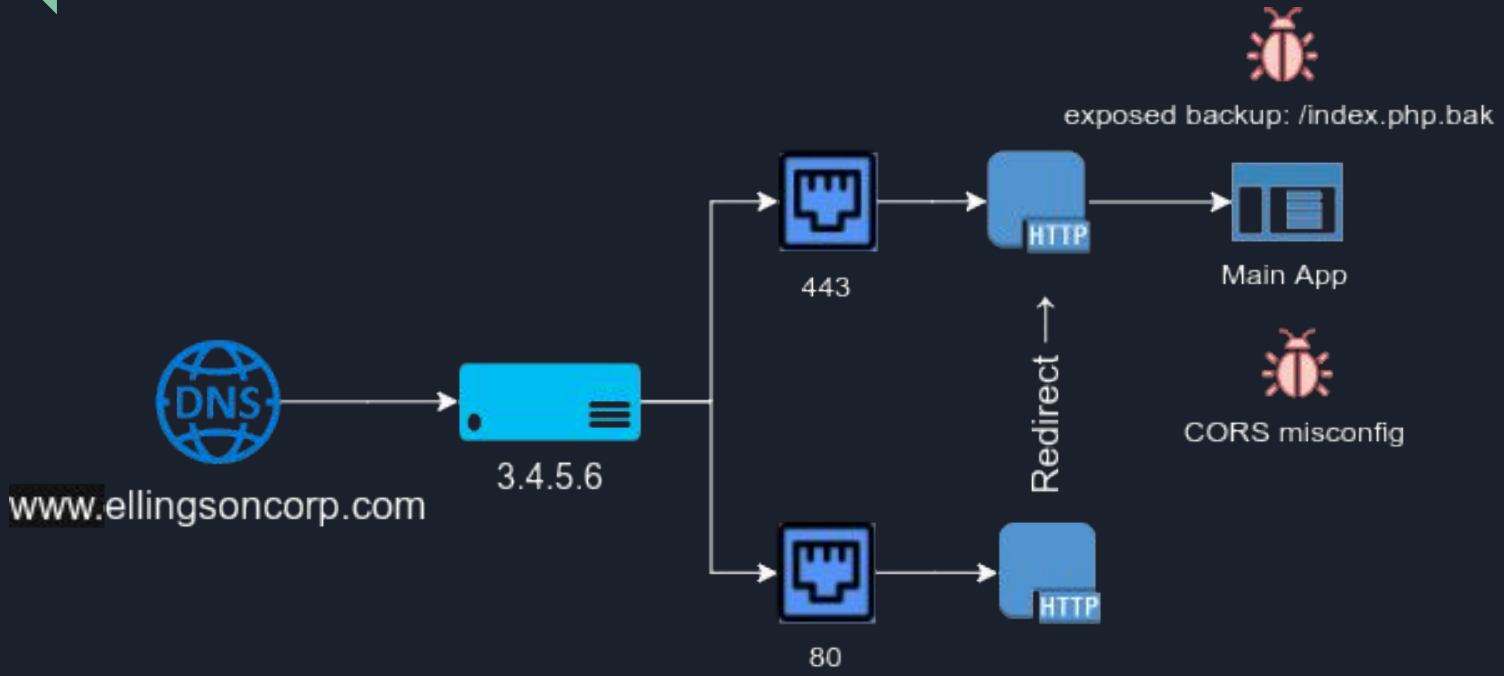

github.com/ellingsoncorp
admin-client
/.env
...
ADMIN_USERNAME=Eugene
ADMIN_PASSWORD=GOD
...
backup-client
/.bash_history
...
export BACKUP_BUCKET=ellingsoncorp-backup.s3.amazonaws.com
...

S3

DNS

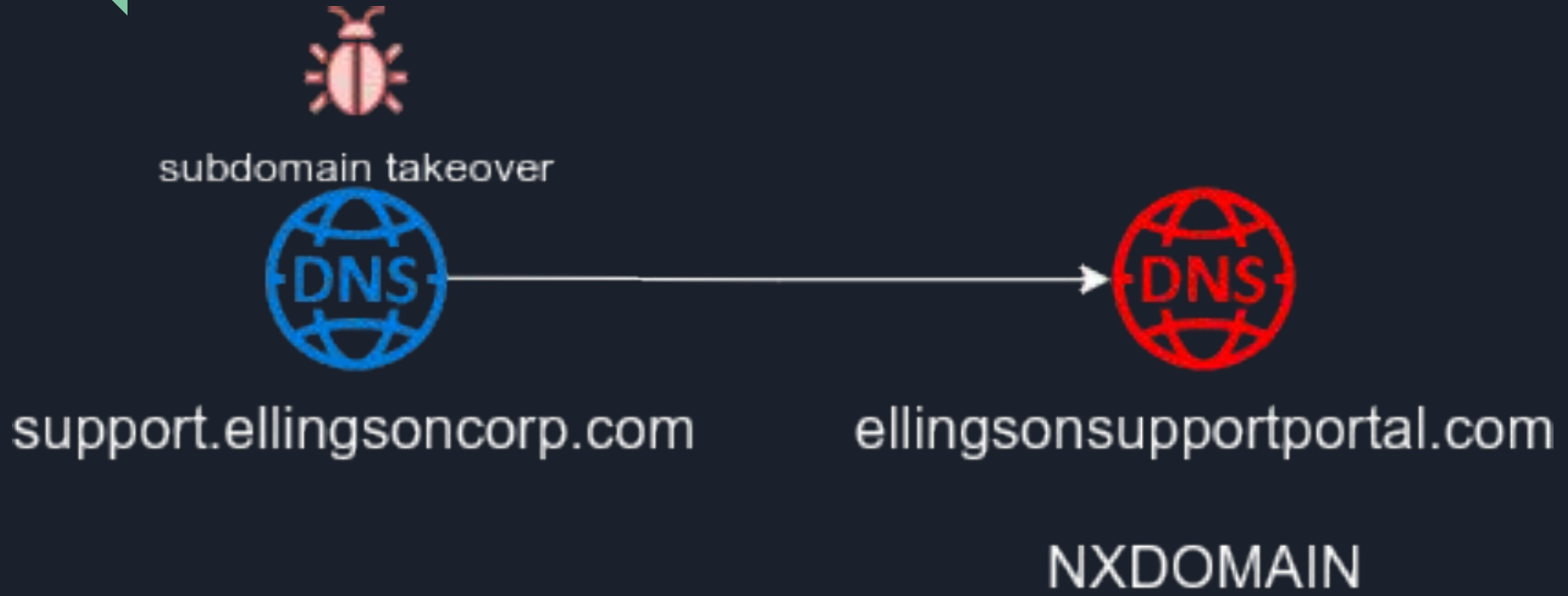

DNS
ellingsoncorp.com
DNS
www.ellingsoncorp.com
DNS
press.ellingsoncorp.com
DNS
support.ellingsoncorp.com
DNS
blog.ellingsoncorp.com
DNS
help.ellingsoncorp.com
DNS
gibson.ellingsoncorp.com

www.ellingsoncorp.com

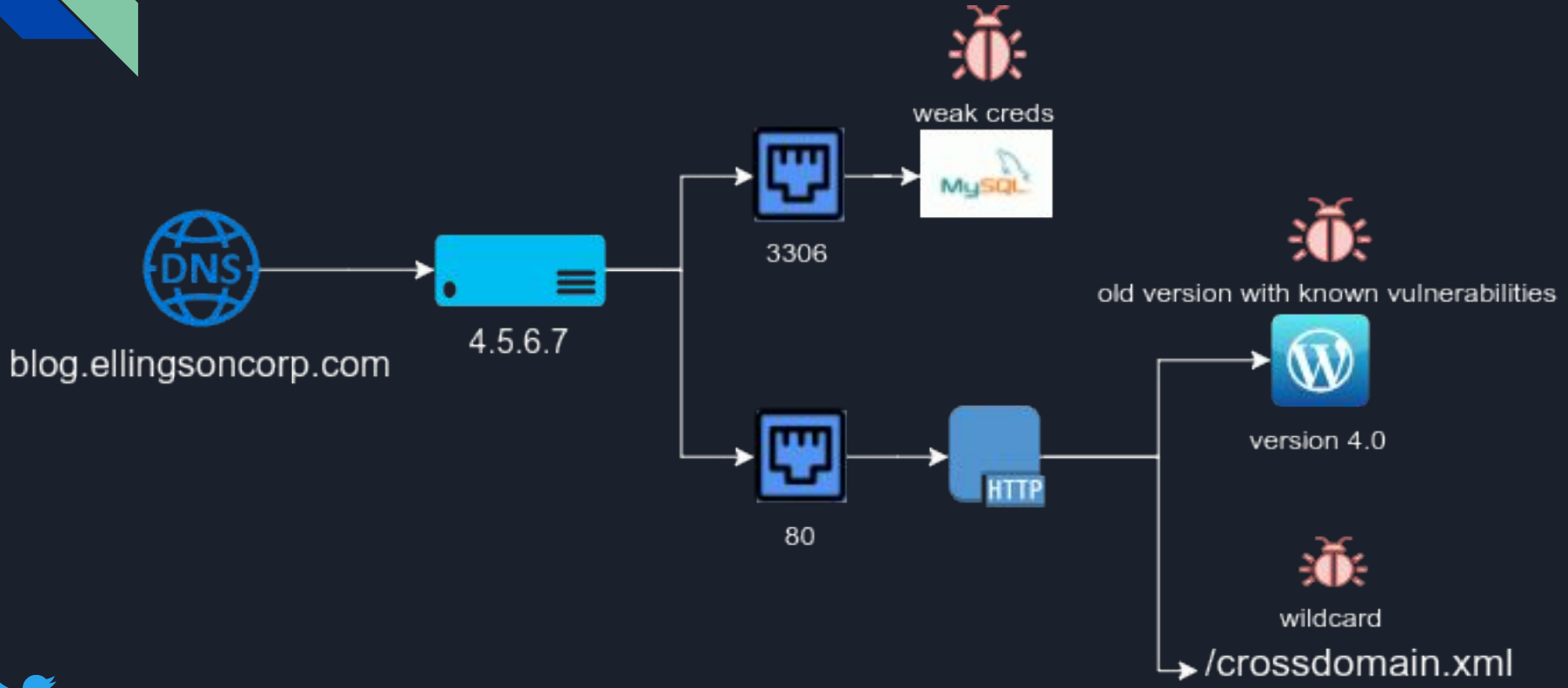


press.ellingsoncorp.com

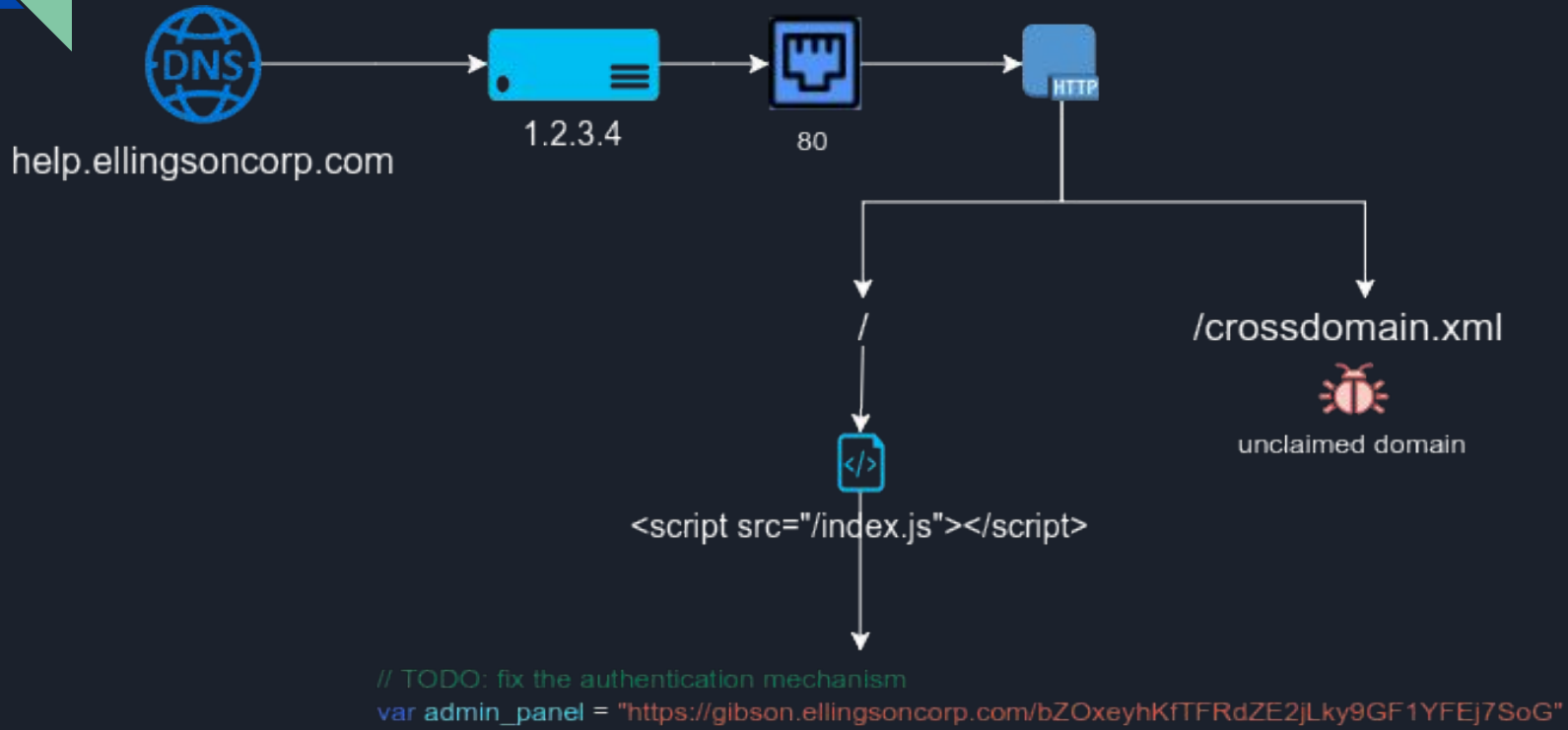
support.ellingsoncorp.com



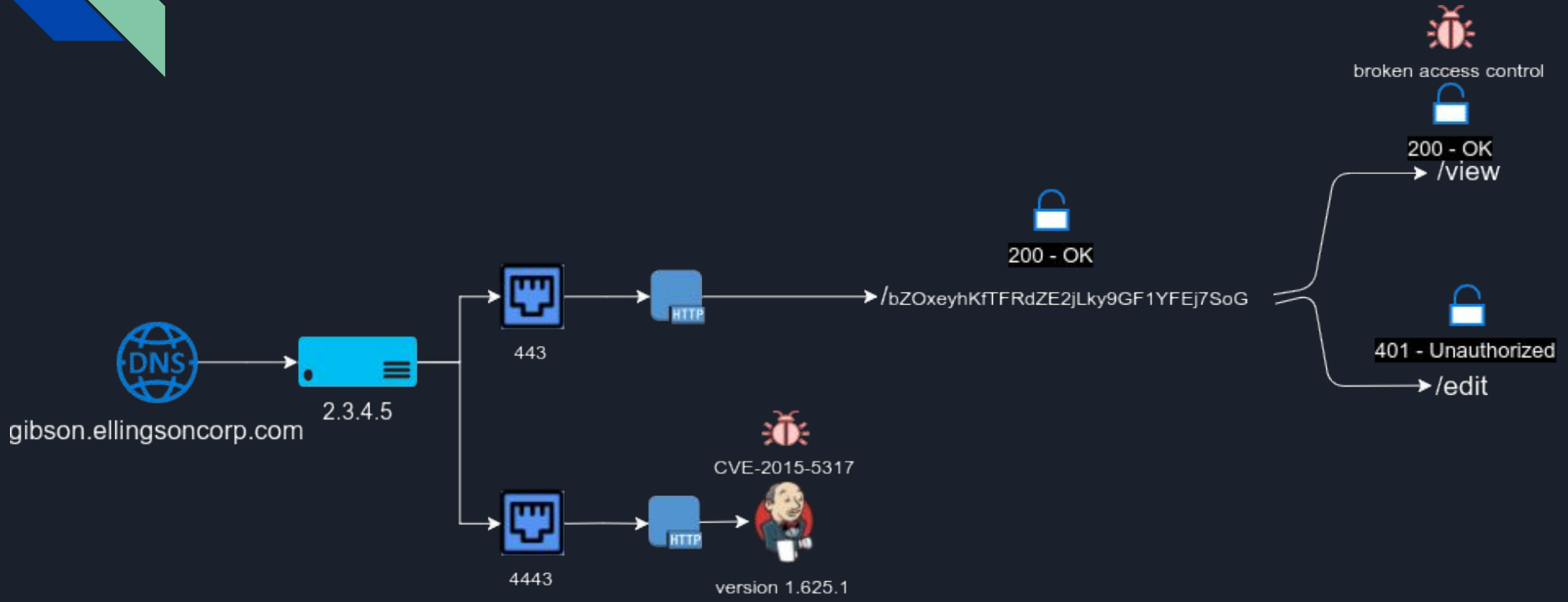
blog.ellingsoncorp.com



help.ellingsoncorp.com



gibson.ellingsoncorp.com



Conclusion

@anshuman_bh @_devalias @mhmdiaa

Conclusion

- We can’t automate everything, but there is a lot we can
- Less wasted time means more fun hacks!
- Explore new tech, don’t be afraid to innovate
- Keep tooling simple and consumable (unix philosophy)
- Improve existing tools, don’t reinvent the wheel!
- Check your ego, collaborate, learn, share, and keep an open mind

Special Thanks

Thanks to the people who write open source tools.

Those who understand that “Sharing is Caring”.

For in the end, “None of us is good as all of us.”

Thanks!

Any questions? Reach out to us!

@anshuman_bh @_devalias @mhmdiaa