Hands-On

ModSecurity and Logging

code.talks
commerce

Philipp Krenn

@xeraa

Let's talk about security...

THIS IS FINE.

A1:2017-Injection

https://www.owasp.org/index.php/Top_10-2017_Top_10

A10:2017-Insufficient Logging & Monitoring

https://www.owasp.org/index.php/Top_10-2017_Top_10

TH-
THIS IS NOT FINE!!
OHMYGOD EVERYTHINGS ON FIRE
WHAT THE HELL IS MY PROBLEM

elastic

Developer 🥑

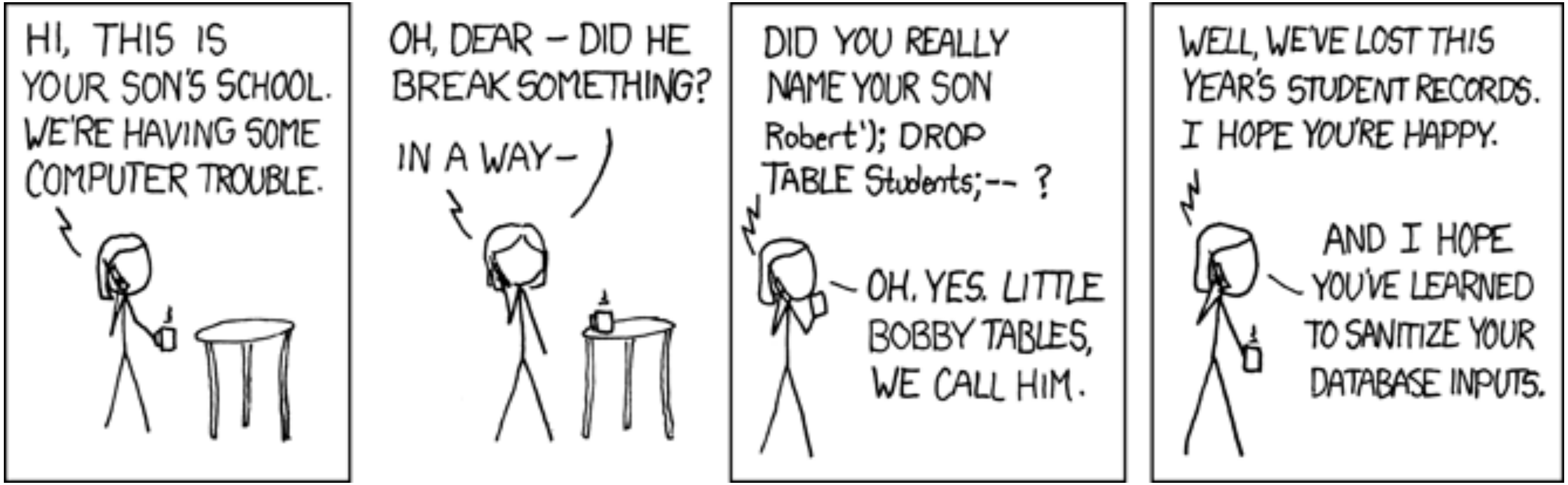
Disclaimer

I build **highly** monitored Hello World apps

Hello World of SQL Injection:

https://xeraa.wtf

https://xeraa.wtf/read.php?id=1 🤔


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

sqlmap®

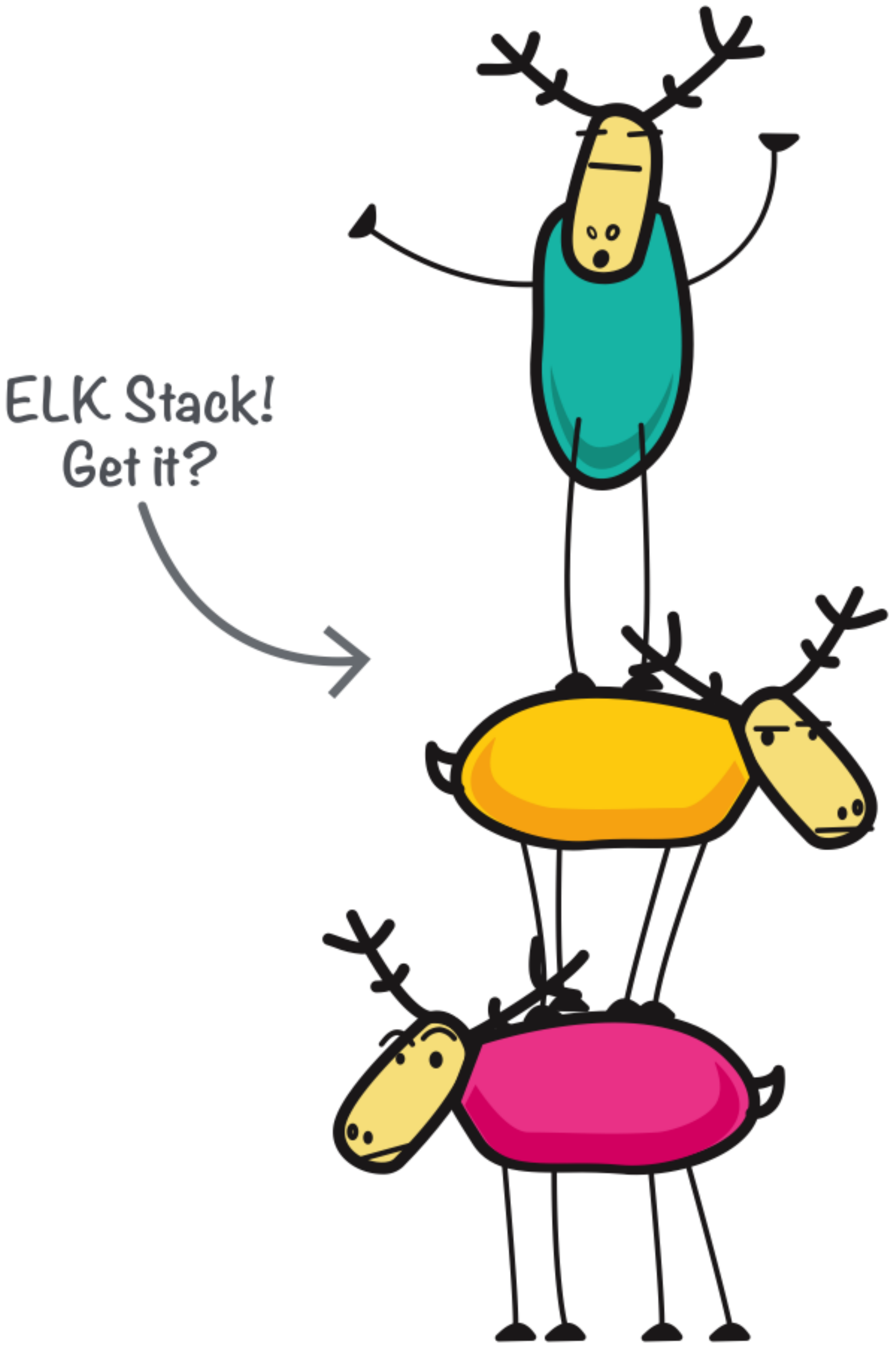
Automatic SQL injection and database takeover tool

Injection

```
;INSERT INTO employees (id,name,city,salary) VALUES
(4,'test','test',10000)
```

ALL THE THINGS!

me looking
for the bug
7.2 GB
of log file



E Elasticsearch

L Logstash

K Kibana

lyft

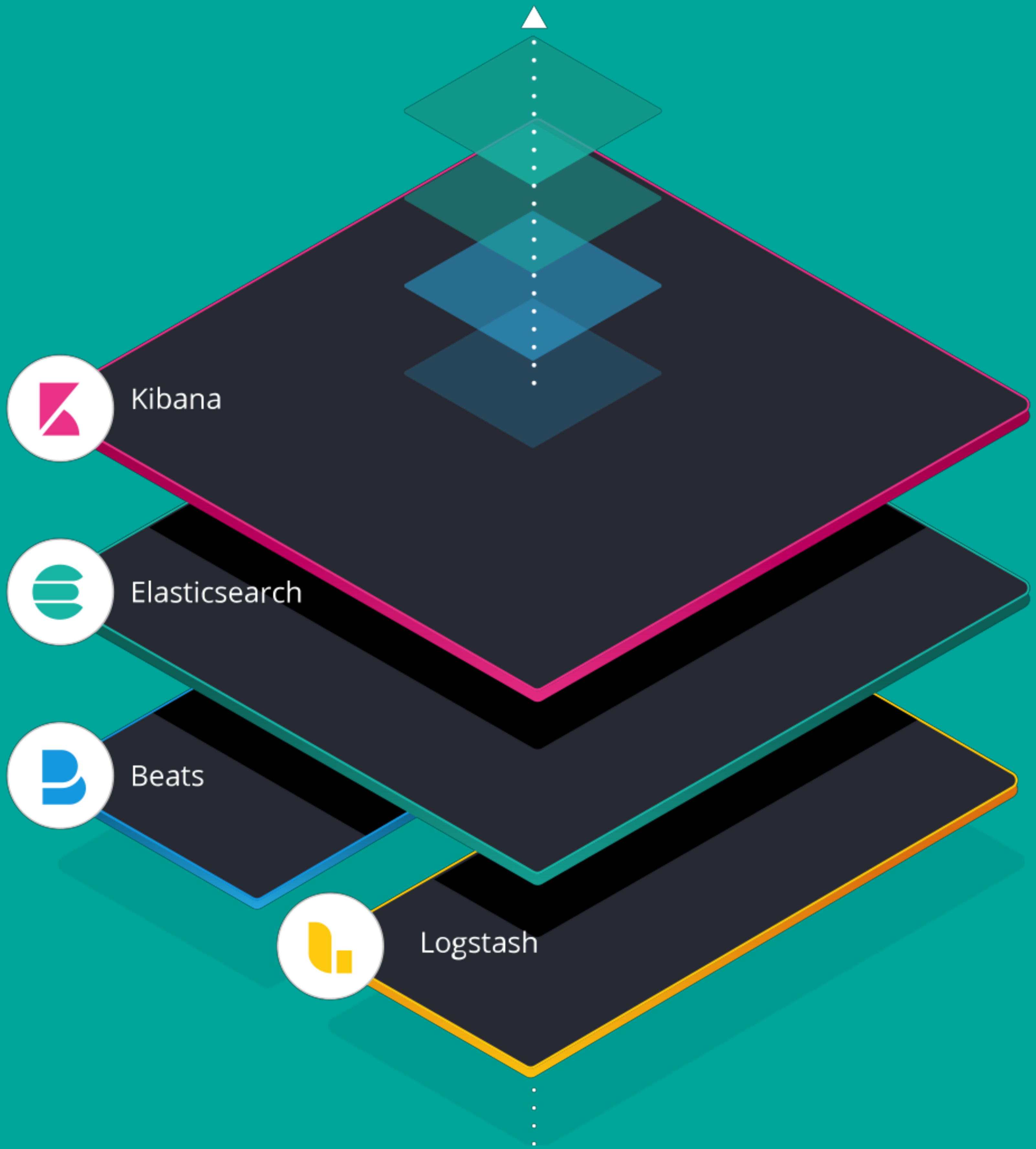
slack

fitbit

Apparently, I'm an ELKB personality.

elastic @xeraa

elastic stack


Kibana
Elasticsearch
Beats
Logstash

What's going on in our app?

DELETE or DROP?

OWASP

ModSecurity Core Rule Set

THE 1ST LINE OF DEFENSE

Custom Rule

```
SecRule REQUEST_FILENAME "form.php" "id:'400001',chain,deny,log,msg:'Spam detected'"
SecRule REQUEST_METHOD "POST" chain
SecRule REQUEST_BODY "@rx (?i:(pills|insurance|rolex))"
```

Conclusion

Examples

https://github.com/xeraa/mod_security-log

Code

Logging

ModSecurity

Questions?

Philipp Krenn @xeraa