Hands-On

ModSecurity & Logging

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


THIS IS FINE.

A10:2017-Insufficient Logging & Monitoring

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


TH-
THIS IS NOT FINE!!
OH MY GOD EVERY THINGS 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

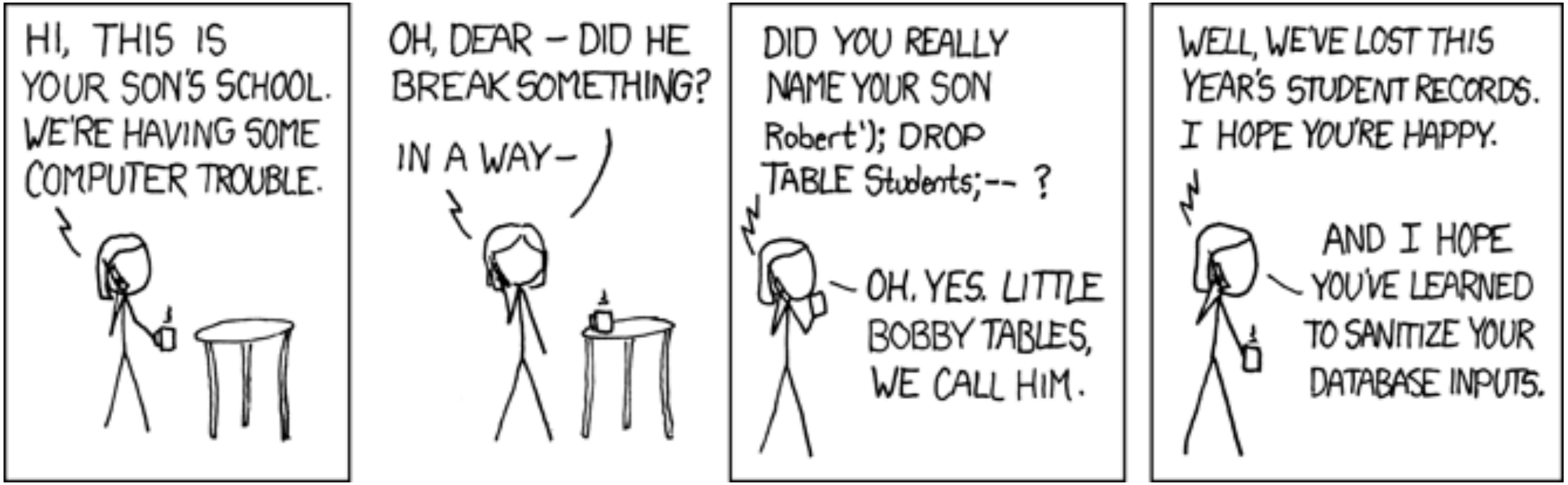
https://xeraa.wtf/login.php 🤔

Hello World of SQL Injection

```
$sql = "SELECT *
        FROM `employees`
        WHERE name='$name' AND password=SHA1('$password')";
```

Hello World of SQL Injection

```
' or true --
```


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.

https://xeraa.wtf/read.php?id=1 🤔


```
sqlmap --url "https://xeraa.wtf/read.php?id=1" --purge
```

Hello World of SQL Injection

```
$sql = "SELECT * FROM employees WHERE id = " . trim($_GET["id"]);
error_log("SQL query [read.php]: " . $sql . "\n", 3, "/var/log/app.log");

mysqli_multi_query($link, $sql);
if($result = mysqli_use_result($link)){
    $row = mysqli_fetch_array($result, MYSQLI_ASSOC);
```

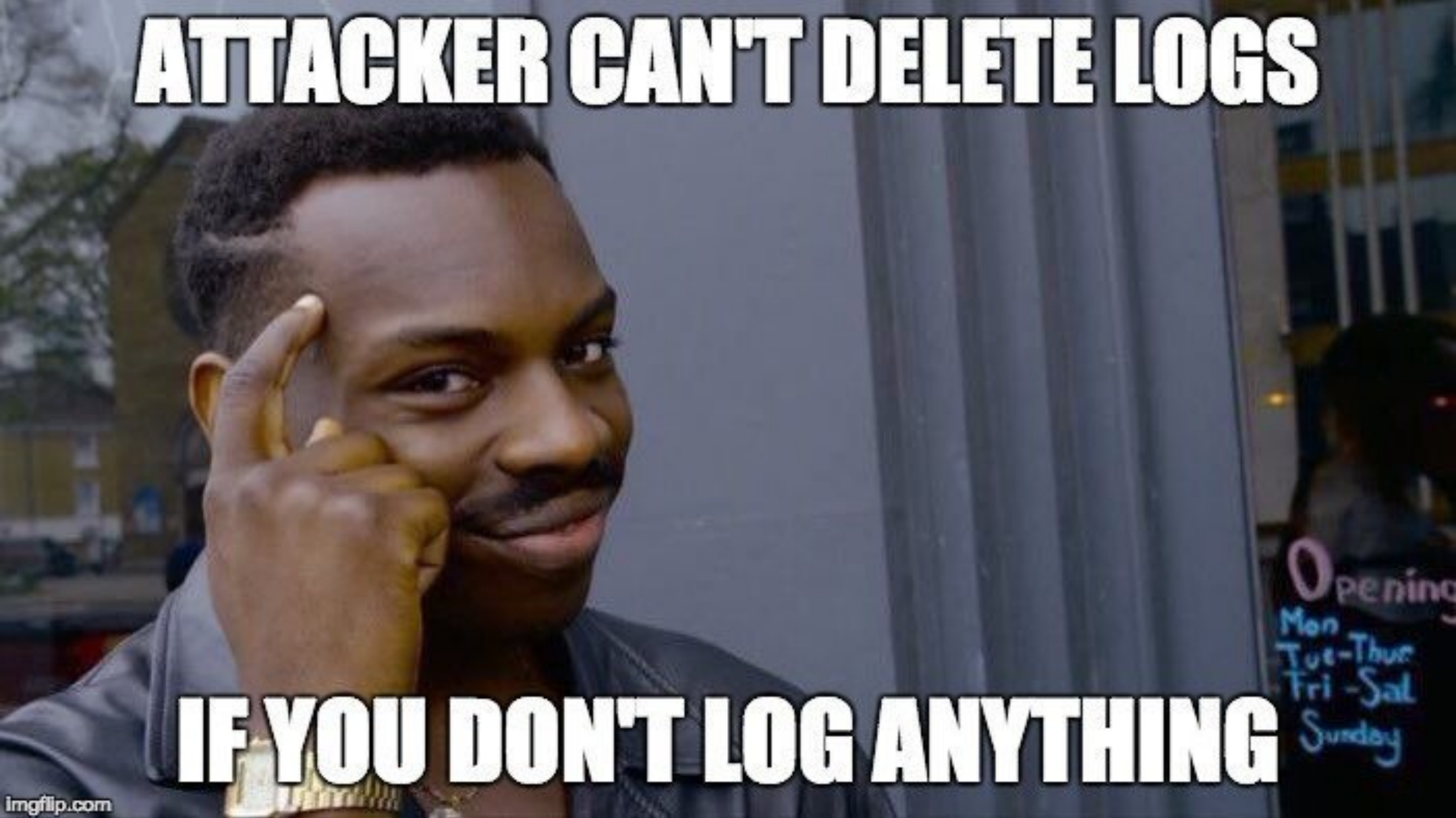
Injection

```
;INSERT INTO employees (name) VALUES ('Bad Actor')
```

No Escaping Either

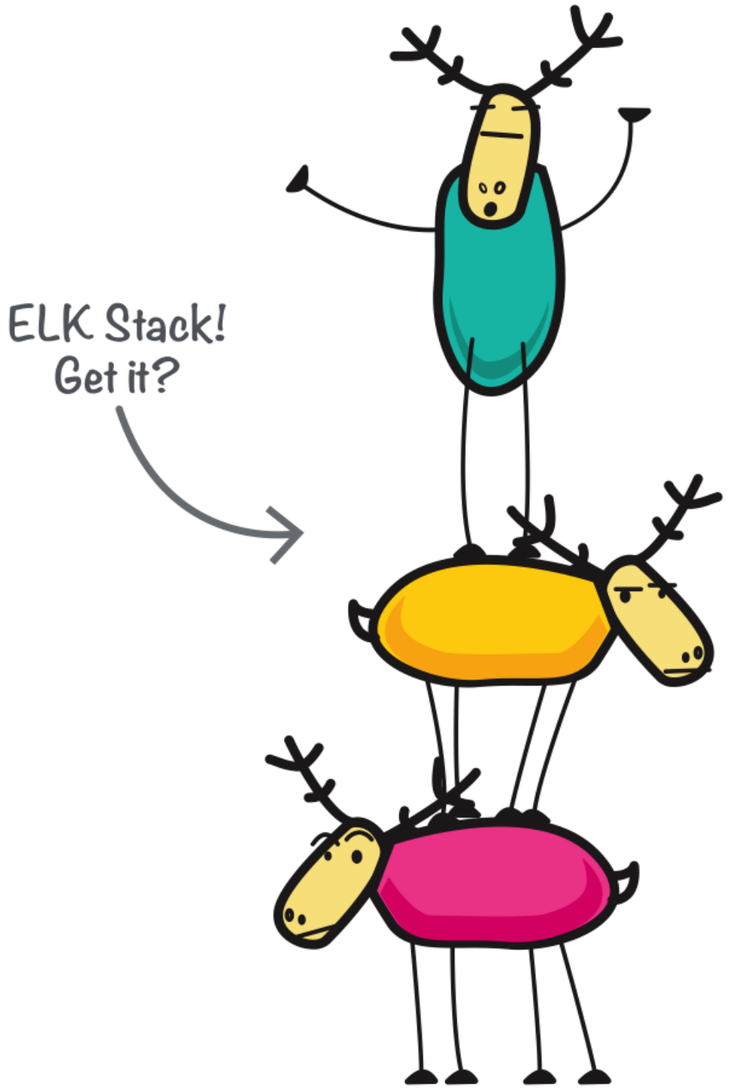
```
;INSERT INTO employees (name) VALUES ('<script>alert("Hello Friend")</script>')
```

What's going on in our app?


ATTACKER CAN'T DELETE LOGS
IF YOU DON'T LOG ANYTHING
Opening
Mon
Tue-Thur
Fri -Sat
Sunday
imgflip.com


ALL THE THINGS!


me looking
for the bug
7.2 GB
of log file



E Elasticsearch

L Logstash

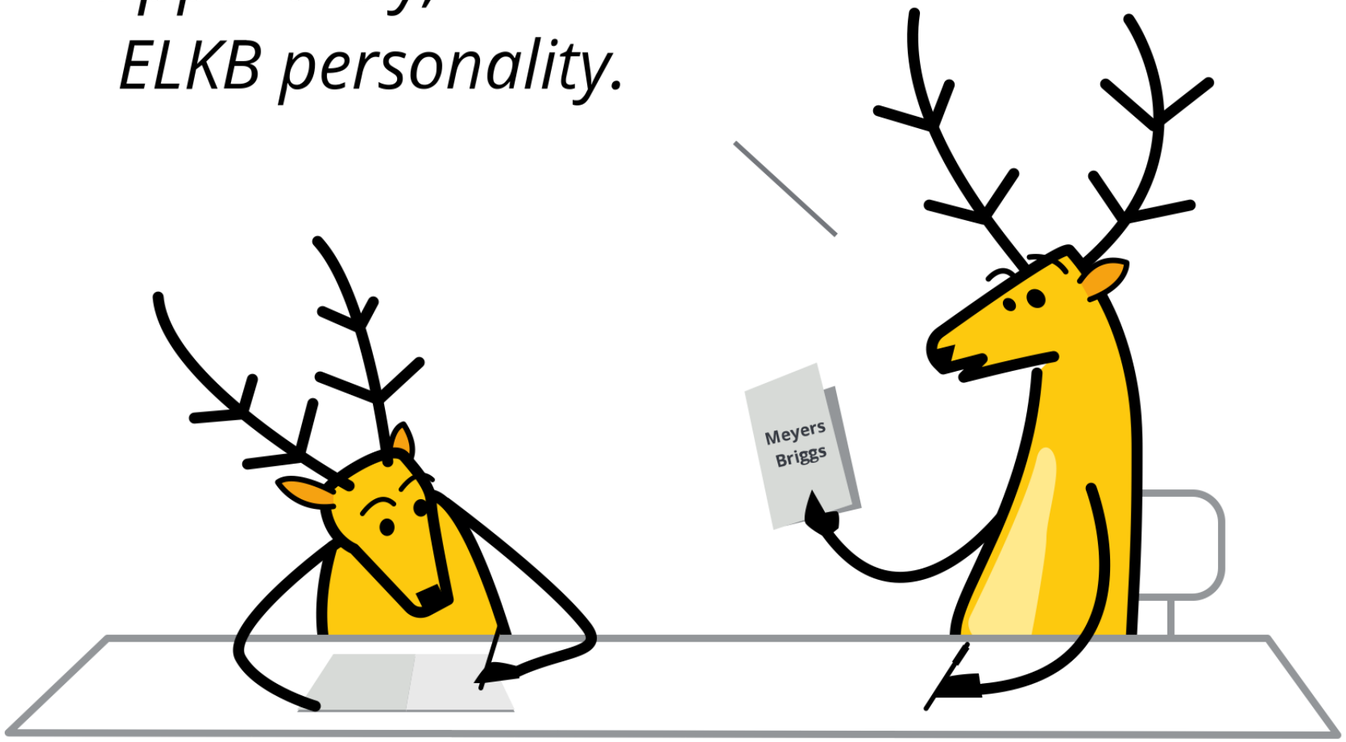
K Kibana

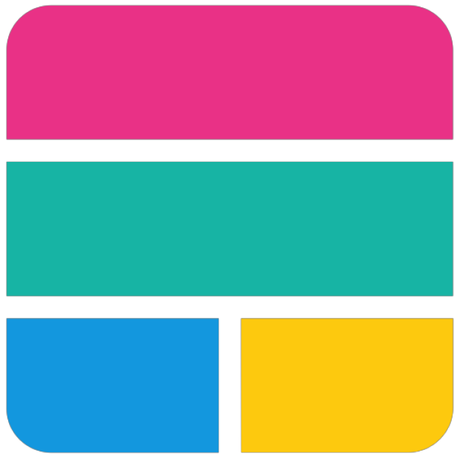

lyft


slack

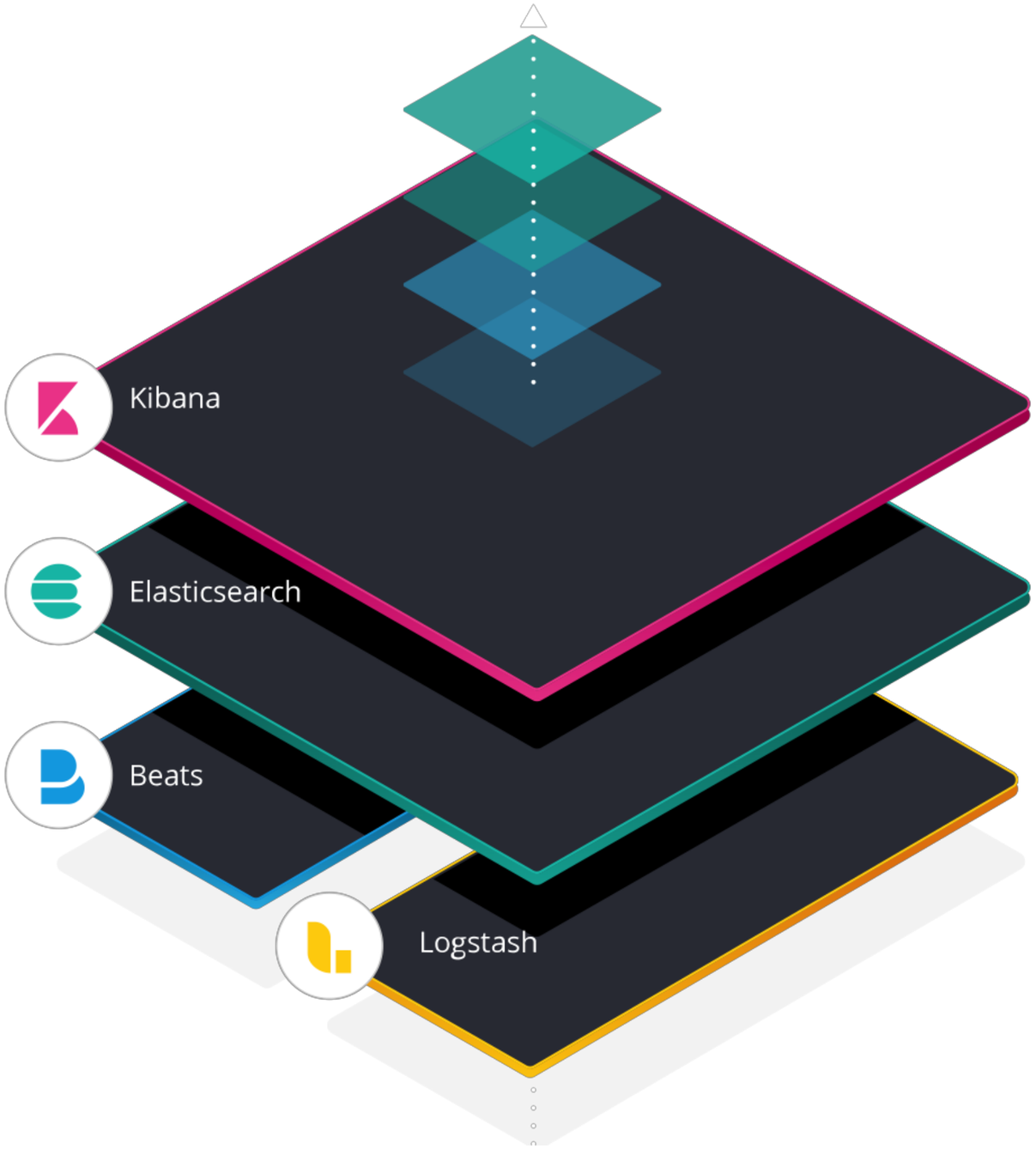

fitbit

Apparently, I'm an ELKB personality.





elastic stack


Kibana
Elasticsearch
Beats
Logstash

55737a,0x71717a6271),NULL,NULL,NULL-- YJoN

2019-04-05 12:07:03.679 SQL query: SELECT * FROM employees WHERE id = 1 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x717a766a71,0x516950484c527a677758,0x71717a6271)-- qFgZ

2019-04-05 12:07:03.679 SQL query: SELECT * FROM employees WHERE id = 1 UNION ALL SELECT NULL,CONCAT(0x717a766a71,0x744f5352425953674669,0x71717a6271),NULL,NULL-- SBru

2019-04-05 12:07:03.679 SQL query: SELECT * FROM employees WHERE id = -6655 UNION ALL SELECT CONCAT(0x717a766a71,0x664d6a6268664b41494f637a6575785576415741424755 4f5552745544584d676c576c4152795165,0x71717a6271),NULL,NULL,NULL-- YiVs

2019-04-05 12:07:04.679 SQL query: SELECT * FROM employees WHERE id = -6770 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x717a766a71,0x774c6653426f53436a567557617369556a4b416e516757576c465a526e484a717373566b7359726e,0x71717a6271)-- jdLc

2019-04-05 12:07:04.679 SQL query: SELECT * FROM employees WHERE id = -7077 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x717a766a71,(CASE WHEN (1022=
1022) THEN 1 ELSE 0 END),0x71717a6271)-- qIrV

2019-04-05 12:07:05.680 SQL query: SELECT * FROM employees WHERE id = ''

2019-04-05 12:07:08.680 SQL query: SELECT * FROM employees WHERE id = ''

2019-04-05 12:08:13.684 SQL query: SELECT * FROM employees WHERE id = ''select * from contacts

2019-04-05 12:08:38.686 SQL query: SELECT * FROM employees WHERE id = ''select * from contacts

2019-04-05 12:09:33.690 SQL query: SELECT * FROM employees WHERE id = ;select * from contacts

2019-04-05 12:09:40.691 SQL query: SELECT * FROM employees WHERE id = 1;INSERT INTO employees (id,name,city,salary) VALUES (4,'test','test',10000)

2019-04-05 12:09:55.693 SQL query: SELECT * FROM employees WHERE id = 4

2019-04-05 12:09:55.693 SQL query: SELECT * FROM employees WHERE id = ;select * from contacts

2019-04-05 12:12:30.698 SQL query: SELECT * FROM employees WHERE id = 3

2019-04-05 12:12:55.700 SQL query: SELECT * FROM employees WHERE id = 3;drop table employees

2019-04-05 12:13:02.701 SQL query: SELECT * FROM employees WHERE id = 4

2019-04-05 12:13:27.703 SQL query: SELECT * FROM employees WHERE id = 4;drop table employee

DELETE or DROP?

OWASP ModSecurity Core Rule Set

THE 1ST LINE OF DEFENSE

elastic

@xeraa

Open source

Cross-platform web application firewall (WAF)

Visibility into HTTP(S) traffic

Rules to implement protections

OWASP ModSecurity Core Rule Set (CRS) Version 3

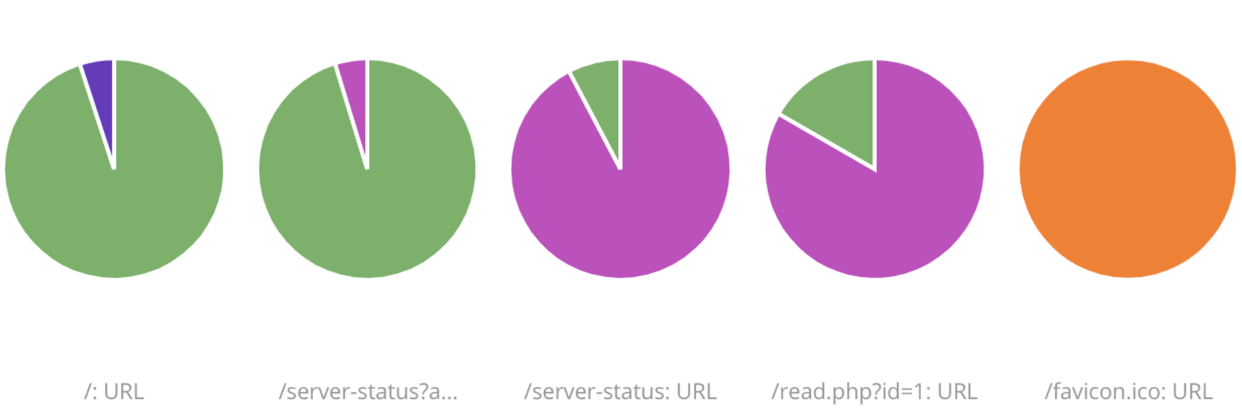
- HTTP Protocol Protection
- Real-time Blacklist Lookups
- HTTP Denial of Service Protections
- Generic Web Attack Protection
- Error Detection and Hiding

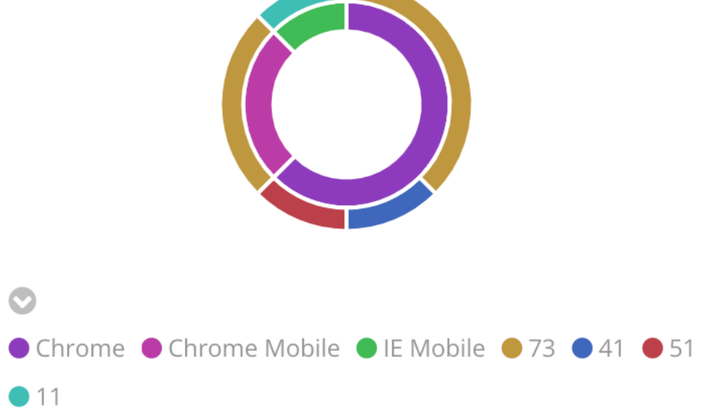
Commercial Rules from Trustwave SpiderLabs

- Virtual Patching
- IP Reputation
- Web-based Malware Detection
- Webshell / Backdoor Detection
- Botnet Attack Detection
- HTTP Denial of Service (DoS) Attack Detection

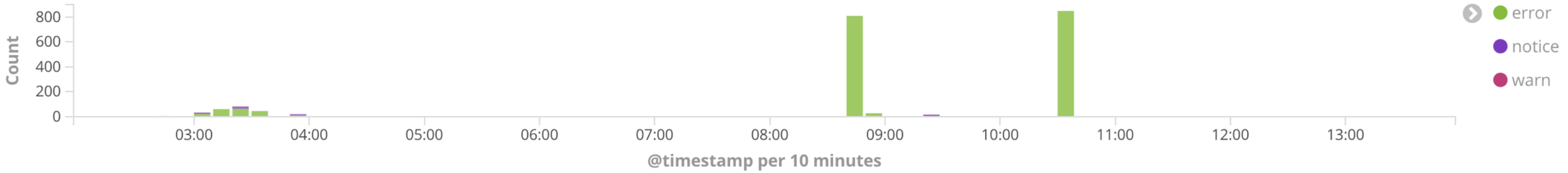
Rerun sqlmap

```
sqlmap --url "https://xeraa.wtf/read.php:8080?id=1" --purge
```





Error logs over time [Filebeat Apache2]



Apache errors log [Filebeat Apache2]

t	apache2.error.message	[client 92.60.183.213:51740] [client 92.60.183.213] ModSecurity: Warning. Pattern match "(?i:(?:[\\\\d\\\\W]\\\\s+as\\\\s*?[\\"'`\\\\w]+\\\\s*?from)|(?:^[\\\\W\\\\d]+\\\\s*?(?:union|select|create|rename|truncate|load|alter|delete|update|insert|desc)\\\\b)|(?:(?:select|create|rename|truncate|load|alter|delete|update|insert|desc)\\\\s+(?:(?:group_)concat|char|load ..." at ARGS:id. [file "/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "451"] [id "942360"] [rev "2"] [msg "Detects concatenated basic SQL injection and SQLLFI attempts"] [data "Matched Data: 3;INSERT found within ARGS:id: 3;INSERT=123"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "9"] [accuracy "8"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "xeraa.wtf"] [uri "/read.php"] [unique_id "XKhlcP611X5vYu@hIDy@pAAAAAg"]
t	apache2.error.module	
#	apache2.error.pid	24,171
t	beat.hostname	ip-172-26-6-78

Log to JSON

`SecAuditLogFormat JSON`

https://www.cryptobells.com/mod_security-json-audit-logs-revisited/

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))"
```


WHAT THE FUCK WAS
I EVEN THINKING

Conclusion

Examples

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

ModSecurity ❤️ Logging

Hands-On

ModSecurity & Logging

Philipp Krenn @xeraa