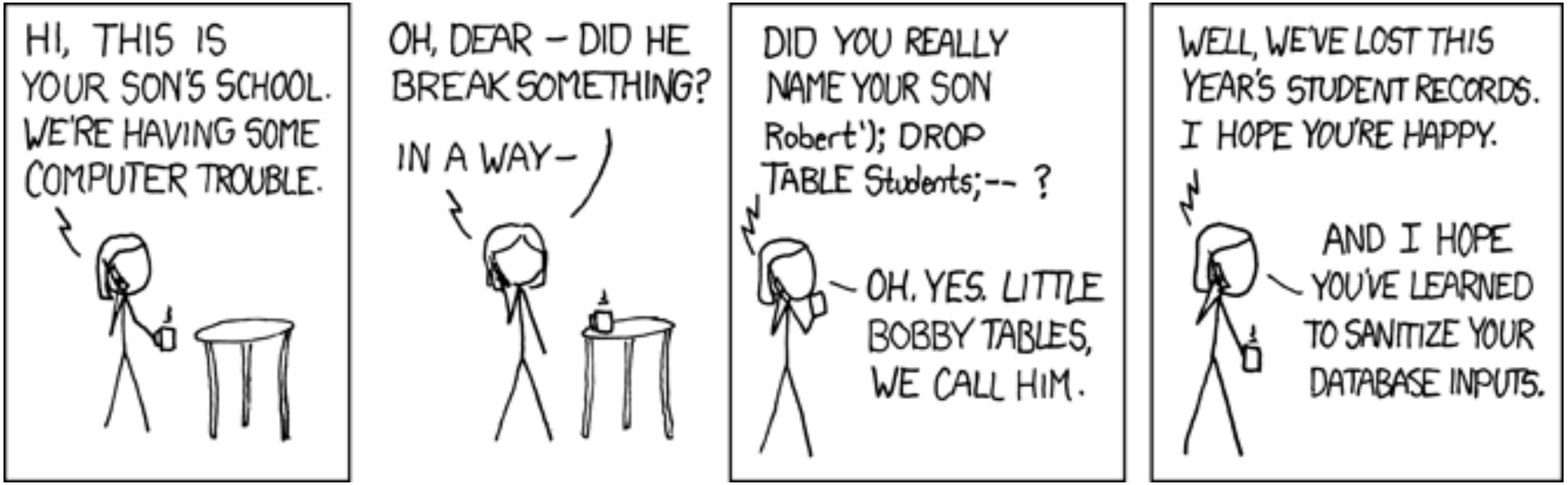
ModSecurity and Logging

Philipp Krenn @xeraa

Let's talk about security...


THIS IS FINE.


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.

A1:2017-Injection

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

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);
```


```
sqlmap --url "https://test.com/bad.php?id=1"
```

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

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))"
```

A10:2017-Insufficient Logging & Monitoring

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


me looking
for the bug
7.2 GB
of log file

Log to JSON

`SecAuditLogFormat JSON`

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

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


WHAT THE FUCK WAS
I EVEN THINKING

Examples

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

ModSecurity ❤️ Logging