



University of California
San Francisco

Web Application Security

Jamie Lam
UCSF School of Medicine
Dean's Office Information Services Unit

7/14/16

Web Application Attacks – 30% in Edu

30% of data breaches in Education involve web application attacks



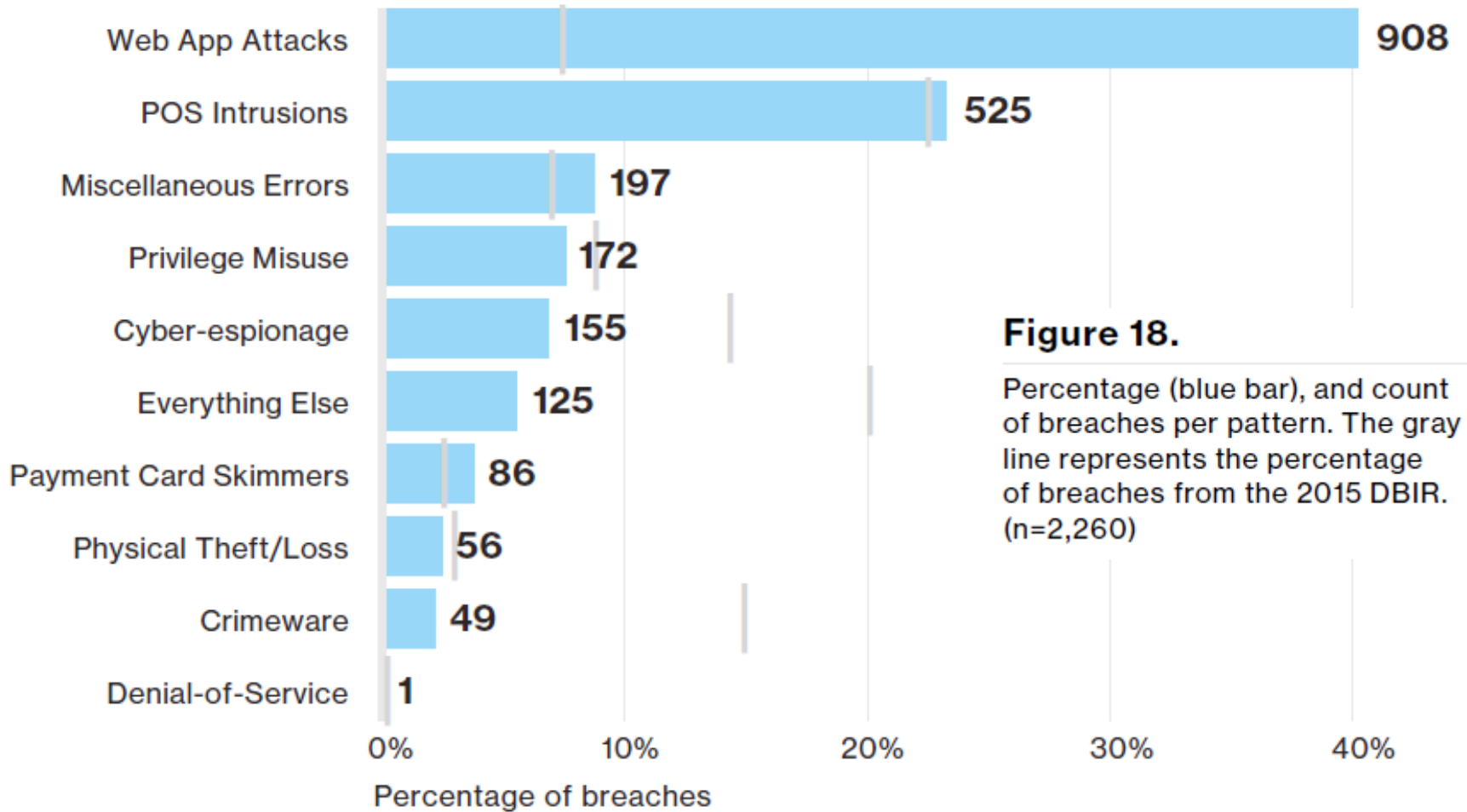
At a glance

Description	Any incident in which a web application was the vector of attack. This includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms.
Top industries	Finance, Information, Retail
Frequency	5,334 total incidents (19,389 additional with secondary motivation), 908 with confirmed data disclosure.
Key findings	The breaches within this pattern are heavily influenced by information gathered by contributors involved in the Dridex botnet takedown. Hundreds of breaches involving social attacks on customers, followed by the Dridex malware and subsequent use of credentials captured by keyloggers, dominate the actions. Defacements are still commonplace and CMS plugins are also a fruitful attack point.

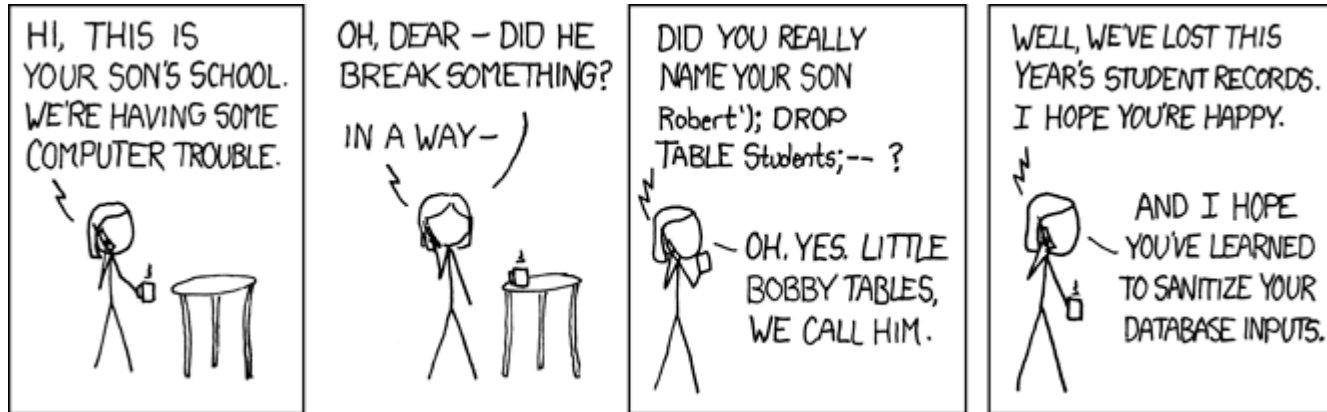
The great complexity of the infrastructure makes web application servers a target for attackers.

Source: 2016 Data Breach Investigations Report - Verizon

Breaches per pattern



Getting started



■ OWASP Top 10

- Most common attack vectors and guides for preventing these attacks

- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

■ SANS Security Checklist for Web Application Design

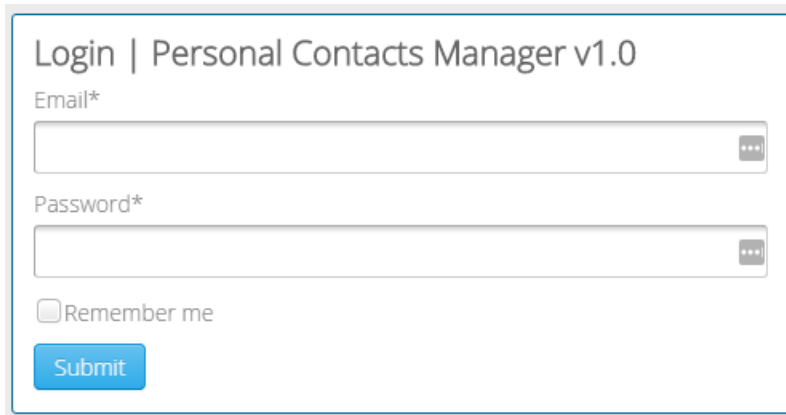
- <https://www.sans.org/reading-room/whitepapers/securecode/security-checklist-web-application-design-1389>

Demo

SQL Injection

- Demo: <http://www.techpanda.org/index.php>

- Source: <http://www.guru99.com/learn-sql-injection-with-practical-example.html>



Login | Personal Contacts Manager v1.0

Email*

Password*

Remember me

Submit

- **Username:** Any email address
- **Password:** Any password appended by:
) OR 1 = 1 --]

- Backend logic for checking user ID: `SELECT * FROM users WHERE email = $_POST['email'] AND password = md5($_POST['password']);`

Demo (con't)

How it works

```
SELECT * FROM users WHERE email = '$email' AND password = md5('$password');
```

Supplied values

{ xxx@xxx.xxx

xxx') OR 1 = 1 --]

```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = md5('xxx') OR 1 = 1 -- ]');
```

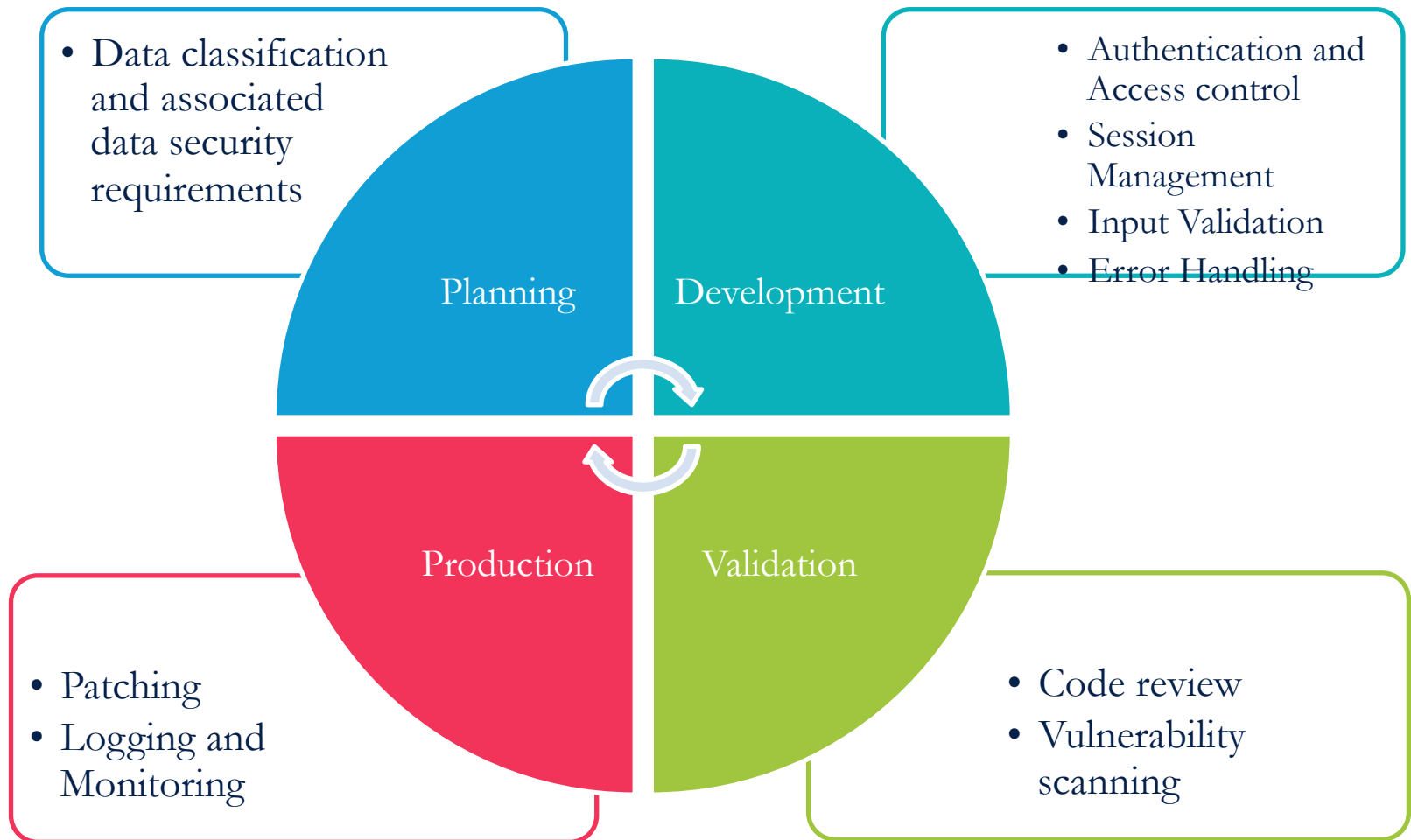
```
SELECT * FROM users WHERE FALSE AND FALSE OR TRUE
```

```
SELECT * FROM users WHERE FALSE OR TRUE
```

```
SELECT * FROM users WHERE TRUE
```

How to secure web application

Incorporate security into web application lifecycle



Web Application Scanning

- Most (All?) campuses provide web application scanning service
 - IBM AppScan
 - Netsparker
 - Qualys
 - Acunetix
- Web application vulnerability scanning tool automatically scans web applications for potential vulnerabilities
 - Quick and automated
 - False positives and false negatives
- Should not be used alone to perform the entire task of securing a web application

Takeaways

- Consider web application security at all points during the web application lifecycle
 - Use the SANS Security Checklist
- Do not trust user input – validate and sanitize (server side a must)
- Scan your web application before go-live, after major changes, and on a regular basis
- Maintenance:
 - Keep server, third-party applications, and library up-to-date
 - Log and monitor server and application activities, and review alerts

UCSF

University of California
San Francisco