Preventing kids drowning is *vitally important*

Turns out...

...they've actually been teaching *IT* *security* all these years

type(self)

- David Beitey (@davidjb)
- Many hats 
- DevOps, SysAdmin, Security Researcher...

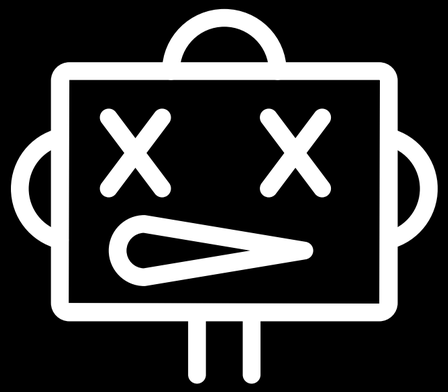
OWASP

Open Web Application Security Project

Top 10

Critical Web App Security Risks*

(*Abridged)



DEVS ALIVE

DO THE FIVE!

5.

Fence the (thread) pool

Broken Authentication

and

Broken Access Control

Vectors

- Known credentials:
  - `admin` / `password` or data breaches
- Password-only auth
- URLs accessible without permission
  https://bank.com/payPerson?name=David&amount=EVERYTHING
- Cross-Site Request Forgeries (CSRF)

Prevention

- *Immediately* change default credentials
- Enforce multi-factor auth (users + servers)
- Rate limit logins
- Principle of least privilege
- Validate actions with tokens

4.

Shut the (logic) gate

Injection

aka

Untrusted input that manipulates your system/users

(SQLi + XSS)

➡ How can we assist you?

FOR YOUR SECURITY

Please do not include personal information such as account numbers or password in this email.

*Your enquiry (max 500 words).

Note: Please avoid punctuation and special characters when composing your message, i.e, '"<>. These characters are not recognised and messages that feature these characters will not be saved or processed.

Big 4 bank, right now

Attacks

https://example.com/contact.php
?name=Robert'); DROP TABLE Students;--

---

https://example.com/search
?query=<script>alert('xss')<script>

Aim: get raw SQL to the database or raw JS/HTML/CSS onto a page

Prevention

- Always treat data as untrusted
- Santise / filter / validate via whitelists
- Use frameworks & platforms with built-in security (eg not raw PHP)
- Monitoring & user awareness

3.

Teach your (apps) to (HTTPS)wim

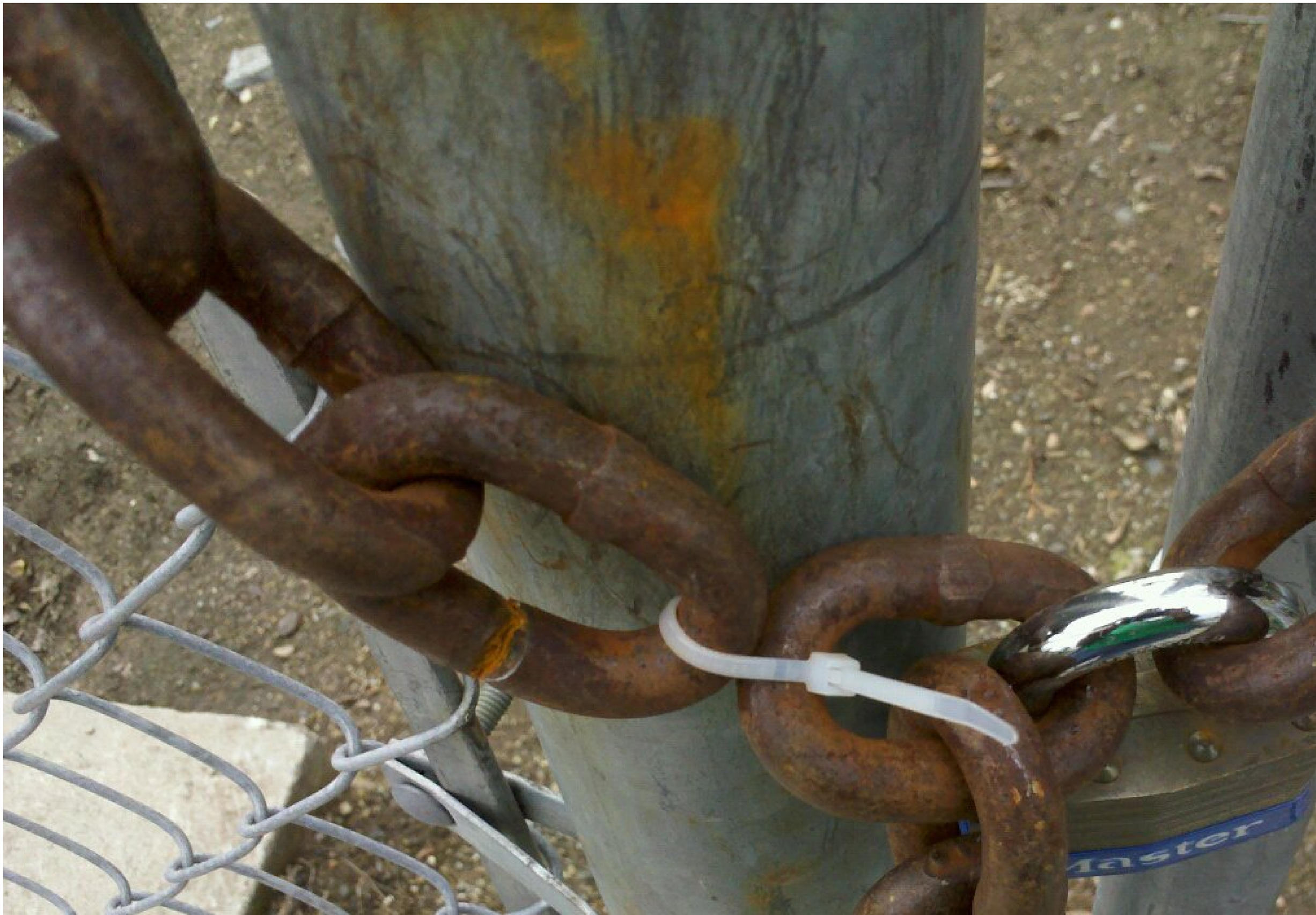
Sensitive Data Exposure

aka

Lack of data protection

Vectors

- Not using TLS (eg `http://`)
- Storing plain-text credentials
- Weakly protected storage (S3 buckets, open databases)...



Prevention

- Always use HTTPS (free certs/Let's Encrypt)
- Avoid storing data unless *necessary*
- Don't roll your own crypto
- Use best practices (eg Django/Rails), esp. for sensitive data

2.

Supervise (deps)

Known Vulnerabilities

aka

Unpatched systems,
unmaintained / untrusted code

TOTAL RESULTS

2,260

TOP COUNTRIES

Australia	2,260

TOP ORGANIZATIONS

Telstra Internet	1,251
iPrimus	587
Dodo Australia	218
TPG Internet	155
Dodo NBN	40

TOP OPERATING SYSTEMS

Linux 2.6.x	1

139.216.159.208

208.159.216.139.sta.dodo.net.au

Dodo Australia

Added on 2019-04-29 06:14:25 GMT

Australia, Townsville

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e867ac98dccff63ff29e20bd24be3139", qop="auth", algorit
hm="MD5"
Content-Length: 0
```

112.141.196.126

126.196.141.112.sta.dodo.net.au

iPrimus

Added on 2019-04-29 05:12:53 GMT

Australia, Townsville

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="16989222ce174c3ff0d674ffe881469b", qop="auth", algorit
hm="MD5"
Content-Length: 0
```

139.216.120.92

Prevention

- Update, monitor & patch *everything* (with testing!)
- Remove unnecessary code
- Use only official, secure software
- Monitor CVE lists & use tools for checking dependencies
- Security-by-obscurity **not** okay

1.

Learn how to (escalate)

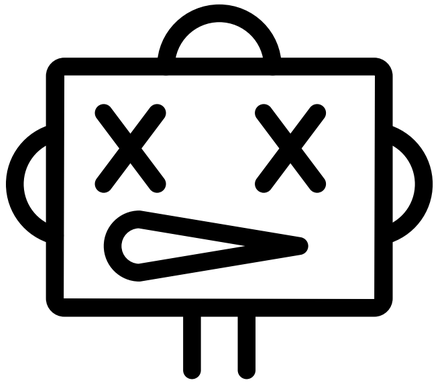
Logging & Monitoring

aka

Insufficient awareness of suspicious activity

Prevention

- Logging with sufficient context
- Monitoring and alerting *humans*
- Create a response/recovery plan



DEVS ALIVE

DO THE FIVE!

- Security is hard
- You won’t stop everything: forward planning
- Many more than 5 or 10 risks
- Easy wins with limited budgets
- Follow best practices

MOAR

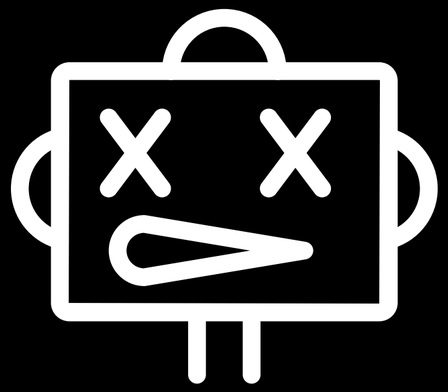
- OWASP Top 10 PDF (owasp.org)
- Security Weakest Link Game (https://www.isdecisions.com/user-security-awareness-game/)
- Google's https://xss-game.appspot.com/
- DEF CON presentations (defcon.org)

Presentation @

https://github.com/davidjb/devs-alive/

Broken HTTPS + Flash + Data leaks + CSRF + ???

Maybe don't trust their IT experience



DEVS ALIVE

DO THE FIVE!