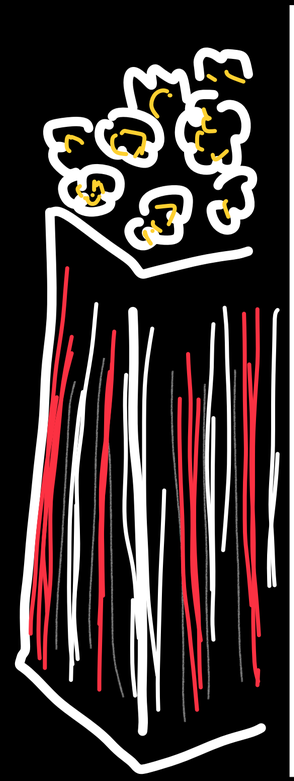
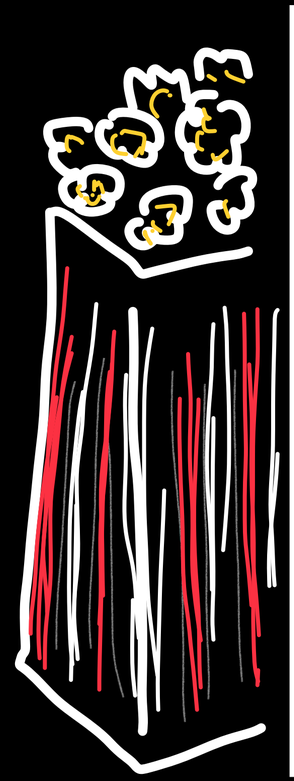
From the CRYPT To the <CODE/>

Web security explored through horror movies

DISCLAIMER

Slight spoiler alert / content warning






Let's split up, gang!

© Paramount

© Bazelevs Prod/Blumhouse Prod

@leichteckig

Videotape you shouldn't look at

© Paramount

© Bazelevs Prod/Blumhouse Prod

@ leichteckig

Videotape you shouldn't look at

Intruder accessing your machine and chats

© Paramount

© Bazelevs Prod/Blumhouse Prod

@ leichteckig


Are we really better
then them?

EternalBlue

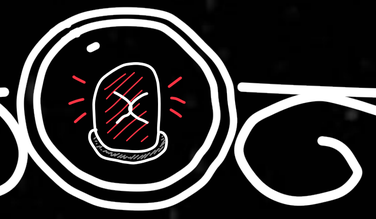
Solarwinds

Heartbleed

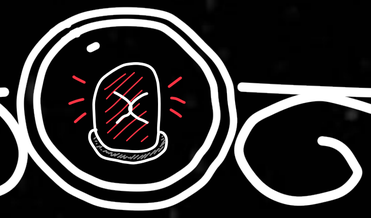
ShellShock

BlueKeep

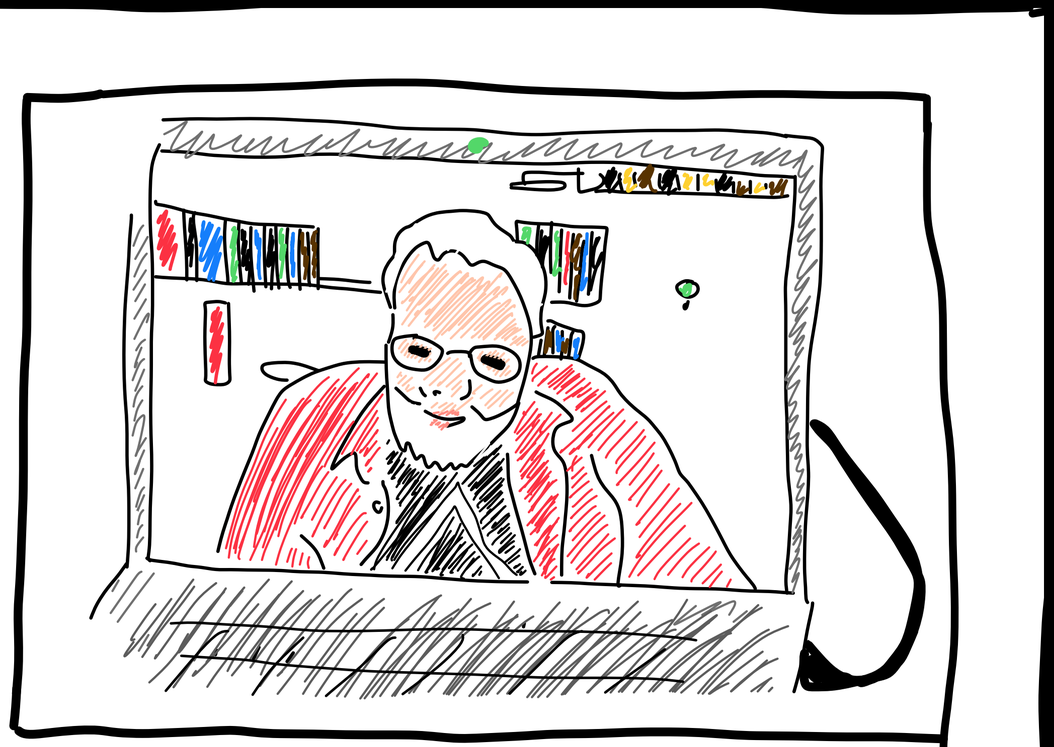
They're the same picture.



We all know what happens
when you ignore the warnings...



Let's draft our own survival playbook



Friendly professor to
the rescue!

Hi!

@leichteckig


CARL LAEMMLE presents
H.G.WELLS'
FANTASTIC SENSATION
THE INVISIBLE MAN
with
GLORIA STUART - CLAUDE RAINS
WM. HARRIGAN - DUDLEY DIGGES - UNA O'CONNOR
HENRY TRAVERS - FORRESTER HARVEY
A UNIVERSAL PICTURE

Broken Access Control

Nobody will see him come, [...] He can hear every secret.

Deny by default

Deny by default

Rate limit API and controller access

Deny by default

Rate limit API and controller access

Invalidate stateful session identifiers

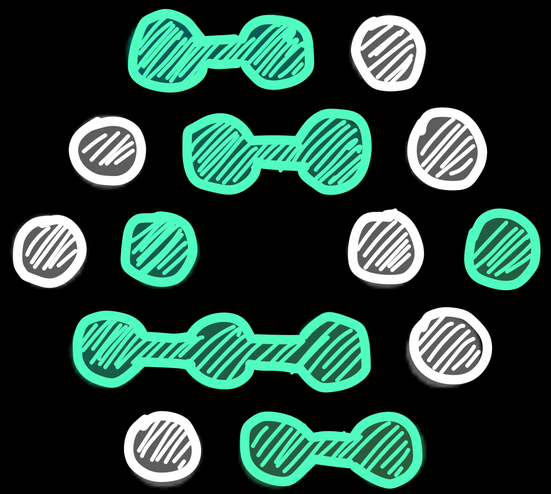
Deny by default

Rate limit API and controller access

Invalidate stateful session identifiers

Implement and reuse access control mechanisms


"Hacking AI
Applications"
By Liran Tal



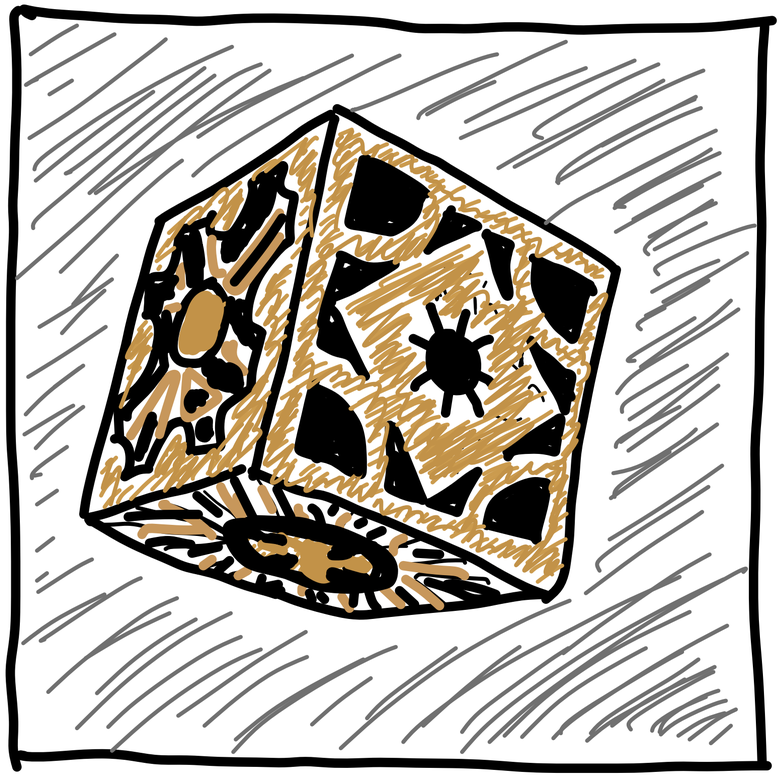
OpenFGA

@ leichteckig


"..THE BEST HORROR FILM EVER TO BE MADE IN BRITAIN."
"THE BEST SLAM-BANG, NO-HOLDS-BARRED, SCARE-THE .... OUT-OF-YOU HORROR MOVIE FOR QUITE A WHILE".
"I HAVE SEEN THE FUTURE OF HORROR FICTION, AND HIS NAME IS CLIVE BARKER".
HELLRAISER.
It will tear your soul apart

2

Cryptographic Failures



The box. You opened it.
We came

Encrypt all
sensitive data

Classify data processed, stored, or transmitted

Encrypt all sensitive data

Classify data processed, stored, or transmitted

Don't store sensitive data unnecessarily

Encrypt all sensitive data

Classify data processed, stored, or transmitted

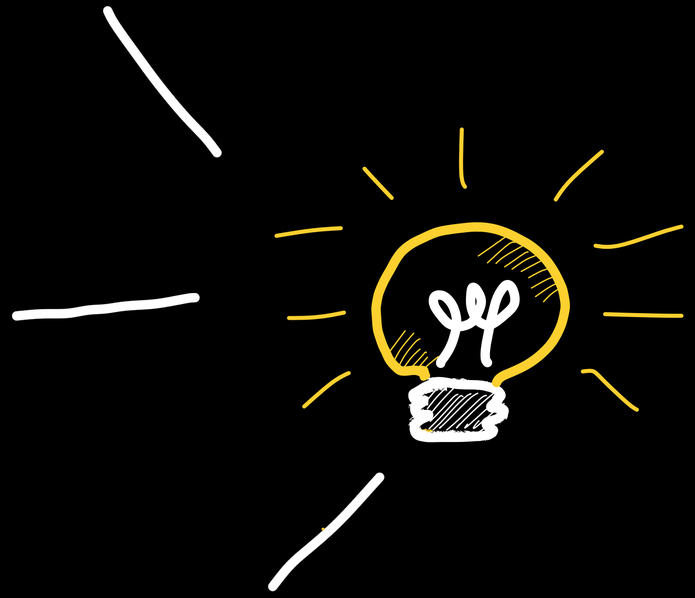
Don't store sensitive data unnecessarily

Encrypt all sensitive data

secure, strong & up-to-date protocols

Classify data processed, stored, or transmitted

Don't store sensitive data unnecessarily



Encrypt all sensitive data

No FTP or SMTP

secure, strong & up-to-date protocols

Classify data processed, stored, or transmitted

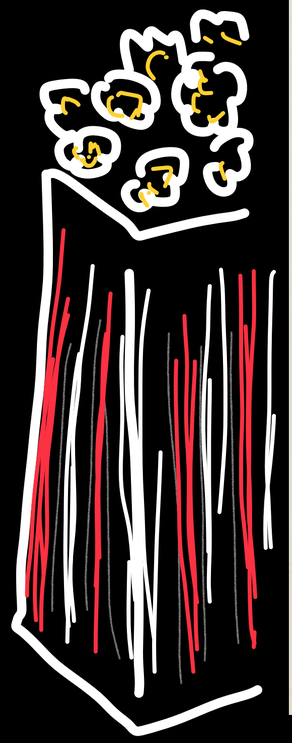
Don't store sensitive data unnecessarily

Encrypt all sensitive data

No FTP or SMTP

Don't cache sensitive responses

secure, strong & up-to-date protocols

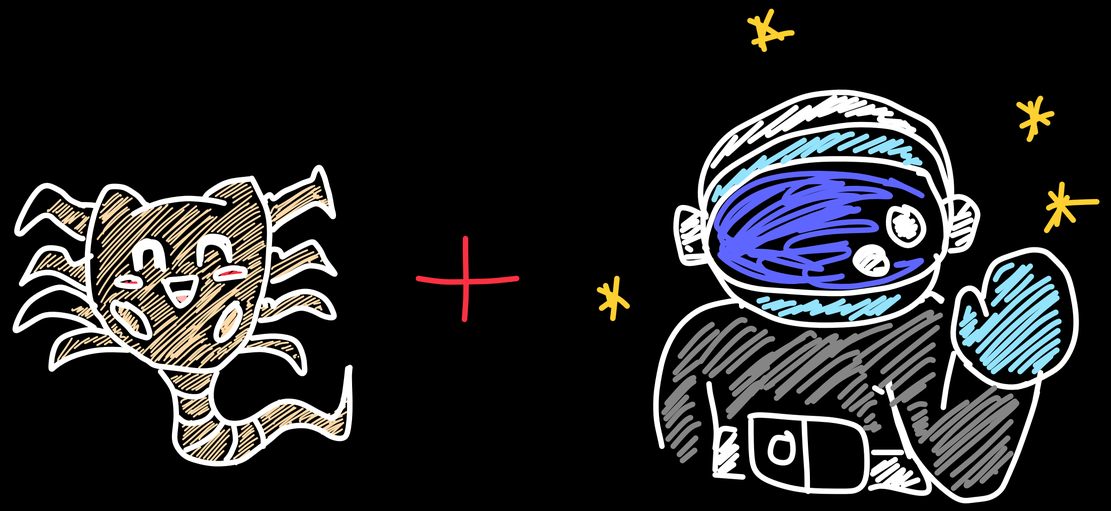



A L I E N
In space no one can hear you scream.
ALIEN
TOM SKERRITT SIGOURNEY WEAVER VERONICA CARTWRIGHT HARRY DEAN STANTON
JOHN HURT IAN HOLM


Free hugs!

...#3: Injection.

... #3: Injection.



... #3: Injection.

Use a safe API

Use a safe API

positive server-side input validation

Use a safe API

positive server-side input validation

Use SQL features

Use a safe API

positive server-side input validation

Use SQL features

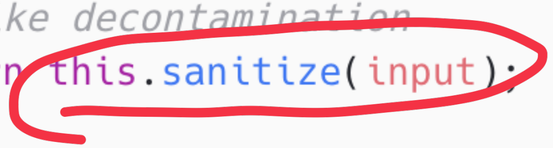
escape special characters

```typescript
// Show defense against "alien" injection
  class QuarantineSystem {
    async validateInput(input: unknown): Promise<SafeInput> {
      // Like scanning for alien life forms
      if (this.detectHostilePatterns(input)) {
        throw new SecurityError('Hostile organism detected');
      }

      // Like decontamination
      return this.sanitize(input);
    }
  }
```

```
// Show defense against "alien" injection
   class QuarantineSystem {
     async validateInput(input: unknown): Promise<SafeInput> {
       // Like scanning for alien life forms
       if (this.detectHostilePatterns(input)) {
         throw new SecurityError('Hostile organism detected');
       }

       // Like decontamination
       return this.sanitize(input);
     }
   }
```



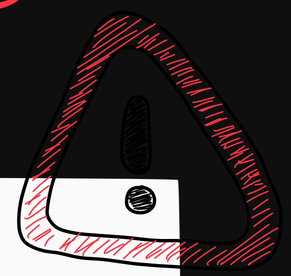
Library or build your own

@leichteckig

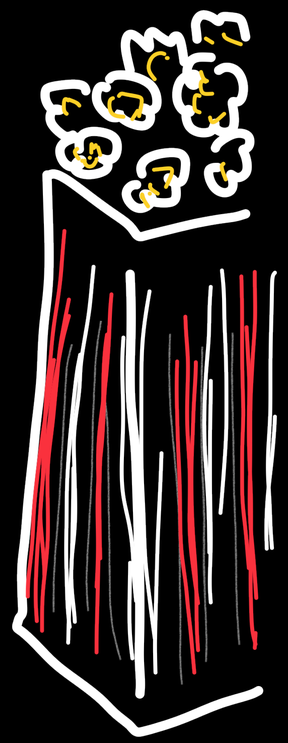
```
private readonly suspiciousPatterns = [
    /exec\s*\(/,           // Command injection
    /<script\b[^>]*>/,     // XSS
    /\b(ALTER|DROP)\b/i,   // SQL injection
    /\b(SELECT.*FROM)\b/, // SQL injection
    /(\%27)|(\')/,         // SQL injection
    /(\/\*[\w\W]*?\*\/)|(--.*)/, // SQL comments
    /((n|%6E)(e|%65)(t|%74)(c|%63)(a|%61)(t|%74))/i, // netcat
    /s(h|%68)e(l|%6C)l/i.          // shell
  ];
```


ChatGPT
WHAT IS MY PURPOSE
You write Regex
ChatGPT
OH MY GOD
imgflip.com

ReDos



```
^([a-zA-Z0-9_\-\.]+)@([a-zA-Z0-9_\-\.]+)\.([a-zA-Z]{2,})$
```




INDESCRIBABLE...
INDESTRUCTIBLE!
NOTHING CAN STOP IT!
THE BLOB
STEVEN McQUEEN
ANETA CORSEAUT
EARL ROWE
PRODUCED BY
JACK H. HARRIS
DIRECTED BY
IRVIN S. YEAWORTH, JR.
SCREENPLAY BY
THEODORE SIMONSON AND KATE PHILLIPS

Software Supply Chain Failures


THE BLOB

Remove ununsed dependencies

etc.

Remove ununsed dependencies

etc.

Inventory of all version numbers

Remove ununsed dependencies etc.

Inventory of all version numbers

Obtain from official sources & secure links

Remove ununsed dependencies etc.

Inventory of all version numbers

Obtain from official sources & secure links

Monitor if library get unmaintained

Remove ununsed dependencies etc.

Inventory of all version numbers

+UPDATE!!

Obtain from official sources & secure links

Monitor if library get unmaintained

Stay as a team

Stay as a team

Take care of your batteries

Stay as a team

Take care of your batteries

Double-check if the killer was defeated

Stay as a team

Take care of your batteries

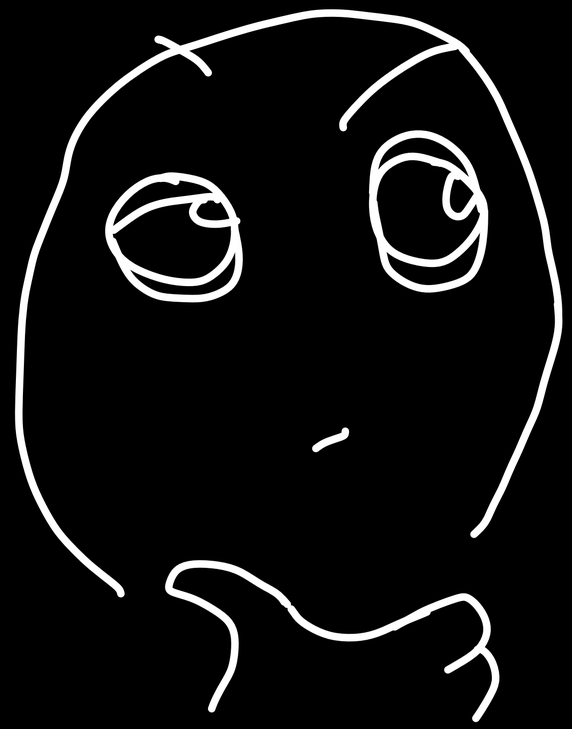
Double-check if the killer was defeated

Take your ~~prof's~~ OWASP's advice seriously


Fin.
Thank you!

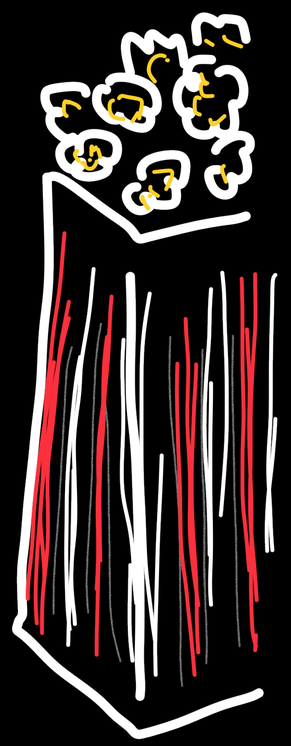

Fin ?
Thank you!


Encore!



Time for a quiz.

@ leichteckig




HOUSE ON HAUNTED HILL
VINCENT PRICE
CAROL OHMART · RICHARD LONG
ALAN MARSHAL · AN ALLIED ARTISTS PICTURE
Produced and Directed by WILLIAM CASTLE · Written by ROBB WHITE

Rank 4: Insecure Design

The house, it's alive!

UI components

@ leichteckig

secure development lifecycle.

UI components

Secure development lifecycle.

Use component libraries

UI components

Secure development lifecycle.

Use component libraries

UI components

Threat modeling.

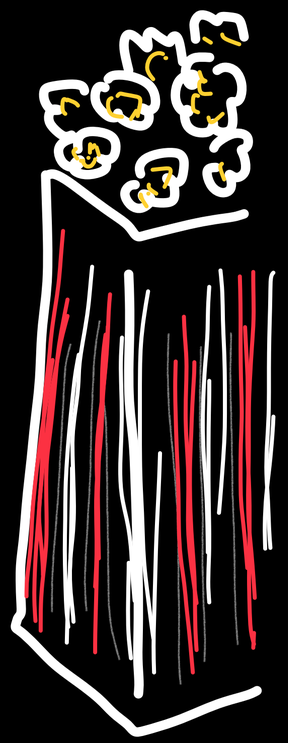
Secure development lifecycle.

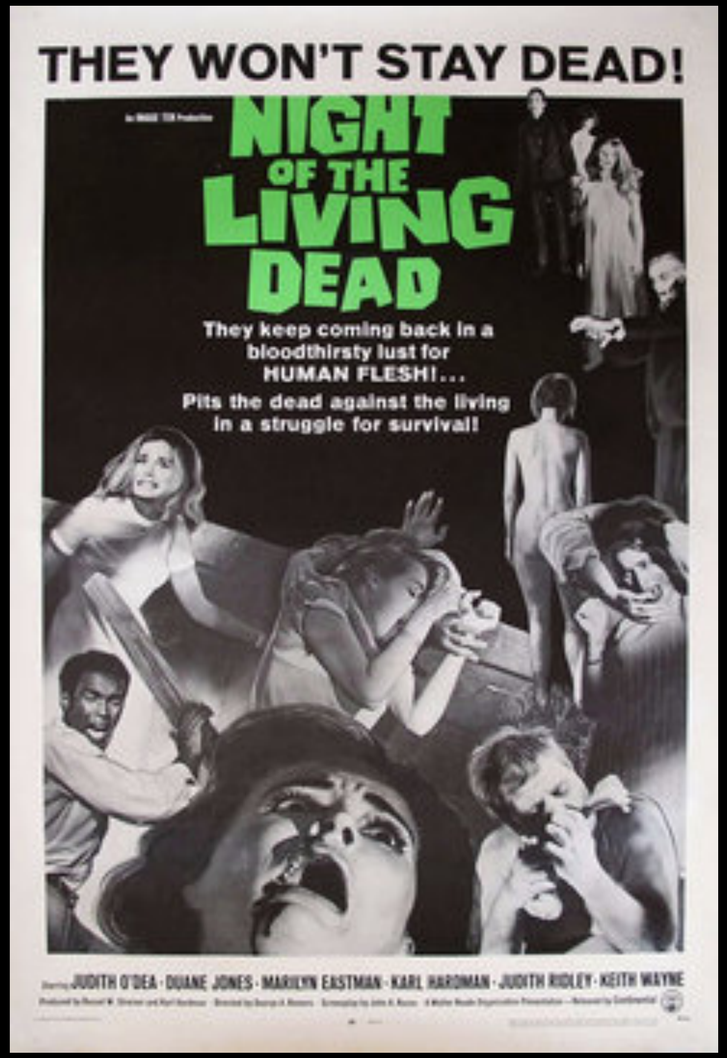
Use component libraries

UI components

Threat modeling.

Write tests!!




THEY WON'T STAY DEAD!
NIGHT OF THE LIVING DEAD
They keep coming back in a bloodthirsty lust for HUMAN FLESH!...
Pits the dead against the living in a struggle for survival!
JUDITH O'DEA · DUANE JONES · MARILYN EASTMAN · KARL HARDMAN · JUDITH RIDLEY · KEITH WAYNE


Fin.
Thank you!