PCH
Packet Clearing House

# How Not To Get Hacked: The Web AppSec Cheat Sheet

**Ashley Jones**
**Packet Clearing House**

**Southwest Career and Technical Academy**
**December 8th 2016**

**https://pch.net/WebAppSec**

PCH
Packet Clearing House

# Agenda

- Introductions
- Items are pch.net/WebAppSec
- Each Item:
  - Overview
  - Example
  - Mitigation
- Interruptions welcome!

PCH
Packet Clearing House

# Why be secure?

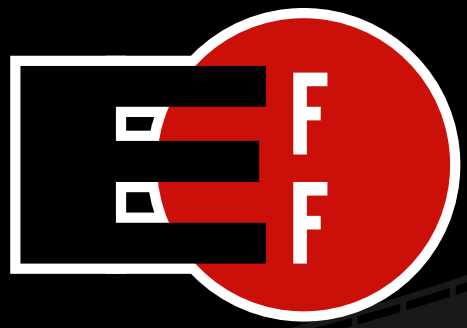
"These [security] errors have been the cause of nearly every major type of cyber attack, including recent penetrations of Google, power systems, military systems, and millions of other attacks on small businesses and home users"

- csoonline.com about sans.org report

PCH
Packet Clearing House

# Why be secure?

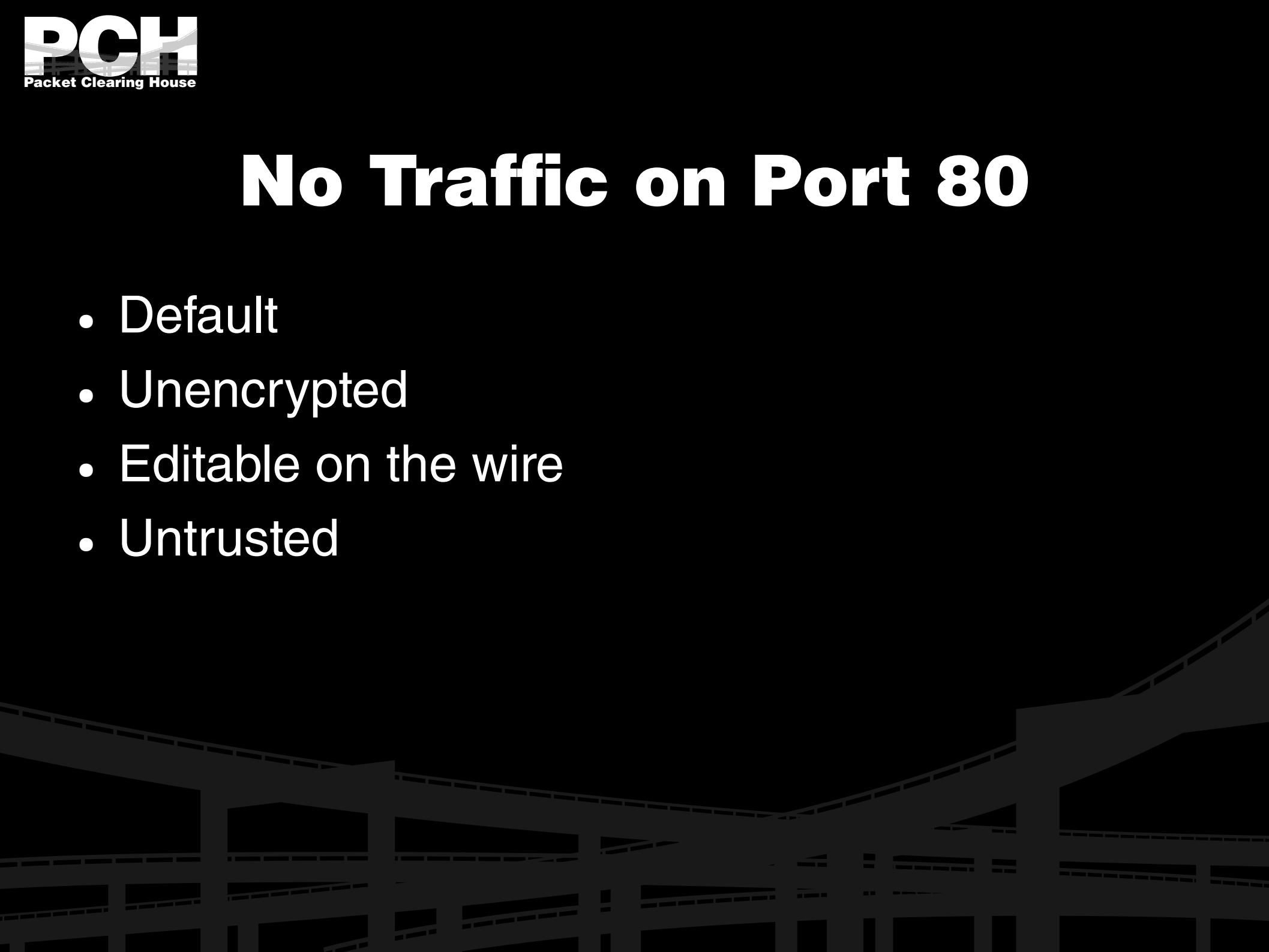


PCH
Packet Clearing House

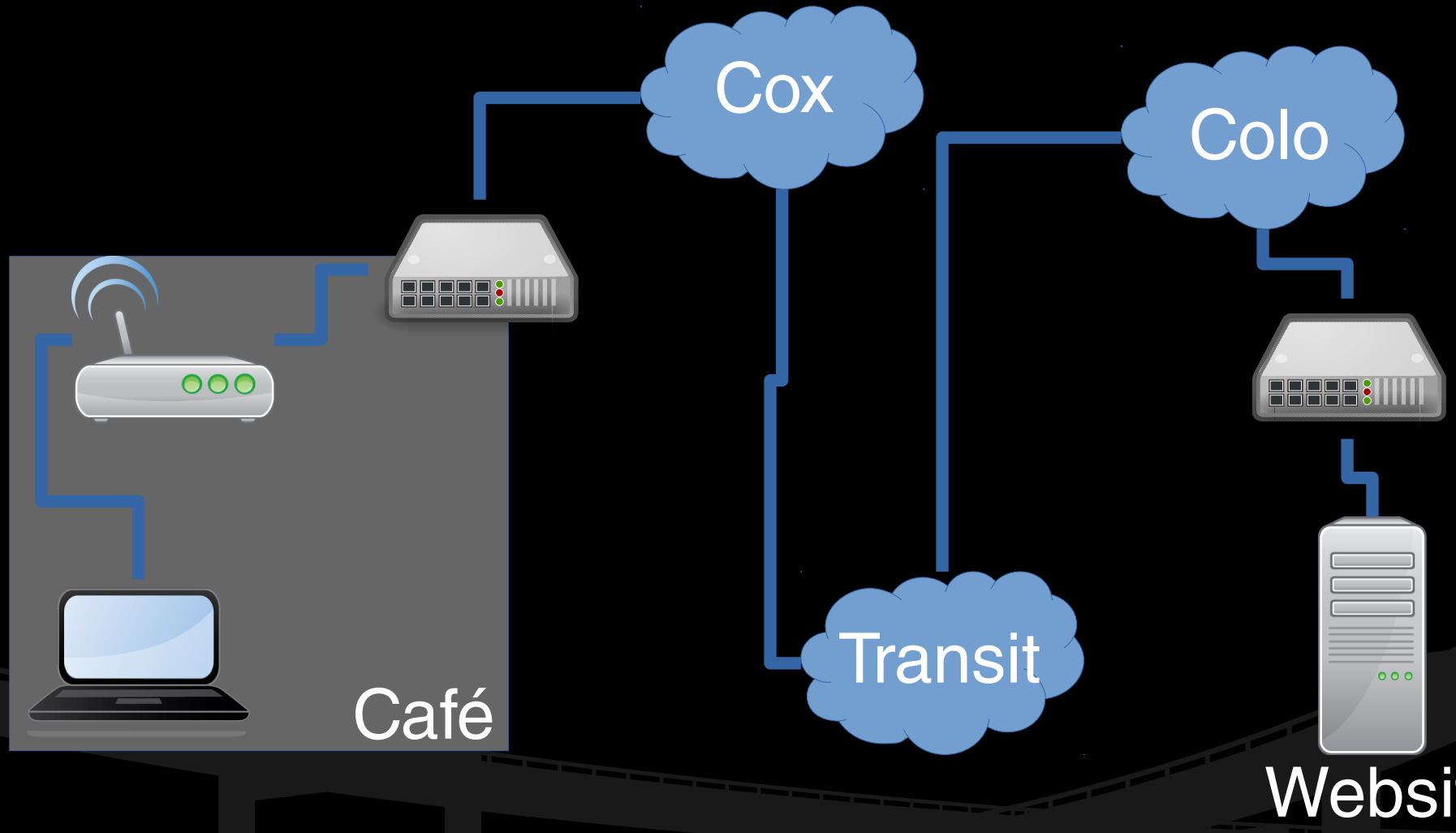
# No Traffic on Port 80

- Default
- Unencrypted
- Editable on the wire
- Untrusted



PCH
Packet Clearing House

# No Traffic on Port 80



PCH
Packet Clearing House

# No Traffic on Port 80

- Setup SSL – Free!
- Redirect from port 80 → 443
- Apache:

```
RewriteEngine On

RewriteCond %{HTTPS} off

RewriteRule (.*) https://%
{HTTP_HOST}%{REQUEST_URI}
```

PCH
Packet Clearing House

# XSS Escaping

- Cross Site Scripting
- Renders JavaScript
- Steals cookies

PCH
Packet Clearing House

# XSS Escaping

```
<input name=search type=text value="<?php echo
$_GET['search']?>" />
```

```
<?php
$username = getUserFromDatabase();
print $username;
?>
```

samy is my hero (fastest virus ever)

PCH
Packet Clearing House

# XSS Escaping

- Never trust user input!
- Repeat: Never, EVER trust user input!
- `htmlspecialchars($_GET['search'], ENT_QUOTES, 'UTF-8')`

PCH
Packet Clearing House

# HTTPOnly Cookies
# Secure Cookies

- HTTPOnly – do not allow JS to access cookies
- Secure – Only accessible via SSL

PCH
Packet Clearing House

# HTTPOnly Cookies
# Secure Cookies

- See #3 about XSS ;)
- Firesheep – assume identity of any networks not using SSL and not using Secure cookies

PCH
Packet Clearing House

# HTTPOnly Cookies
# Secure Cookies

```
setcookie($name, $value, $expire,
$path, $domain, $secure, $httponly)
```

```
setcookie( ‘session’, $sessionId, 0,
‘/’, ‘www.example.com’, true, true);
```

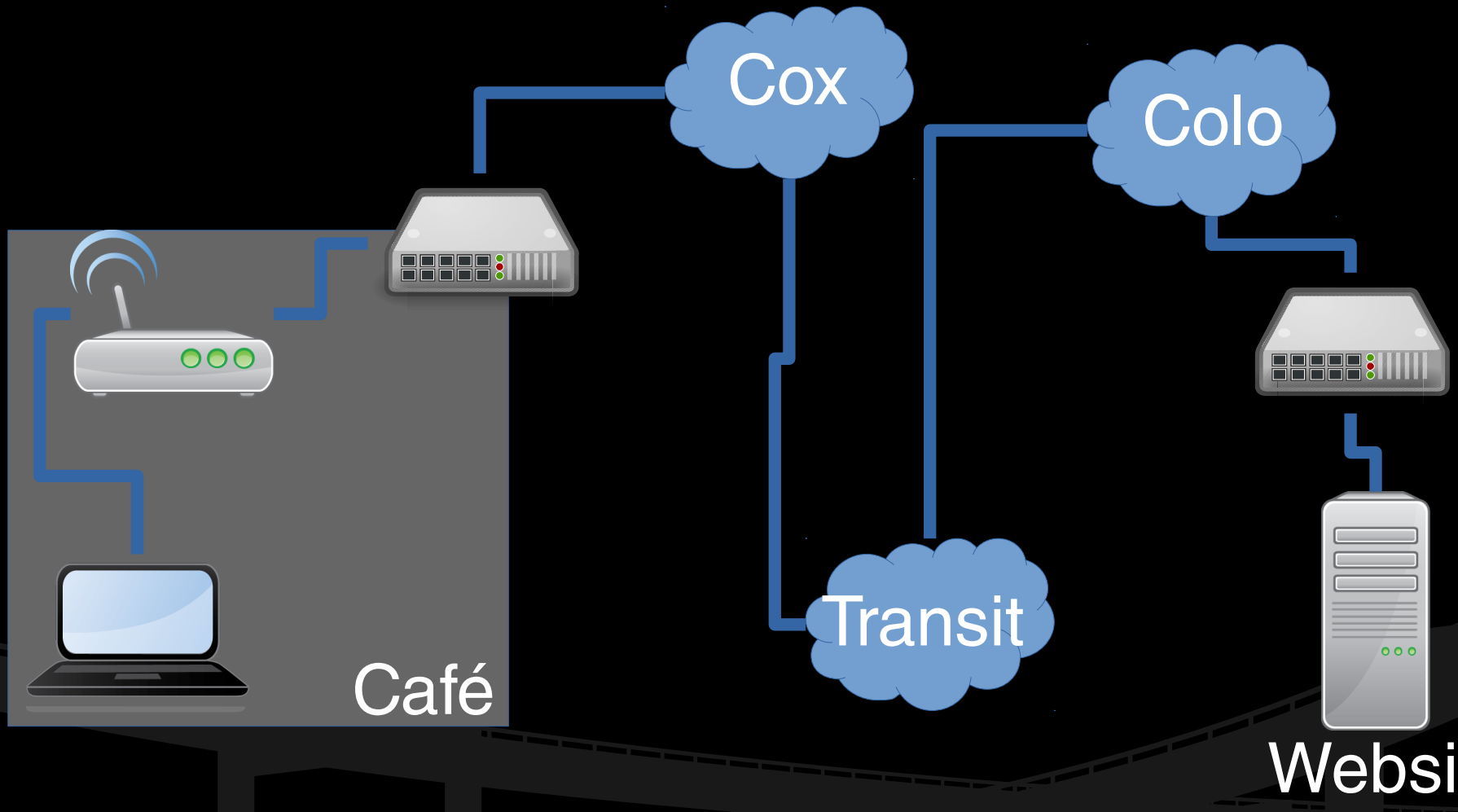
PCH
Packet Clearing House

# HSTS

- HTTP Strict Transport Security
- Port 80 just once
- Cached

PCH
Packet Clearing House

# HSTS



PCH
Packet Clearing House

# HSTS

- “Adding support for HSTS is the single most important improvement you can make for the TLS security of your web sites.” - SSL Labs
- Warning: Watch for sub-domains!
- Apache:

```
Header always set Strict-Transport-Security

“max-age=15768000”
```

PCH
Packet Clearing House

# bcrypt hashes

- Passwords are hashed in the DB
- MD5 is fast, *really* fast

```
md5('packetexchange')

6c6d701fe70651def644
beb954a5b18845065437
```

PCH
Packet Clearing House

# bcrypt hashes

- 200 Billion guesses a second

PCH
Packet Clearing House

# bcrypt hashes

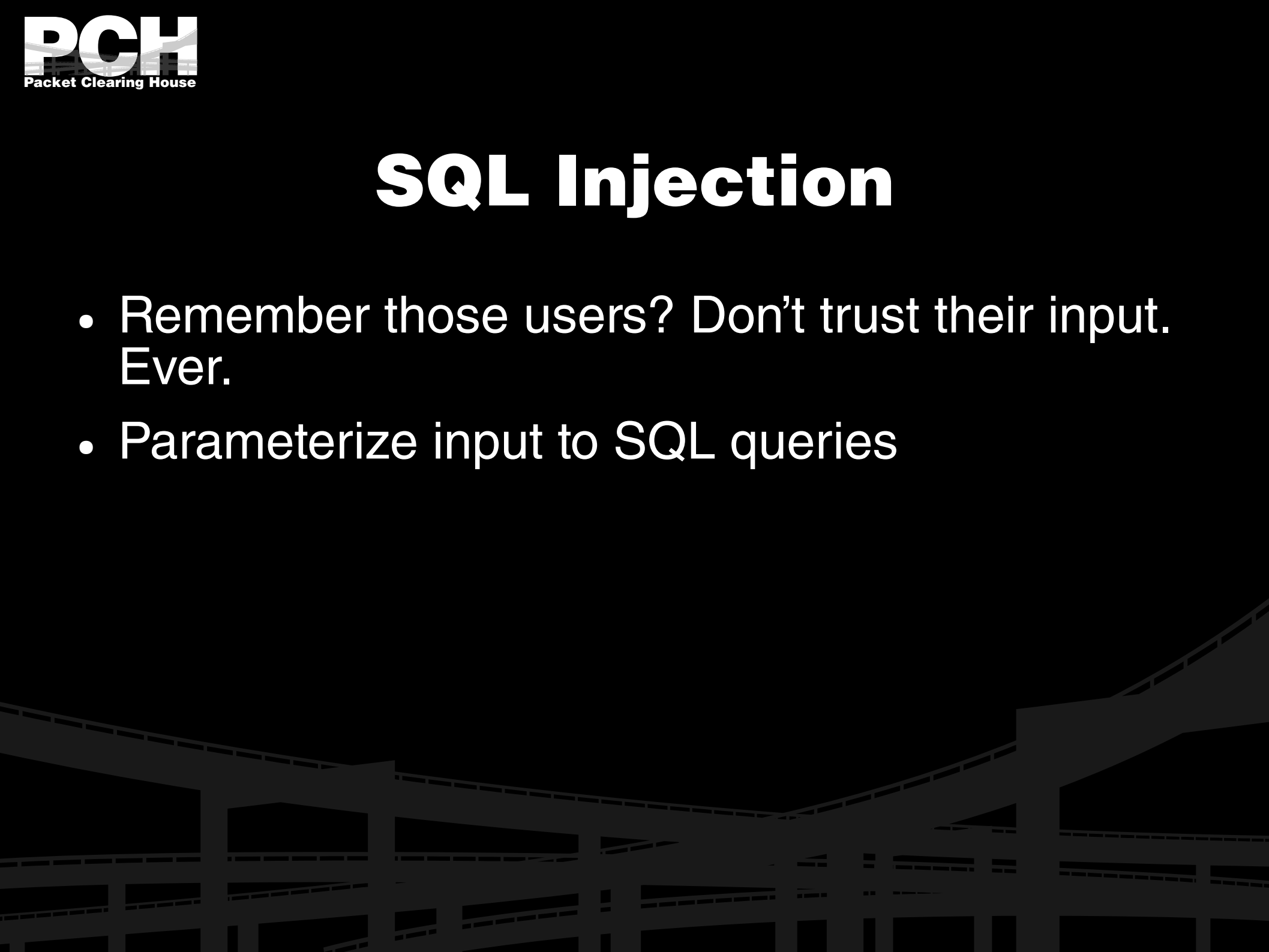
```
password_hash(“packetexchange”,
PASSWORD_DEFAULT)

$2a$08$SXQElyv.pCN1q3FB4OtW4.TeS5hDT
jhINPIIAK8qFW2J3Vl0HiNNm
```

PCH
Packet Clearing House

# SQL Injection

- Remember those users? Don’t trust their input. Ever.
- Parameterize input to SQL queries



PCH
Packet Clearing House

# SQL Injection

```
<input name=search type=text />

$stmt = $dbh->prepare("SELECT * FROM
content where text like '%" .
$_GET['search'] . '%");

$stmt->execute();
```

PCH
Packet Clearing House

# SQL Injection

```
<input name=search type=text />

$stmt = $dbh->prepare("SELECT * FROM
content where text like :search");

$stmt->execute(
  array(':search' => $_GET['search'])
);
```

PCH
Packet Clearing House

# Thanks!

Ashley Jones
Packet Clearing House

Southwest Career and Technical Academy
December 8th 2016

https://pch.net/WebAppSec

Thanks to the resources at
Open Web Application Security Project's site (OWASP)

Inspired off my own blog post