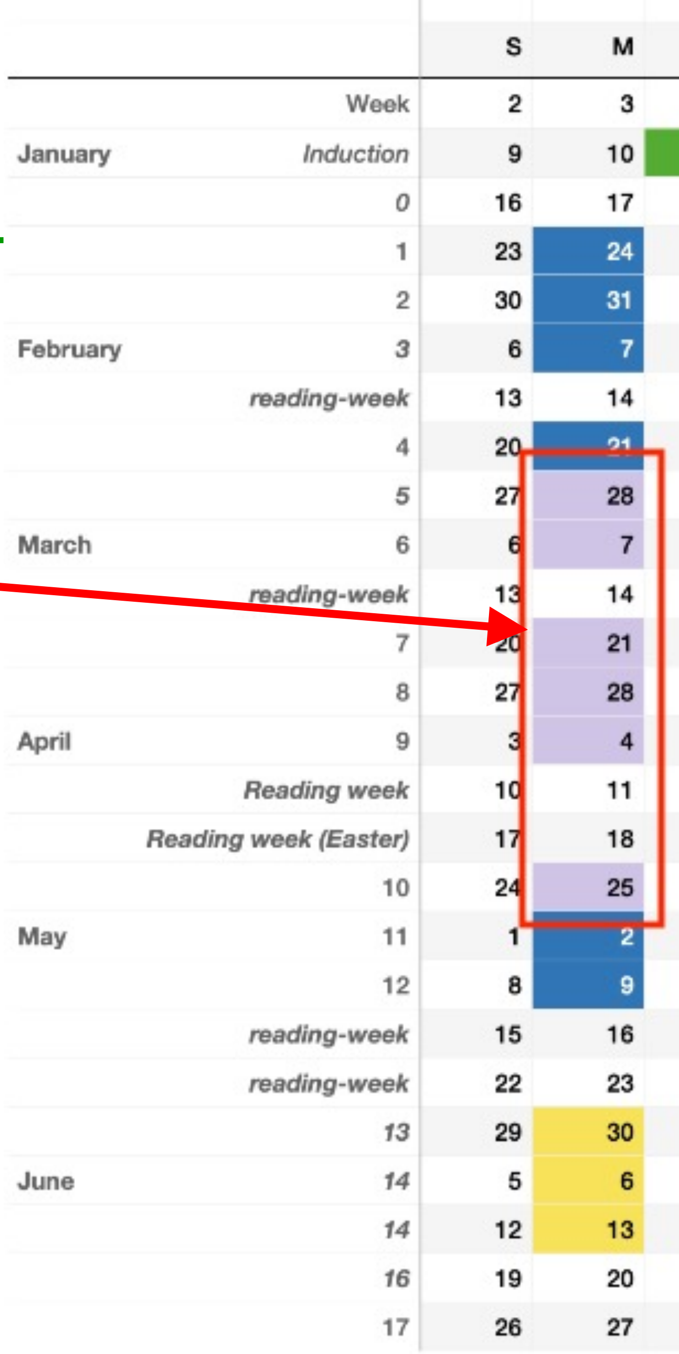
Software Security

Overview

Practicalities

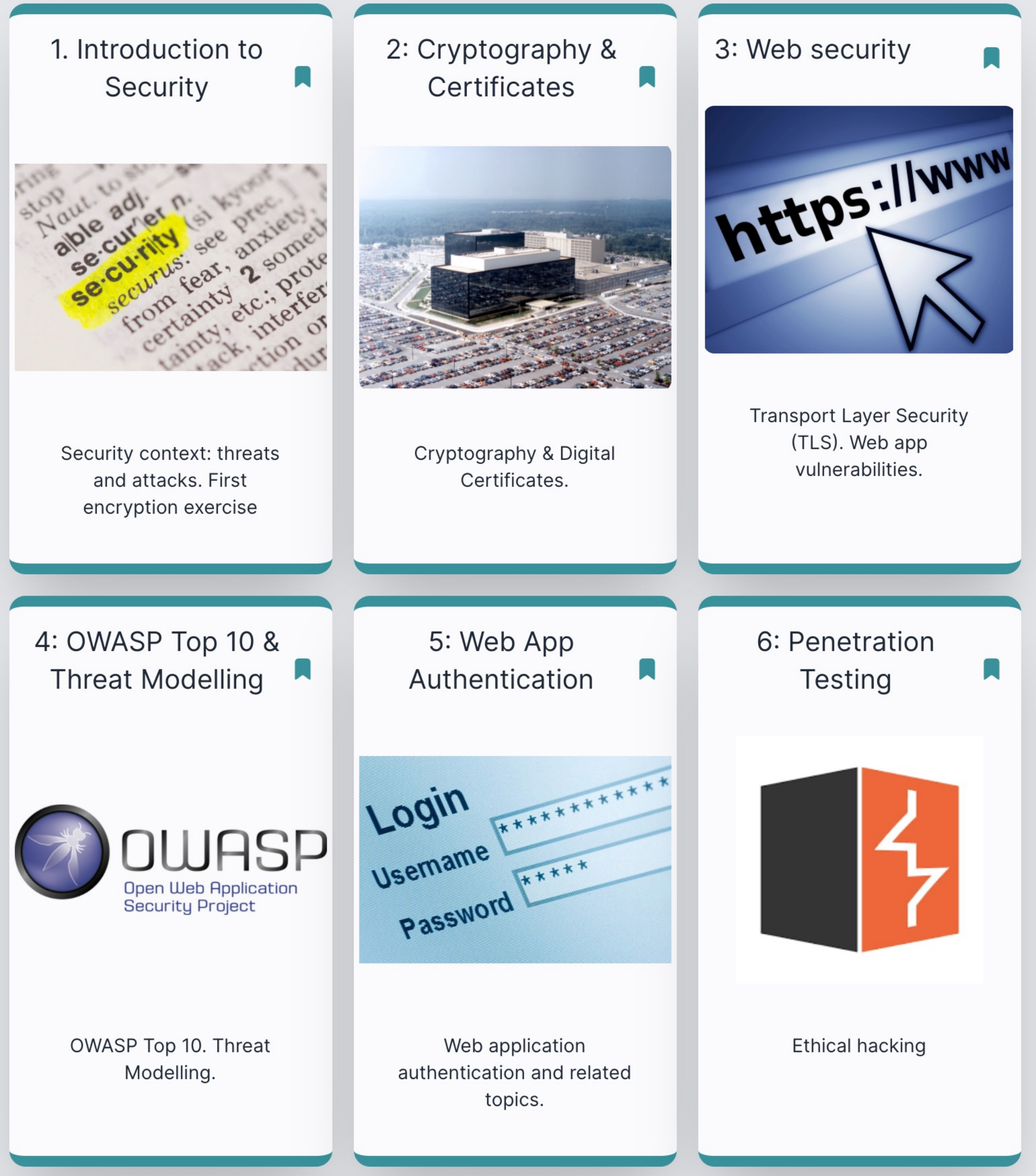
- 6 lecture slots
  - Planned for Monday 12:15 – 2:15
  - Weeks 5-10 inclusive
  - Associated lab exercises each week
  - Join **#software-security** channel on Slack
- Assignment
  - Web application security report
  - Based on doing the labs
    - Choose a web app
      - Model threats
      - Add security features
      - Penetration test



		S	M
	Week	2	3
January	*Induction*	9	10
	0	16	17
	1	23	24
	2	30	31
February	3	6	7
	reading-week	13	14
	4	20	21
	5	27	28
March	6	6	7
	reading-week	13	14
	7	20	21
	8	27	28
April	9	3	4
	Reading week	10	11
	Reading week (Easter)	17	18
	10	24	25
May	11	1	2
	12	8	9
	reading-week	15	16
	reading-week	22	23
	13	29	30
June	*14*	5	6
	14	12	13
	16	19	20
	17	26	27

Main themes

- Introduction
  - Threats, attacks, vulnerabilities; Security services
- Cryptography & certificates
  - Symmetric & public-key encryption
  - Authentication and integrity
  - Key management and certificates
- Web application security
  - TLS (SSL) deployment
  - Web app vulnerabilities & OWASP Top 10
  - Threat Modelling
- Web app authentication
  - Secure key and password storage
  - Web authentication schemes
- Ethical hacking: attack & defence
  - Penetration testing



1. Introduction to Security

Security context: threats and attacks. First encryption exercise

2: Cryptography & Certificates

Cryptography & Digital Certificates.

3: Web security

Transport Layer Security (TLS). Web app vulnerabilities.

4: OWASP Top 10 & Threat Modelling

OWASP Top 10. Threat Modelling.

5: Web App Authentication

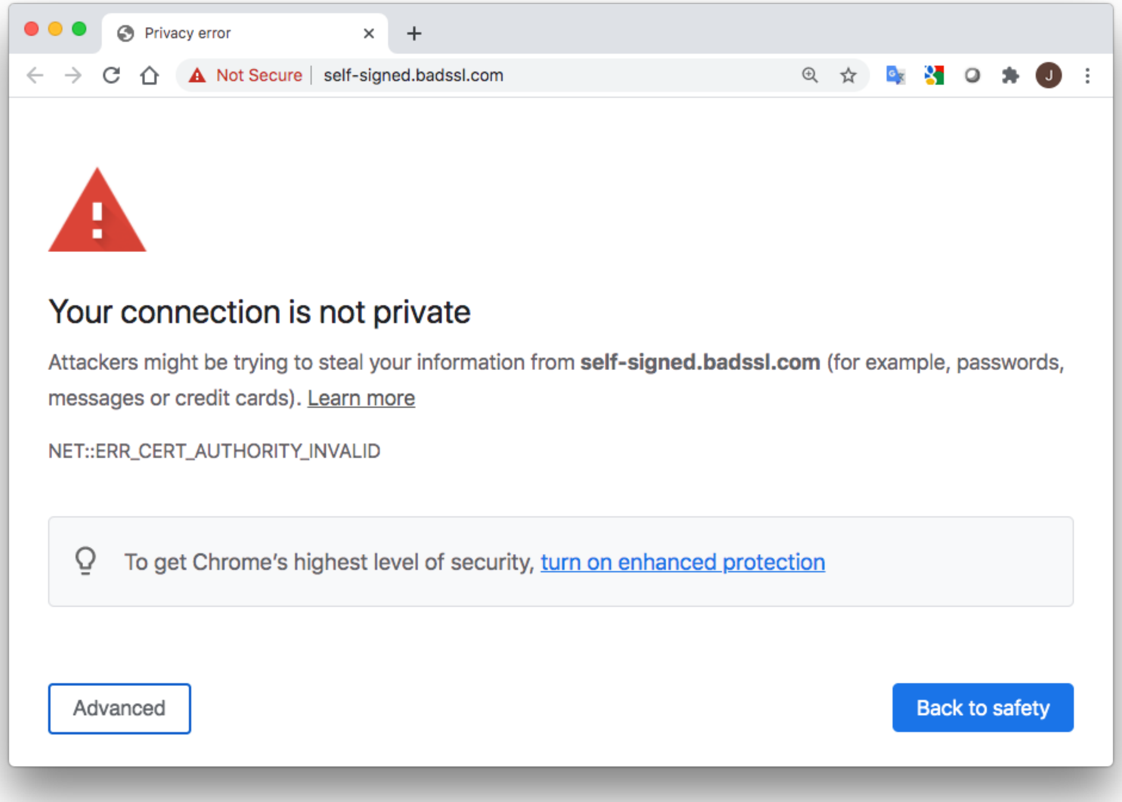
Web application authentication and related topics.

6: Penetration Testing

Ethical hacking

After this module, you should be able to

… understand warnings like these:

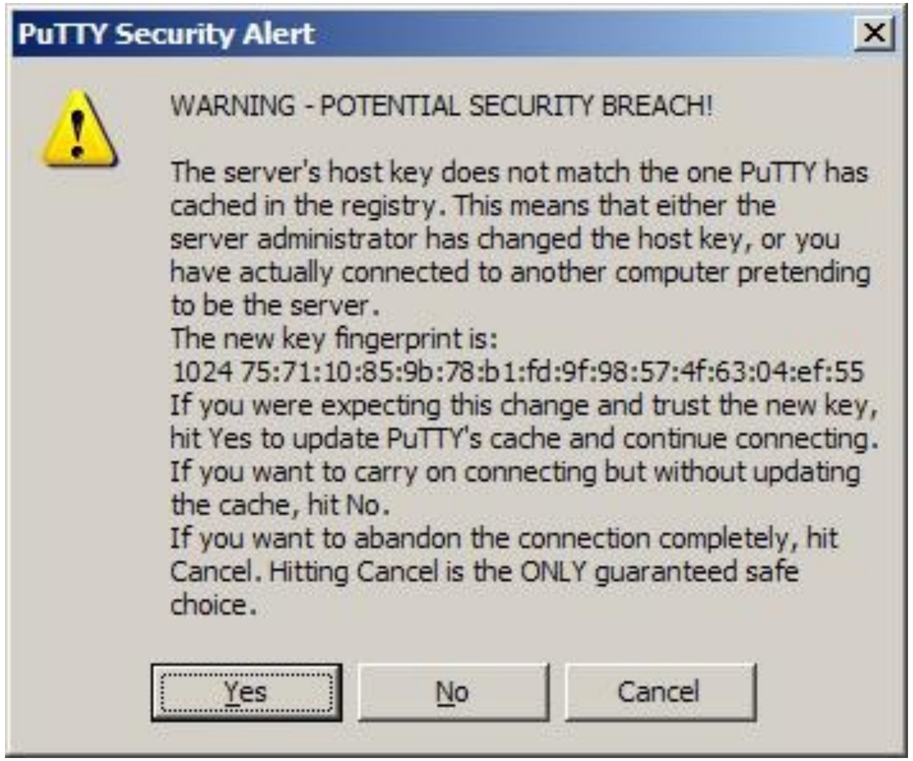


Your connection is not private

Attackers might be trying to steal your information from **self-signed.badssl.com** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

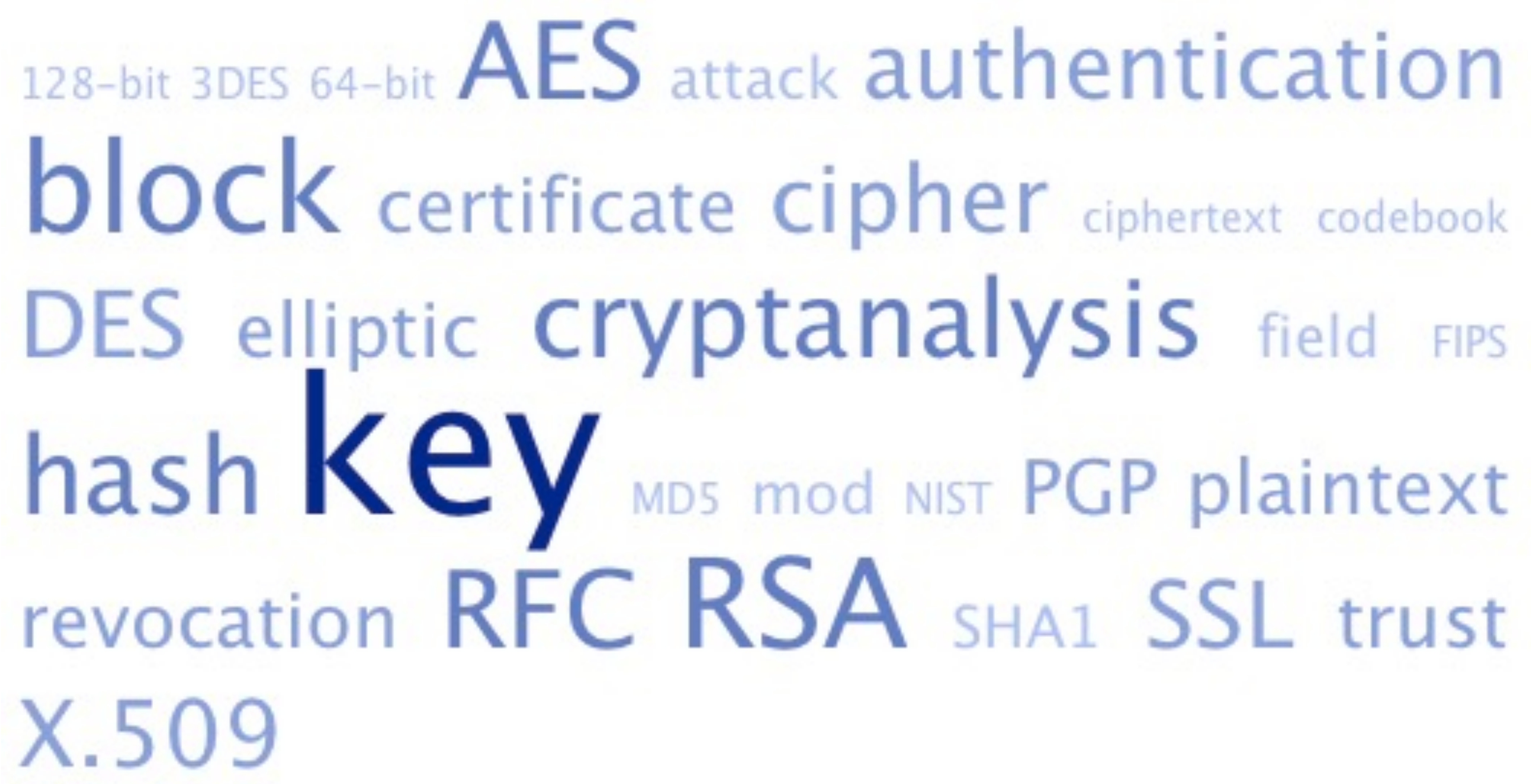


WARNING - POTENTIAL SECURITY BREACH!

The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server.
The new key fingerprint is:
1024 75:71:10:85:9b:78:b1:fd:9f:98:57:4f:63:04:ef:55
If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting.
If you want to carry on connecting but without updating the cache, hit No.
If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.

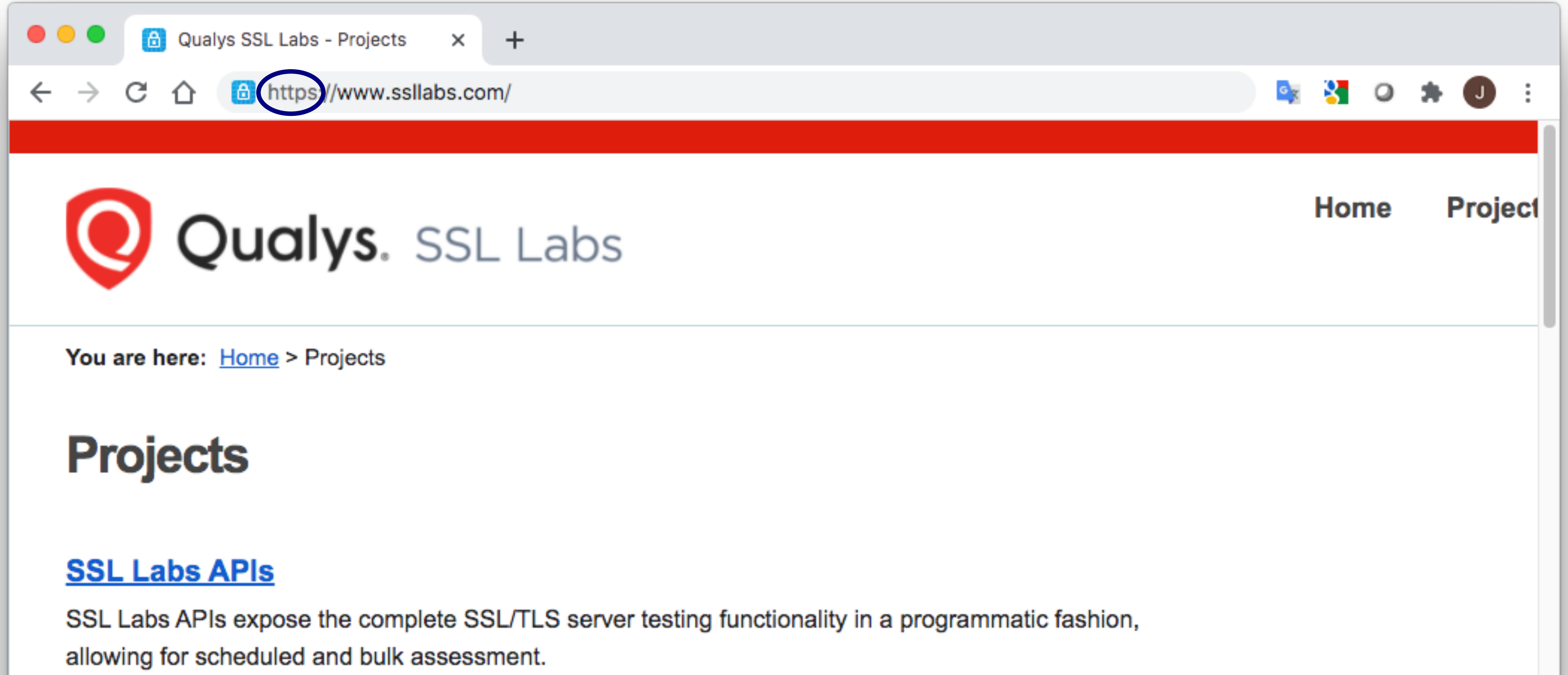
After this module, you should be able to

… follow crypto jargon:



After this module, you should be able to

… set up TLS (https)



You are here: Home > Projects

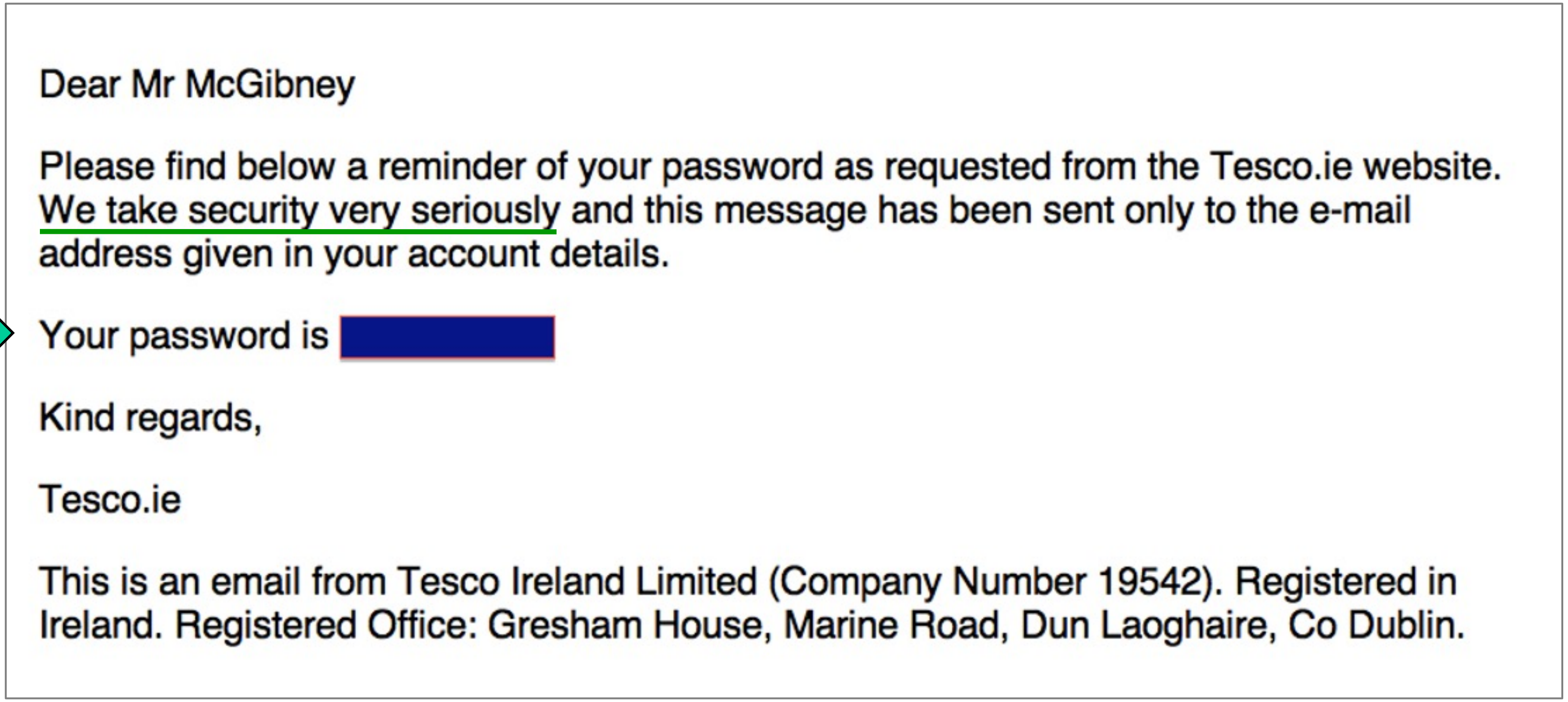
Projects

SSL Labs APIs

SSL Labs APIs expose the complete SSL/TLS server testing functionality in a programmatic fashion, allowing for scheduled and bulk assessment.

After this module, you should be able to

… understand why **this** is bad practice:



Dear Mr McGibney

Please find below a reminder of your password as requested from the Tesco.ie website. We take security very seriously and this message has been sent only to the e-mail address given in your account details.

Your password is [redacted]

Kind regards,

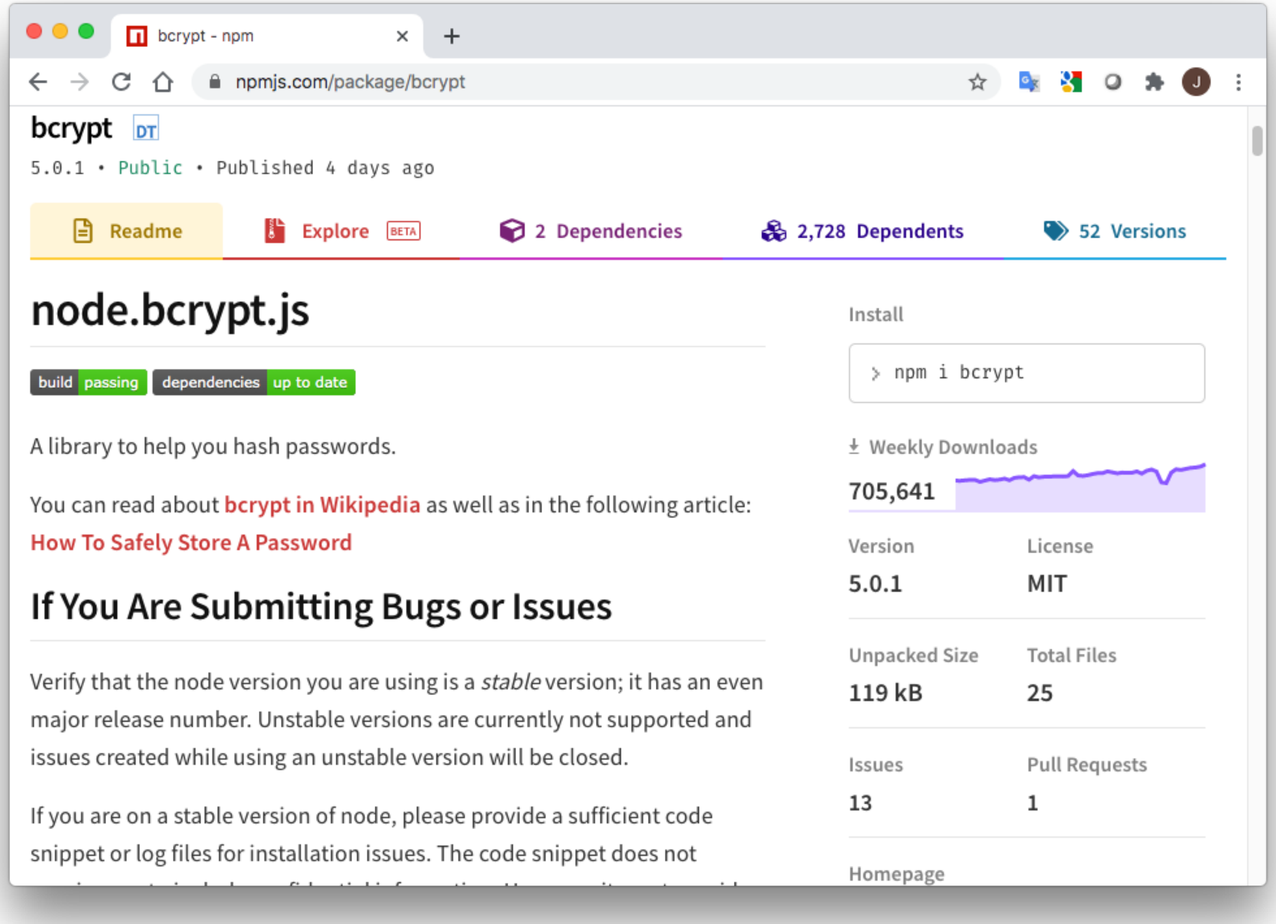
Tesco.ie

This is an email from Tesco Ireland Limited (Company Number 19542). Registered in Ireland. Registered Office: Gresham House, Marine Road, Dun Laoghaire, Co Dublin.

Note this is a historical example; Tesco has changed this practice

After this module, you should be able to

… use good authentication practices



bcrypt - npm

npmjs.com/package/bcrypt

bcrypt DT

5.0.1 • Public • Published 4 days ago

node.bcrypt.js

A library to help you hash passwords.

You can read about bcrypt in Wikipedia as well as in the following article: How To Safely Store A Password

If You Are Submitting Bugs or Issues

Verify that the node version you are using is a *stable* version; it has an even major release number. Unstable versions are currently not supported and issues created while using an unstable version will be closed.

If you are on a stable version of node, please provide a sufficient code snippet or log files for installation issues. The code snippet does not

Install

```
> npm i bcrypt
```

Weekly Downloads

705,641

Version: 5.0.1

License: MIT

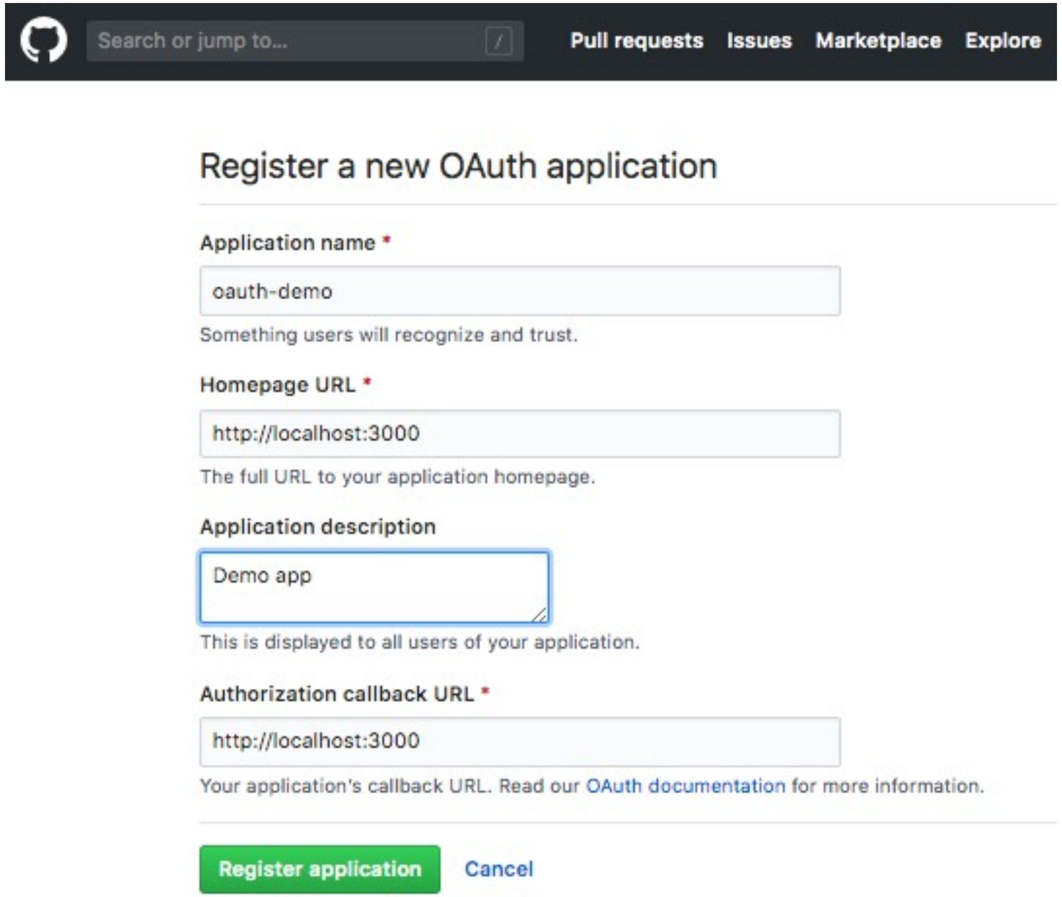
Unpacked Size: 119 kB

Total Files: 25

Issues: 13

Pull Requests: 1

Homepage



Register a new OAuth application

Application name *

oauth-demo

Something users will recognize and trust.

Homepage URL *

http://localhost:3000

The full URL to your application homepage.

Application description

Demo app

This is displayed to all users of your application.

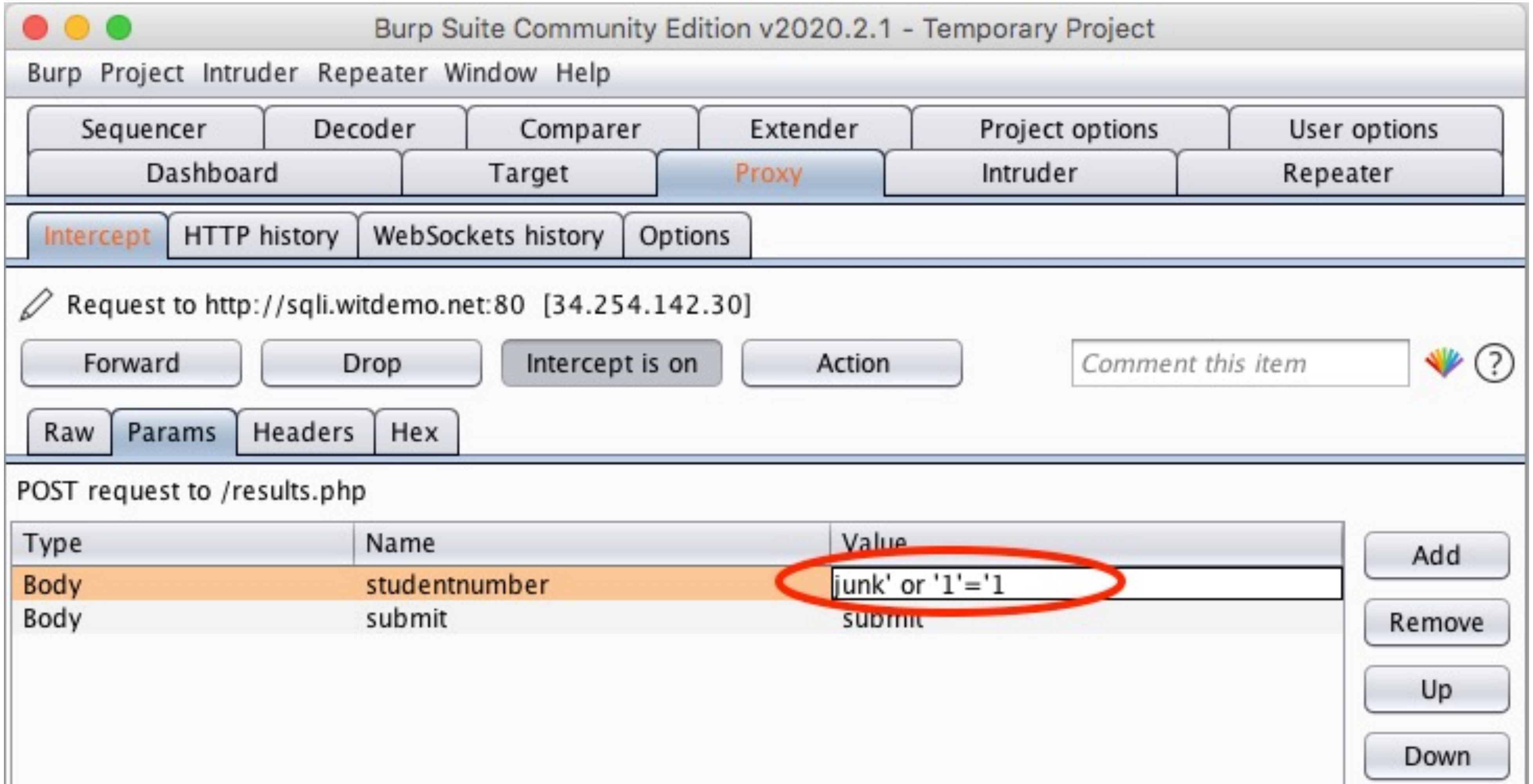
Authorization callback URL *

http://localhost:3000

Your application's callback URL. Read our OAuth documentation for more information.

After this module, you should be able to

… do some penetration testing ("ethical hacking")



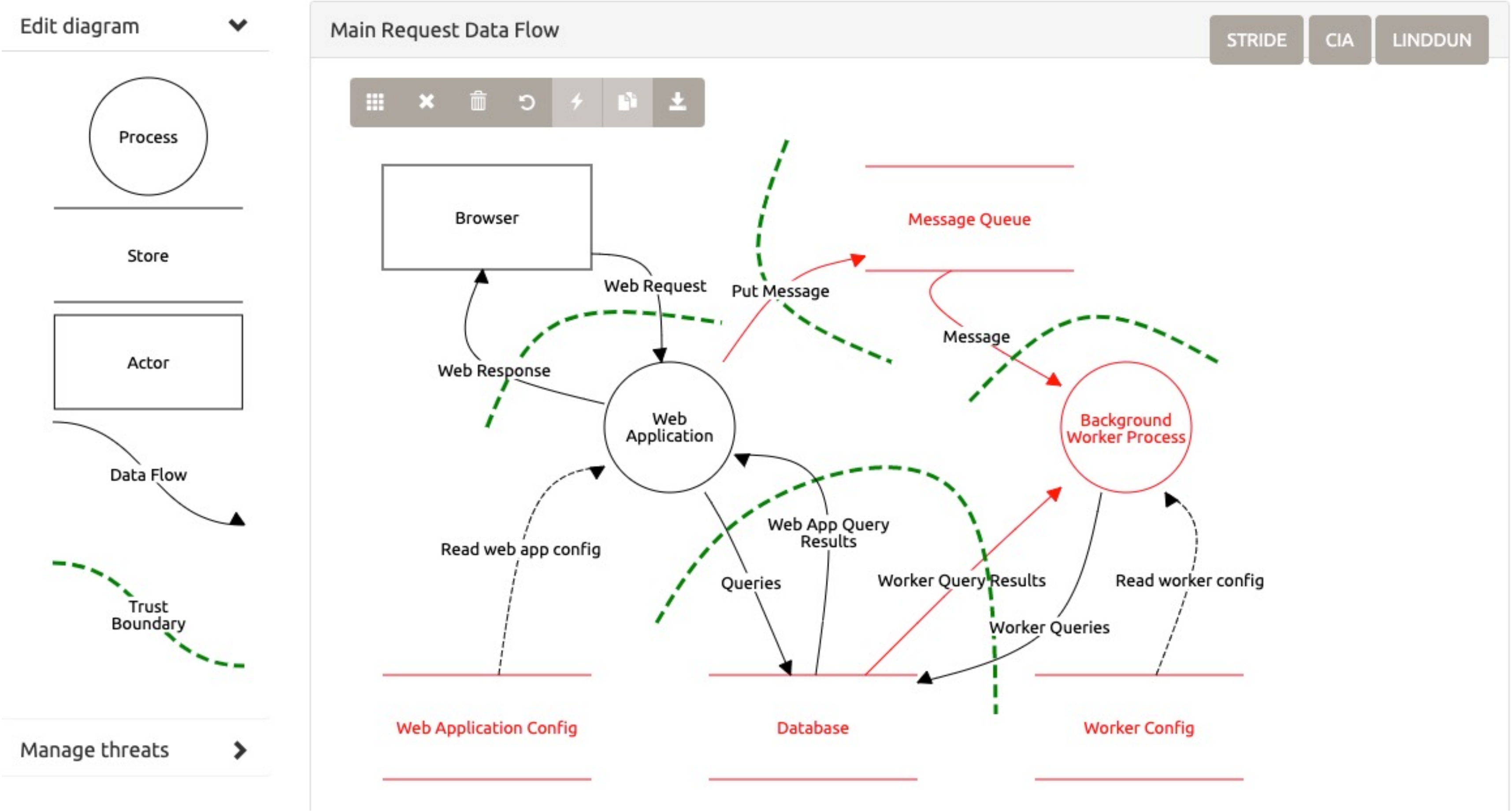
Request to http://sqli.witdemo.net:80 [34.254.142.30]

POST request to /results.php

Type	Name	Value
Body	studentnumber	junk' or '1'='1
Body	submit	submit

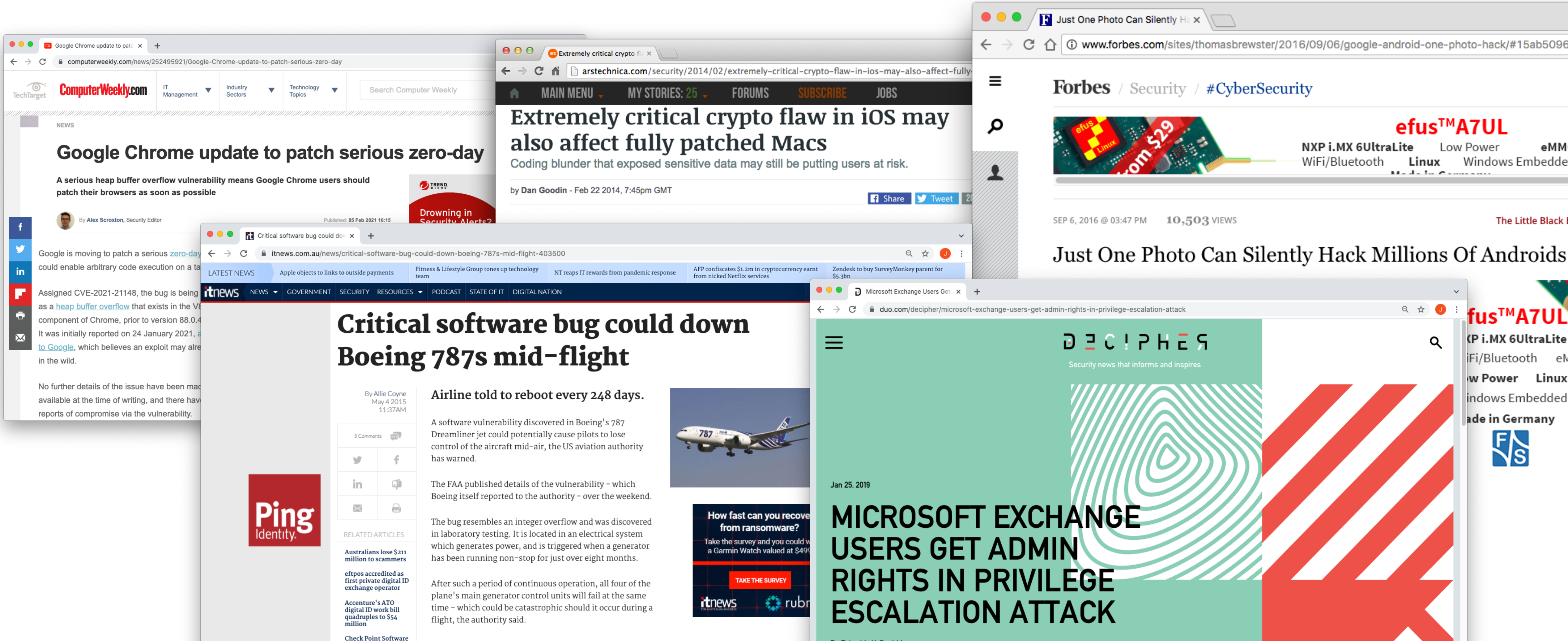
After this module, you should be able to

… do some threat modelling



After this module, you should be able to

… better understand security news (and hype)



computerweekly.com/news/252495921/Google-Chrome-update-to-patch-serious-zero-day

NEWS

Google Chrome update to patch serious zero-day

A serious heap buffer overflow vulnerability means Google Chrome users should patch their browsers as soon as possible

By Alex Scroxton, Security Editor

Published: 05 Feb 2021 16:15

Google is moving to patch a serious zero-day could enable arbitrary code execution on a ta

Assigned CVE-2021-21148, the bug is being as a heap buffer overflow that exists in the V8 component of Chrome, prior to version 88.0.4 It was initially reported on 24 January 2021, a to Google, which believes an exploit may alre in the wild.

No further details of the issue have been mac available at the time of writing, and there hav reports of compromise via the vulnerability.

arstechnica.com/security/2014/02/extremely-critical-crypto-flaw-in-ios-may-also-affect-fully

Extremely critical crypto flaw in iOS may also affect fully patched Macs

Coding blunder that exposed sensitive data may still be putting users at risk.

by Dan Goodin - Feb 22 2014, 7:45pm GMT

www.forbes.com/sites/thomasbrewster/2016/09/06/google-android-one-photo-hack/#15ab5096

Forbes / Security / #CyberSecurity

SEP 6, 2016 @ 03:47 PM 10,503 VIEWS

Just One Photo Can Silently Hack Millions Of Androids

itnews.com.au/news/critical-software-bug-could-down-boeing-787s-mid-flight-403500

LATEST NEWS Apple objects to links to outside payments | Fitness & Lifestyle Group tones up technology team | NT reaps IT rewards from pandemic response | AFP confiscates $1.2m in cryptocurrency earnt from nicked Netflix services | Zendesk to buy SurveyMonkey parent for $5.3bn

Critical software bug could down Boeing 787s mid-flight

By Allie Coyne
May 4 2015
11:37AM

Airline told to reboot every 248 days.

A software vulnerability discovered in Boeing's 787 Dreamliner jet could potentially cause pilots to lose control of the aircraft mid-air, the US aviation authority has warned.

The FAA published details of the vulnerability - which Boeing itself reported to the authority - over the weekend.

The bug resembles an integer overflow and was discovered in laboratory testing. It is located in an electrical system which generates power, and is triggered when a generator has been running non-stop for just over eight months.

After such a period of continuous operation, all four of the plane's main generator control units will fail at the same time - which could be catastrophic should it occur during a flight, the authority said.

RELATED ARTICLES

Australians lose $211 million to scammers

eftpos accredited as first private digital ID exchange operator

Accenture's ATO digital ID work bill quadruples to $54 million

Check Point Software

duo.com/decipher/microsoft-exchange-users-get-admin-rights-in-privilege-escalation-attack

DECIPHER

Security news that informs and inspires

Jan 25, 2019

MICROSOFT EXCHANGE USERS GET ADMIN RIGHTS IN PRIVILEGE ESCALATION ATTACK