# COMP6443 - WEEK 1

## Introduction to Web Security

# WELCOME TO
# COMP6{4,8}43

- 10 weeks, 5 topics across web security, Zoom only.
- 6443 introduces vulnerabilities, focuses on securing code
- 6843 deep dives, focus on breaking applications
- Assessment:
  - 50% Coursework
  - 10% Mid-Semester
  - 40% Final Exam
- Course contact: cs6443@cse.unsw.edu.au

# A NOTE ON ETHICS / LEGALITY

- UNSW hosting this course is an extremely important step forward.
- We expect a high standard of professionalism from you, meaning:
  - Respect the property of others and the university
  - Always abide by the law and university regulations
  - Be considerate of others to ensure everyone has an equal learning experience
  - Always check that you have written permission before performing a security test on a system

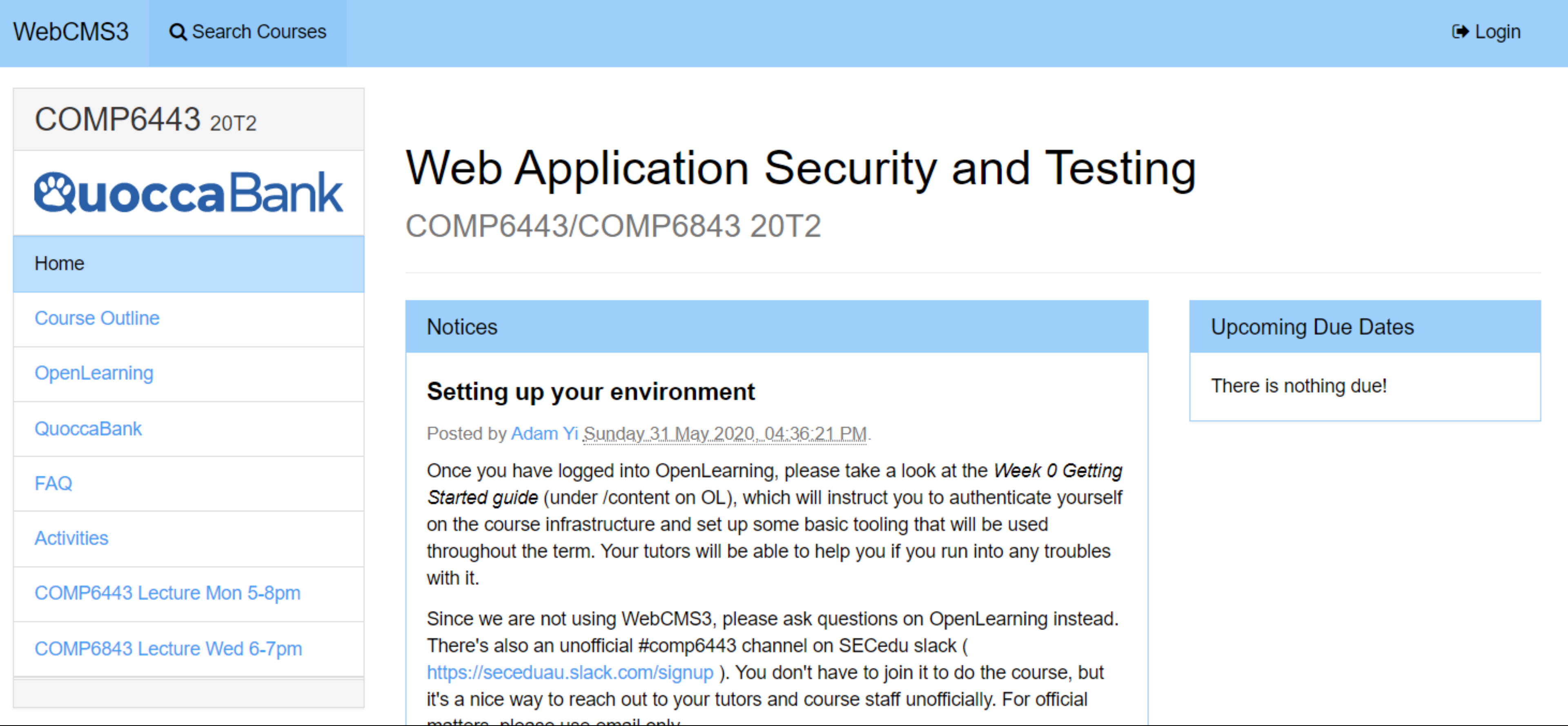
Always err on the side of caution. If you are unsure about anything ask one of the course staff!

# ADMIN – CTFD / FLAGS

- Submit flags on ctfd.quoccabank.com
  - Challenges open at 9:00AM, 02/06
  - Flags -> Marks info is on OpenLearning
- COMP6443 students can submit any COMP6843 flags
  - These become bonus marks, calculated at the end of the course.
- Don’t stress if you can’t find 100% of flags for a week
- Flag submissions are individual

I_FOUND_IT_5f6aecc4af7ad6b6df282a285523245e

(Lectures slides will be available via OpenLearning)



# Web Application Security and Testing

## COMP6443/COMP6843 20T2

### Notices

#### Setting up your environment

Posted by Adam Yi Sunday 31 May 2020, 04:36:21 PM.

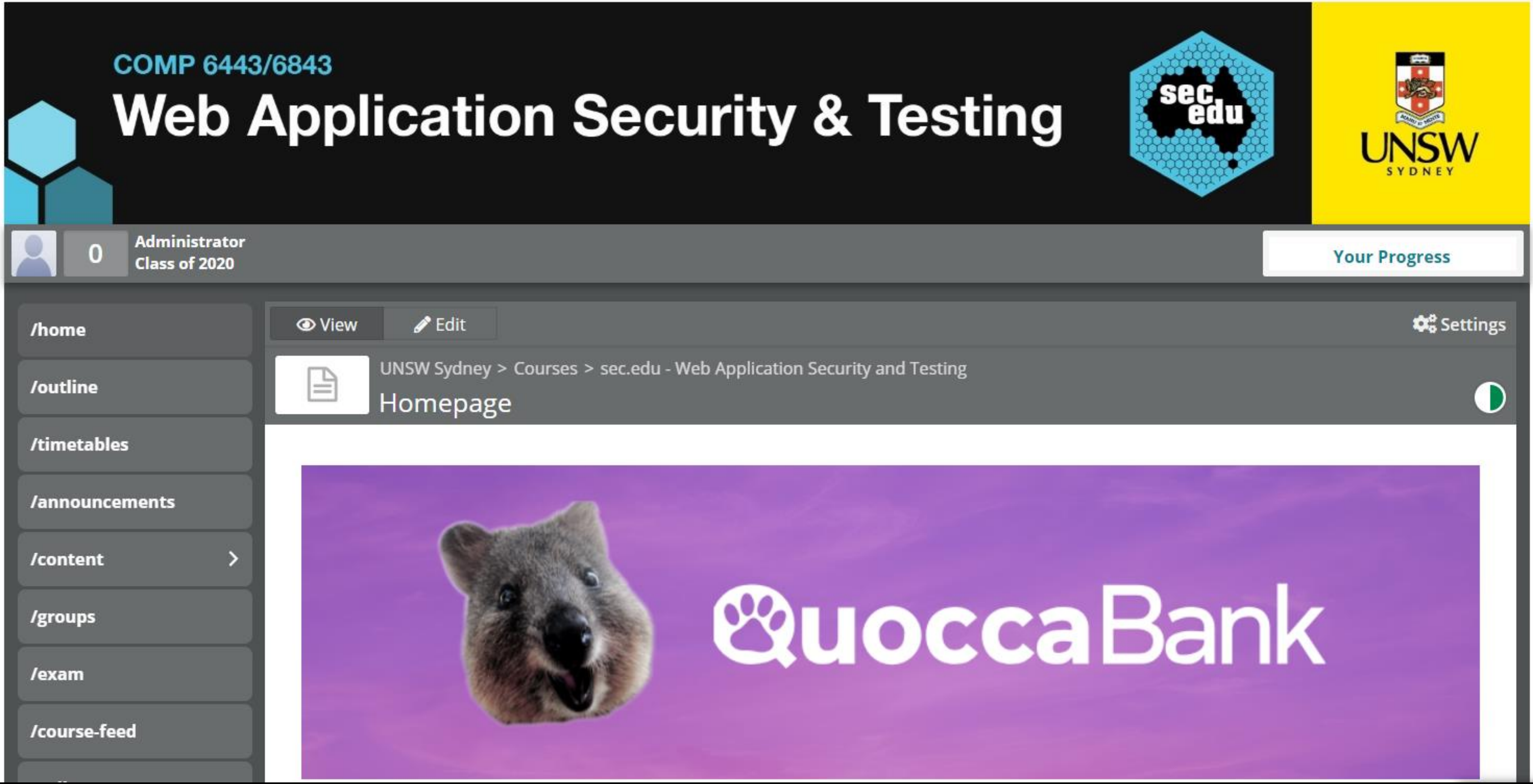
Once you have logged into OpenLearning, please take a look at the *Week 0 Getting Started guide* (under /content on OL), which will instruct you to authenticate yourself on the course infrastructure and set up some basic tooling that will be used throughout the term. Your tutors will be able to help you if you run into any troubles with it.

Since we are not using WebCMS3, please ask questions on OpenLearning instead. There's also an unofficial #comp6443 channel on SECedu slack ( https://seceduau.slack.com/signup ). You don't have to join it to do the course, but it's a nice way to reach out to your tutors and course staff unofficially. For official matters, please use email only.

### Upcoming Due Dates

There is nothing due!

If you're stuck, or can't sign into OpenLearning, please email cs6443@cse.unsw.edu.au



COMP 6443/6843

Web Application Security & Testing

Administrator
Class of 2020

UNSW Sydney > Courses > sec.edu - Web Application Security and Testing

Homepage

# THREAT MODELLING

*Threat modeling is a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized.*

*tl;dr: finding weaknesses and prioritising fixes.*

JEFF J MITCHELL/GETTY IMAGES

How do I attack it?

How do I protect it?

*What can an attacker do within their budget?*

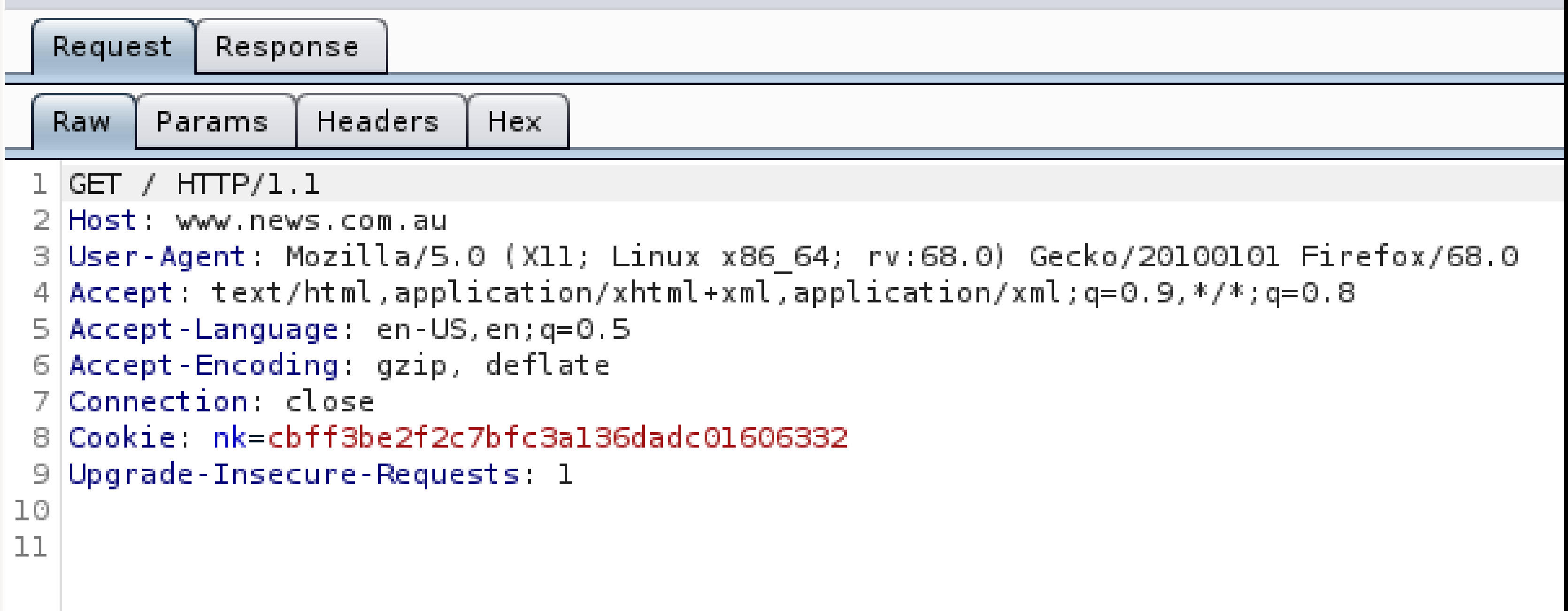
*How likely is an attacker to be caught?*

# HOW2PLAY SECURING SYSTEMS?

USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers
https://www.youtube.com/watch?v=bDJb8WOJYdA

# INTRODUCTION TO THE MODERN WEB

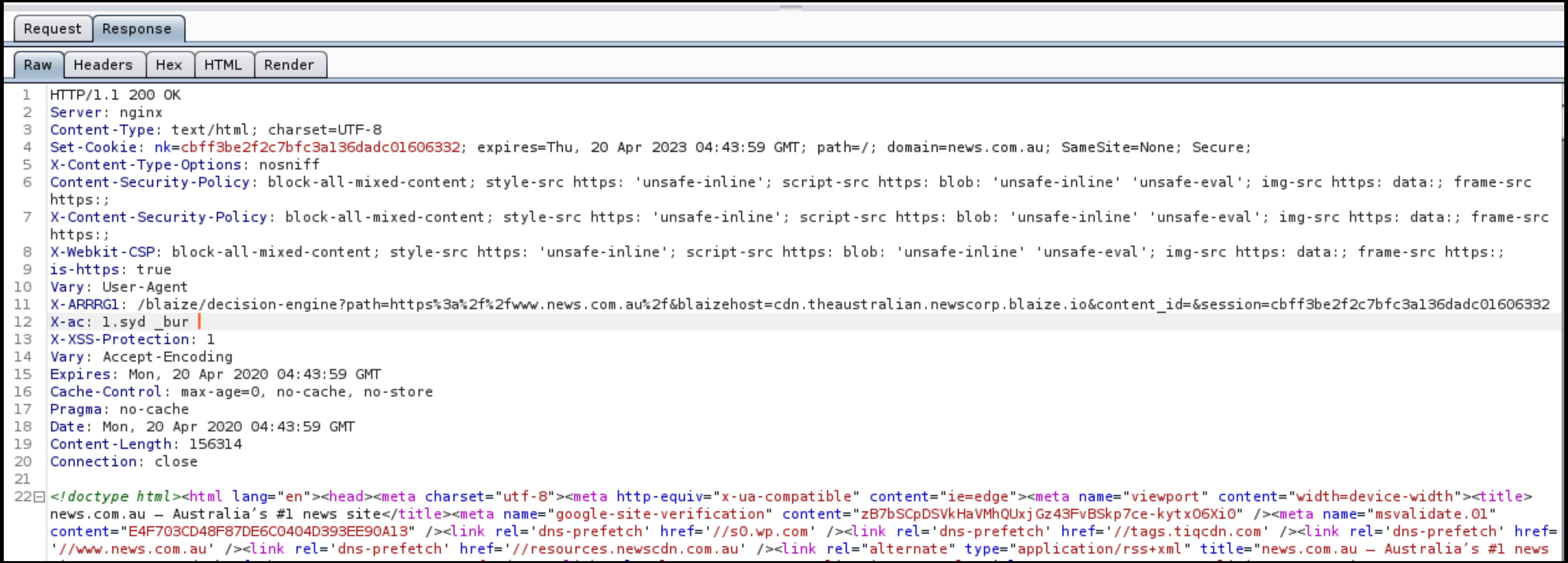
# WHATS IN A WEB REQUEST?



```
GET / HTTP/1.1
Host: www.news.com.au
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: nk=cbff3be2f2c7bfc3a136dadc01606332
Upgrade-Insecure-Requests: 1


```

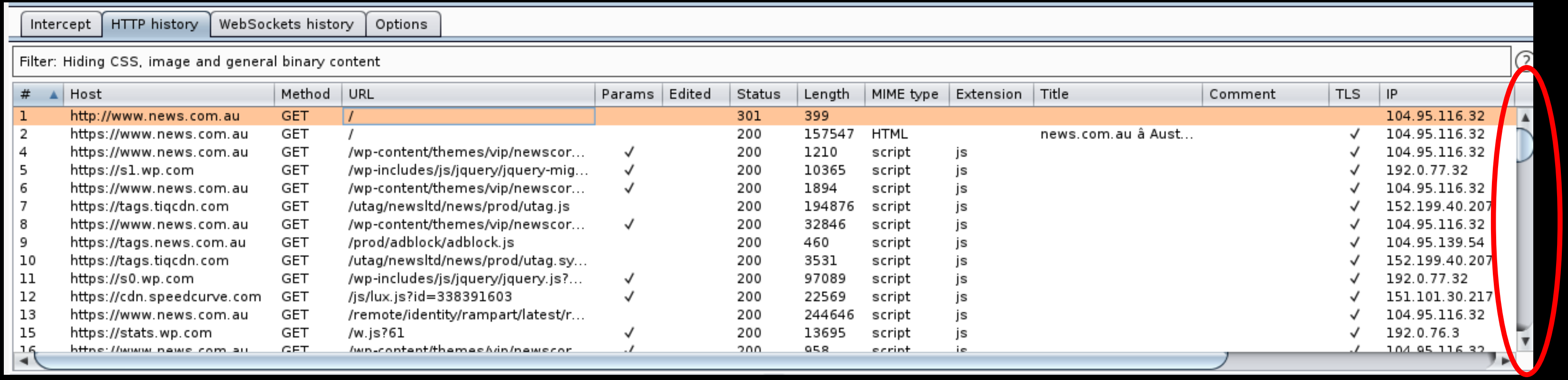
# WHATS IN A WEB REQUEST?



```
HTTP/1.1 200 OK
Server: nginx
Content-Type: text/html; charset=UTF-8
Set-Cookie: nk=cbff3be2f2c7bfc3a136dadc01606332; expires=Thu, 20 Apr 2023 04:43:59 GMT; path=/; domain=news.com.au; SameSite=None; Secure;
X-Content-Type-Options: nosniff
Content-Security-Policy: block-all-mixed-content; style-src https: 'unsafe-inline'; script-src https: blob: 'unsafe-inline' 'unsafe-eval'; img-src https: data:; frame-src https:;
X-Content-Security-Policy: block-all-mixed-content; style-src https: 'unsafe-inline'; script-src https: blob: 'unsafe-inline' 'unsafe-eval'; img-src https: data:; frame-src https:;
X-Webkit-CSP: block-all-mixed-content; style-src https: 'unsafe-inline'; script-src https: blob: 'unsafe-inline' 'unsafe-eval'; img-src https: data:; frame-src https:;
is-https: true
Vary: User-Agent
X-ARRRG1: /blaize/decision-engine?path=https%3a%2f%2fwww.news.com.au%2f&blaizehost=cdn.theaustralian.newscorp.blaize.io&content_id=&session=cbff3be2f2c7bfc3a136dadc01606332
X-ac: 1.syd _bur
X-XSS-Protection: 1
Vary: Accept-Encoding
Expires: Mon, 20 Apr 2020 04:43:59 GMT
Cache-Control: max-age=0, no-cache, no-store
Pragma: no-cache
Date: Mon, 20 Apr 2020 04:43:59 GMT
Content-Length: 156314
Connection: close

<!doctype html><html lang="en"><head><meta charset="utf-8"><meta http-equiv="x-ua-compatible" content="ie=edge"><meta name="viewport" content="width=device-width"><title>news.com.au — Australia’s #1 news site</title><meta name="google-site-verification" content="zB7bSCpDSVkHaVMhQUxjGz43FvBSkp7ce-kytxO6Xi0" /><meta name="msvalidate.01" content="E4F703CD48F87DE6C0404D393EE90A13" /><link rel='dns-prefetch' href='//s0.wp.com' /><link rel='dns-prefetch' href='//tags.tiqcdn.com' /><link rel='dns-prefetch' href='//www.news.com.au' /><link rel='dns-prefetch' href='//resources.newscdn.com.au' /><link rel="alternate" type="application/rss+xml" title="news.com.au — Australia’s #1 news
```

# WHATS IN A WEB REQUEST?



Filter: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status | Length | MIME type | Extension | Title | Comment | TLS | IP |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | http://www.news.com.au | GET | / | | | 301 | 399 | | | | | | 104.95.116.32 |
| 2 | https://www.news.com.au | GET | / | | | 200 | 157547 | HTML | | news.com.au â Aust... | | ✓ | 104.95.116.32 |
| 4 | https://www.news.com.au | GET | /wp-content/themes/vip/newscor... | ✓ | | 200 | 1210 | script | js | | | ✓ | 104.95.116.32 |
| 5 | https://s1.wp.com | GET | /wp-includes/js/jquery/jquery-mig... | ✓ | | 200 | 10365 | script | js | | | ✓ | 192.0.77.32 |
| 6 | https://www.news.com.au | GET | /wp-content/themes/vip/newscor... | ✓ | | 200 | 1894 | script | js | | | ✓ | 104.95.116.32 |
| 7 | https://tags.tiqcdn.com | GET | /utag/newsltd/news/prod/utag.js | | | 200 | 194876 | script | js | | | ✓ | 152.199.40.207 |
| 8 | https://www.news.com.au | GET | /wp-content/themes/vip/newscor... | ✓ | | 200 | 32846 | script | js | | | ✓ | 104.95.116.32 |
| 9 | https://tags.news.com.au | GET | /prod/adblock/adblock.js | | | 200 | 460 | script | js | | | ✓ | 104.95.139.54 |
| 10 | https://tags.tiqcdn.com | GET | /utag/newsltd/news/prod/utag.sy... | | | 200 | 3531 | script | js | | | ✓ | 152.199.40.207 |
| 11 | https://s0.wp.com | GET | /wp-includes/js/jquery/jquery.js?... | ✓ | | 200 | 97089 | script | js | | | ✓ | 192.0.77.32 |
| 12 | https://cdn.speedcurve.com | GET | /js/lux.js?id=338391603 | ✓ | | 200 | 22569 | script | js | | | ✓ | 151.101.30.217 |
| 13 | https://www.news.com.au | GET | /remote/identity/rampart/latest/r... | | | 200 | 244646 | script | js | | | ✓ | 104.95.116.32 |
| 15 | https://stats.wp.com | GET | /w.js?61 | ✓ | | 200 | 13695 | script | js | | | ✓ | 192.0.76.3 |
| 16 | https://www.news.com.au | GET | /wp-content/themes/vip/newscor... | ✓ | | 200 | 958 | script | js | | | ✓ | 104.95.116.32 |

????

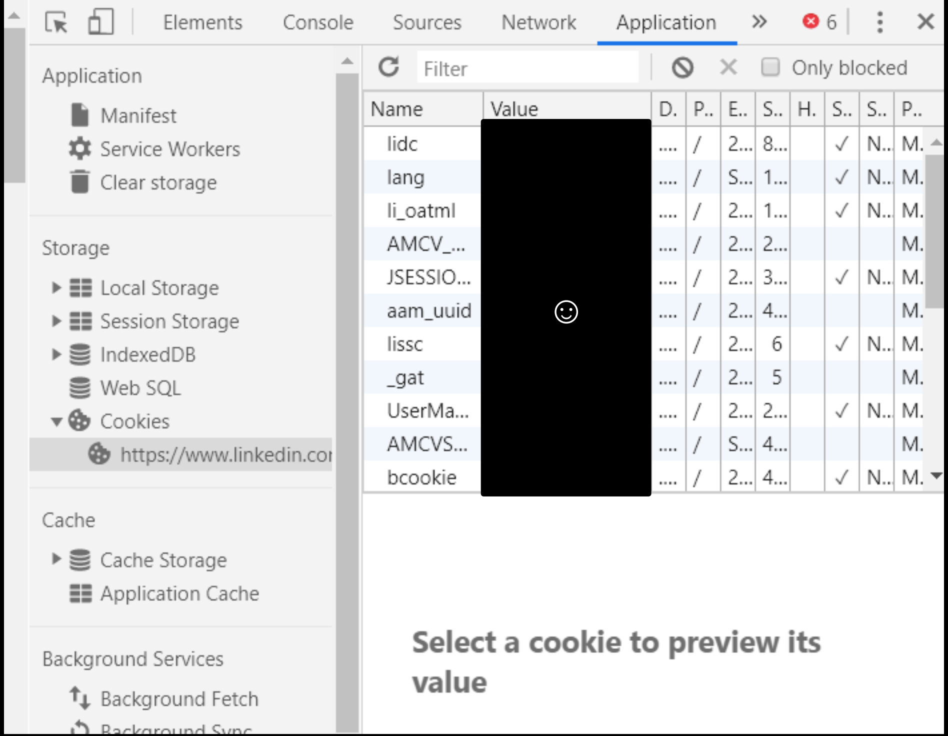
Interesting reading: https://www.iacr.org/tinfoil.html

Challenge: turn off JavaScript by default for a week. What do you notice?

# FUN FACT: LOGOUT DOES NOTHING

Step 1: Log in to linkedin.com
Step 2: Note down your cookies
Step 3: Log out of linkedin.com
Step 4: ????

Do not trust, verify.
Particularly if it’s free.



| Name | Value | D. | P.. | E.. | S.. | H. | S.. | S.. | P.. |
|---|---|---|---|---|---|---|---|---|---|
| lidc | [redacted] | .... | / | 2... | 8... |  | ✓ | N... | M. |
| lang | [redacted] | .... | / | S... | 1... |  | ✓ | N... | M. |
| li_oatml | [redacted] | .... | / | 2... | 1... |  | ✓ | N... | M. |
| AMCV_... | [redacted] | .... | / | 2... | 2... |  |  |  | M. |
| JSESSIO... | [redacted] | .... | / | 2... | 3... |  | ✓ | N... | M. |
| aam_uuid | [redacted] | .... | / | 2... | 4... |  |  |  | M. |
| lissc | [redacted] | .... | / | 2... | 6 |  | ✓ | N... | M. |
| _gat | [redacted] | .... | / | 2... | 5 |  |  |  | M. |
| UserMa... | [redacted] | .... | / | 2... | 2... |  | ✓ | N... | M. |
| AMCVS... | [redacted] | .... | / | S... | 4... |  |  |  | M. |
| bcookie | [redacted] | .... | / | 2... | 4... |  | ✓ | N... | M. |

Select a cookie to preview its value

# RECON

“Yeah that’s a legacy system we have to keep it on that version for compatibility”

Firewall

Status: On

Incoming: Deny

Outgoing: Allow

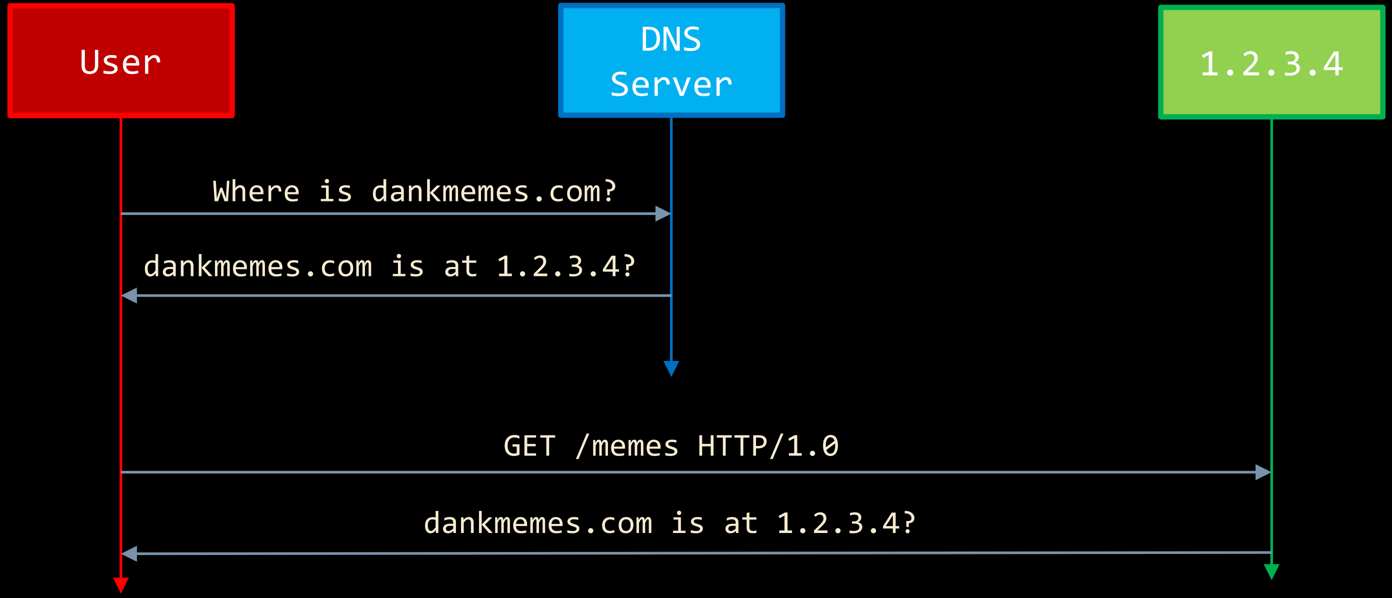
Rules

| To | Action | From |
|---|---|---|
| 51413/tcp | ALLOW IN | Anywhere |
| 51413/udp | ALLOW IN | Anywhere |

“Oh wow, that system is still up?”

“Sorry we’re not responsible for Marketing systems, go talk to <X>”

# INTRO TO DNS


User
DNS Server
1.2.3.4
Where is dankmemes.com?
dankmemes.com is at 1.2.3.4?
GET /memes HTTP/1.0
dankmemes.com is at 1.2.3.4?

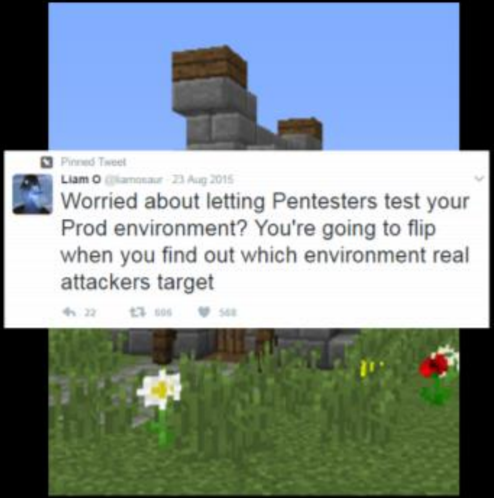
www.website.com

shop.website.com

blog.website.com

stage.website.com

db.website.com



Pinned Tweet

Liam O @liamosaur · 23 Aug 2015

Worried about letting Pentesters test your Prod environment? You're going to flip when you find out which environment real attackers target

22 606 568

api.website.com

dev.website.com

backup-syd.website.com

archive.website.com

s3 Buckets

github

pastebin

third party providers

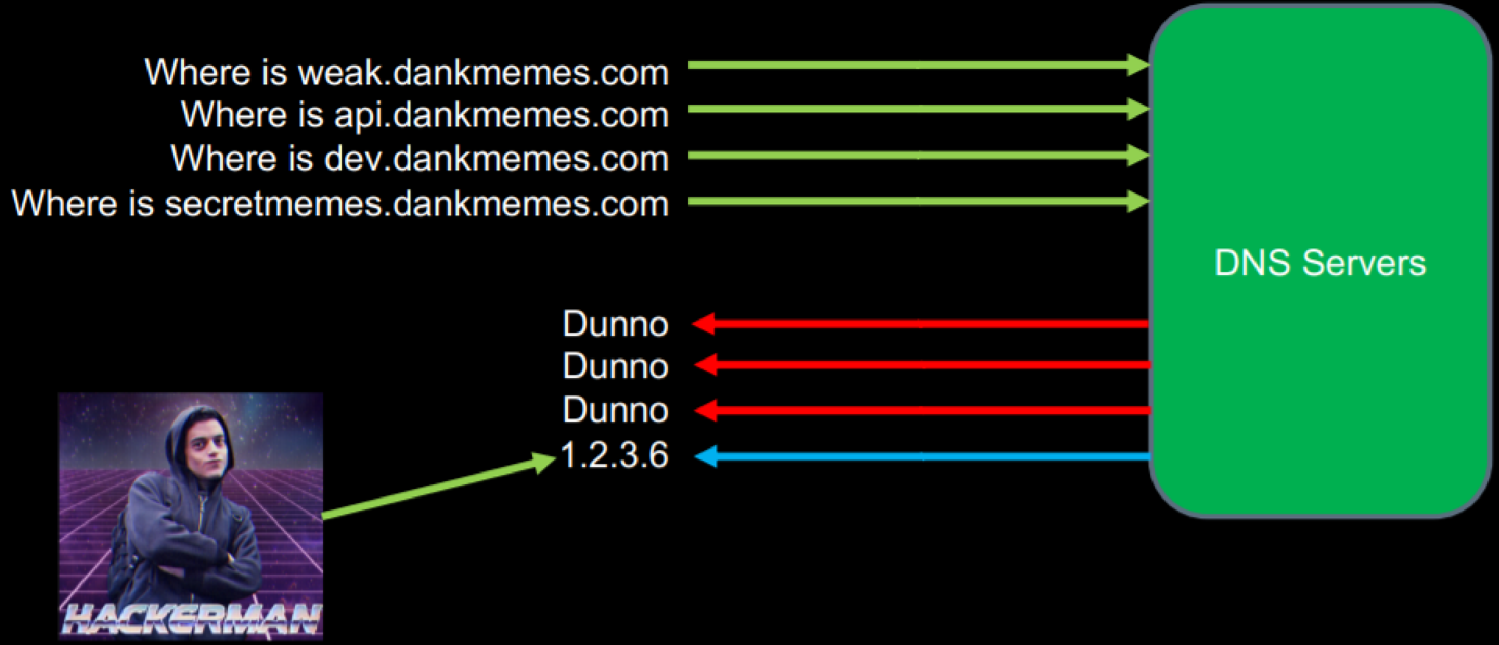
mobile applications

analytics

etc etc…

# SUBDOMAINS

## via brute forcing



Where is weak.dankmemes.com
Where is api.dankmemes.com
Where is dev.dankmemes.com
Where is secretmemes.dankmemes.com

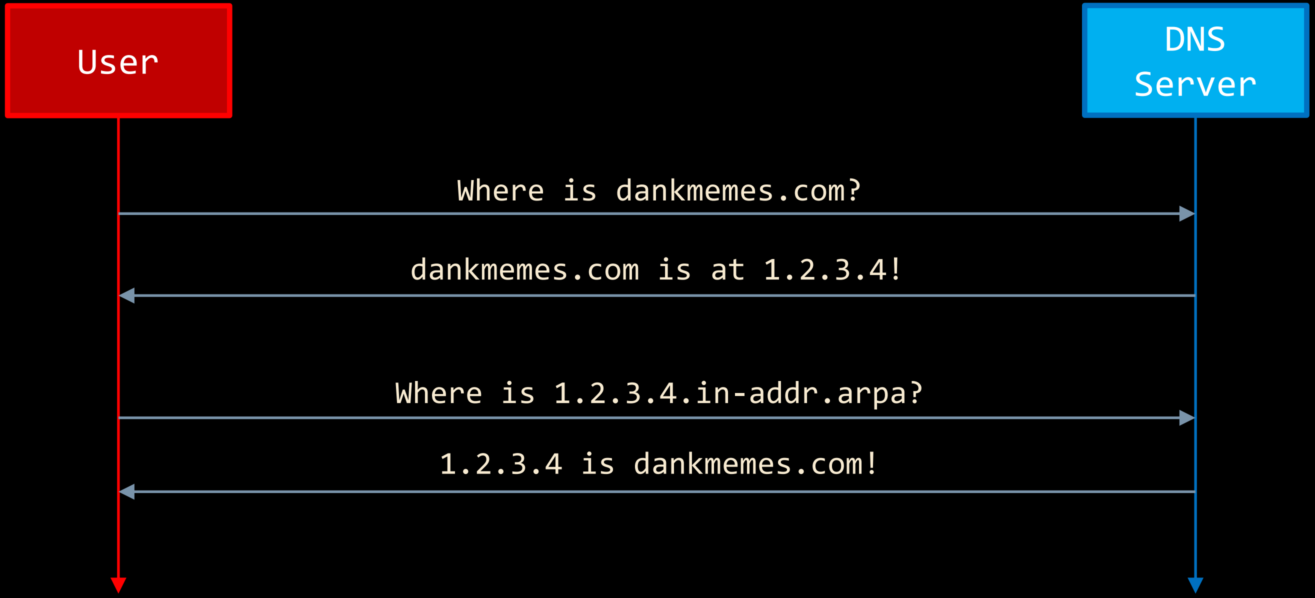
DNS Servers

Dunno
Dunno
Dunno
1.2.3.6

Q: what generates trust in our DNS infrastructure?

# SUBDOMAINS

## via reverse ip



User
DNS Server
Where is dankmemes.com?
dankmemes.com is at 1.2.3.4!
Where is 1.2.3.4.in-addr.arpa?
1.2.3.4 is dankmemes.com!

# SUBDOMAINS

## via search engines

- Web Searches
  - inurl:, filetype: to identify low-hanging fruit
  - web.archive.org
- Domain Searches
  - https://dnsdumpster.com/
  - https://hackertarget.com/ip-tools/
- Certificates
  - crt.sh
  - Domains from shared certs

Intuition is sometimes better than tools. Always manually look at the applications and get a feel for their functionality.

# 1:N / VHOSTS

demo

# ENUMERATING CONTENT

Active: tries millions of combinations of words / characters

- dirb
- dirbuster
- gobuster
- fierce.pl

Passive: watches for new URL’s as you browse a website

- Burpsuite
- LinkFinder
- lots of open source alternatives

Write your own tools.

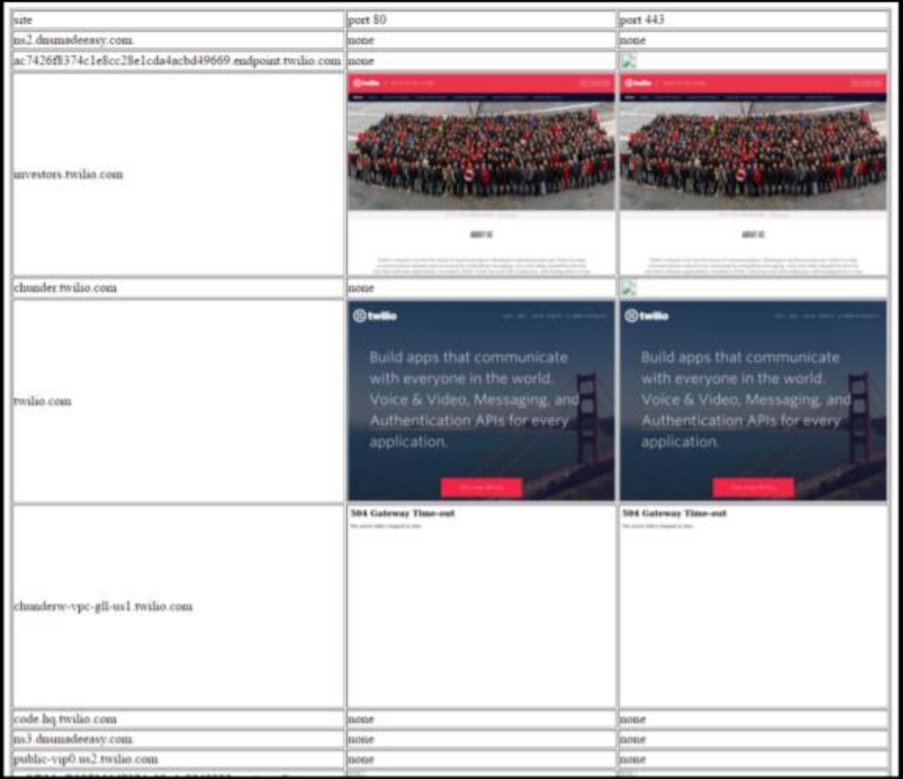
# CONTENT ENUMERATION

demo

# ENUMERATION PROTIPS

- Localisation (by a different developer)
- Technology-specific things
  - Wordpress/Drupal Admin, Themes
  - Build a set of working exploits?
- Databases / Data Stores (e.g. s3 buckets)
- Legacy applications
- Mismatched technology stacks
- What else can you think of?

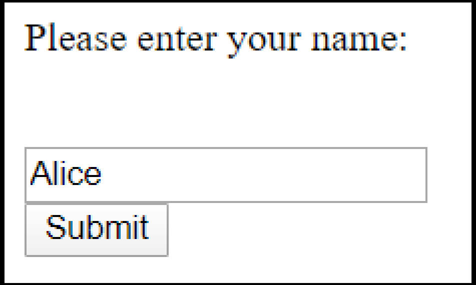
# USING INTUITION



| site | port 80 | port 443 |
|---|---|---|
| ns2.dnsmadeeasy.com. | none | none |
| ac7426f8374c1e8cc28e1cda4acbd49669.endpoint.twilio.com | none | |
| investors.twilio.com | ABOUT US | ABOUT US |
| chunder.twilio.com | none | |
| twilio.com | Build apps that communicate with everyone in the world. Voice & Video, Messaging, and Authentication APIs for every application. | Build apps that communicate with everyone in the world. Voice & Video, Messaging, and Authentication APIs for every application. |
| chunderw-vpc-gll-us1.twilio.com | 504 Gateway Time-out | 504 Gateway Time-out |
| code.hq.twilio.com | none | none |
| ns3.dnsmadeeasy.com. | none | none |
| public-vip0.us2.twilio.com | none | none |

# NEGATIVE USE CASES

Vulnerabilities arise when assumptions are challenged.



Please enter your name:

Alice

Other excellent names:

- Null byte
- Newline
- XML/JSON/SQL
- OS Commands
- Backticks (Unix)
- Large/small names
- Strange character sets
- ...

# WEB SECURITY “SNIFF TEST”

This is not a definitive test of if a website is safe. It’s a test of whether a website makes any attempt to handle unexpected input.

```
‘”>1#--;`wget blah`\x00\nabc
```

Does the HTML Layout break? You may have cross-site scripting.
Do you get a database error? You may have SQL Injection.
Does your callback get pinged? Congratulations, assume it’s compromised.

(Make sure to use a proxy – browsers may modify your request)

# SECURING THE PERIMETER

- Fix the low-hanging fruit first:
  - Delete content that isn't necessary.
  - Restrict access to non-hardened content.
  - Test your applications, fix the bugs.
- Change user behaviour:
  - Use secure passwords (admin:admin is not ok).
  - Patch your environment.
- BeyondCorp https://cloud.google.com/beyondcorp/

Never blame users for unintentional / uninformed failure.

# HANDLING ERRORS

On a public network, what should be the response to a TCP SYN on a closed port?

# WEEK 1 ASSESSMENT

- Watch https://www.youtube.com/watch?v=bDJb8WOJYdA
- Are you able to enumerate the subdomains of the domain “quoccabank.com”? What applications can you find?
- Can you find a flag on kb.quoccabank.com? You’ll need to use haas.quoccabank.com to submit the request.
- Due date is Sunday 7:00pm.

Please call out if you get stuck.
Support one another, your tutors are here to help!

THANKS FOR LISTENING TO US RANT!

questions? email / openlearning