A Hacker's View of Data Breaches

PRIVSECCONSULTING

About me

HOMES.CO.NZ

PRIVSECCONSULTING

About me

- Senior Security Consultant at PrivSec Consulting
  - I hack things
- Former software developer
  - Sorry if you've ever had to use something I've made
- Helps organise ISIG - Information Security Interest Group, last Thursday of every month.
- Active security researcher (I hack things in my spare time):
  - Multiple CVEs (Common Vulnerability and Exposure, aka a 'known and widespread security vulnerability') in:
    - Blackboard, Kramer, Moodle, Outlook, Visual Studio, Excel, Word
    - I think the MSRC (Microsoft Security Response Center) are sick of me
- Frequent flyer with CERT: the real MVP of cybersecurity in Aotearoa. They aren't sick of me. Hi Herve!
- Don't ask me about council software

PRIVSECCONSULTING

This website is one curious hacker away from a major breach

Some things we will look at relating to how privacy and information security interact – specifically around Principle 5 of the 2020 Privacy Act:

- OWASP Top Ten
- Access Control
- Broken access control
- Injection attacks
- Security Misconfigurations
- Nothing ever disappears from the internet
- What you can do
- What do you do if you Find Something On The Internet
- A lot of what we talk about are really simple hacks and techniques that can have really impactful outcomes

PRIVSECCONSULTING

Some definitions

- OWASP: Open Web Application Security Project
- Has a top ten most common web application vulnerabilities,
  - Broken Access Controls
  - Cryptographic failures
  - Injection
  - Software and data integrity
  - etc
- Privacy Act 2020:
  - Replaced the 1993 Privacy Act
  - Designed to strengthen privacy protections
  - Now has:
    - Requirements around reporting breaches
    - Criminal offences
    - The Commissioner can now issue compliance notices
  - Has 13 principles
  - No 5 is "Security and storage of information"

PRIVSECCONSULTING

Some more definitions

- Data breach
  - Help someone has stolen data
- Confidentiality breach
  - Help someone has stolen secret data
- Privacy breach
  - Help someone has stolen personal data

PRIVSECCONSULTING

Disclaimer

- Some of the techniques you will see are illegal, unless:
  - You have prior consent from the website owner
  - You are participating in a bug bounty program
  - You are practicing in a lab environment
- Please don't do crimes!

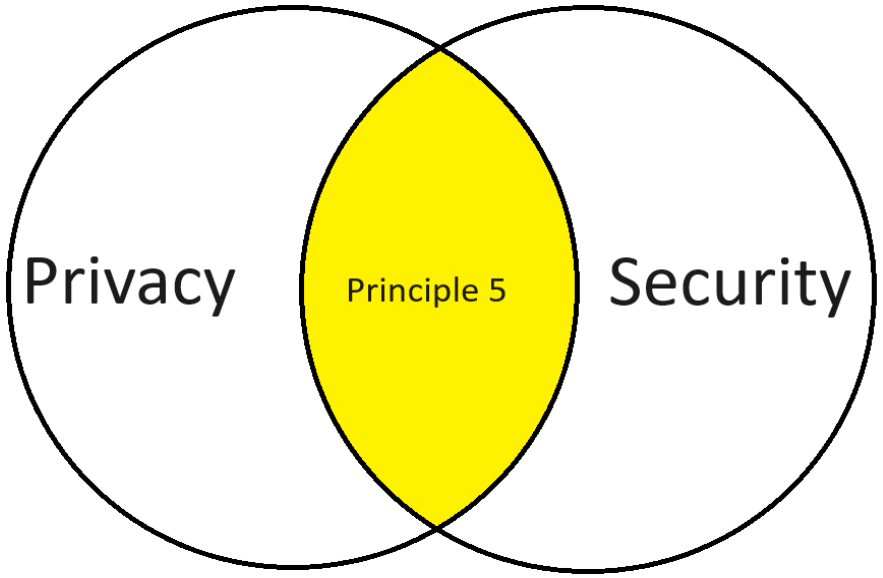
PRIVSECCONSULTING

The guardrails!

PRIVSECCONSULTING

Principle #5

- Don't lose it, misuse it or disclose it!
- An agency that holds personal information must ensure:
  - That the information is protected by such security safeguards as are reasonable in the circumstances to take, against:
    - Loss; and
    - Access, use, modification, disclosure that is not authorised by the agency; and
    - Other misuse



PRIVSECCONSULTING

The OWASP top ten

- Key vulnerability classes which may lead to a security breach
- Not all relate to privacy and data breaches, but a lot do:
  - Broken access control
  - Injection
  - Insecure Design
  - Logging and monitoring failure

PRIVSECCONSULTING

Access control

- What or who can use or otherwise modify a thing in a computing environment
- Sometimes access control is role based (Administrator, SuperAdmin, low privilege user, guest)
- Sometimes things are open by default
- Sometimes things are deny by default
- Varies a lot in complexity depending on the system

PRIVSECCONSULTING

Broken Access Control: A01

- 94% of applications that OWASP have tested have had some form of broken access control
- Ok, so what is it?
- It can be as simple as changing the number in a URL by one
- Or more complex, such as data tampering of an authentication mechanism such as a JWT (JSON Web Token)
- Able to browse to restricted pages as a low privilege user
- Able to update data or retrieve data of another user *cough* OPTUS *cough*

PRIVSECCONSULTING

Broken access control: in the wild

- Former colleague wanted to rent a car
- Signed up, submitted documents (driver's license, Personal Information)
- They were emailed a link to their documents
- They noticed that the URL took the following form
- Nice integer, it would be a shame if someone was to increment it

https://s3.nameofrental.com/documents/11278

PRIVSECCONSULTING

Broken Access Control: In the wild (part 2)

- Came across a client doing large amounts of document processing
- Found a link to a document using a tool called GAU (Get All URLs)
  - More on that later
- Documents were random GUIDs (good! Less guessable)
    - 6B29FC40-CA47-1067-B31D-00DD010662DA
- Clicked on the document
- Was asked for a pin number. A security control!

PRIVSECCONSULTING

Broken Access Control: In the wild (part 2)

- Entered PIN
- A session cookie was generated (a set of characters that the browser sends to let me access things)
- I found part of the website that took integers (1,2,3,4) and my new session cookie
- No access control.
- Computers can count up very fast:
  - So I did
- Half a million documents (passports, contracts, driver's licenses)
- Went back 5+ years
- Called the client straight away
- They fixed within a few days
- Not sure what their data retention policy was..

PRIVSECCONSULTING

Broken Access Control: In the wild (part 3)

- I was a software developer at Homes.co.nz
- (sorry for helping to break the property market)
- I clicked 'inspect element' on the page and enabled a button
- I then realised I could update a property that was claimed by someone else
- Fixed the same day, whoops.
- Similar techniques (with slightly flasher tooling) can be used to escalate privileges
- I escalated from a low privilege user to an administrator on a job yesterday using a version of this.
- The admin role has access to all the data.

PRIVSECCONSULTING

A well-known one that actually happened: Optus

- September 2022
- Names, addresses, dates of birth, passports, drivers' licenses
- 10 million people – approximately a third of Australia
- Was an 'insecure API':
  - Allowed for incrementing integers
  - Ten million network requests doesn't take that long
- Optus apologised and put aside $140 million AUD
  - "sorry"

PRIVSECCONSULTING

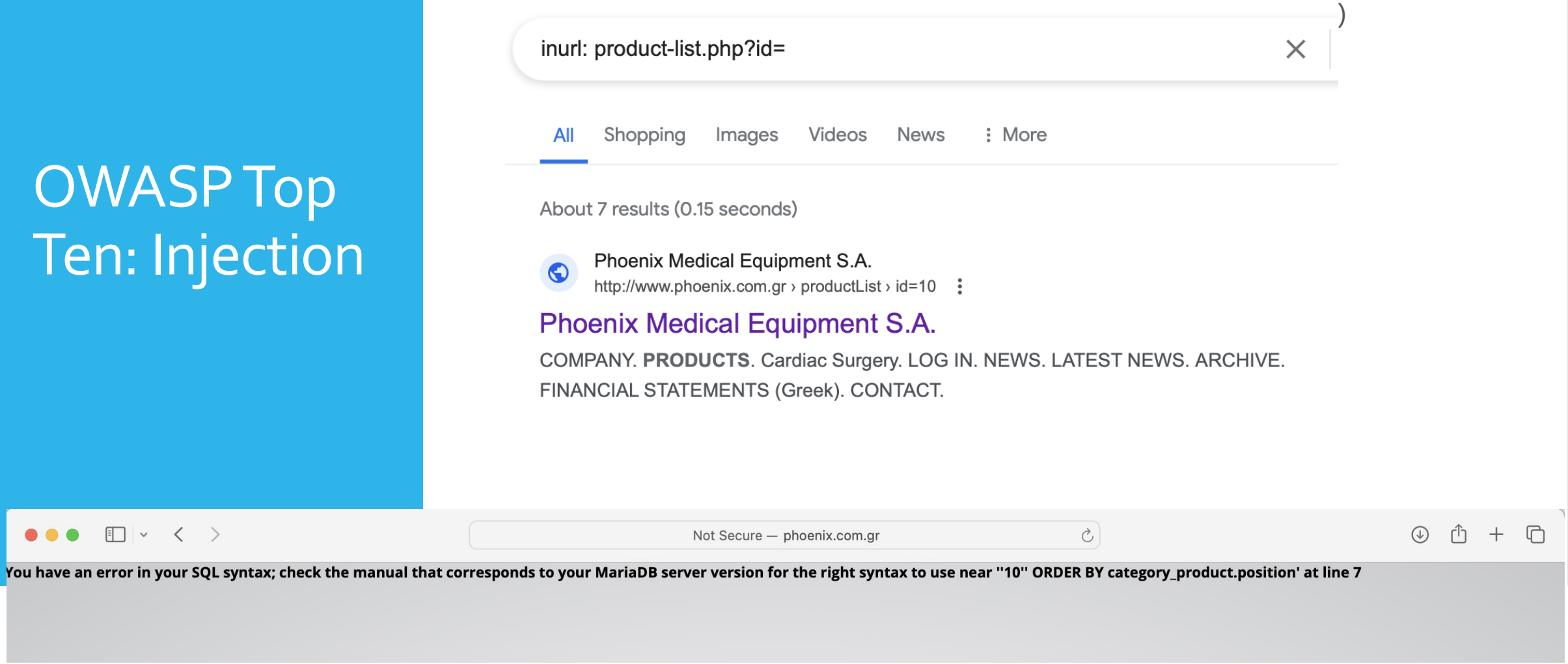
OWASP Top Ten – Injection: A03

- Injection attacks can happen whenever untrusted client data (i.e what you enter in your browser) makes it somewhere bad like a database and is not filtered or sanitised.
- Can be interpreted by the database and a user can issue their own instructions
- Most common is SQL – Structured Query Language Injection
  - A programming language used to talk to Relational Databases
- Some famous ones in recent years:
  - Equifax: Credit reporting agency
  - 143 million users
  - Issues were disclosed by security researchers six months previously (including access control issues) allowing for retrieving other people's information
- Some of this talk was written while waiting for a database to finish dumping

PRIVSECCONSULTING

OWASP Top Ten: Injection

- I mean, this is low hanging fruit, but SQL injection is easily found through google dorking.
- Sometimes found through a simple single quote, which breaks the SQL statement



Injection in the wild:

- I was working on a payments and rates application for a client
- Brand new web application
- Found SQL injection
- Error based (allows for fast extraction)
- Very easy to find
- It was in a preproduction state – they were able to fix the issue before deploying to production/releasing

PRIVSECCONSULTING

Data breaches lead to other data breaches: Credential Stuffing

- When I first started in cybersecurity, we had access to multiple data breach output
- We mostly used it to check whether clients had been caught up in data breaches and whether they were reusing credentials
- I made the mistake of looking up my parents
- Have you ever heard the term password child?
- My Mum had my brother's name
- My Dad had the dog

PRIVSECCONSULTING


when you find out that your
brother is the password child for your mum
and your dad used the dogs name
imgflip.com

Data breaches lead to other data breaches: Credential Stuffing

- Credential stuffing:
  - A lot of people reuse passwords between sites
  - If you're caught up in one breach, your password may be used to access other sites
- 23 and Me suffered a data breach in 2023
- Approximately 14,000 accounts were accessed using credential stuffing from other breaches
- The design of the site and a permissive sharing model meant that records of several million people were compromised

PRIVSECCONSULTING

How can you influence good practice?

- The SDLC (Software Development Life Cycle) is a good place to start
  - Software has things like 'acceptance criteria' before a feature can be made
- If you're doing agile, the idea of a use case implies the existence of a misuse case
- Create both!
- Have privacy based use cases:
  - What is the minimum subset of data you can take
  - Where are you going to store it?
  - How long are you going to keep it for?
  - Who can view it
- Capture privacy and security in user stories and unit tests

PRIVSECCONSULTING

When is a normally low severity bug not

- Username enumeration:
  - Disclosing the existence of a user either through a 'Forgot Password' form error message or similar
  - Generally a low finding, however can be catastrophic
    - What about in a Justice witness or Jury application?
    - Suddenly knowing if a user exists somewhere is a much worse deal
- In 2015 a software engineer figured out that they could send an imessage to an MP using iMessage
- IMessage lets you know if something is delivered
- Eventually MPs figured out how to delink their aph.govt.au email addresses from their phones, after a lot of harassment and abuse

Greg Hunt reportedly sent this message to someone messaging him.
BUZZFEED / FAIRFAX MEDIA GRAPHICS

PRIVSECCONSULTING

Nothing ever disappears from the internet

- A common thing for accounting software to do is to enable people to share links to invoices
- This is by design! You shouldn't have to log in to view an invoice (good)
- Some of the privacy and security controls involve using either a GUID (Globally Unique Identifier) or a UUID (Universally Unique Identifier) to try an prevent brute-forcing of URLs (good!)
- So far so good, they're essentially unguessable
- Have you ever noticed that Google Chrome and other browsers essentially try and cache everything they come across?

PRIVSECCONSULTING

Nothing ever disappears from the internet #2

- Tools such as GAU (Get All Urls) exist to find these
  - Searches a heap of places
  - Archive.org, wayback machine, Open Threat Exchange
  - If you feed the tool a URL such as in.xero.com, or connect.intuit.com…you can suddenly see a host of invoices and companies and data
  - Could then use this information in more targeted attacks

PRIVSECCONSULTING

https://connect.intuit.com/pay/BABCNE/scs-v1-6905d46c0d904852a3eaf7ae0f3051e21c999d2117b4408a84c40a99c31988d1f9d74537ed451bb090d8120fa017bc
https://connect.intuit.com/pay/BABCNE/scs-v1-6905d46c0d904852a3eaf7ae0f3051e21c999d2117b4408a84c40a99c31988d1f9d74537ed451bb090d8120fa017bc?locale=EN_US&fbclid=IwAR2vcVmtGncOeX4qiRhDBHrSZqBIn6kwx1LY_a-SHBAhJeRST4Ho2nBIvno
https://connect.intuit.com/pay/BABCNE/scs-v1-6905d46c0d904852a3eaf7ae0f3051e21c999d2117b4408a84c40a99c31988d1f9d74537ed451bb090d8120fa017bc?locale=EN_US
https://connect.intuit.com/pay/BABCNE/scs-v1-b2653303b3c546aeb19ee60baa7b9f7df2f81456878b4ca99bcdd9b7cab6c36c9559d3f4434474b209240719c9e344
https://connect.intuit.com/pay/BABCNE/scs-v1-b2653303b3c546aeb19ee60baa7b9f7df2f81456878b4ca99bcdd9b7cab6c36c9559d3f4434474b209240719c9e344?locale=EN_US&fbclid=IwAR0aWlD0aVcSNNcddqXkmBzt2hZb2zpvaeXkEOQ2mQmYRfqL2k26gue5kIM
https://connect.intuit.com/pay/BABCNE/scs-v1-b2653303b3c546aeb19ee60baa7b9f7df2f81456878b4ca99bcdd9b7cab6c36c9559d3f4434474b209240719c9e344?locale=EN_US
https://connect.intuit.com/pay/BassettSociety/scs-v1-8da5945a0d6a43a6ba3a4adfd01298305cb6f24300724284a20e7cfae955682da4cf5f5fb74eccaa64a2e1fd62fda6?locale=EN_US
https://connect.intuit.com/pay/BassettSociety/scs-v1-afef63315ea04fea948622d1f4065066d4a6d053f1ed49d3a3a3362417de1d75b07a1526fa4bffb34b5f5d8f034087?locale=EN_US
https://connect.intuit.com/pay/BossKeeperPR/scs-v1-46886fa735994969b47e7c659f950c1f55547d36913d43cf90e6ef6fb9b3e0cdacb77263704e438afb4a57a5a126d7
https://connect.intuit.com/pay/BossKeeperPR/scs-v1-46886fa735994969b47e7c659f950c1f55547d36913d43cf90e6ef6fb9b3e0cdacb77263704e438afb4a57a5a126d7?locale=EN_US
https://connect.intuit.com/pay/BossKeeperPR/scs-v1-c3aea1f5a44447b2900d3f64b7ec3b09a09dfd3a075a40da89d0109a1e2158daae37be39174bc68de16e36a1ea5fa9
https://connect.intuit.com/pay/BossKeeperPR/scs-v1-c3aea1f5a44447b2900d3f64b7ec3b09a09dfd3a075a40da89d0109a1e2158daae37be39174bc68de16e36a1ea5fa9?locale=EN_US
https://connect.intuit.com/pay/BuildingALeadershipMindset/scs-v1-75b72937fb0b4511b0dbc765c1763a4843913bcd722143ed2b1769305ce6485ccba5fa17894ece8cf9709c1c957c2d
https://connect.intuit.com/pay/BuildingALeadershipMindset/scs-v1-75b72937fb0b4511b0dbc765c1763a4843913bcd722143ed2b1769305ce6485ccba5fa17894ece8cf9709c1c957c2d?locale=EN_US
https://connect.intuit.com/pay/BWDVirtual2/scs-v1-c12afaf260b74473a641542b04ffb74fde9e4aa35c5b4ea382358a0710c6e8358ad00c345346f9a01966790b4b437e
https://connect.intuit.com/pay/BWDVirtual2/scs-v1-c12afaf260b74473a641542b04ffb74fde9e4aa35c5b4ea382358a0710c6e8358ad00c345346f9a01966790b4b437e?locale=EN_US
https://connect.intuit.com/pay/CareProviderSolutions/scs-v1-4e3eb258ae3e4b1bb3fc94fc473038d0ba7f2e7426364fca83a05

Oh no

Invoice PDF

[redacted]

INVOICE

[redacted]

INVOICE
DATE
TERMS
DUE DATE

[redacted]

DESCRIPTION	TAX	QTY	RATE	AMOUNT
Flight Change Fee Press Meeting November 1, 2023	HST ON	1	100.00	100.00

SUBTOTAL	100.00
HST (ON) @ 13%	13.00
TOTAL	113.00
BALANCE DUE	**CAD 113.00**

TAX SUMMARY

RATE	TAX	NET
HST (ON) @ 13%	13.00	100.00

If Paying by Wire/ACH:

[redacted]

PRIVSECCONSULTING

Nothing ever disappears from the internet: how it happens

- I had a CTO friend call me
- He was conducting phishing training on his staff (good!)
- None of them were falling for it (even better)
- …SOMETHING was clicking the links
- I helped him track down what was doing it, and it was Google crawlers going through the inboxes of his staff and following the links
- Why u do this google

PRIVSECCONSULTING

It's not just overseas companies that have this issue

- There are several…'local' companies who are aware of this issue
- Some protracted discussions with Google
- The technical guardrails (no-cache, no store headers) don't seem to be working
  - These are instructions from servers to crawlers/bots to say 'don't do that'
- Likely extends to things like DropBox, Google Drive – I haven't looked
- Some have mitigations in place, such as expiration. Not always.

PRIVSECCONSULTING

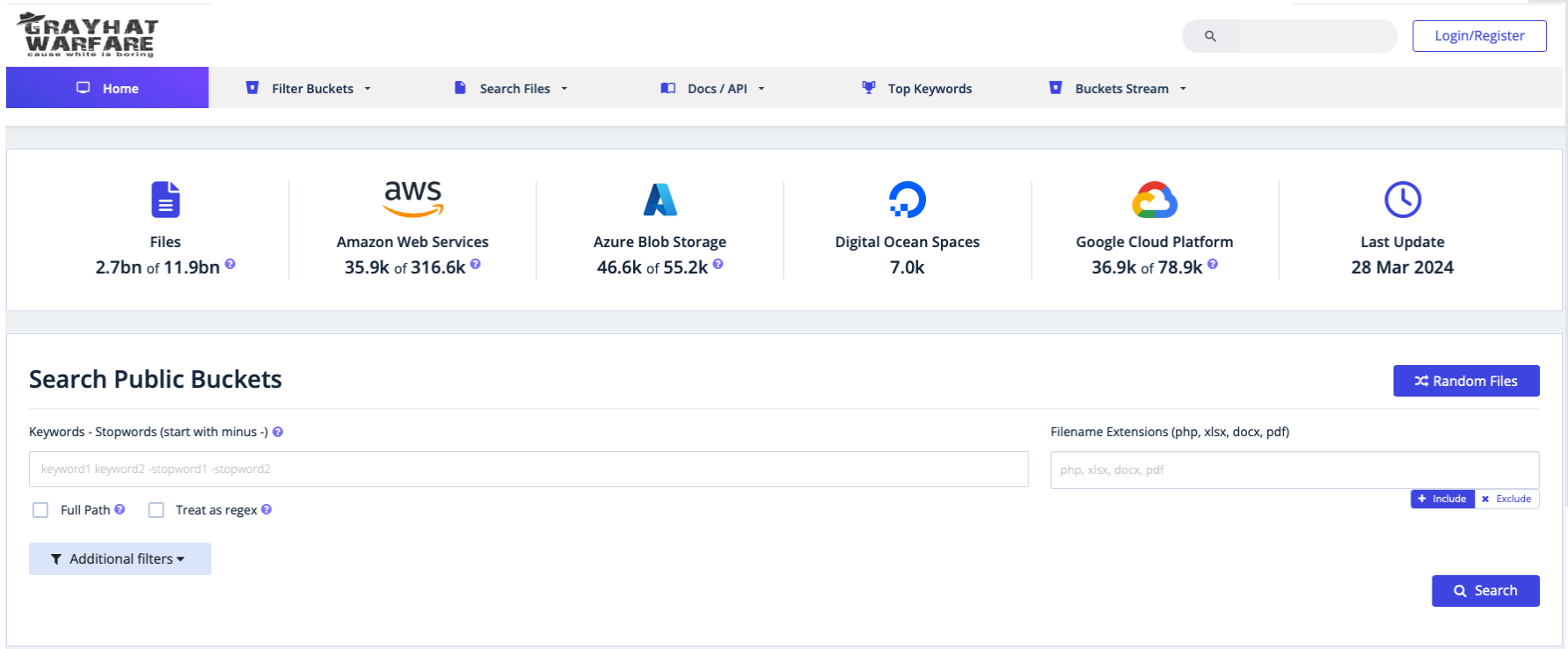
Security misconfigurations A05

- Azure, Amazon etc all have the concept of a 'bucket'
- A place to put files (this is normal)
- A common misconfiguration within cloud services is leaving these buckets public and searchable (this is bad)
- Quite often these contain all sorts of things
  - Invoices
  - Personal Information
  - Source code and secrets
- In July 2020 LPM property management had an exposed public bucket
- 30,000 pieces of information (Passports, Drivers Licenses) were sitting in public view
- Disclosed by a security researcher in May, but was not responded to
- Fixed in July

PRIVSECCONSULTING

Nothing ever disappears from the internet #4: GrayHat Warfare

- GrayHat Warfare have kindly indexed billions of files on hundreds of thousands of buckets
- Microsoft had an issue a few weeks ago where they had left one open with usernames/passwords for internal resources
- Has also happened to Netflix and other big companies



Security Logging and Monitoring Failures: A09

- In 2023 the average length of time to detect a breach was 204 days
- In December 2022 I was working on a job, gained Domain Administrator privileges after compromising an on-prem server and pivoting inwards
  - Domain administrator privileges are like keys to the kingdom
  - You can access all the things (and all the data)
- We notified the client contact we were dealing with
- Heavily enumerated the domain
- February 2023, received an email from another team from the client asking if we were testing 'in December'

PRIVSECCONSULTING

Sometimes a useful feature means that too much data is collected

- Seek has the ability to add your salary to your profile
- It also lets employers know that you've seen their ad
- It also lets employers know what your salary is
- New Zealand is *extremely* small
- You can see who is currently unhappy in their role and looking for a job
- Your boss is probably on seek

PRIVSECCONSULTING

Sometimes it is dark development patterns

- "Dark patterns" can lead to the data being collected in the first place
- Things like confusing wording
- Non-intuitive text boxes
- Having to log in or create account to unsubscribe
- "Personalise your ads"

Tick the relevant box if you DO NOT wish to receive sale and other information relating to Next.

☐ Email ☐ SMS

Sometimes you get to do work that decreases risk

- At RNZ I was asked to move the formal complaints information from the webserver
  - This is good! If the webserver was compromised, it's one less thing to worry about
- It would now send an email instead of dumping into the CMS
- It now has a different threat model – how secure is the formal complaints inbox?
- Not without its issues, I set a cron job to drop the database table at 2am
- The scheduled task timed out at 2:30
- Some poor on-call engineer had to give the site a kick
- Well, it worked on my machine

PRIVSECCONSULTING

What you can do about it:

- If you are a technologist and you are asked to implement something, you can always say no.
- At RNZ in 2019 I was asked to add some 'tracking' javascript to the website.
- I was told that it would send data to Facebook based on session information(!)
- In return, 'anonymised' audience segmentation data would come back to RNZ, which sounded useful
- I told them I would not do the work unless there was a privacy policy in place that was public facing
- I then left to move to cybersecurity. Probably for the best.
- There is now a privacy policy in place

PRIVSECCONSULTING

It still seems like a lot

Why collect information

RNZ collects personal information in order to:

- Deliver services (for example, newsletter subscriptions)
- Provide better services (for example, by monitoring technical errors, identify popular features or content)
- Help with editorial decision making by looking at, for example, where stories are being read, or whether more people click on stories with different headlines.
- Assist in the administration of the organisation (for example, by recruiting staff)

Job applications are not retained for longer than is strictly necessary.

RNZ is required by its Charter (the contract with the NZ Government, which funds RNZ) to provide statistical information about listeners and online audiences in order to demonstrate performance against funding requirements.

RNZ also analyses this information for statistical purposes and to make content and performance improvements to both the website and RNZ's services. This is done by statistical analysis and reporting, identifying trends and diagnosing technical issues.

Storing and disclosing personal information

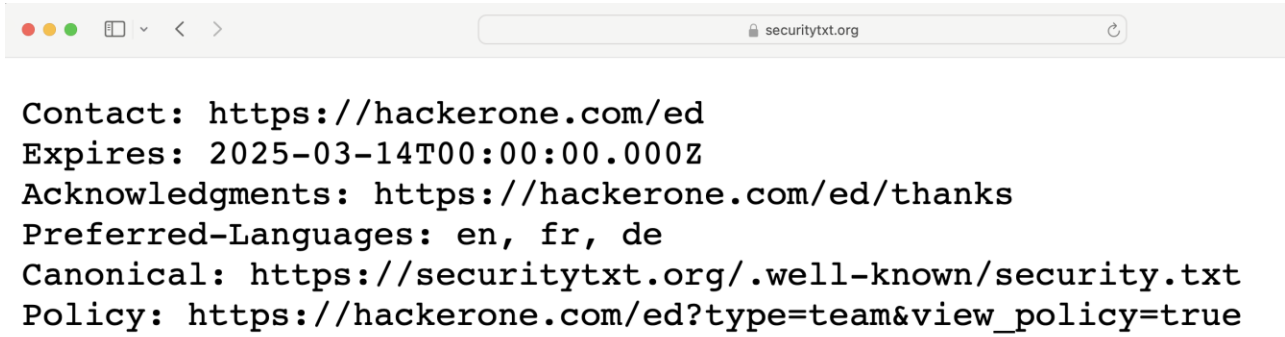
The information we collect is stored on a range of services as listed below.

USER BEHAVIOUR INFORMATION

- Google Analytics is used to provide anonymised usage tracking on our websites to understand user behaviour.
- Nielsen Online SiteCensus is used to collect usage information to track and report on RNZ’s performance

What do you do if you find something in the wild

- Some websites have adopted the security.txt standard
- https://securitytxt.org
- It's a file telling you what to do if you find something wrong
- Otherwise https://cert.govt.nz



PRIVSECCONSULTING

Questions? Thanks for coming!

PRIVSECCONSULTING

Blank page – for crimes