Collaboration not Confrontation

Cybersecurity isn’t a Battle

PRIVSECCONSULTING

Who am I?

- Peter Jakowetz - Managing Director of PrivSec Consulting
- Electrical Engineer by training
- I collect acronyms: CISSP, CISA, CISM, OSCP, PCIP, CRISC, CCSK, CCSP
- Enjoy spending time fixing up the house and hanging with my partner and 18 month old

PRIVSECCONSULTING

What’s today about?

Agenda

- What is it that we do?
- Scoping
- During an engagement - How can we work together to get better outcomes?
- Post Engagement (Reporting)
- Understanding Context – What don’t we know?
- Thoughts
- Resources - How can you become more security conscious?

PRIVSECCONSULTING

What is it that you do…

PRIVSECCONSULTING

So… what is it that you do here

- We audit solutions and systems (GRC)
- We hack stuff to try and break it (Penetration Testing)

--

- We try and make sure solutions have been appropriately secured and data is appropriately protected

PRIVSECCONSULTING

And what developers do

- Write code
- Move jira tickets (don’t worry – we do this too)
- Test code
- Release code

--

- Create software for use by everyone that meets the needs of the stakeholders <3

Pentesting TLDR;

- ‘Simulated cyber-attacks against your systems to try and find exploitable vulnerabilities’
- Mixture of manual and automated testing
- Bypass business logic

PRIVSECCONSULTING

What process do we follow - Pentest

- Scope
- Reconnaissance and Planning
- Scanning and Enumeration
- Finding access vectors/ identifying vulnerabilities
- Maintaining access/ leveraging those vulnerabilities further
- Identifying recommendations to fix
- Writing it all up

GRC/ Audit TLDR;

- We <3 acronyms
- We are identifying the presence or effectiveness of controls (depending on the type of assessment)
- Through a mix of audit methods
  - Discussion
  - Viewing documented processes
  - Seeing what you’ve actually done – i.e. is the box patched?

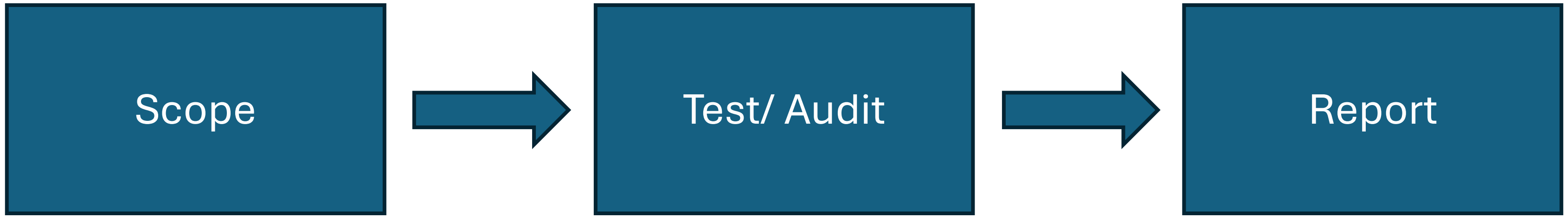
PRIVSECCONSULTING

What processes do we follow - GRC

- Scope
- Come up with an audit plan
- Gather evidence
    - Discussions
    - Documentation
    - System configs/ demonstrations
- Identify recommendations
- Write it up

PRIVSECCONSULTING

Process



Scope

Test/ Audit

Report

Scoping

PRIVSECCONSULTING

Testing Types

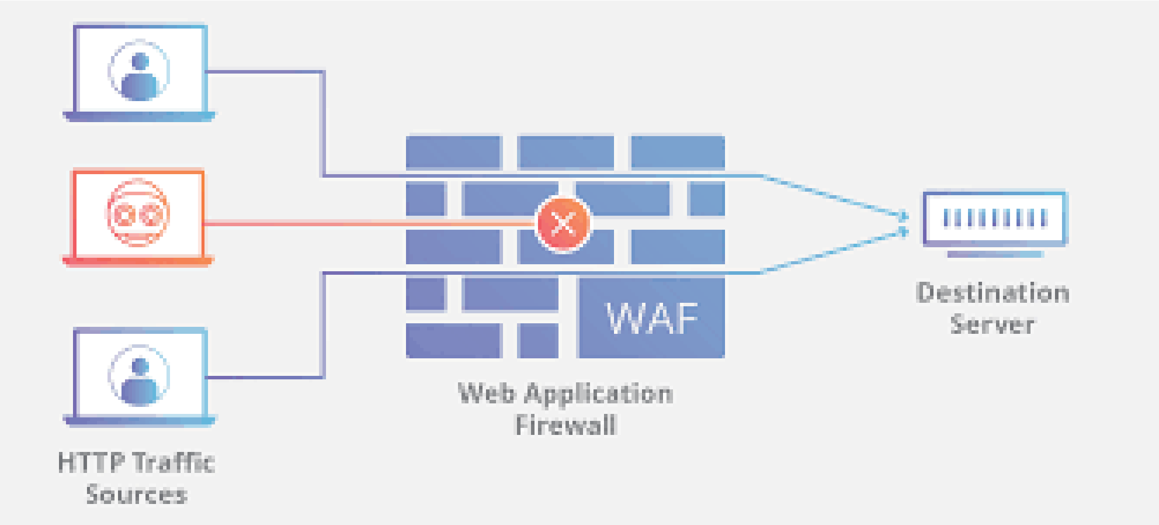
- Black Box
  - No visibility of how things are built
- Grey Box
  - Limited or partial access
- White Box
  - Full knowledge of how the sausage is made
  - That might include having access to source code, documentation etc

Why does the testing type matter?

- “Testers are brought in to see if it’s hackable. Why should we give them any hints?”
  - A testing engagement is typically 1-2 weeks
  - A hacker might be sitting there trying to break your application for weeks/ months/ years
  - Code and knowledge of how the app works can help identify issues quicker (and we can often provide better recommendations on how to fix things)

Case Study – No you can’t bypass our WAF

- We like to do our testing bypassing a WAF
- Gives us better visibility to your app
- We can find better issues and are less hindered in our testing
- More value for everyone (and a more enjoyable time testing)
- We would rather test your app, than your WAF



PRIVSECCONSULTING

Being Prepared - Scoping

- Being prepared during scoping can make sure you get value, and the testers are well prepared
- What roles are present?
- What's the key functionality?
- Any major changes recently?
- What environment do you want tested?
- What's your budget?

PRIVSECCONSULTING

We want to know about your business rules

- Knowledge of how your business works and what’s important to you can allow us to focus our effort
- I.e. is availability super important?
- Race conditions?
- Financial impacts?

PRIVSECCONSULTING

Case Study – Context is key

- We found a race condition in a SaaS app
- Allows you to get additional licenses for free
- These are high value licenses
- Company relies on these licenses for their revenue…
- Suddenly makes it a much more important bug

Case study – Username enumeration

- A common, often low severity or informational finding is regarding ability to enumerate usernames in an application
- Different responses for success/ failure
- On the Countdown app – Who cares?
- For a portal providing support to those who have been subject to domestic violence…. Not very great

Why are you getting the security review done?

- Compliance
  - ISO27001
  - SOC 2
- Regulatory
  - PCI DSS (credit card requirements)
- Customers have asked?
- You’ve recently been breached?
- You want to make sure you’re secure
- You’ve just released a big new feature

Case Study – Low value findings

- Doing some testing on a handful of apps for a client
- They'd been tested annually, and they knew there are a number of present outstanding low issues
- They provided those to us ahead of time
- We could put those in an appendix in the report, and focus our energy on finding new, different vulnerabilities
- Our testers were more engaged
- The client got more value out of the engagement

During the Engagement

Audit - How can you make the process smoother?

- Preparation!
- Prepare screenshots etc ahead of time
- Keep it simple – try and keep the jargon down, being aware the auditor hasn't spent as much time as you with these technologies
- Provide responses in a timely manner – otherwise something may be noted as deficient as evidence was never provided
- If you don't understand what's being asked, ask for it to be clarified

Pentest – How can you make the process smoother

- Preparation!
- Have accounts set up ahead of time
- Have code ready
- Set up a channel for comms
- Make sure the environment is ready

Communication!

- Spin up a slack channel with testers, so that regular conversations can be had during testing
- Make sure everyone knows when testing is happening
- You can then also see if correlations happen between logs/ alerts and the testing activity happening
  - Did it trigger off alerts
  - Has anyone been trying to figure out what’s happening

PRIVSECCONSULTING

Purple team is the way forward

- We work *together* to get a good outcome
- Keep people abreast of what’s happened
- As soon as it’s compromised – provide feedback so we can get instant feedback
- Did you get any alerting?
- Full holistic view of what’s happening – look at multiple aspects.
- You might have logging in place – but have you actually looked at it? Is it triggering alerts?

Tight feedback loops

- Problem statement: I got a report at the end of a week's testing – which has some cool stuff in it, but it was only because we hadn't configured the environment correctly
- How can we get feedback back quicker?
- How can we make sure that the *right* stuff is being tested
- How can testing effort be maximised – so we end up with a robust secure product at the end
- We compromised the thing – what can we see?

PRIVSECCONSULTING

Case Study – Broken comms

- Had a tester come to me saying they’d crashed a non-prod system
- Rocked up to a friendly sys admin and asked them to restart the server
- “but it’s already up…”
- Someone had restarted the server, not aware it was crashing due to being exploited, and hadn’t noted it anywhere or raised any flags

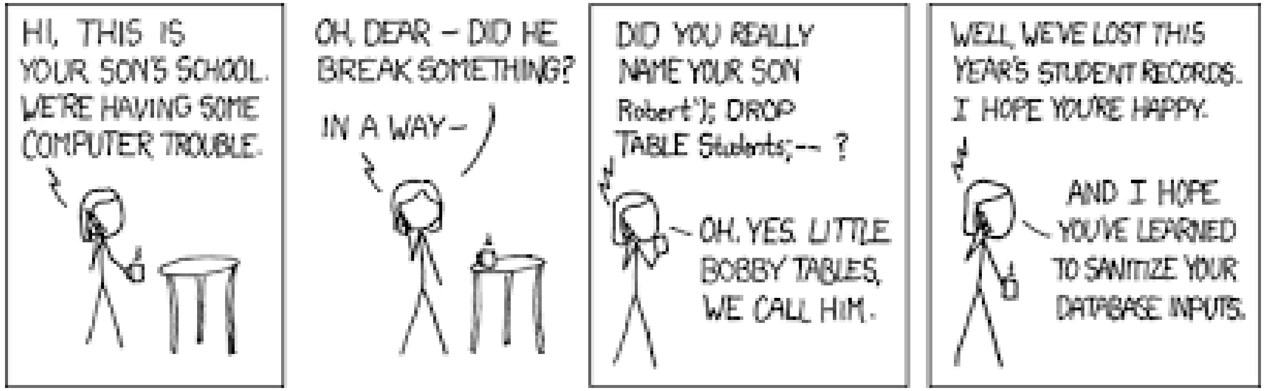
Case Study – Bad Monitoring

- A password spray was done
- 2 bad passwords on every account in the org
- A project manager rocks up 3 days later and asks me if I know why every staff members account he was looking at had failed attempts at the same time on the same day
- The security team and IT teams hadn't noticed

PRIVSECCONSULTING

We don’t want to just say “Haha we popped a shell”

- Popping shells and dumping databases is great!
- But it’s not really the aim of the game all in itself
- If we talk to each other more regularly during testing engagements, then we will still find those bugs – but we can work together


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

PRIVSECCONSULTING

Reporting

Reporting

- Language is important
- ‘Gross negligence’ is probably not the best term to use
  - The lawyers get a bit excited
- Neither is ‘dumpster fire’
- Simple, respectful language that we can all understand

When we’re writing a report

- We have multiple people having to read our reports – so the whole thing probably isn’t for you
- Exec summary == C-level/ Manager
- Management summary == Project Manager
- Technical details == developers/ engineers

Ask questions

- Pentesters and auditors generally (if they’re not jerks) don’t mind answering good questions during testing and audit periods
- Just like you, we like to talk about what we do all day
- We’re generally happy to show you how to hack too, and demystify what we do
- Similarly, we’re happy to put together POCs, and run those through with you
- Have a play reproduction steps, and see if you can do it!

PRIVSECCONSULTING

Case Study – Sometimes we find things we're not expecting

- Internal test
- Tester sits at the end of a line of developers – hoodie, non-corp laptop, never introduced themselves
- At the end of the week is asked whether they're the new team member and do they need any help…

PRIVSECCONSULTING

We don’t necessarily understand your context

- You’ve had some layoffs recently
- That SPA was a quick fix, and was going to be decommissioned 3 years ago
- The boss really wanted that feature, and no one else did
- That was put in just for one customer
- The guy who put that in left 6 years ago and we’ve been too scared to remove it
- That was the interns summer project
- There isn’t any investment for maintenance
- That feature’s being deprecated next month

You might not have been there when the code was written

- Technical debt exists
- Which can also mean security debt
- But that debt is usually what allowed for your job to exist
- We need to understand that apps aren’t rebuilt every day, and as such there will always be history

We definitely weren’t there when the code was written

- We don’t know why the code is the way it is
- We don’t know what was happening that day
- We don’t know the requirements you were working to
- We don’t know how many coffees the scrum master had that day and how much they were breathing down your back
- We don’t necessarily know the regulations etc you have to meet for your org and stakeholders

Functionality vs. Security

- It’s not always black and white
- People want to do their jobs – how can we balance the two requirements out?
- There’s got to be compromise
- There are stakeholder limitations/ cultural limitations/ financial limitations
- A risk based approach (and having a convo) can be really helpful here

PRIVSECCONSULTING

Case Study – Apps used by specific communities

- App for a specific segment of the community
- Lots of PII and funding info
- Not necessarily technically literate stakeholders
- There ends up being a conflict between functionality and security
- I.e. MFA – is that a step too far – especially when 70/80 years old pastors may be the ones using the tool for their community
- How do we balance that?

PRIVSECCONSULTING

Thoughts

PRIVSECCONSULTING

Let’s not poop on each other

- “The testers didn’t even know what they were doing”
- “That app was terrible”
- “They don’t even understand what we do”
- “How could anyone build something that insecure”

PRIVSECCONSULTING

If we work together – we can uplift each other

- We all have our specialties
- You (or your boss) pays us to come in, because we're the experts in our domain
- While most of our testers used to be devs – they don't do it for your org
- If you share some of your insight and work with us, and we work with you – we can get some really good outcomes

PRIVSECCONSULTING

We know some (not so secret) secrets

- We’re looking at different systems and services every day
- At this point, I’ve reviewed hundreds (at least) of systems
- I’ve seen some amazing architectures, and some not so awesome ones too
- I’ve seen some legacy tech which has been implemented awesome and some new tech implemented terribly

If we know context, we can recommend different approaches

- If we talk together, often we can find a way through
- There might be tools we've seen in other engagements we can recommend
- We might be able to suggest a couple of compensating controls if you can't remove a specific issue

Case Study – Large app developed by 3rd party

- Large app
- Multi-million dollar development effort
- ~3 year project
- Well over 100 security issues documented
- Pentesting didn’t go well
- Audit went worse

PRIVSECCONSULTING

We had 2 options

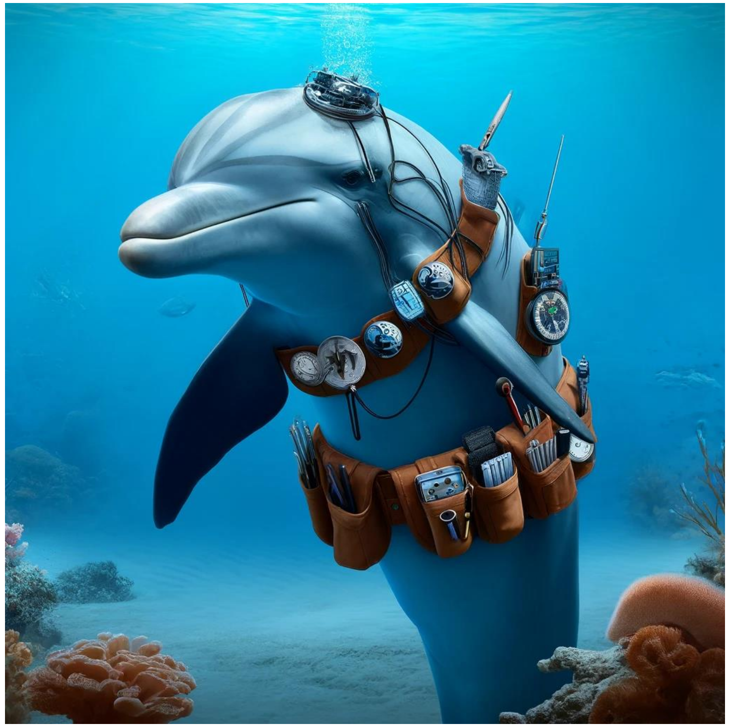
1) Wind up the vendor and make them feel bad
    1) Easy option
    2) Unlikely to win
    3) Everyone feels bad
2) Work *with* the vendor, and aim to resolve the issues
    1) A whole lot more work
    2) You might end up with something secure AND usable
    3) A few less grey hairs, and less whisky consumed

We worked with them…

- And that led to good things
- Development effort took a while
- But we ended up with a secure product
- With no defects at go-live and a clean audit
- Everyone swallowed their pride a bit, and we went forward
- Compromise had to happen on both side – but we ended up with a secure and functional app that is used by a good chunk of NZ

Learnings from Security?

- Break issues into easy to read English
- What are the *real* impacts of an issue
- What is the *real* likelihood of an issue
- Award the small wins
- Regular conversations are good!



PRIVSECCONSULTING

What we’ve found works well

- Using clear concise language
- When development teams or a lead have been involved in scoping
- When we have a mechanism to talk to the technical team during testing
- When the org is well prepared for an audit/ test
- When orgs read and question the report
- When we have a solid understanding of the business context

Resources

PRIVSECCONSULTING

How can you become more security conscious?

- Podcasts are great!
  - Risky.biz
  - Black Hills Information Security podcast
  - Darknet Diaries

- Si’s pentesting guide has lots of great resources:
  - https://www.linkedin.com/pulse/getting-started-penetration-tester-nz-2023-edition-simon-howard

Collaboration

- Discord – InfoSecNZ
- ISIG Wellington – Last Thursday of Each Month
- Meetups – OWASP
- OWASP Day – September 2024 (AKL)
- Christchurch Hacker Con – November 2024 (CHCH)

Links

- Burp Suite - https://portswigger.net/burp/communitydownload
- ZAP Proxy - https://www.zaproxy.org/
- OWASP Secure Coding Practices - https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/

Thanks for having me!

- peter@privsec.nz
- https://www.linkedin.com/in/peterjakowetz/

PRIVSECCONSULTING