When Shoestrings Snap

The perils of hosting web apps on a tight budget

Rory Shillington
Why I love infosec

• Volts and Bits Ltd
• Web App design
• Website maintenance
• IT Support
• IoT
• CTF
By day

Designing, testing and breaking solar inverters
Qualified electrical engineer

I am an expert in this part of the web app
My introduction to non-profit organisations

• As a university student
• Local chapter of a prestigious worldwide organisation
• Non-profit, community service oriented organisation
• Run by volunteers in their spare time
• Very little money - mostly from fundraisers
• What's missing from this list?
What did the organisation do?

- Organise volunteers for other community organisations
- Plant trees
- Mentor students at local schools
- Provide university scholarships
- Funding conference travel
- Leadership training
- Social events
What did the organisation NOT do?

- Backups
- Salt passwords
- Patch servers
- Document IT systems
- Configure firewalls
Why not?

• No glory or visibility in IT tasks
• Limited money to outsource
• Not considered core business
• Boring / lack of interest
• Lack of expertise
• Previous IT Officer had graduated and left town
Here's where I come in...

• After sticking my neck out while assisting with community events

• I joined the committee

• Was nominated as new IT officer / "most technical person in the room"

• Unanimously voted in with much relief
Inherited a dedicated server

- Internet facing IPv4 address
- No firewall
- MTA with mail forwarders
- Several mailing lists
- Behind on patches
- No auth rate limiting. Anywhere.
- Root access!
Inherited a dedicated server

- Public IPv4 address
- No firewall
- MTA with mail forwarders
- Several mailing lists
- Behind on patches
- No auth rate limiting. Anywhere.
- Root access!
The Custom Web App

• Handles personal information of the committee

• Internet accessible

• Login system stores unsalted MD5 hashes of passwords

• Coded in a language I'd never used before

• What could possibly go wrong?

Photo credit: Ian Baker
Where did this come from?
Review the logs!
Review the logs!

118.250.63.69 - - [20/May/2010:17:25:56 +1200]
"GET /events.php?id=221+and+1=0+
%20Union%20Select%20%201%20%20,%20%20UNHEX(HEX(concat(0x5B6B65795D,table_name,0x5B6B65795D))))
%203,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19+FRO
M+INFORMATION_SCHEMA.tables+where+table_schema=Concat(char(98),char(111),char(111),char(107),c
har(115),char(97),char(108),char(101))+LIMIT%200,1--
HTTP/1.1" 200 5077 "-" "-"
Disaster Recovery: What I did

• Inspected advert code
• Searched database for other instances
• Removed advert code
• Reviewed access logs
• Tested samples of SQL injection query strings
• Code inspection & correction
• Reported details to committee
Long term mitigations

• Switched to a well supported library for salted, strongly hashed passwords; changed all passwords

• Removed disused scripts

• Implemented better user input sanitization

• Refactored all database transaction code with prepared statements

• Shifted to virtualised server on enterprise equipment

• Outsourced mail functions
Small business

• Similar issues to non-profit organisations

• No IT department

• Often using very low cost infrastructure

• Lack understanding / interest in technical issues

• IT is often an afterthought, left to one person

• Can be a big a target as they have money
Cue horror story #2

• New client (family friend)

• Client not receiving replies from hosting provider

• Provider's only known contact is a hotmail address

• Can I please help?

• Umm.....
The hosting provider

- Email me their password
- Has 30 websites on a $6/month unlimited domain shared hosting package
- All are running outdated copies of a very popular blogging software
- Backups are broken
What went wrong?

• Client had basic technical knowledge but lacked experience required to assess quality of supply chain

• Client was not aware of the risks faced

• Hosting provider did little to mitigate or inform
How could we mitigate?

• Outsource technical functions to capable hands

• Generally that means cloud / managed services when you are under resourced

• Education - understanding that not all services are created equal, cheap is cheap for a reason

• Find a trusted advisor who actually knows their stuff - thats probably you!!
Case study: email forwarding

• Let's say you register your domain and have some basic hosting attached

• Already well established using webmail and hey, they give you 100x the storage of your cheap hosting

• The obvious thing to do is forward all email from domain alias to webmail

• CPANEL makes this really really easy!
Bad idea

- All emails are forwarded including junk
- Forwarders may execute upstream of spam filters
- Forwarders may not set forwarding headers correctly
- Some webmail providers will then think your server is the source and blacklist your IP
- Particularly bad if you share an IP with others - the risk goes both ways

Image credit: Wikimedia Commons
A Better Approach

• Create mail accounts with hosting provider
• Configure webmail provider to download emails via POP3
• All major providers support this arrangement
• Alternatively, register your domain via webmail provider
Talking of spam...

- Looks like a domain is about to expire
- Actually unsolicited SEO services
- Busy people might not pay close attention
- Non-technical people may not understand
- Email contains personal info from whois to look legitimate
Conclusion

- Non-profit organisations and small businesses face substantial challenges with their IT systems
- Basics such as email and website hosting can be major headaches
- Non-technical people can be particularly vulnerable to malicious actors as well as ineptitude of providers
- We as technical individuals can and indeed should help where possible - go volunteer!
Questions?

Rory Shillington
Volts and Bits
https://voltsandbits.com
@voltsandbits