Lessons from a decade of bug hunting

Atlantic Security Conference 2019

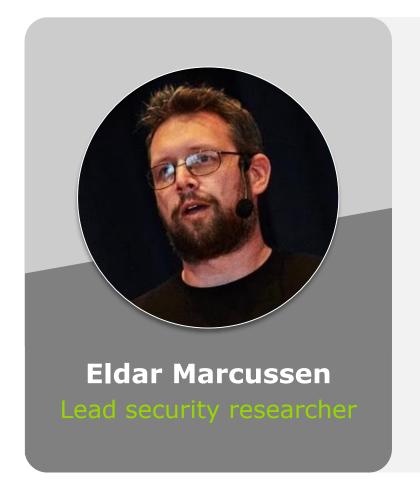


SMART AND SAFE DIGITAL

Content

- **01 BUG HUNTING**
- **02 DISCLOSURE**
- **03 CONCLUSION**

`whoami`



Proven history of performing security research that result in Oday vulnerabilities, conference presentation and security tools. I have written a source code scanner and auditing source code is often part of my security research process. My past research and security tools have also featured in industry related cyber security text books.

A former

Developer

System administrator

Penetration tester

Husband and Father

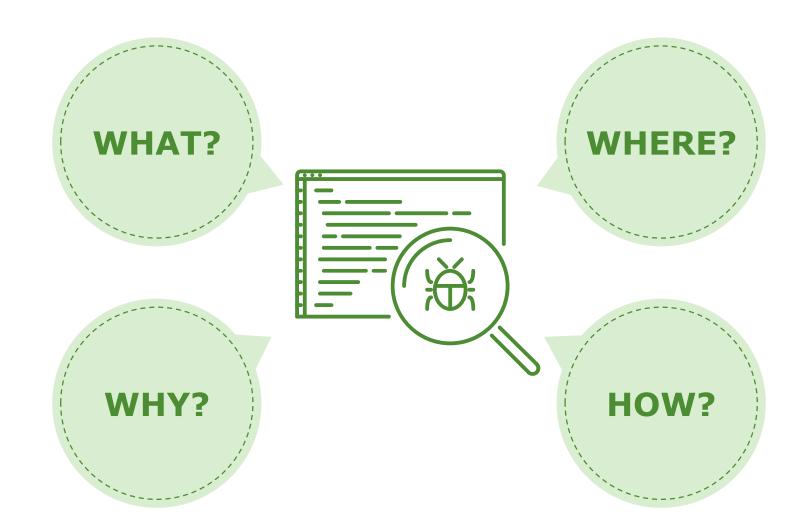
Currently

Security researcher

Trainer

O1 BUG HUNTING

Bughunting



Identifying weaknesses



Read the documentation

Learn to recognize weakness patterns in source code

Learn to recognize weakness patterns in design/process

Anticipate poor decision making

Implement short test cases to verify behavior if unsure

Take breaks from complex/difficult code

Simplifying bug hunting

- AVOID FALSE POSITIVES
- THIS MIGHT MEAN MISSING VULNERABILITIES (false negatives)
 - You can always take another look later
- SHORTLIST OF VULNERABILITY CLASSES
 - > Easy to analyse
 - > Avoids drowning in XSS



Reporting vulnerabilities

Vulnerability enthusiasm

DISCLOSURE VALIDATION EXPLOITATION DISCOVERY • Reading some code or Overcoming technical Spotting something worth a Writing advisory second look challenges Analysing a crash Advisory QA "Popping shells" Confirming the vulnerability Contacting vendor Requesting CVE Lots of emails Waiting for patch Publishing advisory

Reporting vulnerabilities



DISCLOSURE

"Types" of disclosure



No disclosure

Researcher finds a vulnerability and does not notify vendor, choosing rather to sit on vulnerability or sell it privately



Private disclosure

Researcher notifies
vendor about the
vulnerability.
Vulnerability is not
disclosed to end users



Coordinated disclosure

Researcher notifies
the vendor and
maintains
communication with
the vendor before
disclosing the
vulnerability publicly

Researcher discloses the full details of the vulnerability publicly.



Full disclosure

Non-traditional ways of doing disclosure, such as shorting vendors shares



Other

COORDINATED, NOT RESPONSIBLE

Problems with the disclosure debate



Vulnerability tourism



Assumptions



Strawman arguments



Lack of empirical data



Shallow arguments



Disclosure policy compliance

Don't be that guy

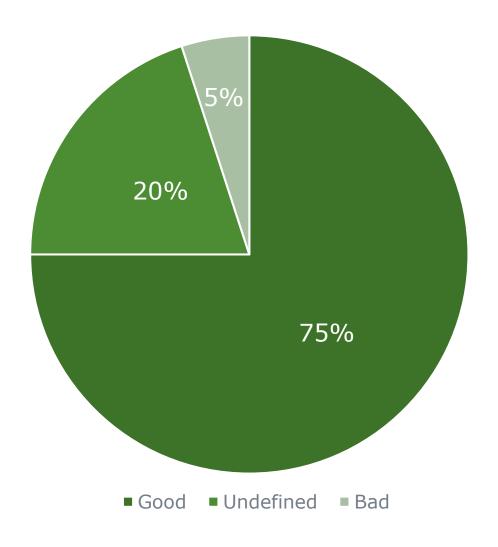


Replying to

I do hope this tweet is a last resort and you've at least attempted responsible disclosure...

Personal stories

Disclosure experiences



DEALING WITH VENDORS

- This is a placeholder text.
- This text can be replaced with your own text.

Disclosure experiences

Contact vendor (Ask how they want to receive vulnerability details)

Send vulnerability details

Waiting

Emails

Waiting

Patch available

Release advisory

OR

Contact vendor (No response)

Contact vendor (No response)

Contact vendor (No response)

Release advisory

Cacti superlinks plugin

18-06-2014 28-10-2014 ??-??-2014 19-12-2014 11-07-2016 13-01-2018 SQL injection Confirmed that Vendor claims Release exploit to Patched Superlinks Plugin website functionality added published on fixed in SVN push vendor to updated to this trivially fix download link to core codebase **Exploit-DB** RCE indicate functionality Link Link Link is now in core Link 2017 2016 2015 2018 2019 2014 20-11-2014 I escalate the 29-01-2017 22-03-2019 29-10-2014 download still 23-10-2014 Version 1.0.0 Vulnerable Reported issue to serving 29-06-2015 -Independently officially plugin still vulnerable code vendor discovered Attempted integrates available for Link Link during pentest escalation again download superlinks

phpMoAdmin

28-02-2015

Exploit for sale on 1337Day





04-06-2015

Random person chimes in with personal opinions 14-07-2015

Developer dismisses issue

15-07-2015

Developer agrees its a problem and suggests someone should provide the patch 15-12-2016

Developer commits a patch and closes issue

02-01-2018

Open issue advising developer and providing CVE for reintroduction of issue



2015

2016

2017

2018

2019

10-03-2015

Issue opened on github





14-07-2015

Upon wanting to play with the vulnerability I discover it is unpatched and escalate on the thread

15-07-2015

I escalate on twitter and several people chime in on the github thread **Dec 2017**

I revisit the code planning to use it as a training example and find the patch has been reverted

22-03-2019

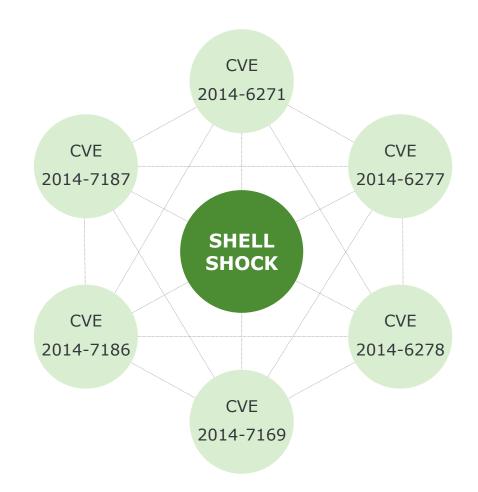
Issue still present

Public disclosure stories

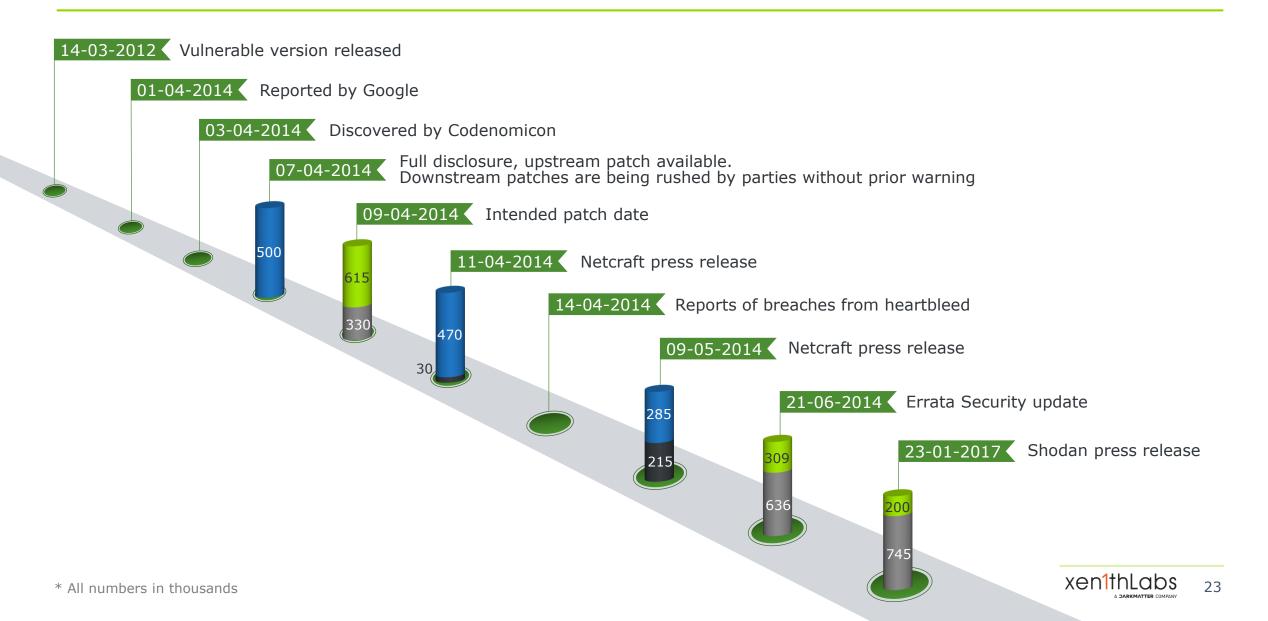
Shell shock (bashdoor)

- Initial report: 12 September 2014
- Initial patch: 24 September 2014
- Wide spread abuse: Within hours of disclosure
- Additional patches: 25-30 September 2014
- Abuse slowly died off

Attackers exploited Shellshock within hours of the initial disclosure by creating botnets of compromised computers to perform distributed denial-of-service attacks and vulnerability scanning. Security companies recorded millions of attacks and probes related to the bug in the days following the disclosure.



Heartbleed



Eternal blue

Several 14-03-2017 12-05-2017 researchers have Microsoft WannaCry takes recommended the internet releases patch disabling SMBv1 and security with storm for years bulleting MS-17causing millions 010 of dollars in damage Pre-2016 2018 2016 2017 16-09-2016 31-12-2018 Microsoft 14-04-2017 officially Estimated Shadowbrokers millions of recommends disabling SMBv1 release exploit systems still following Badlock code vulnerable

Other disclosure stories

- https://www.csoonline.com/article/3338112/vendor-allegedly-assaults-security-researcher-who-disclosed-massive-vulnerability.html
- https://beyondbinary.io/articles/seagate-nas-rce/
- https://www.ring0.lol/posts/2014/07/27/coindrawer-bug-bounty-finale/
- https://twitter.com/Agarri FR/status/1112401090023170049
- https://medsec.com/entries/stj-lawsuit-response.html
- https://threatpost.com/the-vulnerability-disclosure-process-still-broken/137180/
- https://www.wired.com/2015/09/fireeye-enrw-injunction-bizarre-twist-in-the-debate-over-vulnerability-disclosures/

03 CONCLUSION

