Handling security bugs with responsible disclosure and bug bounty programs

SAP Inside Track 2018

Internetwache.org / @internetwache

September 1, 2018
We’re Internetwache.org since 2012!

• Sebastian Neef aka @gehaxelt
• MSc student @ TUB / IT-Sec Freelancer
• Runs the ”AG-Rechnersicherheit” @ TUB
• CTF-Player @ ENOFLAG

• Tim Philipp Schäfers aka @TimPhSchaefers
• Cyber Security Consultant
• Author of two german InfoSec books
The internetwache.org project

- Discovering and reporting (web) security issues
- Active participation in responsible disclosure and bug bounty programs
- Internet scans and creation of security awareness

[Image: internetwache.org]

[Link: https://en.internetwache.org]
Security bugs?!

- Hacks & security breaches happen every day.
- Lots of things exposed to the internet that shouldn’t :-/
- Lots of things not up2date :-(
- Lots of things not receiving security patches :'-(

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

By Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber

Sept. 7, 2017

Forbes

Hackers Swipe Data On 2 Million T-Mobile Subscribers

17,206 views | Aug 24, 2018, 11:00am
Security bugs?!

- Hacks & security breaches happen every day.
- Lots of things exposed to the internet that shouldn’t :-/
- Lots of things not up2date :-(
- Lots of things not receiving security patches :'-(

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

By Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber

Sept. 7, 2017

Hackers Swipe Data On 2 Million T-Mobile Subscribers

The New York Times
How to prevent this?

- Integrate "security" from the beginning on
- Do "penetration tests" often
- Consider responsible disclosure and bug bounty programs
- Accept security reports and act accordingly

When you report a potential PII data leak to a #security vendor (❗️) and you only get the following response "I spoke to our marketing department on this and they assured me there is no data leak here".
Security Research

- Problem I: Security testing usually illegal (cf. § 202c StGB)
- Problem II: (Whitehat) Security researchers live in fear of conducting and publishing their research
- Problem III: How to contact the vendor / right people?
Responsible disclosure and bug bounty programs

- Main idea: "Hack us!"
- Embrace independent security work
- Tell what is allowed and/or where to test
- No legal repercussions (if adhered to the rules)
- Optionally monetary or material rewards or "hall of fames"

Responsible disclosure and bug bounty programs

- Main idea: “Hack us!”
- Embrace independent security work
- Tell what is allowed and/or where to test
- No legal repercussions (if adhered to the rules)
- Optionally monetary or material rewards or “hall of famers”

Some examples...
## Google bug bounty

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
<th>Applications that permit taking over a Google account [1]</th>
<th>Other highly sensitive applications [2]</th>
<th>Normal Google applications</th>
<th>Non-integrated acquisitions and other sandboxed or lower priority applications [3]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote code execution</td>
<td>Command injection, deserialization bugs, sandbox escapes</td>
<td>$31,337</td>
<td>$31,337</td>
<td>$31,337</td>
<td>$1,337 - $5,000</td>
</tr>
<tr>
<td>Unrestricted file system or database access</td>
<td>Unsandboxed XXE, SQL injection</td>
<td>$13,337</td>
<td>$13,337</td>
<td>$13,337</td>
<td>$1,337 - $5,000</td>
</tr>
<tr>
<td>Logic flaw bugs leaking or bypassing significant security controls</td>
<td>Direct object reference, remote user impersonation</td>
<td>$13,337</td>
<td>$7,500</td>
<td>$5,000</td>
<td>$500</td>
</tr>
</tbody>
</table>

Vulnerabilities giving access to client or authenticated session of the logged-in victim

| Execute code on the client                         | Web: Cross-site scripting            | $7,500                                                   | $5,000                                  | $3,133.7                   | $100                                                                            |
|                                                    | Mobile / Hardware: Code execution    |                                                          |                                         |                            |                                                                                 |
| Other valid security vulnerabilities               | Web: CSRF, Clickjacking               | $500 - $7,500                                           | $500 - $5,000                          | $500 - $3,133.7            | $100                                                                            |
|                                                    | Mobile / Hardware: Information leak; privilege escalation |                                                  |                                         |                            |                                                                                 |
Paypal path traversal

![Paypal path traversal screenshot](https://example.com/paypal-path-traversal-screenshot.png)
Responsible disclosure and bug bounty programs

For a company
  • + Reduced security risks
  • + Reputation within the security community
  • + Quality enhancement
  • - High Workload
  • - False positives

For a researcher
  • + Point of contact
  • + No legal consequences
  • + Possibility to gain money and experience
  • - First to find
  • - Disclosure policy
  • - High competition
Responsible disclosure and bug bounty programs II

For a company
• + Reduced security risks
• + Reputation within the security community
• + Quality enhancement
• - High Workload
• - False positives

For a researcher
• + Point of contact
• + No legal consequences
• + Possibility to gain money and experience
• - First to find
• - Disclosure policy
• - High competition
Pentesting vs. Bug Bounty

Classical Pentesting
- Few testers
- Every X month
- Contract-based
- Fixed costs
- One report
- Limited scope

Resp. Disc + Bug Bounty Programs
- Many testers
- 24/7 ongoing
- Voluntarily
- Variable costs
- Multiple reports
- Broad scope
Pentesting vs. Bug Bounty

Classical Pentesting
- Few testers
- Every X month
- Contract-based
- Fixed costs
- One report
- Limited scope

Resp. Disc + Bug Bounty Programs
- Many testers
- 24/7 ongoing
- Voluntarily
- Variable costs
- Multiple reports
- Broad scope
Conclusion

- Responsible disclosure and bug bounty programs can improve one’s security.
- They’re not a replacement for own security practices and tests.

For companies: Start your program now!
For researchers: Participate now!
Questions?

Now it’s your time to speak :-) 

- Website: https://internetwache.org/
- Twitter: @internetwache
- E-Mail: contact@internetwache.org