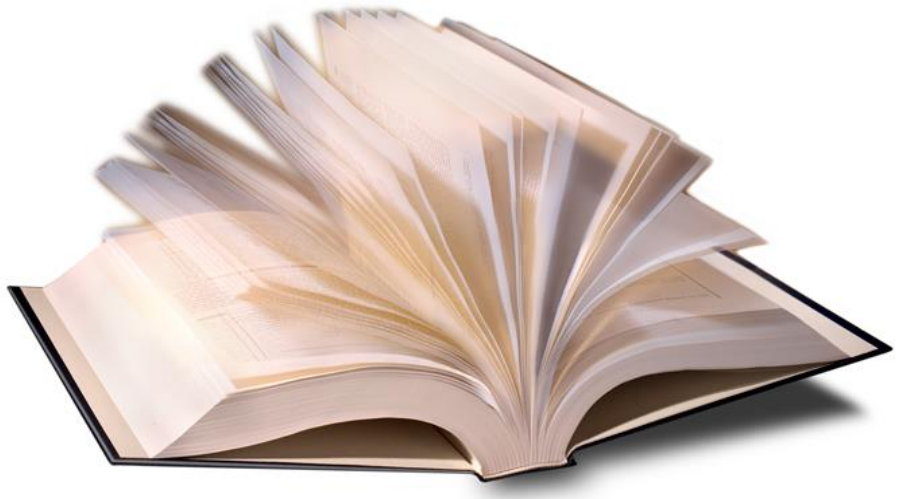
SPARKS

Advantages and disadvantages of Bug Bounty and Responsible Disclosure programs



Author:

Cernica Ionut Cosmin

Who am I

- Security Engineer at SafeTech Innovations
- Bug Bounty Hunter
- Security Researcher
- Student!

Agenda

- Bug bounty vs Responsible Disclosure
- Bug bounty stories
- Responsible disclosure stories
- Advantages and disadvantages

Bug Bounty

VS

Responsible Disclosure

SPARKS

Bug Bounty stories!

- 1. Bypass authentication in billsafe.de (direct object reference)
- 2. Bypass authentication in billsafe.de (md5)
- 3. Bypass authentication in qr.paypal-labs.com
- 4. Delete any account (they didn’t recognize this problem)
- 5. Bruteforce on users accounts - 2 times
- 6. Many CSRF
- 7 Many XSS
- 8. I was able to take random mail address
- 9. I was able to take ~2.800.000 emails address
- 10. I was able to spoof any paypal button and XSS.

- CSRF
- Bypass CSRF protection
- Validate any phone number on your facebook account
- Able to see if a specific person visited my timeline and if someone is invisible on facebook chat.

- Reset password of any account.
- Old version of JBoss, shell deployment. (https://espcare.att.com/)
- XSS

MARKTPLAATS.NL

ebay classifieds group

- Important privilege escalation

YAHOO!

- 5*XSS, CSRF, Information disclosure

Google™

- 2*CSRF

SPARKS

Responsible Disclosure stories!

- Authentication bypass on community.ebay.co.jp

- Reset password of a random account.
- Reset password of any account.
- Information disclosure – confirmation token.

- Reset password of a random account – 2 times

- Reset password of any account.

- Session puzzling

- Reset password of an random account – 3 times

- Stored XSS

- I was able to enter in any account.
- They appreciated my work and gave me a pro version of XMind.

- Information Disclosure. Directory listing with important files (web server logs, source code disclosure, etc)

- Information Disclosure (/server-status/)

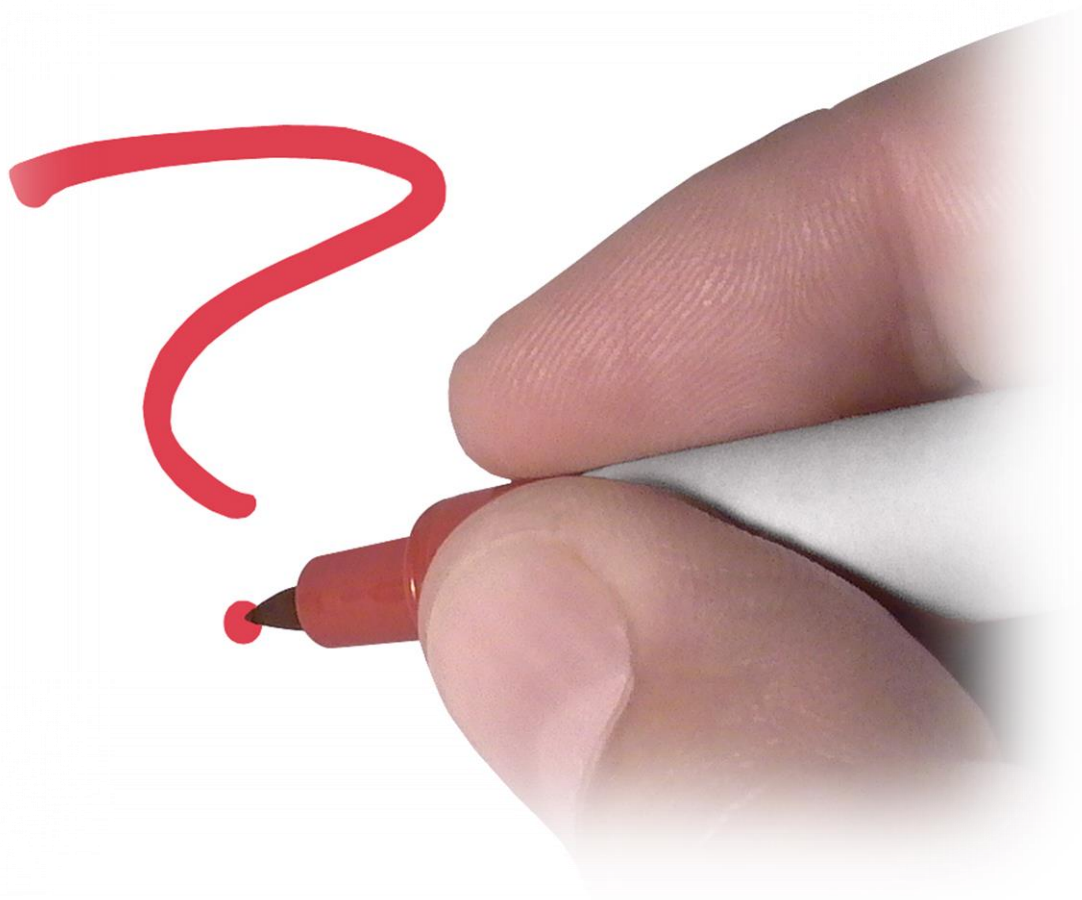
Conclusion - Advantages

- Gain experience doing something legal
- Fame
- Work from home
- Companies can test the security of all points of view
- Remuneration as of the severity of the problems found
- Much easy to get a job in IT security

Conclusions - Disadvantages

- Lack of transparency
- Inspection - reporting process difficult in some cases

Questions?



Thank you!

If you want a career in IT security send your resume to the address: office@safetech.ro