Nov 7th, 9:00 AM - 5:00 PM

# Bounty techniques for web vulnerability scanning

Tanzer Abazi
*University for Business and Technology*, tanzer.abazi@ubt-uni.net

Mentor Hoxhaj
*University for Business and Technology*, mentor.hoxhaj@ubt-uni.net

Edmond Hajrizi
*University for Business and Technology*, ehajrizi@ubt-uni.net

Gazmend Krasniqi
*University for Business and Technology*, gazmend.krasniqi@ubt-uni.net

# Bounty techniques for web vulnerability scanning

Tanzer Abazi[1], Mentor Hoxhaj[1], Edmond Hajrizi[1], Gazmend Krasniqi[1]

[1]UBT, Computer Science,
{tanzer.abazi, mentor.hoxhaj, ehajrizi, gazmend.krasniqi}@ubt-uni.net

**Abstract.** With the advancement of technology and the raising of massive amount of data, the used techniques for data security are continually a challenge. This paper contributes on identifying the gaps and evaluating security level on web portals hosted or managed by Republic of Kosovo institutions or businesses, whose data privacy and security could be a big business concern. The results have been obtained from real case scenario, where 25 security researchers have contributed in white hack activities. These activities, were part of a one day conference called. "The DAY when hacking is legal", held in Pristine

**Keywords**: bugs, Information Security, security researchers, hackers, websites, vulnerabilities

## 1. Introduction

This The National Agency for Protection of Personal Data in cooperation with DARTS Security has created a plan for increasing the awareness of citizens, a responsibility derived from the Law on Protection of Personal data, with the purpose of informing the citizens on their constitutionally and legally guaranteed rights on while data is being processed, as well as their rights to complain whenever they consider data is not processed in accordance with existing laws, the campaign were called 'Privacy in Digital Age' contained a lot of activities related with information security , one of the activities within the international conference which was held on 27th of January 2015 for the first time in his format was the workshop 'The DAY when hacking is legal'.[1]
The purpose of this activity was to raise awareness of Kosovo institutions or companies who deal with data processing on data security, especially the companies who store or otherwise manage their data online, including their web sites. In other side stimulating and identifying security researchers who can legitimately become a white hat hackers. [2]
The supporters of this event were companies who run online businesses. The business profiles various from web portals, e-commerce, job application, advertisement, etc. The ten numbers of websites has been tested for security holes by twenty-five hackers. In real-time the links of the websites that have to be tested were listed in the projector. For each reported bugs to the jury, after the validation the hacker have been paid per reported bugs.
Juries of three professionals have decided at the end of the activity to give prizes to each hacker, who has achieved to identify "security bugs" as Critical, Medium or Informative. The jury will not disclose the contents of the bugs, as it will compromise the security of the companies the web applications of which have been screened. Hackers have been paid for reported bugs (price per bug). We used to see similar method so called bug bounty program.[3]

## 2. Hackers

The Applicants were filtered through interview by Organizer (Darts Security), where interested hackers applied as individuals but also as a group of three. Each applicant has signed a non-disclosure agreement that ensures that teams or individuals discovering a security breach or private information will not disclose the information's. In NDA was predefined the clausal mentioning the time interval on which the competitors have the right to scan the websites.

From the population of 43 applicants, twenty-five security researchers have been selected among applied hackers. There have been four groups of hackers within 3 professionals, and the others have applied as individual.
Questioner containing 11 questions has been answered by 9 hackers attending the workshop.

- Six hackers claimed that they were part of some hackers groups in Kosovo and Region.
- Enjoyable Academic level with one Master Degree, three of the hackers are still attending Master, three others have graduated on bachelor degree, the rest were high school students.
- The average age of the hackers attending the workshop was 21 years old.
- The average age of experience in information security by the hackers was 1.5 years. Starting from 10 years of information security experience to 6 months.
- Anonymously all the hackers liked the format of workshop 'The DAY when hacking is legal'
- By the hackers there is no high cyber security level in Kosovo, even is not enough. Also the hackers knowledge in Kosovo is ranged as medium.
- Four from the nine hackers are actually employed with related information security position.

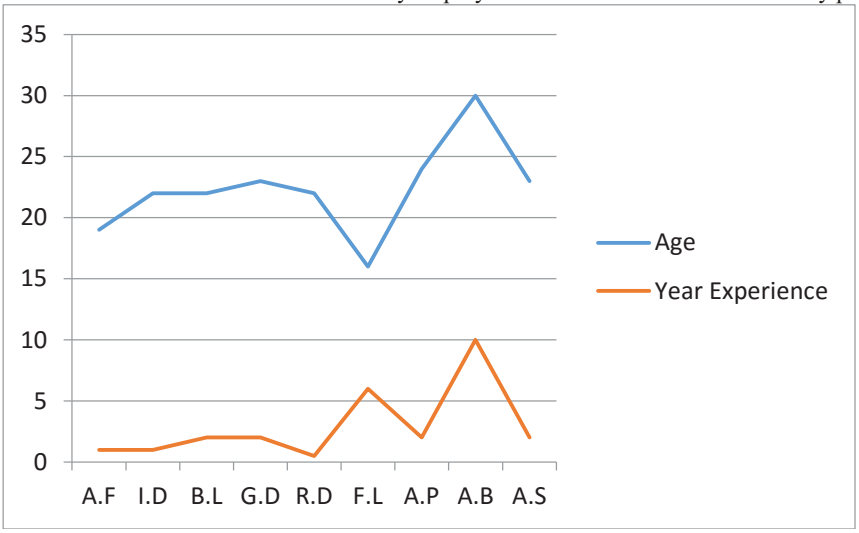


**Figure 1.** Hackers Average Age compare to year experience in IS

During the workshop there were two issues, one to find and report the vulnerabilities as faster as you can and the other was the concurrence hackers trying to interrupt each other in their scanning duties.

## 3. Websites

There were 10 websites selected for Penetration Testing, three of them were from Republic of Kosovo institutions(public sector) and seven others were from private sector. The idea behind is that the hackers have always abilities to scan your websites, because the websites are online and could be accessed everywhere from the internet. But what 'The DAY when hacking is legal' did is giving the websites owners the detailed report not from one hackers logic, but from twenty-five of them. In the same time the hackers would learn how you can make money even doing the right things like White Hat hacker.

**Table 1.** Websites that have been scanned

| Domain | Bugs |
|---|---|
| http://www.rks-gov.net | 2 |
| http://www.kryeministri-ks.net | 2 |

| | |
|---|---|
| http://www.valamobile.com/ | 3 |
| http://www.amdp-rks.org/ | NO |
| http://www.uni-pr.edu | 1 |
| http://www.uni-prizren.com | 5/6 |
| http://www.tollomed.com/ | 1 |
| http://www.stikk-ks.org/ | 2 |
| http://www.pcworld.al/ | 2 |
| http://www.sollaborate.com | NO |

None of the bugs found on the workshop were reported before to websites owners.

## 4. Vulnerabilities

There were some criteria for hackers to submit the report, they needed to follow the standard required in order to get the award. The first hacker who reported the bug got the award, duplicate bugs were not awarded. During eight hours of scanning have been found 19 vulnerabilities, 18 of them were awarded, 1 was duplicate.
Based on the given time of scanning there are almost three bugs per hour. For more about refer the table.

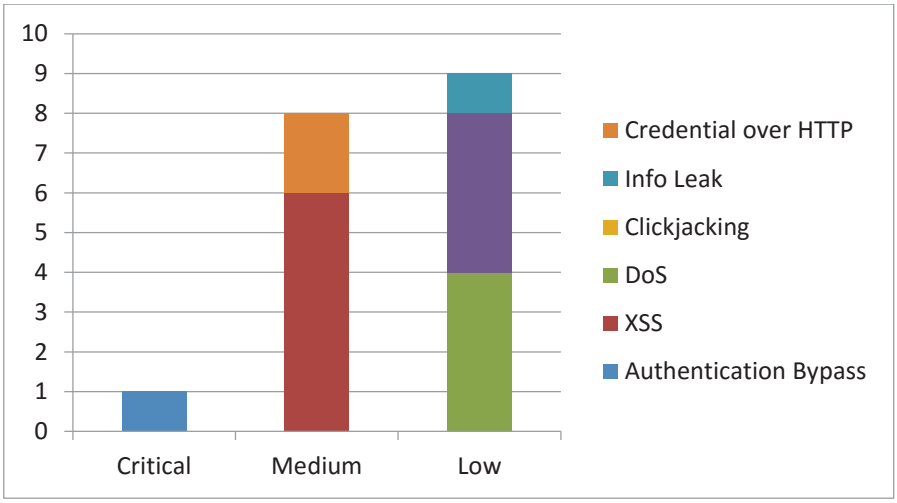


**Figure 2.** Vulnerabilities reported on the workshop

## Conclusion

Bug Bounty as the future of Vulnerability Scanning, it gives you the better quality of report. The well known hackers all over the world not depending geographically can scan and give you a clear report about vulnerabilities of your product.
Based on parameters like hackers, websites, and vulnerabilities during the workshop we can conclude that there is medium level of cyber security in Kosovo. In the other side Intelligence Agencies identified hackers, closely saw how they work, who they are and what can they do.

There is a new age of hackers with good experience that can be potentially developed and usefully in the future, but for the current situation hackers declared that there is no stimulation for the hackers, there is not enough job positions required for information security.[4]

### 5.1 Contributors

Thanks go to jury members, that have professionally evaluated the bugs: Prof. Dr. Blerim Rexha, Mr. Shpend Kurtishaj, Mr. Labeat Avdullahu.

## References

1. http://www.pda-ks.com, 20th of October 2015
2. http://www.pda-ks.com/?page=1,8, 21th of October 2015
3. https://en.wikipedia.org/wiki/Bug_bounty_program, 21th of October 2015
4. http://mzhe.rks-gov.net/repository/docs/Lara_Pace.Kosovo-WB.Presentation-June-2015.pdf, 28th of November 2015