****

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY 2015

IT 501 - Information and Network Security

Assignment 01 – Year 1 Semester 2

Lecturer: Mr.Lakmal Rupasighe

**Security and penetration testing 1**

S.S.Niranga - MS14901836

# Abstract

A penetration test is a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as end-users’ adherence to security policies.[[1]](#endnote-1)

# Acknowledgement

I would like to express my special thanks of gratitude to Dr. Samantha Thelijjagoda for providing me with the opportunity to study at SLIIT as well as my Mr.Lakmal Rupasinghe who gave me this golden opportunity to do this assignment on the topic "Security and penetration testing", which also helped me in doing a lot of research and I came to know about so many new things and I am really thankful to them. Secondly, I would also like to thank wife and friends who helped me a lot in finishing this project within the limited time.

I am making this assignment not only for marks, but to also increase my knowledge.

Thanks again to all who helped me.

Table of Contents

[Abstract 2](#_Toc413096842)

[Acknowledgement 3](#_Toc413096843)

[Install Kali Linux and explore 5](#_Toc413096844)

[**Linux commands.** 6](#_Toc413096845)

[What is bug bounty? 7](#_Toc413096846)

[https://bugcrowd.com/ 7](#_Toc413096847)

[**Creating an account with bugcrowd.com** 8](#_Toc413096848)

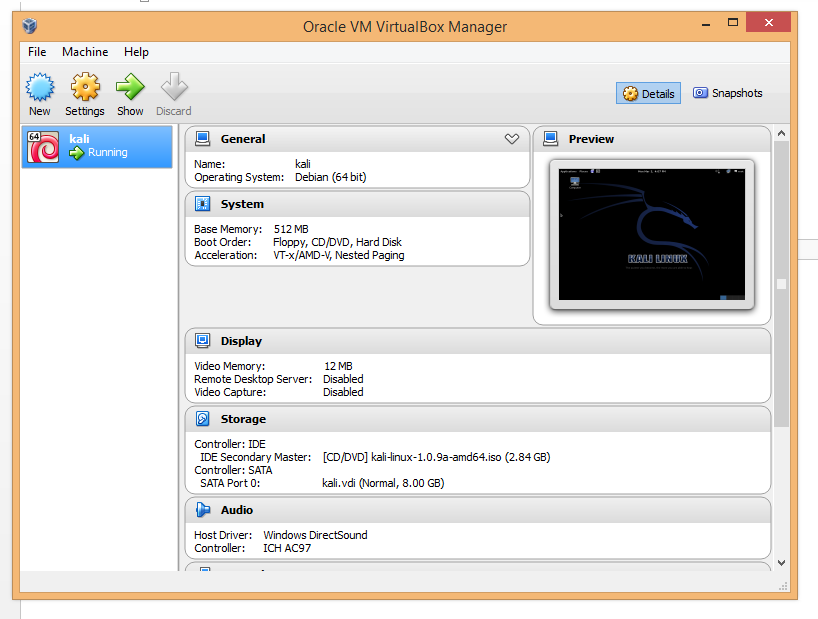
[https://hackerone.com/ 9](#_Toc413096849)

[**Creating an account with hackerone.com** 9](#_Toc413096850)

[References 11](#_Toc413096851)

# Install Kali Linux and explore

Install virtual box and run kali Linux.

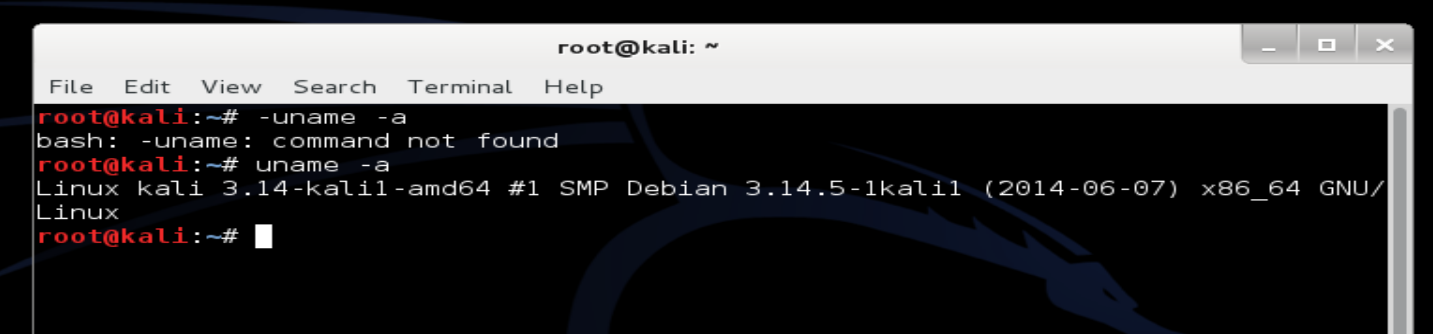




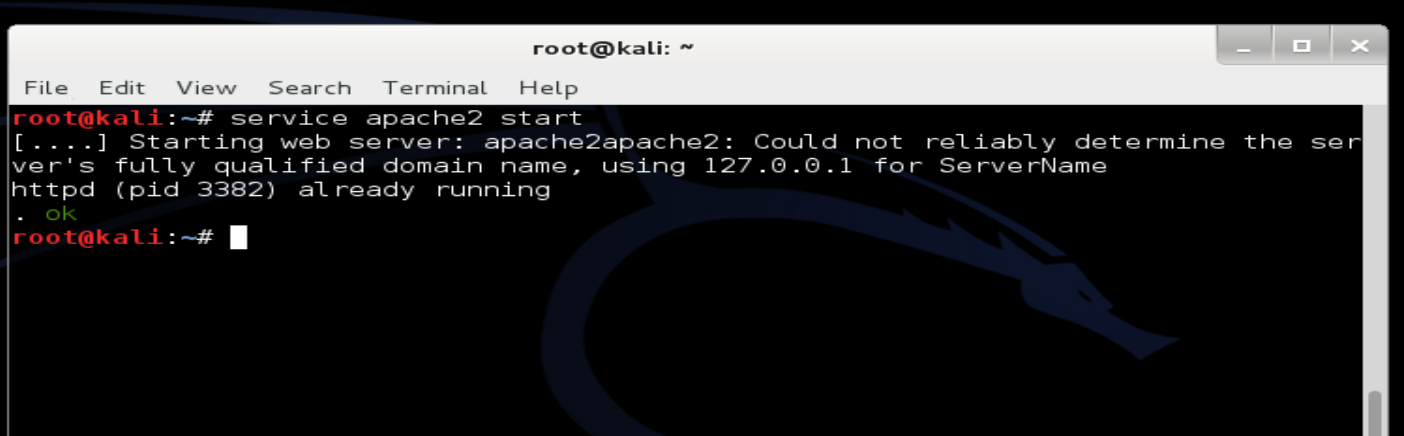


## **Linux commands.**

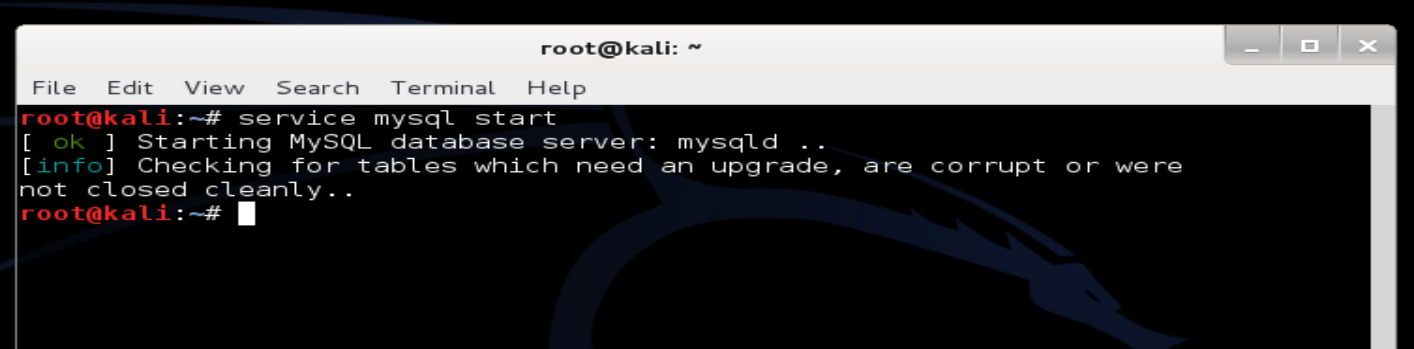
Get the Linux version - uname –a



Start web service- service apache2 start



Start DB



# What is bug bounty?

Many software vendors and web sites run bug bounty programs, often paying out cash rewards to software security researchers and white hat hackers for discovering and reporting software vulnerabilities that could be exploited. Bug reports must document enough information for for the organization offering the bounty to be able to reproduce the vulnerability. Bug bounty programs are often initiated to supplement internal code audits and penetration tests as part of a vulnerability management strategy.

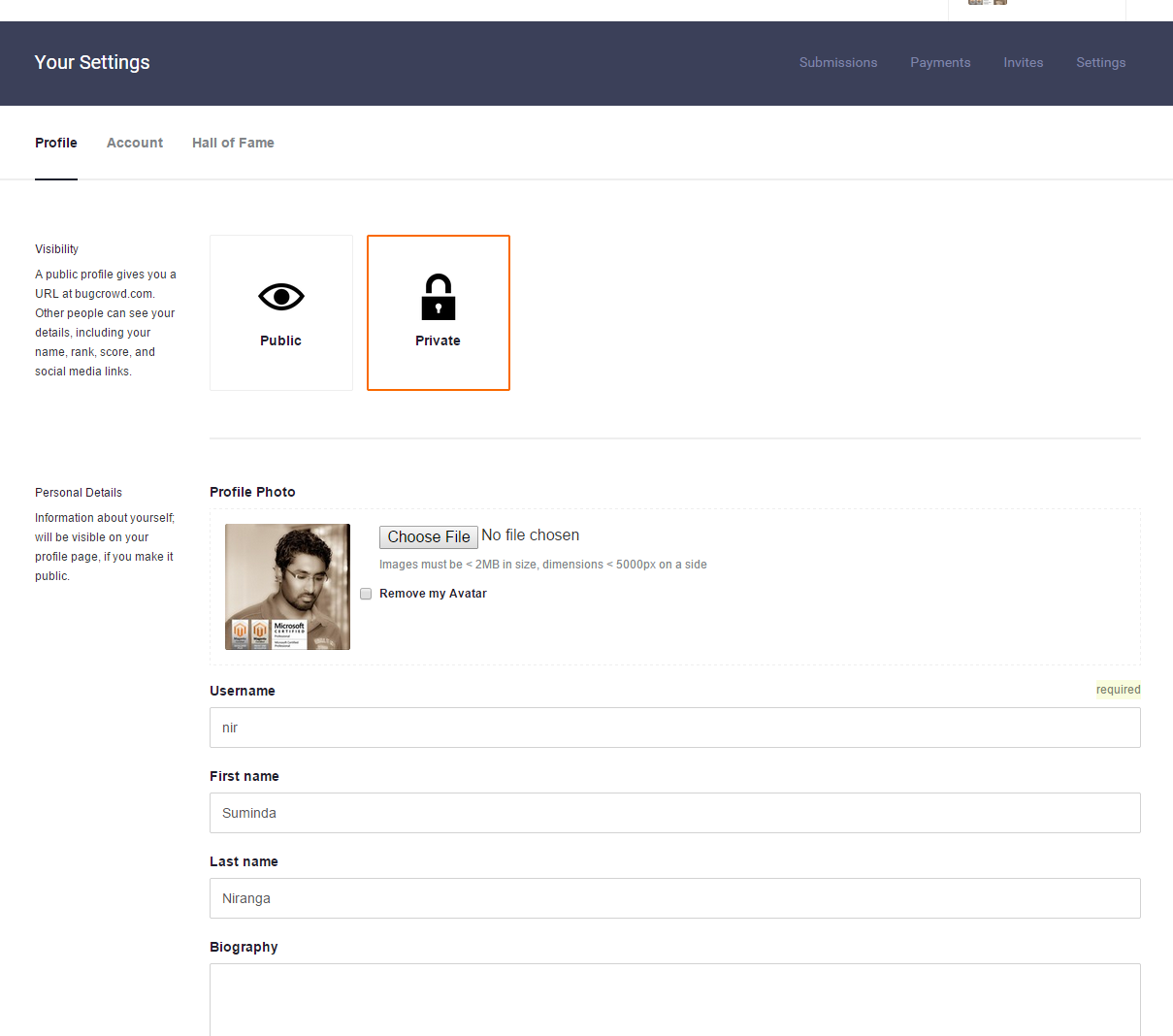
Most companies offer bounties on a sliding scale based on the size of the organization and how much impact on users a bug might have. For example, Mozilla pays out a $3,000 flat rate bounty for bugs that fit its criteria, while Facebook has given out as much as $20,000 for a single bug report. Google paid Chrome operating system bug reporters a combined $700,000 in 2012 and in one of the biggest recent bounties, Microsoft paid UK researcher James Forshaw $100,000 for an attack vulnerability in Windows 8.1.[[2]](#endnote-2)

# <https://bugcrowd.com/>

Bugcrowd was founded in 2012 by CEO Casey Ellis and CTO Chris Raethke to help level the vulnerability assessment playing field. By leveraging the economic, expertise, and sheer numbers of the crowd, the company is redefining the cyber security market.

Their revolutionary approach to cyber security combines a proprietary vulnerability reporting platform with the largest crowd of security researchers on the planet. They also provide a range of responsible disclosure and managed service options that allow companies to commission a customized security testing program that fits their specific requirements. Based in San Francisco, Bugcrowd is backed by Icon Ventures, Paladin Capital and Square Peg Ventures.[[3]](#endnote-3)

## **Creating an account with bugcrowd.com**

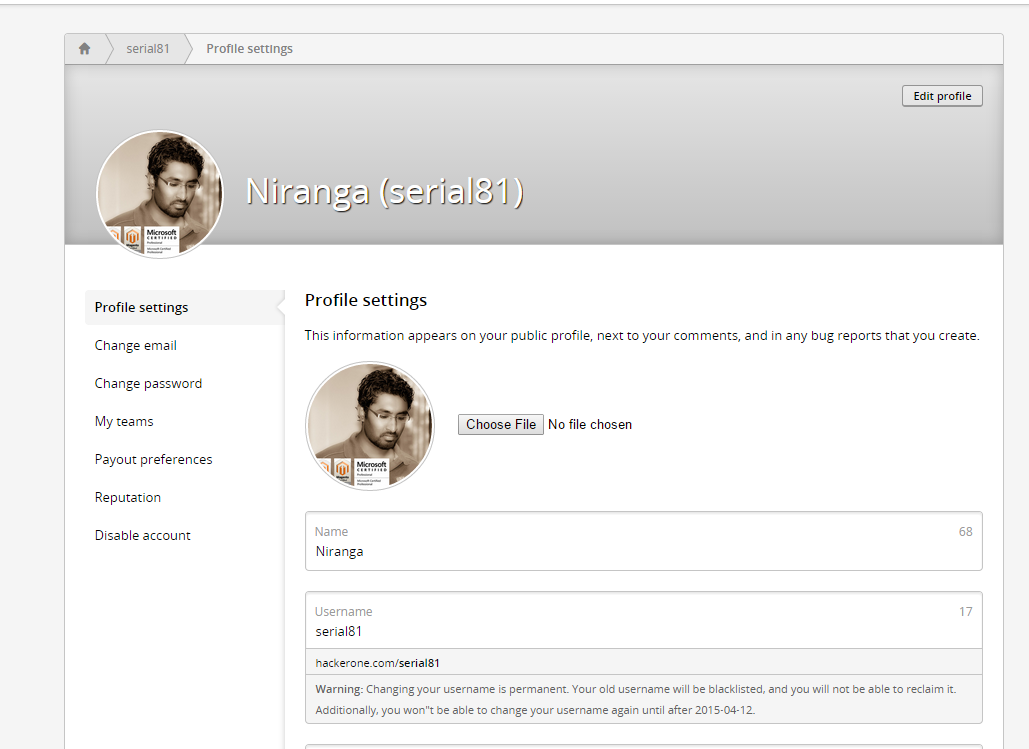


# <https://hackerone.com/>

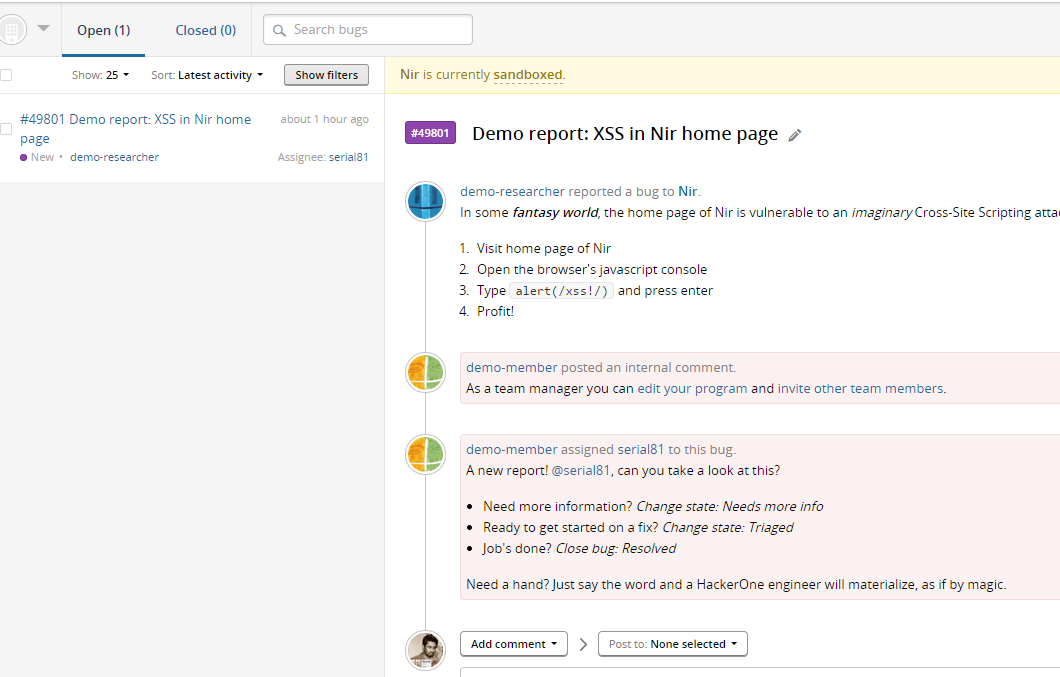
The people behind HackerOne have pioneered Bug Bounty programs and security response at Facebook, Google, and Microsoft. They are working to improve vulnerability coordination for everyone.

They've worked as security researchers, managed security teams for both open and closed source software, and even helped develop the ISO standard on vulnerability disclosure.[[4]](#endnote-4)

## **Creating an account with hackerone.com**



Logged in as a researcher.



# References

1. <http://www.coresecurity.com/penetration-testing-overview> [↑](#endnote-ref-1)
2. <http://whatis.techtarget.com/definition/bug-bounty-program> [↑](#endnote-ref-2)
3. <https://bugcrowd.com/about> [↑](#endnote-ref-3)
4. <https://hackerone.com/> [↑](#endnote-ref-4)