A INTERNSHIP REPORT

ON

"Penetration Testing"

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE

IN

THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD

OF THE DEGREE

BACHELOR OF ENGINEERING

in

INFORMATION TECHNOLOGY

SUBMITTED BY

Nitin Santosh Gavhane

Exam No.: T190658520

Under the Guidance

of

Prof. Richa Agarwal

DEPARTMENT OF IT ENGINEERING

KJEI'S TRINITY COLLEGE OF ENGINEERING AND RESEARCH

KONDHAWA SASWAD ROAD, PUNE 411048

SAVITRIBAI PHULE PUNE UNIVERSITY

2021-2022

Table of Content:

CERTIFICATE

INTERNSHIP COMPLETION CERTIFICATE

Declaration

I do herby declare that the work presented in this report has been carried out by me and has not been previously submitted to any other university/college/organization for other academic qualification/degree/certificate. The work I have presented does not breach any copyright and no portion of this report is copied from any work done earlier or otherwise.

Nitin Santosh Gavhane	Richa Agarwal	Prof. Gajanan Arsalwad
Roll_No: IT3020	(Project Guide)	(HOD IT)

Internship Place Details:

Starting Date of Internship: 9 December 2021

Ending Date of Internship : 15 February 2022

Duration Of Internship : 3 months

Internship Position : Cyber Security Penetration Tester

Company Name : Secureise Cyber Security Training Services Pvt.Ltd

Stipend : Performance Based

Mode Of Internship : Online

Introduction

An internship is a professional learning experience that offers meaningful, practical work related to a student's field of study or career interest. An internship gives a student the opportunity for career exploration and development, and to learn new skills. It offers the employer the opportunityto bring new ideas and energy into the workplace, develop talent and potentially build a pipeline for future full time employees.

The internet has considerably enhanced various business critical operations of company's indifferent industry sectors across the globe. However, as more and more organizations become partially or completely dependent on the internet, computer security and the serious threat of computer criminals comes to the foreground. The explosive growth of the Internet has brought many good things: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few.

Title:

Internship in Cyber Security.
Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

Objective:

With an increasing number of users, devices and programs in the modern enterprise, combined with the increased deluge of data -- much of which is sensitive or confidential -- the importance of cybersecurity continues to grow. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further.

With an internship you have the opportunity to excel and possibly land a jobwith the company. Internships give a taste of what a profession is like, help build a resume and let us meet people who can help you in your career.

Motivation:

Internships are a great way to connect classroom knowledge to real world experience. Learning is one thing, but taking those skills into the workforce and applying them is a great way to explore career paths and specializations that suit individual interests.

Having an internship gives us experience in the career field you want to pursue. Not only does this give individuals an edge over other candidates when applying for jobs, but it also prepares for what to expect in their field and increases confidence in their work.

Methodological Details:

- Testing Phase
- Reporting Phase

Explore Phase:

• As a Cyber Security expert, I had worked on various technology like HTML, CSS, Wordpress, JS(Basics)

• A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities

• As we can find targets from the google by searching for responsible disclosure policy of a website. I recommend to start with responsible disclosure , so there are more chances for acceptence of report. And then after a experience start with Bug Bounty Platform.

• While users could create content, they didn't own it or benefit fromits monetization.

Reporting Phase:

Find a bug or vulnerability, you must file a report to disclose your findings. Generally, you have to explain where the bug was found, who it affects, how to reproduce it, the parameters it affects, and provide Proof-of-Concept supporting information. You can upload any files or logs as supporting evidence.

This not only helps quickly reproduce the issue but moves your submission through the review process faster, with no delays due to missing information.!

Bug Reports –

- Bug Report - config file disclosure
- Access any person Location, Device, IP address/Provider Info Vai using Clickjacking and Reflected xss attack (Subdomain: intercom-vigilante.agicap.com)
- more

Bug Bounty Platforms:

1. Bugcrowd:
   https://www.bugcrowd.com/

2. Hackerone:
   https://www.hackerone.com/

3. Synack:
   https://www.synack.com/

4. Japan Bug bounty Program:
   https://bugbounty.jp/

5. Cobalt:
   https://cobalt.io/

6. Zerocopter:
   https://zerocopter.com/

7. Hackenproof:
   https://hackenproof.com/

8. BountyFactory:
   https://bountyfactory.io

9. Bug Bounty Programs List:
   https://www.bugcrowd.com/bug-bounty-list/

10. AntiHack:
    https://www.antihack.me/

We have a target then how to start ?

If you have chosen your target, then you should start finding the subdomain of the target.

or we can start with the IP blocks of the targets which we can get from the ASN (some of the websites are mentioned in below)

Why we need subdomain?

Sometimes targeting the main domain is not possible to find bugs which will frustrated to the noobs. Because the top or other researchers are already found and reported the bugs to the target. For newbie should start with the other subdomains. (its true that most common vulnerabilities are already reported by the researcher so keep in mind that we have to find a unique target and unique bug.)

How to find Sub-domains?

As per my recon I am using the following tools to find the sub-domains for the target.

Subfinder
Amass
Sublist3r
Aquatone
Knockpy

We can also find sub-domain via online recon tools. (sites are given below)

Virustotal (Use its API in tools)
Dnsdumpster
Findsubdomains
Pentest-tools
Hackertarget

Sub-domain Takeover Vulnerability:

Goto this link and learn about some basics to advance concepts of Subdomain takeover vulnerability.

https://github.com/EdOverflow/can-i-take-over-xyz

Discovering Target Using ASN (IP Blocks):

https://whois.arin.net/ui/query.do

Discovering Target Using Shodan
https://www.shodan.io/search?query=org%3A%22Tesla+Motors%22

Brand / TLD Discovery:
This will increase the target scope by searching for a Aquiasition of a target

Acquisition — -> crunchbase, wikipedia

link discovery — ->burp spidering

weighted& reverse tracker → domlink, builtwith

Parsing JS is very useful to find the directories which is used by the target. we can use these type of tools instead of brute-forcing the directory list on the target

Note: Brute-Forcing of directory also good thing to do. Always use the multiple techniques to find the directory from the targets(I found Hotsar Aws Credentials with Directory Buster & Burp Intruder)

linkfinder
DIRsearch
Dirb
Content Discovery: " Gobuster"
Credential Bruteforce: "BrutesprayBrutespray"

These tools are having the ability to brute-force the different type of protocols like http, ssh,smtp, etc

Technology Identification and Vulnerability findings:

Here I used Wappalyzer and build with addons on the browsers. Whatweb tool also I used to find the what technologies they used on the target.

The following tools to find technologies and technology based vulnerabilities on the target.

WPScan

Cmsmap

Before start testing I recommend this book for bug hunter bcoz it help a lot to understand & Exploit the bug!

The testing is based on our opinion. some of them start with the xss and other vulnerabilities which we can easily found from the target.

Still you are stuck with the testing for a bug means you can start reading the following books which always helpful for Bug hunter or Application Penetration Tester.

for our Mobile hacking friends:

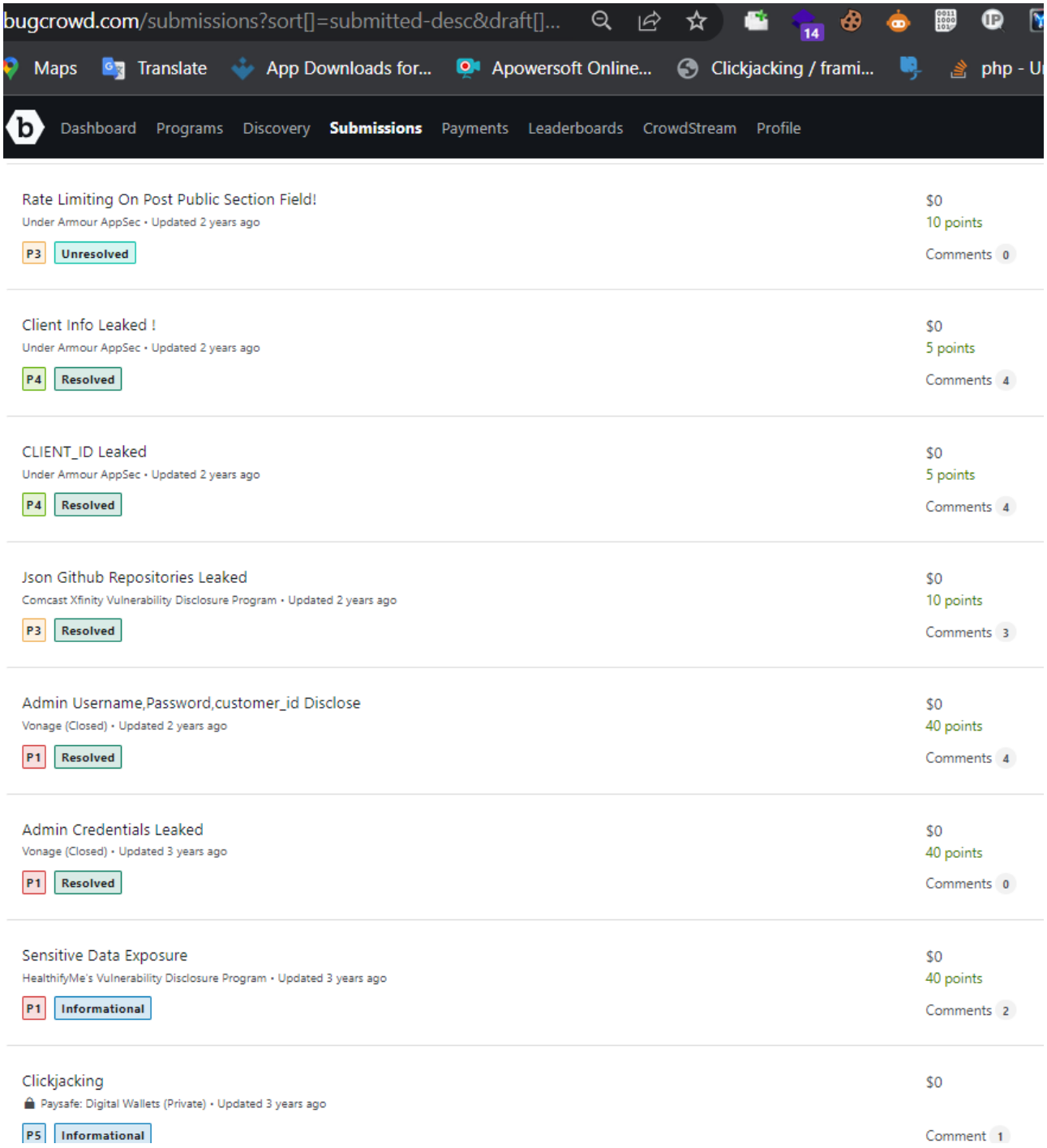
1. The Mobile Application Hacker's Handbook
2. iOS Application Security
3. Owasp Mobile AppSec

I hope these books are very helpful for how to test for a bugs

Popular Google Dorks Use(finding Bug Bounty Websites):

1. site:.eu responsible disclosure
2. inurl:index.php?id=
3. site:.nl bug bounty
4. "index of" inurl:wp-content/ (Identify Wordpress Website)
5. inurl:"q=user/password" (for finding drupal cms)

Result:


bugcrowd.com/submissions?sort[]=submitted-desc&draft[]...
Maps
Translate
App Downloads for...
Apowersoft Online...
Clickjacking / frami...
Dashboard
Programs
Discovery
Submissions
Payments
Leaderboards
CrowdStream
Profile
Rate Limiting On Post Public Section Field!
Under Armour AppSec • Updated 2 years ago
P3
Unresolved
$0
10 points
Comments 0
Client Info Leaked !
Under Armour AppSec • Updated 2 years ago
P4
Resolved
$0
5 points
Comments 4
CLIENT_ID Leaked
Under Armour AppSec • Updated 2 years ago
P4
Resolved
$0
5 points
Comments 4
Json Github Repositories Leaked
Comcast Xfinity Vulnerability Disclosure Program • Updated 2 years ago
P3
Resolved
$0
10 points
Comments 3
Admin Username,Password,customer_id Disclose
Vonage (Closed) • Updated 2 years ago
P1
Resolved
$0
40 points
Comments 4
Admin Credentials Leaked
Vonage (Closed) • Updated 3 years ago
P1
Resolved
$0
40 points
Comments 0
Sensitive Data Exposure
HealthifyMe's Vulnerability Disclosure Program • Updated 3 years ago
P1
Informational
$0
40 points
Comments 2
Clickjacking
Paysafe: Digital Wallets (Private) • Updated 3 years ago
P5
Informational
$0
Comment 1

Conclusion:

In conclusion, I can say that this internship was a great experience. Thanks to this internship, I aquired deeper knowledge concerning my technical skills, but I also personally benified. Currently Bug Bounty is a common part of cybers ecurity, and it is one of the most popular in word. If we surf Internet, we can see millions of websites offer Bounty/Reward for Bug finding. I learned to live in different environment from the one I in everyday life. I could do more things than I thought, like learning new things by myself.

Internship offer us a chance to put what their learning into actions in a real-world environment is helps to better understand the theories andstrategies which have been reading about

internship helps to learn about the work environment but it also helps to learn about your goal and will have a much clearer idea of your strengths and weaknesses.

Internships given me an exposure to gain a competitive experience, equip and develop with more than technical as well as soft skills. Also, an opportunity to establish critical networking connections andso on.

Future Scope:

If some has no experience in the field, finding work can be real challenge. A successful Internship can help an individual turn and experience into a career opportunity, So as a successful internship some future scopes are:

- To work in Cyber Security.
- Can work as a Software Engineer.
- Can work as a Web Developer.
- Can work as a Web Designer.

References:

- https://github.com/ngalongc/bug-bounty-reference
- https://pentester.land/list-of-bug-bounty-writeups.html
- https://tikam02.github.io/Bug-Bounty-Resources/