Weekly Diary
For
Industrial Training

Name of the Industry: Secure Cyber Future

From:

Name of the Supervisor

Designation of the Supervisor:

Name of the Student: Vaishnavi Parulekar

Branch of Engineering: Computer Engineering

Name of Polytechnic: Vidyalankar Polytechnic

(**Special instructions to students:**

1) Write down the daily activity on the same day
2) Make note of the important actual activity/ies only.
3) Summarize at the week-end.
4) Add extra sheets if needed for daily or weekly activity report.)

Week 1: From: 5/6/2024 To: 12/06/24

Expected Work:

i. **Study of organization chart of industry / plant with responsibilities of the different post.**

ii. **General Study of Industry, its location, its history and its product range, its size, number of employees, Its turnover etc.**

Day	Activities Carried Out
1	**Install the Burp Suite** -Install the Burp Suite and connected it with FireFox Settings such that the FireFox was manually poxy configured i.e. with HTTP proxy 127.0.0.1 and Port 8080
2	**Learned about how to use the Burp Suite** -Learned how to use Proxy, Repeater, Target and Intruder in the Burp Suite And learned how to use it for performing security testing of web applications. -Burp Proxy operates as a web proxy server between the browser and target application so we can get the parameters to send to Intruder and Repeater. -The Proxy enables us to intercept, inspect, and modify traffic that passes in both directions. -Burp Intruder is a powerful tool for performing highly customizable, automated attacks against website.
3	**Learned about XSS vulnerability** -Cross-site scripting (XSS) is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website. Attackers often initiate an XSS attack by sending a malicious link to a user and enticing the user to click it. -Its types such as Reflected XSS, where the malicious script comes from the current HTTP request. Stored XSS, where the malicious script comes from the website's database. DOM-based XSS, where the vulnerability exists in client-side code rather than server-side code.
4	**Learned about XSS vulnerability** - Understood the types of impacts of XSS. - if the java script line of code is injected in the vulnerable part and the output comes 1 so that particular part of the website is vulnerable. - Learned this by the videos provided.
5	**Did Testing of XSS vulnerability for adidad.cvicte.sk website** https://adidas.cvicte.sk/ by injecting the script **"/><script>alert (1) </script>**
6	**Made the report for this adidad.cvicte.sk website** -Regarding the vulnerability of the website -Procedure, Risk and Mitigation

Weekly summarization of the above activities:

-Learned how to use Burp Suite

-Learned in detail about Cross Site Scripting (XSS)

-Learned how we can use XSS for a vulnerable website

-Learned about its Risk and Mitigation

-Learned about the impacts of a vulnerable website.

Signature of the Student: _________________Signature of the Industrial Supervisor______________

Week 2: From: 13/6/2024 To: 17/6/2024

Expected Work:

i. Study of layout specification of major machines, equipments and raw materials/ components used.

List the sections of Industry visited and list the major machines, equipment and raw material etc., studied

Day	Activities Carried Out
1	**Downloaded SQL Map and installed the latest version of Python**.
2	**Learned how to use SQL Map with the help** of the commands like –crawl 2, --batch, --technique=” U”, --risk, --tables, --dump etc. To fetch the database from the website.
3	**Did a penetration testing task on the website, sistemas.pedagogica.edu.sv using SQL Map and Burp Suite**. -The website did not have end points so through, **site: http://sistemas.pedagogica.edu.sv/inurl:id=** by this Google dork https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271 the endpoints were made. -To fetch the database and columns of the website, with their names. -Used Burp Suite for SQL injection by doing crawling. -Made the report for this website with documentation of identified vulnerabilities and recommendations for remediation.
4	**Learned about CORS (Cross-Origin Resource Sharing) vulnerability**. -CORS defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. - We can check the Insecure CORS by using curl command in the command prompt. It can also be checked by using the Burp Suite **- Access-Control-Allow-Origin: *** **- Access-Control-Allow-Origin: https://dhanishthaparu.com** **-Access-Control-Allow-Origin: *** **Access-Control-Allow-Credentials: true** **-Access-Control-Allow-Methods: GET, POST, PUT, DELETE** -By the videos provided
5	**Learned about CORS (Cross-Origin Resource Sharing) vulnerability.** **-**Exploitation of insecure CORS. - Example, vaishnavi.com uses a text font that's hosted on parulekar.com. When visiting example.com, the user's browser will make a request for the parulekar from parulekar.com in this vaishnavi.com is Origin website and the website to test is parulekar.com using curl command Example: curl https://www.parulekar.com /H “Origin: https://www.vaishnavi.com” -I

Weekly summarization of the above activities:

- Downloaded SQLMap and installed the version of Python.

- Learned how to use SQLMap with the help of the commands.

- Did a penetration testing task on the website, sistemas.pedagogica.edu.sv using SQLMap and Burp Suite.

-Made the Report

- Learned about CORS (Cross-Origin Resource Sharing) vulnerability. By using

-Access-Control-Allow-Origin: *

-Access-Control-Allow-Origin: https://dhanishthaparu.com

-Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true

-Access-Control-Allow-Methods: GET, POST, PUT, DELETE

- Exploitation of insecure CORS can be done by curl command. By the provided videos.

Signature of the Student: _______________ Signature of the Industrial Supervisor_______________

Week 3: From: 18/6/24 To:22/6/24

Expected Work:

i. Study of production process along with production planning and control procedures.

List the sections of Industry visited and list the major production process, and products for which planning and control procedures etc. are studied:

Day	Activities Carried Out
1	**-Recevied task 3 regarding CORS vulnerability** it was To test the website [demandbase.com](https://www.demandbase.com) with a focus on its origin domain api.demandbase.com.
2	**-Used Curl command**. - curl https://www.demandbase.com /H "Origin: https://api.demandbase.com" -I - The Access-Control-Allow-Origin: *. Came by using this curl command. Then pasted the link: https://www.demandbase.com/wp-js in the html file and saved the file as cors.html. Then tried to exploit it but it was not able to exploit as it was misconfigured. -Made the report by highlighting the Procedure, Potential impacts of the vulnerabilities and Recommendations for mitigation.
3	**Learned about email Rate limiting** -By using Temp mail. Creating an account in the website than log out and then log in type the email address turn the proxy (intercept on) and do forget password the traffic will get collected. -By the videos provided.
4	**Learned about email Rate limiting** -Sent it to the intruder add the payload as null payload. -By the videos provided
5	**Learned about email Rate limiting** -There are same number of emails in the inbox as the null payloads in the intruder and when status code is 200 means the attack is successful i.e. the number of payloads used the same number of emails have been sent. -By the videos provided

Weekly summarization of the above activities:

-Gave task 3 regarding CORS vulnerability test the website [demandbase.com](https://www.demandbase.com) with a focus on its origin domain api.demandbase.com.

-Made the report for CORS vulnerability

-Learnt the procedure of email rate limiting.

-By the videos provided

Signature of the Student: ________________ Signature of the Industrial Supervisor________________

Week 4: From: 25/06/2024 To: 28/06/24

Expected Work:

i. Study of testing and quality assurance process

List the sections of Industry visited and list the major testing and quality assurance process studied there.

Day	Activities Carried Out
1	**Learned about email rate limiting from You tube**
2	**Received the task 4 of email rate limiting**. - To verify the "Forgot Password" functionality of invoicer.ai. -By using Burp Suite - And followed the steps as learned in the videos
3	**Made the Report** **-** highlighting the Procedure, Potential impacts of the vulnerabilities and Recommendations for mitigation.
4	**Learnt about Google Dorks** **-**Google hacking database.

Weekly summarization of the above activities:

-Learnt about email rate limiting.

-Provided the task 4 for email rate limiting on invoicer.ai website

-Made the Report

-Learnt about Google dorks

Signature of the Student: _______________ Signature of the Industrial Supervisor_______________

Week 5: From 1/07/2024 To 4/07/2024

Expected Work: Study of preventive and breakdown maintenance & safety practice adopted in industry

List the sections of Industry visited and list

i. The major machines/ plant whose preventive and breakdown maintenance procedure studied.

ii. The major safety practices adopted in the industry

iii. Organization chart of the industry with responsibilities of different department/posts.

Day	Activities Carried Out
1	**Learnt about Google Dorks** -They are queries that use advanced operators to find specific information on the internet. - The GHDB has several search queries and operators that can uncover numerous sensitive files, vulnerable web servers, and applications
2	**Learnt about Google Dorks** Filetype, inurl ,intitle, site: , intext , link etc.
3	**Recevied task 5 regarding Google dorks on google hacking database**. -The task was to find 5 vulnerable websites using google dorks. (https://www.exploit-db.com/google-hacking-database). - Specified Google Dorks used to find these vulnerabilities.
4	**Made the report by highlighting the** **-** Detailed descriptions of the vulnerabilities found on each site. - Potential impacts of the identified vulnerabilities. - Recommendations for remediation if applicable**.**

Weekly summarization of the above activities:

-Learnt about Google dorks

-Found 5 Vulnerable sites on the google dorks they were

SQL injection

Files containing password of Gmail

Admin login page

Network or Vulnerability data

Vulnerable servers

-Made the report

Signature of the Student: _______________Signature of the Industrial Supervisor_______________

Week 6: From 10/07/2024 To 13/07/2024

Expected Work: Report Writing
List the sections of Industry visited and list the major manual/ broachers such as operational manual, safety manual, maintenance manual ,quality manual standard referred/studied there for preparation of report.

Day	Activities Carried Out
1	**Received the task 6** **-**In this task I had to find all the 5 vulnerabilities on (https://www.exploit-db.com/google-hacking-database). - They were XSS SQL CORS vulnerability Email rate limiting Google Dorks vulnerable sites
2	**Searched for these vulnerabilities in the provided website** -Found XSS, CORS vulnerability and Google Dorks vulnerable sites
3	**Searched for these vulnerabilities in the provided website** -Found SQL and Email rate limiting
4	**Made the Report** **-**Detailed description for each vulnerability

Weekly summarization of the above activities:

-Received task 6

-Found the 5 vulnerabilities on google hacking database by visiting different dorks.

-They were XSS, SQL, CORS vulnerability, Email rate limiting and Google Dorks vulnerable sites.

-Took a note of the website visited

-Made the report

Signature of the Student: _______________ Signature of the Industrial Supervisor_______________