CS-MINOR-SEP

Name – Anjali Kumari

Email- anjalirajwar101@gmail.com

Collage Name – BIT Sindri

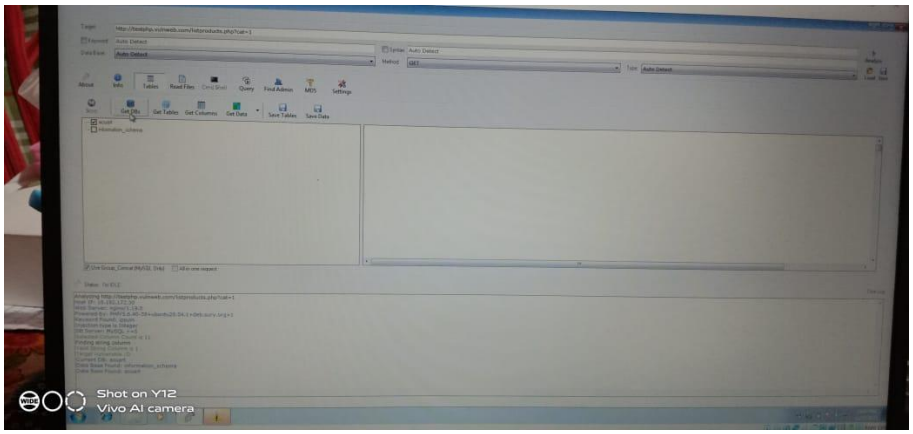
Domain – Cyber Security

Project Name : Cyber Security Minor Project

5. Perform SQL injection on by using Havij Tool(Download it from Internet) on http://testphp.vulnweb.com Write a report along with screenshots and mention preventive steps to avoid SQL injections.

Step1. First download Havij from here and install it. Then open it and enter the vulnerable page url in the target column (for this tut I am using my own vulnerable webpage).

Step2. Set the database option to ‘auto detect‘ and hit analyze. This should show you the current database name as shown below.



Step 3. Click on the “info” tab. This will show you information about the victim’s system. We can see information like Host IP address, web server version etc.

Target: http://testphp.vulnweb.com/listproducts.php?cat=1

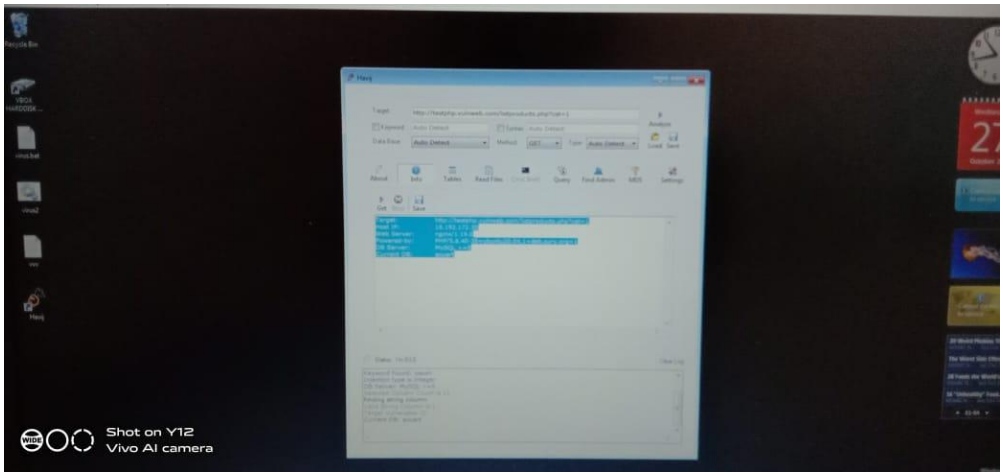
Host IP: 18.192.172.30

Web Server: nginx/1.19.0

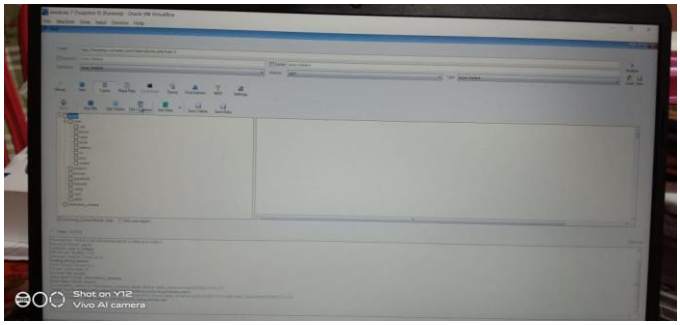
Powered-by: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

DB Server: MySQL >=5

Current DB: acuart



Step 5. Click on the “Tables” tab.



Step6. Click on “Get DBs” option. This will list all the databases as shown below.

Step 7. To get tables in a specific database, select the database and click on “Get Tables”. This will list all the tables present in the selected database. I selected database “shunya” here.

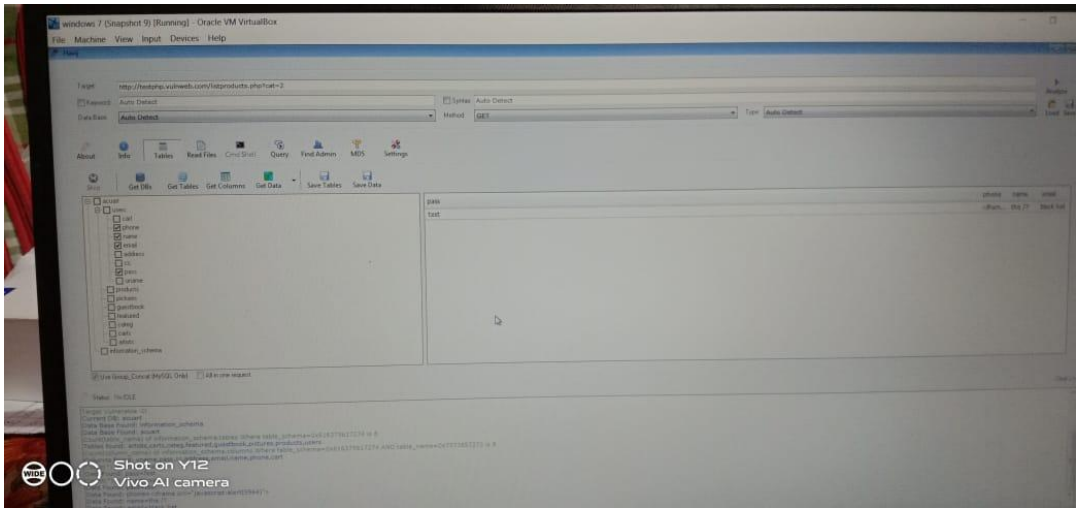
Step8. We can see that there is on table ‘users’ in our database ‘shunya’ .To get columns , select the table ‘ users’ and click on “Get Columns”

This will list all the columns in the table. We can see that we have five columns in the table ‘users’.all the columns. It’s time to dump the values of columns. Select

the columns whose data we want to dump and click on “Get data”. Here I selected all the columns.

We got all the data including usernames and passwords. But passwords seem to be encrypted. No problem. Click on the password hashes and copy them. Then click on “MD5” tab and paste the password. Click on “Start”. Havij automatically decrypts the password for us. Decrypt all passwords in the similar manner.

Click on “Find admin”. This option finds the admin page of the website automatically. When it finds the admin page, you can try the username and passwords to get access to the website.



Steps to prevent SQL injection attacks

1. Validate User Inputs
2. Sanitize Data By Limiting Special Characters
3. Enforce Prepared Statements And Parameterization
4. Use Stored Procedures In The Database
5. Actively Manage Patches And Updates
6. Raise Virtual Or Physical Firewalls
7. Harden Your OS And Applications
8. Reduce Your Attack Surface
9. Establish Appropriate Privileges And Strict Access
10. Limit Read-Access
11. Encryption: Keep Your Secrets Secret
12. Deny Extended URLs
13. Don’t Divulge More Than Necessary In Error Messages
14. No Shared Databases Or User Accounts
15. Enforce Best Practices For Account And Password Policies
16. Continuous Monitoring Of SQL Statements

17. Perform Regular Auditing And Penetration Testing

18. Code Development & Buying Better Software

19. Stopping SQL injections recap

- Privileged Access Management (PAM)
- Penetration Testing
- Security Information and Event Management (SIEM)
- Next-Generation Firewall (NGFW)
- Network Access Control (NAC)
- Intrusion Detection and Prevention (IDPS)
- Threat Intelligence
- User and Entity Behavior Analytics (UEBA)

Thank You…