TITLE OF THE PROJECT – MALWARE DETECTION AND CLASSIFICATION

TEAM MEMBERS –

Rohit Patiballa	VIT Vellore	Rohit.Patiballa2021@vitstudent.ac.in
Saumyaa Prajapat	VIT Vellore	Saumyaa.Prajapat2021@vitstudent.ac.in
Sreya Gopakumar	VIT Vellore	Sreyagopakumar.Nair2021@vitstudent.ac.in
Aniket Rai	VIT Vellore	Aniket.Rai2021@vitstudent.ac.in

INDEX

ABSTRACT

Malware, short for malicious software, represents a persistent and ever-evolving threat in the realm of cybersecurity. It encompasses a wide range of harmful software programs designed to compromise the security, privacy, and functionality of computer systems, networks, and digital devices. As a response to this ongoing challenge, the field of Malware Detection and Classification has emerged as a critical and dynamic domain within cybersecurity. In this abstraction, we delve into the multifaceted world of malware detection and classification, exploring its significance, key methodologies, and the continuous evolution of threat landscapes.

Malware detection and classification is the process of identifying and categorizing malicious software that can harm computer systems. This process is crucial for protecting computer systems from potential risks. Malware detection and classification can be performed using various techniques, including machine learning, deep learning, and static analysis. The most common approach is to use machine learning algorithms to analyze the behavior of malware and classify it into different categories. Deep learning techniques have also been used to detect and classify zero-day malware, which is malware that has never been seen before. Malware detection and classification can be performed using dynamic analysis, which involves analyzing the behavior of malware in a controlled environment, or static analysis, which involves analyzing the code of malware without executing it. The goal of malware detection and classification is to develop effective tools that can detect, classify, and block malware threats in real time.

Some of the ideas our team has brainstormed during our brainstorming session are –

- Behavioral Analysis for Android Apps: Develop a system that analyzes the behavior of Android applications in real-time, monitoring for unusual or malicious activities such as unauthorized data access or suspicious network requests.
- Phishing and Social Engineering Detection: Develop systems that not only identify traditional malware but also detect phishing attempts and social engineering attacks.
- Zero-Day Detection: Developing systems capable of identifying and mitigating threats that have never been seen before, to counteract the unpredictable nature of zero-day exploits.
- Real-Time Detection: Build systems that can detect and classify malware in real-time to prevent immediate threats.
- Adaptive Malware Detection: Create systems that can adapt and evolve to detect new strains of malware based on previous detection and classification.
- Real-Time Link Scanning: Use URL scanning services and real-time link analysis to identify and block links in emails that lead to malicious or phishing websites

STAGE 1 REPORT

List of Vulnerabilities

1. VULNERABILITY NAME: HTTP METHODS ALLOWED (PER DIRECTORY)

CWE : 650 (https://**CWE :** .mitre.org/data/definitions/650.html)
DESCRIPTION : By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
Business Impact : the vulnerability related to "HTTP METHODS ALLOWED (PER DIRECTORY)" can have significant business impacts, including data breaches, damage to your reputation, and potential legal and regulatory consequences due to the unauthorized access to sensitive data on your web server.
Vulnerability Path : https://opensourcefootball.com(75.2.60.5)
Vulnerability Parameter: https://75.2.60.5/opensourcefootball.com / HTTP Methods Allowed
About this vulnerability: By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. The following HTTP methods are considered insecure:PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request. **Ways to exploit vulnerabilities:** Using the PUT method, you can upload any file on the server. This can be used to perform Cross Site Scripting (XSS). How you do this is explained below.

```
PUT /XSS.html HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE5.01; Windows NT)
Host: www.myblog.com
Accept-Language: en-us
Connection: Keep-Alive
Content-type: text/html
```

Content-Length: 182
(Input your XSS script here)
The server responds back with a 201 status code which says “file was created successfully”.
HTTP/1.1 201 Created
Date: Mon, 05 May 2014 12:28:53 GMT
Server: Apache/2.2.14 (Win32)
Content-type: text/html
Content-length: 30
Connection: Closed

Now we can try to access this uploaded XSS.html file in browser. As soon as you access this page, you get an XSS pop-up. Likewise, this can be further exploited to perform Command Injection as well, though I haven't tried this yet. If application uses XML, then XML External Entity attack can also be performed. Have not done this too yet. Directory Traversal attack may be possible, too.

Recommendation/solution : - As this list may be incomplete, the plugin also tests if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

2. VULNERABILITY NAME: HSTS MISSING FROM HTTPS SERVER

CWE : 523
DESCRIPTION : The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.
Business Impact : In brief, the business impact of the "HSTS Missing from HTTPS Server" vulnerability includes potential data exposure, the risk of man-in-the-middle attacks, a loss of customer trust, possible regulatory compliance issues, and negative SEO impact. This can result in data breaches, reputation damage, reduced website traffic, legal consequences, and lower search engine rankings.
Vulnerability Path : https://opensourcefootball.com(75.2.60.5)
Vulnerability Parameter: https://75.2.60.5/opensourcefootball.com/HSTS

Missing From HTTPS Server Threats

HSTS addresses the following threats:

· User bookmarks or manually types http://example.com and is subject to a man-in-the-middle attacker

· HSTS automatically redirects HTTP requests to HTTPS for the target domain

· Web application that is intended to be purely HTTPS inadvertently contains HTTP links or serves content over HTTP

· HSTS automatically redirects HTTP requests to HTTPS for the target domain

· A man-in-the-middle attacker attempts to intercept traffic from a victim user using an invalid certificate and hopes the user will accept the bad certificate

· HSTS does not allow a user to override the invalid certificate message

Ways to exploit vulnerabilities: One of the example is you log into a free Wi-Fi access point at an airport and start surfing the web, visiting your online banking service to check your balance and pay a couple of bills. Unfortunately, the access point you're using is actually a hacker's laptop, and they're intercepting your original HTTP request and redirecting you to a clone of your bank's site instead of the real thing. Now your private data is exposed to the hacker.Strict Transport Security resolves this problem; as long as you've accessed your bank's website once using HTTPS, and the bank's website uses Strict Transport Security, your browser will know to automatically use only HTTPS, which prevents hackers from performing this sort of man-in-the-middle attack.

All present and future subdomains will be HTTPS for a max-age of 1 year. This blocks access to pages or subdomains that can only be served over HTTP. HTTP Copy to Clipboard

Strict-Transport-Security: max-age=31536000; includeSubDomains

Although a max-age of 1 year is acceptable for a domain, two years is the recommended value as explained on https://hstspreload.org.

In the following example, max-age is set to 2 years, and is suffixed with preload, which is necessary for inclusion in all major web browsers' HSTS preload lists, like Chromium, Edge, and Firefox.

HTTP Copy to Clipboard

Strict-Transport-Security: max-age=63072000; includeSubDomains; preload

Recommendation/solution: Configure the remote web server to use HSTS.

- To fix the HSTS Missing from HTTP Server error, follow the 5 steps below.
    1. Create a Full Website Backup before adding the HTTP Transport Security Header
    2. Use an HTTP to HTTPS Redirect with 301 Status Code
    3. Add the HSTS Header to the Web Server for Forcing the Usage of HTTPS
    4. Add the Website to the HSTS Preload List of Google for Protection
    5. Audit and Validate the HSTS Header from the Website

Fixation and solution of HSTS Missing from HTTPS Server provides a better trust for the websites from search engines and web users.

3. **VULNERABILITY NAME: SSL CERTIFICATE 'COMMONNAME' MISMATCH**

CWE : : 297 (https://**CWE :** .mitre.org/data/definitions/297.html) OWASP 2017-A3

DESCRIPTION : The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Vulnerability Path : https://opensourcefootball.com(99.83.231.61)

Vulnerability Parameter: https://75.2.60.5/opensourcefootball.com/SSL Certificate 'commonName' Mismatch

Business Impact : A "Common Name" (CN) mismatch in an SSL certificate can lead to:

- Trust issues.
- Security risks.

- User loss.
- Reputation damage.
- Legal and compliance problems.

Common Consequences:

Scope	Impact	Likelihood
Access Control	Technical Impact: *Gain Privileges or Assume Identity* The data read from the system vouched for by the certificate may not be from the expected system.	
Authentication Other	Technical Impact: *Other* Trust afforded to the system in question - based on the malicious certificate - may allow for spoofing or redirection attacks.	

Example 1

The following OpenSSL code obtains a certificate and verifies it.

(bad code)

Example Language: C

```
cert = SSL_get_peer_certificate(ssl);

if (cert && (SSL_get_verify_result(ssl)==X509_V_OK)) {

 // do secret things

}
```

Even though the "verify" step returns X509_V_OK, this step does not include checking the Common Name against the name of the host. That is, there is no guarantee that the certificate is for the desired host. The SSL connection could have been established with a malicious host that provided a valid certificate.

Solution: If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

4. VULNERABILITY NAME: SSL CERTIFICATE SIGNED USING WEAK HASHING ALGORITHM (KNOWN CA)

CWE : -310 (https://**CWE :** .mitre.org/data/definitions/310.html)
OWASP 2017-A3
DESCRIPTION : This vulnerability poses a significant risk to IT infrastructure as it can be used to compromise the security of the SSL certificate. Attackers can exploit the weak hashing algorithm to gain access to sensitive data or to launch malicious attacks on the system (OWASP Testing Guide, 2020). As a result, the system may be vulnerable to malicious attacks, data leakage, and other security incidents.
Vulnerability Path : https://opensourcefootball.com(99.83.231.61)

Vulnerability Parameter: https://75.2.60.5/opensourcefootball.com/SSL Certificate 'commonName' Mismatch

Business Impact : In brief, the business impact of having an SSL certificate signed using a weak hashing algorithm (known CA) includes:

- Data Breach Risk: Increased vulnerability to data breaches.
- Loss of Customer Trust: Decreased trust from users, potentially leading to reduced engagement and sales.
- Regulatory Compliance Issues: Non-compliance with data protection regulations, resulting in fines and legal repercussions.
- Reputation Damage: Negative publicity and damage to the organization's reputation.
- Financial Consequences: Potential financial losses due to breach-related costs and customer churn.

Addressing this vulnerability is crucial to maintaining a secure and trusted online presence.

1. Exploits: an example of the vulnerability The following example code illustrates the use of a weak

hashing algorithm to sign an SSL certificate.

```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr

openssl x509 -req -days 365 -in server.csr -signkey server.key -sha1
```

In the code above, the command “sha1” is used to sign the SSL certificate using the SHA-1 algorithm.

This is an example of a weak hashing algorithm and should be avoided in order to protect the SSL certificate from being compromised (OWASP Testing Guide, 2020).

Solution: The most effective solution to this vulnerability is to use a stronger algorithm to sign the SSL certificate. Specifically, SSL certificates should be signed with a SHA-2 algorithm, which is more secure than the SHA-1 algorithm (OWASP Testing Guide, 2020). Additionally, the system should be regularly monitored for any signs of potential security incidents such as suspicious activity, data leakage, or malicious attacks.

5. Vulnerability Name: CGI Generic SQL Injection(blind)

Risk Factor : High
CWE : : 20, 77, 89, 91, 203, 643, 713, 722, 727, 751, 801, 810, 928, 929
OSWAP CATEGORY : A03:2021- Injection
DESCRIPTION : By sending specially crafted parameters to one or more CGI scripts hosted
on the remote web server, Nessus was able to get a very different response, which suggests
that it may have been able to modify the behavior of the application and directly access the underlying database. An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system. Note that this script is experimental and may be prone to false positives.
Vulnerablity Path : http://testfire.net/
Business Impact : An attacker could exploit this vulnerability to:

- Bypass authentication and gain access to sensitive data, such as customer records,financial information, or trade secrets.
- Modify or delete data in the database, which could disrupt business operations or lead to financial losses.
- Take control of the web server or underlying operating system, which could allow them to launch further attacks or disrupt the business's online operations.
- Recommendation: Modify the affected CGI scripts so that they properly escape arguments.

6. **Vulnerability Name: CGI Generic Cookie Injection Scripting**

Risk Factor : Medium
CWE : : 477, 642, 715, 722
OSWAP CATEGORY : A03:2021- Injection
DESCRIPTION : The remote web server hosts at least one CGI script that fails to adequatelysanitize request strings with malicious JavaScript.
By leveraging this issue, an attacker may be able to inject arbitrary cookies. Depending on the structure of the web application, it may be possible to launch a 'session fixation' attack using this mechanism. Please note that:
-Nessus did not check if the session fixation attack is feasible.
-This is not the only vector of session fixation.
Vulnerablity Path : http://testfire.net/
Business Impact : An attacker could exploit this vulnerability to:

- Steal session cookies and impersonate users:- This could allow the attacker to access users' accounts, steal sensitive data, or make unauthorized transactions.
- Launch session fixation attacks:- This could allow the attacker to force a victim to use a predetermined session cookie, which could allow the attacker to impersonate the victim or steal their data.
- Inject malicious code into cookies:- This could allow the attacker to execute arbitrary code on the victim's browser, which could lead to data theft, account takeover, or malware infection.

Recommendation: Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

7. **Vulnerability Name: CGI Generic HTML Injection(quick test)**

Risk Factor : Medium
CWE : : 80, 86
OSWAP CATEGORY : A03:2021- Injection
DESCRIPTION : The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML to be executed in a user's browser within the security context of the affected site. The remote web server may be vulnerable to IFRAME injections or cross-site scripting attacks:
-IFRAME injections allow 'virtual defacement' that might scare or anger gullible users. Such injections are sometimes implemented for 'phishing attacks.
-XSS are extensively tested by four other scripts.
-Some applications (e.g. web forums) authorize a subset of HTML without any ill effect. In this case, ignore this warning.
Vulnerablity Path : http://testfire.net/
Business Impact :
An attacker could exploit this vulnerability to:
- Inject malicious HTML into web pages:- This could allow the attacker to deface the website, redirect users to malicious websites, or steal their data.
- Launch cross-site scripting (XSS) attacks:- This could allow the attacker to steal session cookies, hijack user accounts, or execute arbitrary code on the victim's browser.
- Phish users:- The attacker could inject malicious HTML into web pages to create phishing forms that look like legitimate login forms. If a user enters their credentials nto a phishing form, the attacker can steal them.

Recommendation: Either restrict access to the vulnerable application or contact the vendor for an update.

8. **Vulnerability Name: CGI Generic XSS(quick test)**

Risk Factor : Medium
CWE : : 20, 74, 79, 80, 81, 83, 86, 116, 442, 692, 712, 722, 725, 751, 801, 811, 928, 931
OSWAP CATEGORY : A03:2021- Injection and A08:2021- Software and Data Integrity Failures
DESCRIPTION : By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of

the application and directly access the underlying database.An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system. Note that this script is experimental and may be prone to false positives.

Vulnerablity Path : http://testfire.net/

Business Impact :

An attacker could exploit this vulnerability to:

• Inject malicious HTML into web pages:- This could allow the attacker to deface the
website, redirect users to malicious websites, or steal their data.

• Launch cross-site scripting (XSS) attacks:- This could allow the attacker to steal session cookies, hijack user accounts, or execute arbitrary code on the victim's browser.

• Phish users:- The attacker could inject malicious HTML into web pages to create
phishing forms that look like legitimate login forms. If a user enters their credentials into a phishing form, the attacker can steal them.

Recommendation: Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address any cross-site scripting vulnerabilities.

9. Vulnerability Name: Web Application Potentially Vulnerable to Clickjacking

Risk Factor : Medium

CWE : : 693

OSWAP CATEGORY : A05:2021- Security Misconfiguration

DESCRIPTION : The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or Ul redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions. X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors. Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The frame-ancestors' policy directive restricts which sources can embed the protected resource. Note that while the X-Frame-Options and

Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

Vulnerablity Path : http://testfire.net/

Business Impact : An attacker could exploit this vulnerability to:

- Trick users into clicking on malicious buttons or links, such as fake login buttons or phishing links.
- Steal sensitive data, such as credit card information or login credentials.
- Make unauthorized transactions on the user's account.
- Launch denial-of-service attacks by flooding the victim's browser with requests.

Recommendation: Return the X-Frame-Options or Content-Security-Policy (with the \'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

10. Vulnerability Name: TLS Version 1.0 Protocol Detection

Risk Factor : Medium

CWE : : 327

OSWAP CATEGORY : A02:2021-Cryptographic Failures

DESCRIPTION : The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Vulnerablity Path : http://testfire.net/

Business Impact : The business impact of TLS Version 1.0 Protocol Detection can be significant, depending on the nature of the business and the

types of data that are being transmitted. Potential business impacts:

- **Data breaches:** Attackers can exploit vulnerabilities in TLS 1.0 to intercept and decrypt traffic, including sensitive data such as passwords, credit card numbers, and personal information. This could lead to data breaches that could damage a company's reputation and result in financial losses.
- **Compliance violations:** Many industries, such as healthcare and finance, have regulations that require companies to use secure encryption protocols. Failure to comply with these regulations could result in fines, penalties, and other legal consequences.
- **Loss of customer trust:** Customers are increasingly aware of the importance of cybersecurity. If they learn that a company is using outdated and insecure encryption protocols, they may lose trust in that company and take their business elsewhere.

Recommendation: Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

11. Vulnerability Name: TLS Version 1.1 Protocol Deprecated

Risk Factor : Medium
CWE : : 327
OSWAP CATEGORY : A02:2021-Cryptographic Failures
DESCRIPTION : The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1 As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
Vulnerability Path: http://testfire.net/
Business Impact: The business impact of TLS Version 1.1 Protocol Deprecated can be similar to the business impact of TLS Version 1.0 Protocol Detection, as described in my previous response. Potential business impacts:

- **Data breaches:** Attackers can exploit vulnerabilities in TLS 1.0 to intercept and decrypt traffic, including sensitive data such as passwords, credit card numbers, and

personal information. This could lead to data breaches that could damage a company's reputation and result in financial losses.

- **Compliance violations:** Many industries, such as healthcare and finance, have regulations that require companies to use secure encryption protocols. Failure to comply with these regulations could result in fines, penalties, and other legal consequences.
- **Loss of customer trust:** Customers are increasingly aware of the importance of cybersecurity. If they learn that a company is using outdated and insecure encryption protocols, they may lose trust in that company and take their business elsewhere.

Recommendation: Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.1.

12. Vulnerability Name: SSL/TLS Diffie-Hellman Modulus<=1024 Bits(Logjam)

Risk Factor : Low
CWE: CWE-2015-4000
DESCRIPTION : The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.
Vulnerablity Path : http://testfire.net/

13. Vulnerability Name: Web Server Transmits Cleartext Credentials

Risk Factor : Low
CWE : : 522, 523, 718, 724, 928, 930
OSWAP CATEGORY : A02:2021- Cryptographic Failures
DESCRIPTION : The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.
Vulnerablity Path : http://testfire.net/

Business Impact : An attacker eavesdropping on the traffic between a web browser and a server could obtain the logins and passwords of valid users. This could allow the attacker to:

- Gain access to user accounts, including sensitive data such as credit card information,personal information, or financial data.
- Launch denial-of-service attacks by flooding the victim's account with requests.
- Impersonate users to commit fraud or other malicious activities.

Recommendation: Make sure that every sensitive form transmits content over HTTPS.

14. Vulnerability Name: Web Server Allows Password Auto-Completion

Risk Factor : Low

OSWAP CATEGORY : A07:2021- Identification and Authentication Failures

DESCRIPTION : The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Vulnerablity Path : http://testfire.net/

Business Impact : The business impact of a web server allowing password auto-completion is low, but it is still a good practice to mitigate this risk. If a user's browser is compromised, an attacker could gain access to their saved credentials and use them to access the web server.

Recommendation: Add the attribute ‘autocomplete=off’ to these fields to prevent browsers from catching credentials

This is stage 1 where we understand web application testing we took help from OWASP top 10 understand them :-

- A01:2021-Broken Access Control moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWE : s) mapped to Broken Access Control had more occurrences in applications than any other category.
- A02:2021-Cryptographic Failures shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
- A03:2021-Injection slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWE : s mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
- A04:2021-Insecure Design is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
- A05:2021-Security Misconfiguration moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
- A06:2021-Vulnerable and Outdated Components was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWE : s, so a default exploit and impact weights of 5.0 are factored into their scores.
- A07:2021-Identification and Authentication Failures was previously Broken Authentication and is sliding down from the second position, and now includes **CWE :** s that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of

standardized frameworks seems to be helping.

- A08:2021-Software and Data Integrity Failures is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWE : s in this category. Insecure Deserialization from 2017 is now a part of this larger category.
- A09:2021-Security Logging and Monitoring Failures was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.
- A10:2021-Server-Side Request Forgery is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

STAGE 2 REPORT

NESSUS

Overview –

Nessus is a widely used vulnerability scanning and assessment tool that helps organizations identify and mitigate security risks within their computer networks and systems. Developed by Tenable, Nessus is known for its robust and comprehensive capabilities in assessing network assets for potential vulnerabilities and weaknesses.

Key features and functions of Nessus include:

- Vulnerability Scanning: Nessus performs automated scans of network devices, servers, and applications to detect known and potential vulnerabilities. It uses a database of thousands of security checks to identify weaknesses in the system.

- Comprehensive Assessment: It assesses a wide range of vulnerabilities, including software vulnerabilities, misconfigurations, and compliance issues based on industry standards like CIS, DISA STIGs, and more.

- Scalability: Nessus can be used in both small and large-scale environments, making it suitable for businesses of varying sizes. It can scan a single host or an extensive network with numerous devices.

- Customization: Users can customize scans to suit their specific requirements, such as scheduling scans, defining scanning policies, and specifying target hosts and ports.

- Threat Intelligence Integration: It can integrate with threat intelligence feeds to provide real-time information about emerging threats, ensuring that vulnerabilities are assessed in the context of the latest security landscape.

- Reporting and Remediation: Nessus generates detailed reports that highlight identified vulnerabilities and recommended actions for remediation. This helps organizations prioritize and address security issues effectively.

- Compliance Auditing: The tool offers compliance templates for various regulatory standards and best practices, assisting organizations in ensuring that their systems meet specific compliance requirements.

- Scanning Across Diverse Environments: Nessus can scan a variety of operating systems, applications, and devices, making it versatile for heterogeneous network environments.

- Integration with Other Security Tools: It can be integrated with other security solutions and tools to enhance the overall security posture of an organization.

Nessus plays a critical role in proactively managing and enhancing network security. By regularly scanning and identifying vulnerabilities, organizations can reduce the risk of security breaches and data compromises. It empowers IT and security professionals to take informed actions to strengthen their defenses and protect sensitive information.

Target website - https://vit.ac.in/
Address:- 162.241.216.11

List of vulnerability

S.No	Vulnerability Name	Severity	Plugins
1	DNS Server Spoofed Request Amplification DDoS	High	35450
2	SSL Medium Strength Cipher Suites Supported (SWEET32)	High	42873
3	TLS Version 1.0 Protocol Detection	Medium	104743
4	TLS Version 1.1 Protocol Deprecated	Medium	157288
5	SSL Anonymous Cipher Suites Supported	Medium	31705
6	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium	65821
7	DNS Server Cache Snooping Remote Information Disclosure	Medium	12217
8	SMTP Service Cleartext Login Permitted	Low	54582

REPORT

1. **Vulnerability Name:-** DNS Server Spoofed Request Amplification DDoS

Severity:- High

Plugin:- 35450

Description:- The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

Solution:- Restrict access to your DNS server from public network or reconfigure it to reject such queries.

Business Impact:- A DNS (Domain Name System) Server Spoofed Request Amplification DDoS (Distributed Denial of Service) attack can have significant business impacts. Here are some of the potential consequences:

- Service Disruption: DDoS attacks, including DNS amplification attacks, can overwhelm a company's DNS servers, causing disruptions in online services and website availability. This can lead to downtime, which can impact a business's ability to serve customers and generate revenue.

- Loss of Reputation: Service disruptions due to DDoS attacks can erode customer trust and damage a company's reputation. Customers may view the business as unreliable and seek alternatives.

- Financial Loss: Downtime and service disruptions can result in immediate financial losses. For example, e-commerce companies can lose sales during the outage. Additionally, businesses might have to invest in cybersecurity measures and incident response, which can be costly.

- Increased Operational Costs: Implementing security measures and incident response can increase operational costs. Businesses may need to hire cybersecurity experts, invest in DDoS mitigation solutions, and upgrade their infrastructure to defend against such attacks.

- Legal and Regulatory Consequences: In some cases, a DDoS attack may lead to legal and regulatory consequences. For instance, if customer data is compromised during the attack, a company might face legal actions and regulatory fines for failing to protect sensitive information.

- Customer Churn: Customers may choose to switch to competitors if they perceive a business as being unable to protect its services from DDoS attacks. Customer churn can be a long-term consequence of such incidents.

- Impact on Employee Productivity: When business services are disrupted, employees may be unable to perform their tasks efficiently, impacting overall productivity.

- Reputational Damage: News of a successful DDoS attack can attract negative media attention, further harming the business's reputation and potentially scaring away potential customers or partners.

- Strategic Disruption: In some cases, DDoS attacks may be strategically motivated, targeting specific companies or sectors to create confusion or disrupt operations as part of a broader geopolitical or competitive strategy.

2. **Vulnerability Name:-** SSL Medium Strength Cipher Suites Supported (SWEET32)

Severity:- High

Plugin:- 42873

Description:- The remote host supports the use of SSL ciphers that offer medium

strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Solution:- Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Business Impact:- The vulnerability SSL Medium Strength Cipher Suites Supported (SWEET32) can have significant business impacts, particularly on organizations that rely on secure data transmission over the internet. Here are some of the potential consequences:

- Data Exposure: SWEET32 attacks target the encryption used in SSL/TLS, making it easier for attackers to decrypt and access sensitive data being transmitted over the internet. This can result in the exposure of confidential information, such as customer data, payment information, and proprietary business data.

- Data Breach: The exposure of sensitive data due to SWEET32 vulnerabilities can lead to data breaches, with significant legal, financial, and reputational consequences. Companies may face regulatory fines, lawsuits, and damage to their brand reputation.

- Regulatory Non-Compliance: Organizations that handle personal and financial data are often subject to data protection regulations, such as GDPR (General Data Protection Regulation) or HIPAA (Health Insurance Portability and Accountability Act). A SWEET32 vulnerability could lead to non-compliance with these regulations, resulting in legal consequences.

- Loss of Customer Trust: Data breaches and security vulnerabilities erode customer trust. Customers may lose confidence in a company's ability to protect their data, leading to a loss of business and brand damage.

- Financial Impact: Remediation efforts, legal fees, and potential fines resulting from a SWEET32-related data breach can have a significant

financial impact on a business.

- Disruption of Services: As organizations work to patch and mitigate the vulnerability, they may need to temporarily disable vulnerable encryption ciphers. This can disrupt online services and transactions, potentially resulting in lost revenue.

- Intellectual Property Theft: Businesses may also be at risk of intellectual property theft if attackers gain access to proprietary information or trade secrets due to SSL/TLS vulnerabilities.

- Reputational Damage: News of a security vulnerability or data breach can harm a company's reputation, causing long-term damage that may deter potential customers, partners, and investors.

- Legal and Regulatory Consequences: Depending on the industry and location, businesses may face legal actions, regulatory fines, and compliance audits as a result of the vulnerability.

- Increased Security Costs: To address SWEET32 vulnerabilities, organizations may need to invest in security upgrades, such as updating SSL/TLS configurations, implementing stronger encryption ciphers, and ensuring proper patch management.

3. **Vulnerability Name:-** TLS Version 1.0 Protocol Detection

Severity:- Medium

Plugin:- 104743

Description:- The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution: - Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Business Impact: - The vulnerability related to the detection of TLS (Transport Layer Security) Version 1.0 Protocol can have several business impacts, as it is a security concern associated with outdated and less secure encryption protocols. Here are some potential consequences:

- Security Risks: TLS 1.0 is an older and less secure version of the TLS protocol. Its use exposes the organization to security risks, making it easier for attackers to intercept and decrypt sensitive data being transmitted over the internet. This can lead to data breaches and unauthorized access to confidential information.

- Data Exposure: The use of less secure encryption protocols may expose sensitive data, such as customer information, payment details, and proprietary business data, to potential interception and exploitation.

- Compliance Issues: Many data protection regulations and industry standards (e.g., GDPR, PCI DSS) require the use of secure encryption protocols. Failing to disable outdated and insecure versions like TLS 1.0 can lead to non-compliance with these regulations, resulting in legal consequences and fines.

- Reputation Damage: Security vulnerabilities and non-compliance can harm an organization's reputation. News of security weaknesses and potential data breaches can erode customer trust and lead to reputational damage.

- Legal and Regulatory Consequences: Organizations may face legal actions, regulatory fines, and compliance audits due to non-compliance with security and data protection regulations. The costs associated with handling legal matters and regulatory fines can be significant.

- Business Disruption: To address the vulnerability, organizations may need to disable or phase out the use of TLS 1.0, which could disrupt online services and transactions. This disruption can result in lost revenue and customer dissatisfaction.

- Increased Security Costs: Mitigating the vulnerability may require investment in security upgrades, including disabling outdated protocols and implementing stronger encryption ciphers, as well as regular security assessments and patch management.

- Intellectual Property Theft: Weak encryption protocols can expose intellectual property and proprietary business information to potential theft and compromise.

- Competitive Disadvantage: A perceived lack of strong security measures can put an organization at a competitive disadvantage, as customers may choose more secure alternatives.

- Increased Operational Overhead: Organizations may need to allocate additional resources to monitor and address security vulnerabilities, which can increase operational costs.

4. **Vulnerability Name: -** TTLS Version 1.1 Protocol Deprecated

Severity: - Medium

Plugin: - 157288

Description: - The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Solution:- Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Business Impact: - The vulnerability related to the deprecation of the TLS (Transport Layer Security) Version 1.1 protocol can have several business impacts, as it signifies the use of an outdated and less secure encryption protocol. Here are potential consequences:

- Security Risks: TLS 1.1 is considered less secure compared to more recent TLS versions (e.g., TLS 1.2 and TLS 1.3). Its use exposes an organization to security risks, making it easier for attackers to intercept and decrypt sensitive data during transmission. This can lead to data breaches and unauthorized access to confidential information.

- Data Exposure: The use of deprecated and less secure encryption protocols may expose sensitive data, such as customer information, payment details, and proprietary business data, to potential interception and exploitation.

- Compliance Issues: Many data protection regulations and industry standards require the use of secure encryption protocols. Failing to disable deprecated versions like TLS 1.1 can lead to non-compliance with these regulations, resulting in legal consequences and fines.

- Reputation Damage: Security vulnerabilities and non-compliance can harm an organization's reputation. News of security weaknesses and potential data breaches can erode customer trust and lead to reputational damage.

- Legal and Regulatory Consequences: Organizations may face legal actions,

regulatory fines, and compliance audits due to non-compliance with security and data protection regulations. The costs associated with handling legal matters and regulatory fines can be significant.

- Business Disruption: To address the vulnerability, organizations may need to disable or phase out the use of TLS 1.1, which could disrupt online services and transactions. This disruption can result in lost revenue and customer dissatisfaction.

- Competitive Disadvantage: A perceived lack of strong security measures can put an organization at a competitive disadvantage, as customers may choose more secure alternatives.

- Increased Operational Overhead: Organizations may need to allocate additional resources to monitor and address security vulnerabilities, which can increase operational costs.

5. **Vulnerability Name:-** SSL Anonymous Cipher Suites Supported

Severity:- Medium

Plugin:- 31705

Description:- The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Solution:- Reconfigure the affected application if possible to avoid use of weak ciphers.

Business Impact:- The presence of the vulnerability "SSL Anonymous Cipher Suites Supported" can have several business impacts, as it is associated with a lack of security in the SSL (Secure Sockets Layer) protocol. Anonymous Cipher Suites are weak and lack proper authentication and encryption, making them susceptible to various security risks. Here are potential consequences for businesses:

- Data Exposure: The use of SSL Anonymous Cipher Suites can expose sensitive data, such as customer information, payment details, and proprietary business data, to potential interception and exploitation. This may lead to data breaches and unauthorized access to confidential information.

- Compliance Issues: Many data protection regulations and industry standards require the use of secure encryption protocols. Failing to address vulnerabilities related to SSL Anonymous Cipher Suites can lead to non-compliance with these regulations, resulting in legal consequences, fines, and the need for expensive remediation efforts.

- Security Risks: Anonymous Cipher Suites lack proper authentication and encryption, making them highly vulnerable to various attacks, including man-in-the-middle attacks and eavesdropping. These vulnerabilities can put the organization's sensitive information at risk.

- Reputation Damage: Security vulnerabilities and non-compliance can harm an organization's reputation. News of security weaknesses and potential data breaches can erode customer trust and lead to reputational damage.

- Legal and Regulatory Consequences: Organizations may face legal actions, regulatory fines, and compliance audits due to non-compliance with security and data protection regulations. The costs associated with handling legal matters and regulatory fines can be significant.

- Business Disruption: To address the vulnerability, organizations may need to disable and replace SSL Anonymous Cipher Suites, which could disrupt online services and transactions. This disruption can result in lost revenue and customer dissatisfaction.

- Competitive Disadvantage: A perceived lack of strong security measures can put an organization at a competitive disadvantage, as customers may choose more secure alternatives.

- Increased Operational Overhead: Organizations may need to allocate additional resources to monitor and address security vulnerabilities, which can increase operational costs.

6. **Vulnerability Name:-** SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Severity:- Medium

Plugin:- 65821

Description:- The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Solution:- Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Business Impact:- The presence of the vulnerability "SSL RC4 Cipher Suites Supported (Bar Mitzvah)" can have several business impacts, as it relates to the use of the RC4 encryption algorithm, which is considered weak and susceptible to

security risks. Here are potential consequences for businesses:

- Data Exposure: The use of RC4 cipher suites can expose sensitive data, such as customer information, payment details, and proprietary business data, to potential interception and exploitation. This may lead to data breaches and unauthorized access to confidential information.

- Compliance Issues: Many data protection regulations and industry standards require the use of strong and secure encryption protocols. Failing to address vulnerabilities related to RC4 cipher suites can lead to non-compliance with these regulations, resulting in legal consequences, fines, and the need for costly remediation efforts.

- Security Risks: RC4 is considered a weak encryption algorithm, and vulnerabilities related to it, including the Bar Mitzvah attack, make it susceptible to various attacks, such as information disclosure and potential data leakage.

- Reputation Damage: Security vulnerabilities and non-compliance can harm an organization's reputation. News of security weaknesses and potential data breaches can erode customer trust and lead to reputational damage.

- Legal and Regulatory Consequences: Organizations may face legal actions, regulatory fines, and compliance audits due to non-compliance with security and data protection regulations. The costs associated with handling legal matters and regulatory fines can be significant.

- Business Disruption: To address the vulnerability, organizations may need to disable and remove RC4 cipher suites, which could disrupt online services and transactions. This disruption can result in lost revenue and customer dissatisfaction.

- Competitive Disadvantage: A perceived lack of strong security measures can put an organization at a competitive disadvantage, as customers may choose more secure alternatives.

- Increased Operational Overhead: Organizations may need to allocate additional resources to monitor and address security vulnerabilities, which can increase operational costs.

7. **Vulnerability Name:-** DNS Server Cache Snooping Remote Information Disclosure

Severity:- Medium

Plugin:- 12217

Description:- The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

Solution:- Contact the vendor of the DNS software for a fix.

Business Impact:- The vulnerability "DNS Server Cache Snooping Remote

Information Disclosure" can have several business impacts, as it involves the unauthorized disclosure of sensitive information through DNS server cache snooping. Here are potential consequences for businesses:

- Data Exposure: DNS server cache snooping can lead to the exposure of sensitive information, such as domain names, IP addresses, and other DNS records, which can be exploited by malicious actors. This may result in the unauthorized disclosure of confidential data and potentially expose internal network structures and configurations.

- Security Risks: Information disclosure through DNS cache snooping can lead to security risks, as attackers can gain valuable insights into an organization's infrastructure, potentially facilitating targeted attacks and vulnerabilities exploitation.

- Competitive Disadvantage: If customer trust is eroded due to security vulnerabilities, it can put the organization at a competitive disadvantage, as customers may choose more secure alternatives.

- Regulatory Non-Compliance: Depending on the nature of the information disclosed, organizations may face non-compliance with data protection regulations and industry standards, leading to legal consequences, fines, and the need for remediation efforts.

- Legal and Regulatory Consequences: Organizations may face legal actions, regulatory fines, and compliance audits due to non-compliance with security and data protection regulations. The costs associated with handling legal matters and regulatory fines can be significant.

- Reputation Damage: Security vulnerabilities and non-compliance can harm an organization's reputation. News of security weaknesses and potential data breaches can erode customer trust and lead to reputational damage.

- Business Disruption: To address the vulnerability, organizations may need to implement security measures, which could potentially disrupt online services and transactions. This disruption can result in lost revenue and customer

dissatisfaction.

- Increased Operational Overhead: Organizations may need to allocate additional resources to monitor and address security vulnerabilities, which can increase operational costs.

8. **Vulnerability Name:-** SMTP Service Cleartext Login Permitted

Severity:- Low

Plugin:- 54582

Description:- The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.

Solution:- Configure the service to support less secure authentication mechanisms only over an encrypted channel.

Business Impact:- The presence of the vulnerability "SMTP Service Cleartext Login Permitted" can have several business impacts, as it indicates that the SMTP (Simple Mail Transfer Protocol) service allows cleartext login, which can expose sensitive information and credentials. Here are potential consequences for businesses:

- Credential Exposure: Allowing cleartext login in SMTP can lead to the exposure of login credentials, including usernames and passwords, which are transmitted in plain text. This makes it easier for attackers to intercept and compromise email accounts.

- Unauthorized Access: The vulnerability may result in unauthorized access to email accounts and potentially confidential or sensitive information stored in email communications.

- Data Breach: Unauthorized access to email accounts can lead to data breaches, which may involve the exposure of sensitive information, customer data, intellectual property, and other confidential data.

- Compliance Issues: Many data protection regulations and industry standards require the use of secure authentication and encryption for email services. Allowing cleartext login can lead to non-compliance with these regulations, resulting in legal consequences, fines, and the need for costly remediation efforts.

- Legal and Regulatory Consequences: Organizations may face legal actions, regulatory fines, and compliance audits due to non-compliance with security and data protection regulations. The costs associated with handling legal matters and regulatory fines can be significant.

- Reputation Damage: Security vulnerabilities and non-compliance can harm an organization's reputation. News of security weaknesses and potential data breaches can erode customer trust and lead to reputational damage.

- Business Disruption: To address the vulnerability, organizations may need to disable cleartext login, which could disrupt email services and communication. This disruption can result in lost productivity and customer dissatisfaction.

- Competitive Disadvantage: A perceived lack of strong security measures can put an organization at a competitive disadvantage, as customers and partners may choose more secure alternatives for email communication.

- Increased Operational Overhead: Organizations may need to allocate additional resources to monitor and address security vulnerabilities, which can increase operational costs.

Stage - 3 Report

Knowledge of SOC / SIEM

◆ SOC –

The Security Operations Center (SOC) is a centralized team of security experts responsible for monitoring, detecting, responding to, and recovering from security threats and incidents.

SOCs use a variety of security tools and technologies to collect, analyze, and correlate security data from across the organization. The primary function of the SOC is to protect an organization's assets from unauthorized access, use, disclosure, disruption, modification, or destruction. The SOC also plays an important role in incident response, helping to ensure that security incidents are resolved quickly and effectively.

◆ SOC – cycle –

The SOC cycle is a continuous process of monitoring, detecting, responding to, and recovering from security threats and incidents.
The cycle includes the following steps:

- **Monitoring:** SOC analysts monitor security data from a variety of sources, such as network devices, firewalls, intrusion detection systems, and security information and event management (SIEM) systems.
- **Detection:** SOC analysts use security tools and technologies to identify potential security threats and incidents.
- **Response:** SOC analysts investigate identified threats and incidents, and take appropriate action to mitigate the risk. This may include containing the threat, remediating the vulnerability, and eradicating the malware.
- **Recovery:** SOC analysts work to restore the affected systems and data to their normal state.

◆ SIEM

Security information and event management (SIEM) systems are tools that collect, analyze, and correlate security data from a variety of sources. SIEM systems can help SOC analysts identify potential security threats and incidents more quickly and effectively.

SIEM systems typically use a variety of techniques to analyze security data, including:

- **Rule-based correlation:** SIEM systems can be configured with rules that define specific patterns of activity that may indicate a security threat or incident.
- **Anomaly detection:** SIEM systems can also use anomaly detection techniques to identify unusual or suspicious activity.
- **Machine learning:** Some SIEM systems also use machine learning to identify potential security threats and incidents.

◆ SIEM Cycle

The SIEM cycle is a continuous process of collecting, analyzing, and correlating security data to identify potential security threats and incidents.
The cycle consists of the following steps:

- **Collection:** SIEM systems collect security data from a variety of sources, such as network devices, firewalls, intrusion detection systems, and endpoint security solutions.
- **Normalization:** SIEM systems normalize the collected data so that it can be easily analyzed and correlated.
- **Analysis:** SIEM systems use security rules and correlations to identify potential security threats and incidents.
- **Reporting:** SIEM systems generate reports that can be used by SOC analysts to investigate potential threats and incidents.

◆ MISP

MISP (Malware Information Sharing Platform) is an open-source platform that allows organizations to share and collaborate on threat intelligence. MISP can help organizations to stay informed about the latest threats and vulnerabilities, and to develop and implement effective security solutions.
MISP can be used to share a variety of threat intelligence data, including:

- **Indicators of compromise (IoCs):** IoCs are specific pieces of data that can be used to identify a security threat or incident.
- **Threat actors:** MISP can be used to share information about known threat actors, such as their tactics, techniques, and procedures (TTPs).
- **Vulnerabilities:** MISP can be used to share information about known vulnerabilities, such as their exploitability and impact.

◆ Your college network information

The following is a high-level overview of a typical college network:

- **Core network:** The core network is the backbone of the college network. It connects the various subnetworks together and provides high-speed access to the internet.
- **Distribution network:** The distribution network connects the core network to the various buildings and facilities on campus.
- **Access network:** The access network provides connectivity to individual devices, such as computers, laptops, and smartphones.

The college network may also include a variety of other components, such as:

- **Wireless network:** The wireless network provides wireless connectivity to devices on campus.
- **Security infrastructure:** The security infrastructure includes firewalls, intrusion detection systems, and other security devices that protect the network from unauthorized access and attacks.
- **Network management system:** The network management system is used to monitor and manage the network.

◆ How you think you deploy soc in your college –

To deploy a SOC in your college, you would need to:

- Identify the security data that you need to collect and analyze.
- Select and implement the appropriate security tools and technologies.
- Hire and train SOC analysts.
- Develop and implement SOC procedures and workflows.

Here is a specific example of how you could deploy a SOC in your college:

- You could start by collecting security data from your college's network devices, firewalls, and intrusion detection systems.
- You could then implement a SIEM system to analyze and correlate the collected data.
- You could hire and train SOC analysts to monitor the SIEM system and respond to security threats and incidents.
- You could develop and implement SOC procedures and workflows to ensure that the SOC is operating efficiently and effectively.

◆ Threat intelligence

It is information about existing or potential threats that can be categorized into three types: strategic, operational, and tactical. Knowledge in SOC is critical for

threat intelligence because it allows SOC analysts to better understand the threats they are facing and to develop more effective defenses.
Strategic threat intelligence provides information about the overall threat landscape, including the motivations, capabilities, and targets of threat actors. This type of intelligence can help SOC analysts to identify and prioritize the threats that pose the greatest risk to their organization.
Operational threat intelligence provides more specific information about individual threats, such as the tactics, techniques, and procedures (TTPs) used by threat actors. This type of intelligence can help SOC analysts to detect and respond to threats more effectively.
Tactical threat intelligence provides real-time information about ongoing attacks or campaigns. This type of intelligence can help SOC analysts to mitigate the impact of attacks and to prevent further damage.

◆ Incident response

Incident response is the process of identifying, investigating, and remediating security threats and incidents. It is a critical part of any organization's security posture, as it helps to minimize the impact of security breaches and protect the organization's assets.
The incident response process typically consists of the following steps:

- **Preparation**
- **Detection**
- **Investigation**
- **Remediation**
- **Recovery**

◆ Qradar & understanding about tool

QRadar can be used to collect and analyze security data from a variety of sources, including network devices, firewalls, intrusion detection systems, and endpoint security solutions. QRadar can also correlate security events and identify patterns that may indicate a security threat or incident.

QRadar can be used to assist with all phases of the incident response process, including:

- **Detection:** QRadar can be used to identify potential security threats and incidents by monitoring security data and generating alerts.
- **Investigation:** QRadar can be used to investigate potential security threats and incidents by providing security analysts with a centralized view of

security data and events. QRadar can also be used to automate tasks associated with the investigation, such as collecting data and generating reports.

- **Remediation:** QRadar can be used to remediate security threats and incidents by providing security analysts with information about the threat and by automating tasks associated with remediation, such as deploying patches and isolating infected systems.
- **Recovery:** QRadar can be used to recover from security threats and incidents by providing security analysts with information about the impact of the incident and by automating tasks associated with recovery, such as restoring data from backups and reconfiguring systems.

Overall, QRadar is a valuable tool that can be used to improve the effectiveness of incident response. By using QRadar, organizations can more quickly and effectively identify, investigate, and respond to security threats and incidents.

Conclusion

◆ Stage 1 –

The OWASP Top 10 for 2021 in web application testing highlights the most critical security risks faced by web applications. Notable shifts and additions were observed compared to the previous edition. The top 10 categories are as follows:

1. **A01: Broken Access Control -** Identified as a critical concern, with the highest number of occurrences in applications, emphasizing the importance of robust access control mechanisms.
2. **A02: Cryptographic Failures -** Shifted to the second position, emphasizing the significance of addressing cryptographic failures to prevent sensitive data exposure and system compromises.
3. **A03: Injection -** Despite sliding to the third position, it remains a substantial threat, with numerous occurrences in applications, including Cross-site Scripting.
4. **A04: Insecure Design** - A new addition, emphasizing the necessity of implementing threat modeling, secure design patterns, and reference architectures to mitigate design-related risks.
5. **A05: Security Misconfiguration -** Elevated from the previous edition, indicating the increased importance of addressing misconfigurations, especially in highly configurable software. This category now includes XML External Entities (XXE).
6. **A06: Vulnerable and Outdated Components -** Recognized as a prevalent issue, this category emphasizes the need to address components with known

vulnerabilities, despite the challenge of testing and assessing risk associated with it.

7. **A07: Identification and Authentication Failures -** Moved down from the second position, now focusing on identification-related failures and benefiting from the increased availability of standardized frameworks.
8. **A08: Software and Data Integrity Failures -** Highlighting the importance of verifying integrity in software updates, critical data, and CI/CD pipelines. This category includes the previously highlighted Insecure Deserialization.
9. **A09: Security Logging and Monitoring Failures -** Expanded to include various types of failures, underscoring the challenges associated with testing and the potential impact on visibility, incident alerting, and forensics.
10. **A10: Server-Side Request Forgery -** Added based on community feedback, although the data indicates a relatively low incidence rate, it still highlights the importance of addressing this potential threat.

Understanding and addressing these top 10 categories is critical for enhancing the security posture of web applications, safeguarding sensitive data, and preventing potential system compromises.

The OWASP Top 10 provides a useful framework for understanding web application vulnerabilities and prioritizing security efforts. It is important for organizations to regularly test their web applications for vulnerabilities and implement appropriate measures to address them.

Additionally, organizations should implement threat modeling, secure design patterns and principles, and reference architectures to address risks related to design flaws. By following these recommendations and staying up-to-date with the latest security standards, organizations can help to protect their sensitive data and maintain the trust of their customers.

- **Stage 2 –**

Nessus, a comprehensive vulnerability scanning tool, assumes a pivotal role in the proactive management and fortification of network security within organizations. Its robust capabilities facilitate the regular detection of vulnerabilities, thereby enabling preemptive measures to mitigate the risk of security breaches and data compromises. By employing Nessus, IT and security professionals are empowered with actionable insights, fostering informed decision-making to bolster their defensive strategies and safeguard sensitive information.

Through its sophisticated scanning mechanisms, Nessus diligently examines network infrastructures, systems, and applications, meticulously identifying potential weaknesses and security gaps. This comprehensive approach allows organizations to gain a comprehensive understanding of their security landscape, thereby laying the groundwork for the implementation of targeted remediation strategies.

Moreover, Nessus provides detailed vulnerability reports, furnishing organizations with a comprehensive overview of the identified risks, their potential impact, and recommended remedial actions. These reports serve as valuable resources for IT and security professionals, equipping them with the necessary information to prioritize and address vulnerabilities effectively, ensuring that critical issues are resolved in a timely and efficient manner.

Furthermore, Nessus facilitates the automation of security assessments, significantly streamlining the scanning process and enabling organizations to conduct regular and systematic evaluations without imposing excessive manual overhead. This automation not only enhances the efficiency of vulnerability management but also allows for the timely identification of emerging threats, ensuring that security measures remain agile and adaptive in the face of evolving risks.

The integration of Nessus into an organization's security framework fosters a proactive security culture, emphasizing the significance of continuous monitoring and risk mitigation. By leveraging Nessus's capabilities, organizations can fortify their defenses, proactively anticipate potential security challenges, and uphold the integrity and confidentiality of their data assets. With its comprehensive scanning, insightful reporting, and automation features, Nessus serves as a cornerstone in the arsenal of tools aimed at safeguarding networks and fortifying overall cybersecurity resilience.

- **Stage 3 –**

A Security Operations Center (SOC) is a centralized unit that oversees and manages an organization's security posture. It is responsible for preventing, detecting, analyzing, and responding to cybersecurity incidents and threats. A Security Information and Event Management (SIEM) system, such as IBM QRadar, is a crucial component of an SOC, providing real-time analysis of security alerts generated by network hardware and applications. The QRadar Dashboard, within the context of an SOC, serves as a central hub for monitoring and managing security

events, providing security professionals with critical insights into the organization's security landscape.

The QRadar Dashboard offers a comprehensive and customizable overview of the organization's security status, presenting key metrics, alerts, and trends that require immediate attention. Through a user-friendly interface, security analysts can quickly assess the overall security posture, identify potential threats, and prioritize response efforts. The Dashboard's intuitive design allows for efficient navigation and the quick retrieval of essential security information, enabling SOC personnel to make timely and informed decisions to safeguard the organization's digital assets.

One of the primary functions of the QRadar Dashboard is to provide real-time visibility into security events, enabling security analysts to monitor network traffic, detect anomalies, and identify potential security breaches or unauthorized access attempts. The Dashboard consolidates data from various sources, such as log files, network devices, and security appliances, offering a comprehensive view of the organization's security environment. This holistic approach facilitates the identification of patterns and trends that could indicate potential security threats or vulnerabilities, allowing the SOC to proactively respond to emerging risks.

Moreover, the QRadar Dashboard facilitates the tracking and analysis of security incidents and events, enabling SOC personnel to investigate security alerts and prioritize response actions based on the severity and impact of each incident. The Dashboard's interactive visualization tools and customizable widgets provide actionable insights, empowering security analysts to assess the scope and magnitude of security incidents and devise effective strategies to mitigate potential risks. Furthermore, the QRadar Dashboard supports the generation of comprehensive reports and analytics, allowing SOC personnel to evaluate the effectiveness of security measures, identify recurring threats, and make data-driven decisions to enhance the organization's overall security posture.

Future Scope

- **Stage 1 –**

Future Scope of Web Application Testing
Web application testing is a critical part of cybersecurity, as web applications are a prime target for cyberattacks. In the future, web application testing will play an even more important role in cybersecurity, as web applications become increasingly complex and sophisticated.

Here are some of the key trends that are shaping the future of web application testing in the field of cybersecurity:

- **Increased focus on security testing**: As the threat landscape continues to evolve, web application testers will need to focus more on security testing. This includes testing web applications for common vulnerabilities such as SQL injection, cross-site scripting, and insecure direct object references.
- **Rise of web application pentesting:** Web application pentesting is the process of simulating attacks on web applications to identify and fix security vulnerabilities. Web application pentesting is becoming increasingly important, as it can help organizations to identify and fix vulnerabilities before they are exploited by attackers.
- **Adoption of new technologies:** Web application testers will need to adopt new technologies to keep up with the latest threats. For example, many web application testers are now using artificial intelligence (AI) and machine learning (ML) to automate tasks such as vulnerability discovery and exploit generation.
- **Collaboration with security teams:** Web application testers will need to collaborate closely with other security teams, such as incident response teams and security operations teams. This will help to ensure that security vulnerabilities are identified and fixed quickly and efficiently.

In the future, web application testing will become even more integrated into the overall cybersecurity strategy of organizations. Web application testers will play a critical role in helping organizations to protect their web applications from cyberattacks.

Here are some specific examples of how web application testing will be used to improve cybersecurity in the future:

- **Use of AI and ML to detect and prevent security attacks**: AI and ML can be used to analyze web application traffic and identify patterns that may indicate an attack. This information can then be used to prevent the attack from being successful.
- **Development of new security testing tools and techniques:** As web applications become more complex, new security testing tools and techniques will be developed to help testers identify and fix security vulnerabilities.
- **Increased focus on application security training:** Organizations will increase their investment in application security training to help their developers and testers learn about the latest security threats and how to mitigate them.
- **Adoption of security best practices:** Organizations will adopt security best

practices such as DevSecOps and secure coding to help them develop and deploy secure web applications.

Overall, the future of web application testing in the field of cybersecurity is very promising. Web application testers will play a critical role in helping organizations to protect their web applications from cyberattacks.

- **Stage 2 –**

Future scope of testing process

Nessus is a powerful vulnerability scanner that can be used to identify a wide range of vulnerabilities in web applications, servers, and networks.

Future Scope of Nessus

Here are some of the key trends that are shaping the future of Nessus:

- **Integration with other security tools:** Nessus will be integrated with other security tools, such as security information and event management (SIEM) systems and security orchestration, automation, and response (SOAR) platforms. This will help organizations to automate their security testing and response processes.
- **Use of AI and ML to improve vulnerability detection and remediation:** Nessus will use AI and ML to improve its ability to detect and remediate vulnerabilities. For example, Nessus could use AI to identify new vulnerabilities that have not yet been catalogued.
- **Support for new technologies:** Nessus will add support for new technologies, such as cloud computing, IoT, and containerized applications. This will help organizations to test their environments for vulnerabilities, regardless of the technologies they are using.
- **Increased focus on risk-based testing:** Nessus will be used to perform risk-based testing, which focuses on testing the areas of networks and applications that pose the greatest risk to organizations. This will help organizations to make the most of their security testing resources.

Future Use Cases for Nessus

Here are some specific examples of how Nessus will be used in the future:

- Nessus will be used to **automate the security testing process**. Nessus can be integrated with other security tools to automate the process of scanning for vulnerabilities, reporting on findings, and remediating vulnerabilities. This

will free up security analysts to focus on more strategic tasks.

- Nessus will be used to test **cloud-based environments.** Nessus can be used to scan cloud-based environments for vulnerabilities, such as insecure configurations and exposed sensitive data. This will help organizations to protect their cloud-based assets from cyberattacks.
- Nessus will be used to test **IoT devices**. Nessus can be used to scan IoT devices for vulnerabilities, such as insecure firmware and default passwords. This will help organizations to protect their IoT devices from cyberattacks.

◆ Stage 3 –

Future scope of SOC / SEIM –

As the threat landscape continues to evolve, organizations will need to invest in SOCs and SIEMs to protect their networks and data from increasingly sophisticated cyberattacks.

Future Trends in SOCs and SIEMs –

Here are some of the key trends that are shaping the future of SOCs and SIEMs:

- **Integration with AI and ML:** SOCs and SIEMs will be increasingly integrated with AI and ML technologies. This will help SOC teams to automate tasks such as log analysis, threat detection, and incident response.
- **Shift to cloud-based SOCs and SIEMs:** Many organizations will move their SOCs and SIEMs to the cloud. This will offer a number of benefits, such as scalability, flexibility, and cost savings.
- **Increased focus on risk-based monitoring and response:** SOC teams will focus on monitoring and responding to threats based on risk. This means that they will focus on the threats that pose the greatest risk to the organization, rather than monitoring and responding to all threats equally.
- **Collaboration with other security teams:** SOC teams will collaborate more closely with other security teams, such as incident response teams and security operations teams. This will help to improve the overall security posture of the organization.

Future Use Cases for SOCs and SIEMs

Here are some specific examples of how SOCs and SIEMs will be used in the future:

- SOCs and SIEMs will be used to **monitor and detect threats in real time**. AI and ML technologies will be used to analyze log data and identify patterns that may indicate an attack. This information can then be used to prevent the

attack from being successful.

- SOCs and SIEMs will be used to **automate incident response**. AI and ML technologies can be used to automate tasks such as triaging incidents, investigating incidents, and remediating incidents. This can help SOC teams to respond to incidents more quickly and effectively.
- SOCs and SIEMs will be used to **improve security compliance**. SOCs and SIEMs can be used to generate reports on security events and compliance status. This information can be used by organizations to demonstrate compliance to auditors and regulators.

Topics explored

Throughout our journey of this project we've explored a lot of topics on the way. Some of the key topics we've explored all along are :

- The basic definition of "Malware Detection and Classification" , which helped us understand how important it is to detect malwares and mitigate them.
- Types of Malware , their categories and how to classify them , which helped us understand the types and categories of various malware such as Ransome ware , Trojan horse etc.
- Next, searching for ways to detect them the tools that can be used has given us the list of tools which can be used such as Nmap , Nessus etc.
- Then we've brainstormed the types of Malware attacks that we know of and the way we could classify them using "Mural" tool where all the team members have brainstormed the ideas and tried to classify them.
- Further, searching for a practice website to perform the vulnerability tests on and a main website helped us get the next stage.
- Once the tests were made, vulnerabilities were to be classified so we looked up for the OWASP vulnerabilities and it helped us to classify the vulnerabilities.
- Next, we explored our knowledge on SOC and SIEM cycles.
- Further we discovered the topics of Incident response and also tried Qradar tool by IBM and tried to understand it.
- As our next step, we explored Nessus tool and how to use it.
- As our final understanding, we've explored –
    - Future scope of Web application testing
    - Future scope of testing process
    - Future scope of SOC/SIEM

- As our final step we've classified the tools we've explored during the whole project phase.

Tools explored –

S. No	Tools	Description	Technology
1.	Nessus	Nessus is a vulnerability scanner that helps identify security issues in computer systems and networks. It performs scans, audits configurations, and detects malware. It provides detailed reports and recommendations for fixing vulnerabilities.	Nessus is built with C and uses a client- server architecture. It utilizes plugins for scans, has a web-based interface, and stores data in a database.
2.	OpenVAS	OpenVAS is an open-source vulnerability scanner that helps identify security issues in networks and systems.	It utilizes a client-server architecture and is written in C. OpenVAS offers a wide range of scanning capabilities and provides detailed reports for vulnerability management.
3.	Acunetix	Acunetix is a web application security scanner that helps identify vulnerabilities in web applications and APIs	It is written in C++ and utilizes advanced scanning techniques to detect common security flaws like SQL injection, cross- site scripting (XSS), and more
4.	Nslookup	It's a command-line tool used to query the Domain Name System (DNS) to obtain information about domain names and IP addresses.	NSlookup is a command-line tool that uses the DNS protocol and is built into operating systems, requiring no additional software.

5.	Shodan	Shodan is a search engine for internet-connected devices and services. It allows users to search for specific devices or services based on various criteria such as IP address, location, open ports, and specific vulnerabilities	Shodan is built using a combination of technologies including Python, JavaScript, and various web technologies for its interface.