

# NARASARAOPETA INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering

ETHICAL HACKING (IV - CSE) – I SEM

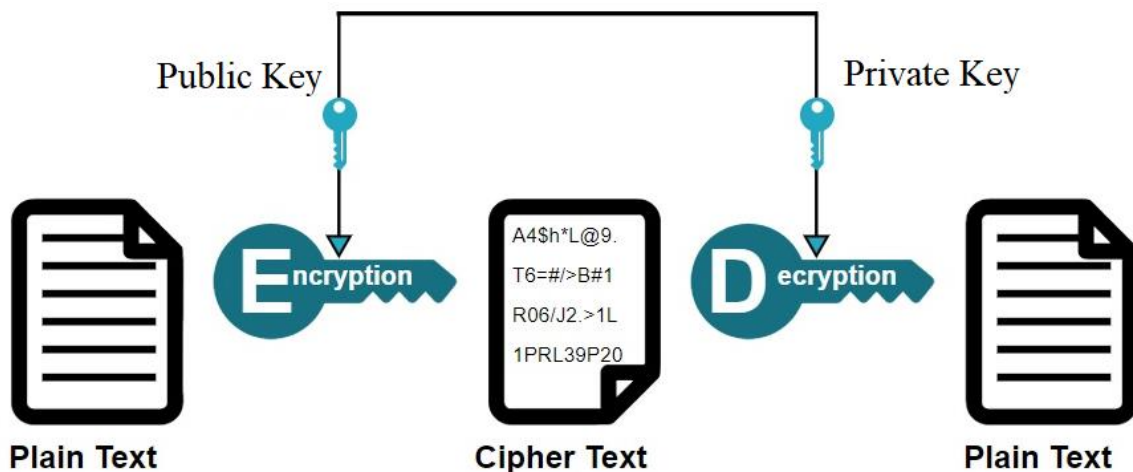
## UNIT V

Cryptography: Cryptography, Digital Signature, Hash Functions, Steganography: Steganography Process, watermarking, Steganography Methods and Attacks, Steganography tools, Vulnerability Assessment: Vulnerability, The Open Web Application Security Project (OWASP), Prevention, Damn Vulnerable Web Application (DVWA), installation and testing of DVWA.

### CRYPTOGRAPHY:

Cryptography is a technique which is used for the secured communication by changing the message or information into encoded format. Some special algorithms are used to encrypt the information and the information exchange became secure.

The algorithms used in cryptography are mathematical algorithms and converts the plain text information into unreadable coded format which is known as Cipher text. While the process of cryptography, the information is encrypted by using a KEY which makes it more secure. Receiver would not be able to decrypt the information without knowing the key used to encrypt the information.



These keys are transmitted between the sender and receiver and are generally of two types :

#### 1. Public key:

In the public key, the data is encrypted using the recipient's public key and it can't be decrypted without the matching private key.

In this concept, one key which encrypts the plain text and another key which decrypts the cipher text is required and they will not work if interchanged.

In case if the locking key is public than anyone can send the encrypted information to the private key holder but decrypting the information would not be possible without the private key. Hence it enhances the confidentiality of the communication taking place.

## 2. Private key

In the private key, the data is encrypted using the private key and can be decrypted only by the matching public key. The keys will not work if interchanged. In case the locking key is private, it used to verify that the document is locked by the owner and hence it is mostly used in making of digital signatures.

- The information can be decrypted by the user having the matching public key of the cipher text. While the communication, the public key is published whereas the private is kept confidential between the sender and receiver.
- The information can only be decrypted if the private key is present but the one sided encrypted messaged can be sent using the public key. The security and confidentiality is totally dependent upon private key.

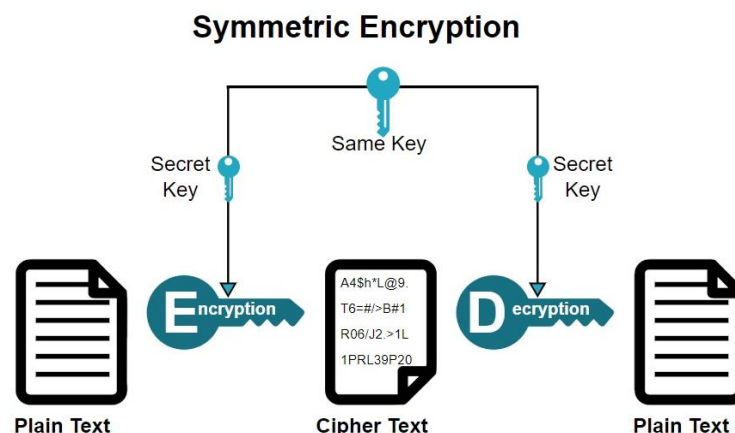
## Types of Cryptography

Basic cryptography technologies can include two types of encryptions:

1. Symmetric-key Cryptography
2. Asymmetric-key Cryptography

### 1. Symmetric-key Cryptography

Symmetric key encryption is a type of encryption where the same key is used for both the encryption and decryption of the data.



- **Key Generation:** A secret key is generated by the encryption algorithm. The key should be kept confidential and only shared between the parties that need to communicate securely.
- **Encryption:** The plaintext (original data) is encrypted using the secret key. This process transforms the plaintext into ciphertext (unreadable data) in such a way that it can only be reversed with the same key.
- **Transmission:** The ciphertext is then transmitted securely to the recipient.
- **Decryption:** The recipient, possessing the secret key, uses it to decrypt the ciphertext and recover the original plaintext.

## 2. Asymmetric Key Encryption:

Asymmetric Key Encryption method uses different keys for encryption and decryption. This encryption method uses public key and private key methods. This public key method helps completely unknown parties share information like email ID. The private key helps to decrypt the messages and also helps in verifying the digital signature.

**Key Pair Generation:** Each participant in the communication generates a pair of keys – a public key and a private key. The public key can be freely distributed, while the private key must be kept secret.

**Public Key Distribution:** The public keys are distributed to others who may need to send encrypted messages to the owner of the key pair. The private key is kept secret and never shared.

**Encryption:** If someone wants to send an encrypted message to a recipient, they use the recipient's public key to encrypt the message. Once encrypted with the public key, only the corresponding private key can decrypt and reveal the original message.

**Decryption:** The recipient, who owns the private key corresponding to the public key used for encryption, uses their private key to decrypt the received ciphertext and recover the original message.

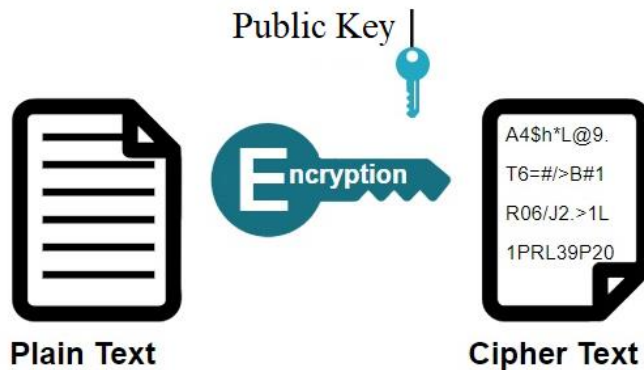
**There are two terms which play an important role in cryptography:**

1. Encryption
2. Decryption

### 1. Encryption:

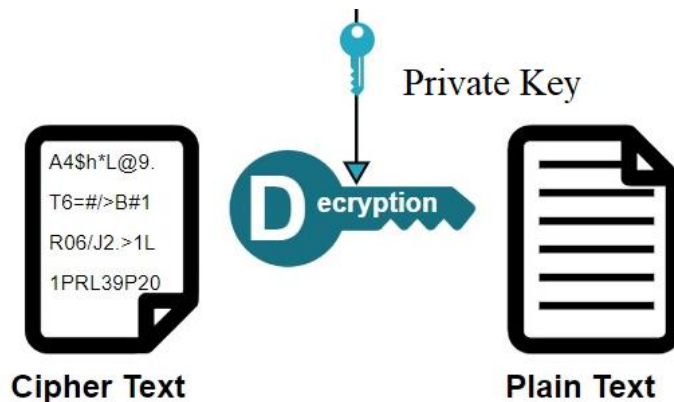
In the encryption, the information present in plain text is encoded using specific algorithm by means of a KEY.

- The information which obtained as an output is known as encrypted data. Encryption is a process of transforming information (plaintext) into an unreadable form (ciphertext) using an algorithm and a cryptographic key.
- The purpose of encryption is to ensure the confidentiality and security of the information being transmitted or stored, preventing unauthorized access or interception.



#### **b. Decryption:**

Decryption is the process of converting the cipher text into plain text. In the process of decryption, the receiver decodes the encrypted information by using the key shared. To decrypt the information, presence of private key is must and without it decryption can't be done. Both of encryption and decryption make up the whole term cryptography.



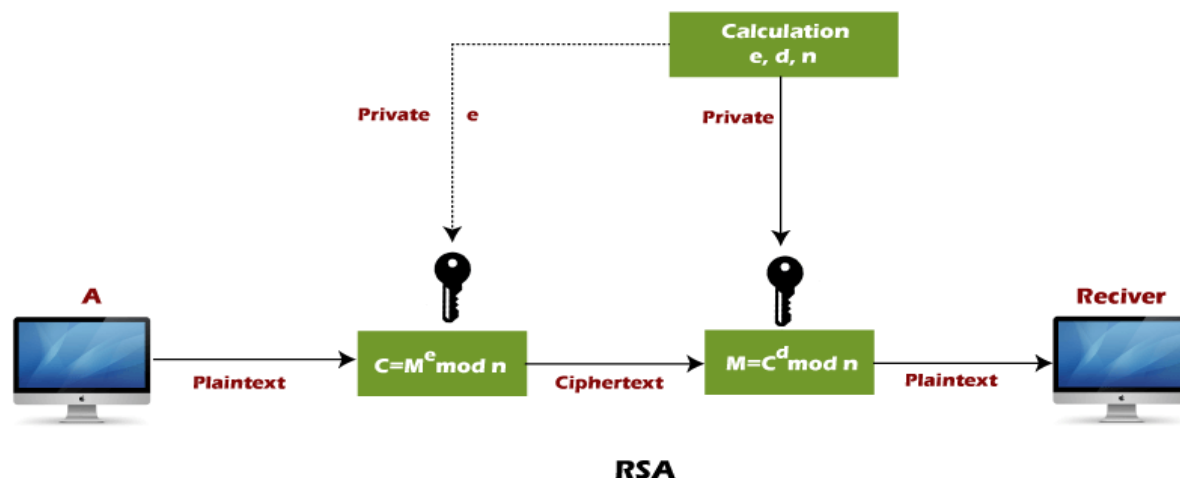
#### **Important Cryptography Algorithms:**

1. Rivest Shamir adleman (RSA)
2. MD5
3. Secure Hashing Algorithm (SHA)

## 1. Rivest Shamir Adleman (RSA) :

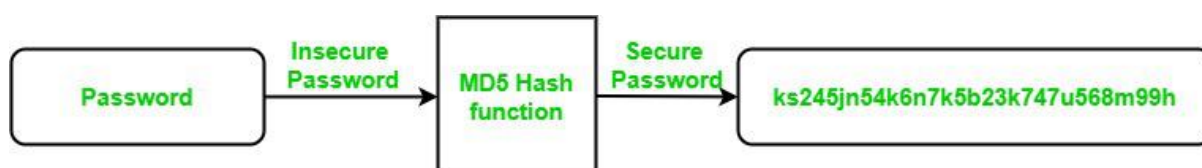
RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and the Private key is kept private.

- RSA is the very first public key based cryptographic system and which is widely used for the secured data transmission.
- In the RSA, a user generates a public key based upon two large prime numbers having an auxiliary value. User publishes the generated public key keeping the prime numbers secret.
- The published public key can be used by anyone for encrypting the information. A user having the knowledge of prime number can efficiently break the encrypted message and can decode it.
- Decoding the RSA Encryption is generally known as RSA Problem. RSA is one of the slowest algorithms and due to this is not much used for encrypting the user data.



## 2. MD5:

MD5 is widely used hashing algorithm for generating 128-bit hash. It is generally used as a data verification checksum against unintentional corruptions. Md5 is one way hash function, but it can be cracked or reversed by using Brute-Force Attacks. MD5 is the advanced series of message digest functions. Looking at security point of view, md5 hash security had compromised many times.



Use Of MD5 Algorithm:

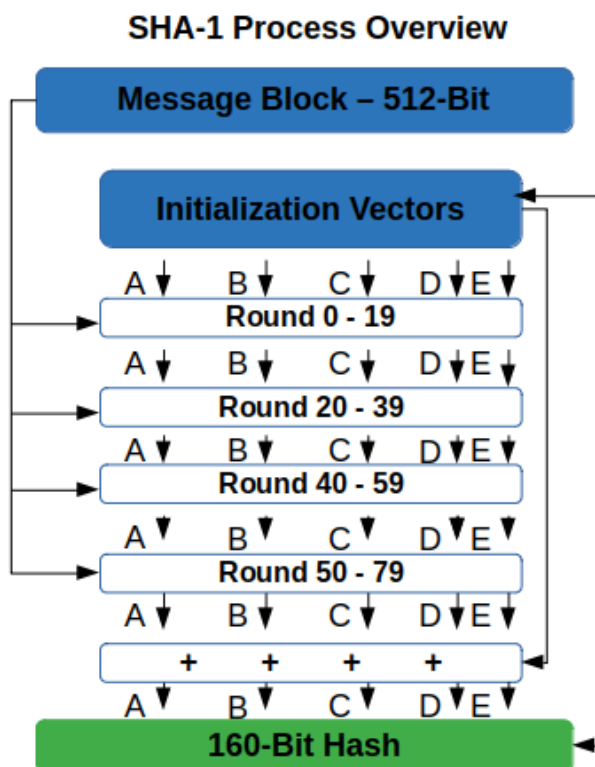
- It is used for file authentication.
- In a web application, it is used for security purposes. e.g. Secure password of users etc.
- Using this algorithm, We can store our password in 128 bits format.

### 3. Secure Hashing Algorithm:

SHA is a hashing algorithm which takes an input of arbitrary length. The out of SHA is 160-bit and it is quite slow than md5. Secured Hashing Algorithm is generally used for the Authentication related encryption purposes. It is also used for integrity checksum and for secured web connections. SHA is generally bigger than md5 in length.

Versions of SHA are following :

1. SHA-1
2. SHA-2
3. SHA-3

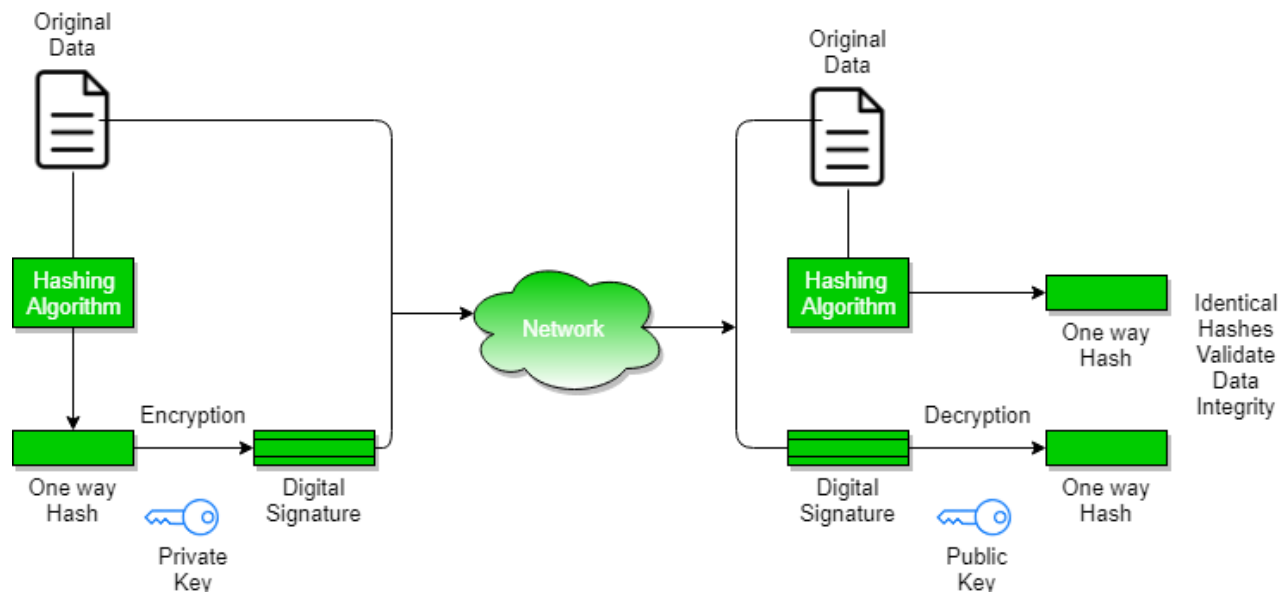


1. Add padding bits to the original message.
2. Add length bits to the end of the padded message.
3. Initialize MD buffers to compute the message digest.

4. Process the message in successive 512 bits blocks. Each block goes through a complex process of expansion and 80 rounds of compression of 20 steps each.
5. Produce a final 160 bits hash value. After the last block is processed, the current hash state is returned as the final hash value output.

### Digital Signature :

- Digital signature is used for defining the authenticity of the digital documents. It is based upon private key encryption because the user locks the document by using his digital signature.
- Digital signature is an electric signature of the user which is used for secure digital purposes and used for authenticating confidential information.
- To generate a random private key, a key generation algorithm is used which select a random key from the possible keys.



- Generated private key and information is combined by using the signing algorithm, finally signature verifying algorithm is used which checks whether the public key is matching or not.
- Key Generation Algorithms: Digital signature is electronic signatures, which assure that the message was sent by a particular sender.
- Signing Algorithms: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed.
- Signature Verification Algorithms : Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value.

## Hash Functions:

Hash functions are also defined as one-way cryptography. A hash function is a mathematical function that takes an input (or "message") and produces a fixed-size string of characters, which is typically a hash value or hash code. The output, often referred to as the hash digest, is a unique representation of the input data. In the hash functions there is no involvement of the key during the encryption process. The plain text information is converted into hash by the suitable algorithm.

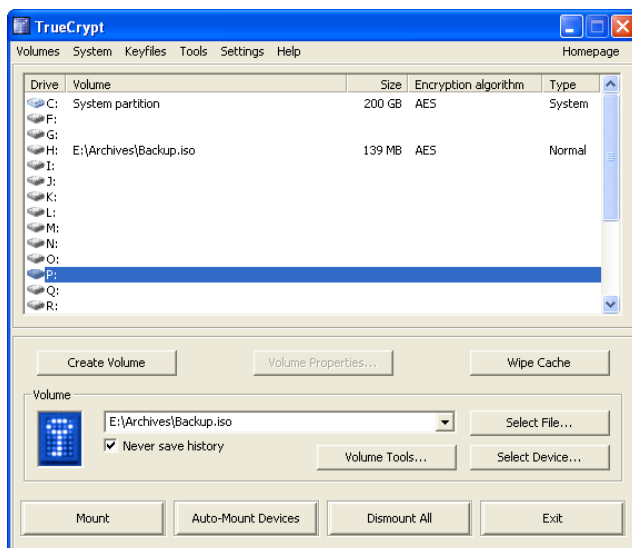
- **Fixed Output Size:** A hash function produces a fixed-size output regardless of the size of the input. For example, the SHA-256 hash function always produces a 256-bit (32-byte) hash value.
- **Deterministic:** For the same input, a hash function will always produce the same output. This property is crucial for consistency and reliability.
- **Efficient:** Hash functions should be computationally efficient, allowing for quick calculation of the hash value.



## Practical:

### 1. True Crypt:

TrueCrypt was known for providing on-the-fly encryption, allowing users to create encrypted virtual disk drives or encrypt entire storage devices such as hard drives or USB flash drives.



DOWNLOAD :- [www.truecrypt.org/downloads](http://www.truecrypt.org/downloads)



## 2. Online MD5 Encryption :

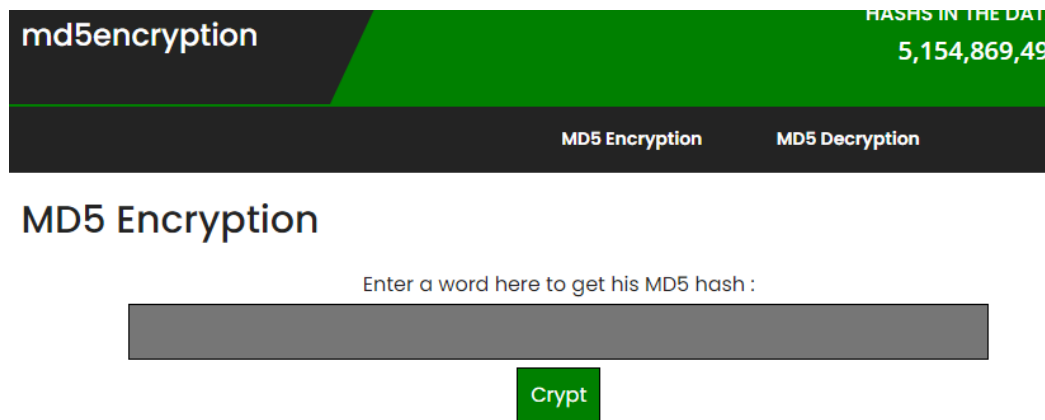
1. Open your web browser and visit to [www.md5encryption.com](http://www.md5encryption.com).
2. Input message which you want to encrypt and click on encrypt it.

For Ex: Hello

3. The MD5 hash will be generated.

For Ex: f814893777bcc2295fff05f00e508da6

3. This word used in example is a normal dictionary word and can be easily cracked using brute force.



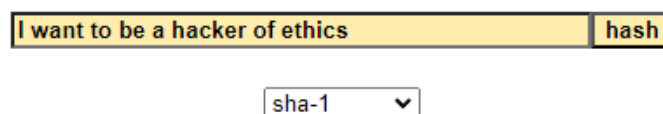
## 3. Using SHA-1 :

Open your browser and go to “ [www.sha1-online.com](http://www.sha1-online.com) ” . z Now it will open a website from where you can convert your simple text into sha-1 hash.

Insert you text , for ex : in below fig. text is “I want to be a hacker of ethics” and click on hash button.

Now you can have your sha1 hash. It is alphanumeric hash.

### SHA1 and other hash functions online generator

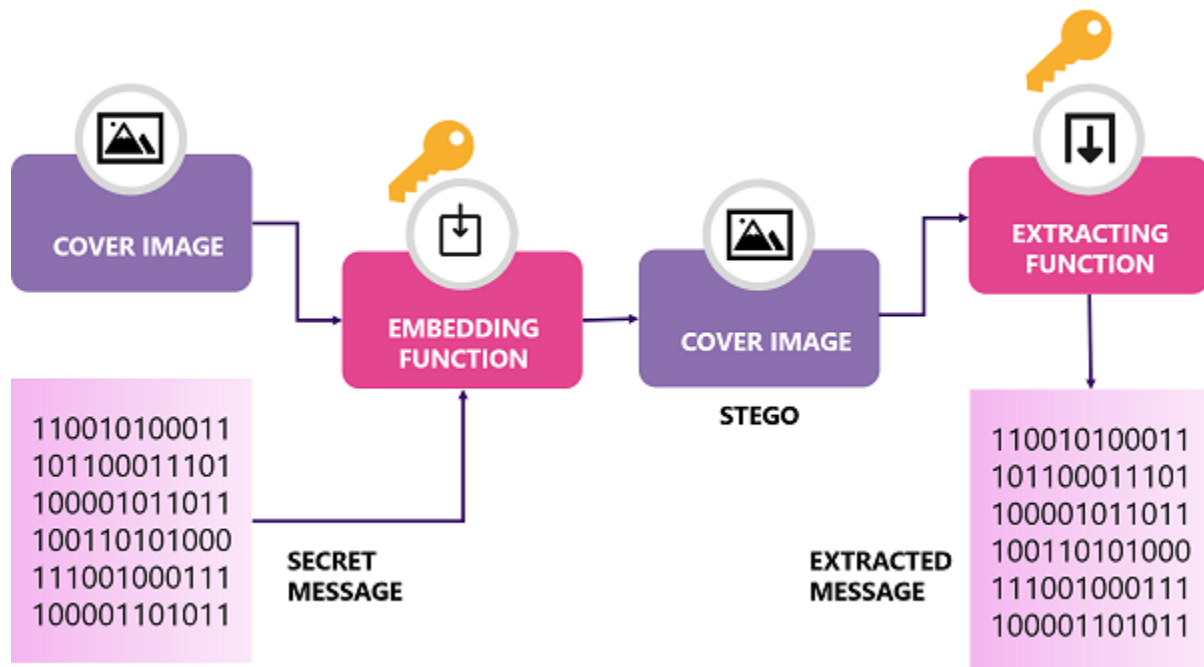


**Result for sha1:** **ad4d95a4d6bb86abd1a54bc9fa6e2f9a507dd2a4**

## Steganography

“Steganography is an art of hiding the information within the files. Sensitive messages and information are hidden into the multimedia files without being detected by the process of steganography.”

- It allows anonymous and secure interchange of information without being detected easily.
- The hidden information is not visible with naked eyes and hence the chance of being detected just by seeing the files containing the hidden information is near to impossible.
- Steganography can be done with media, files and folders.
- Steganography is sometimes used as an authentication watermark by the digital music and movie companies which is invisible to the users but is useful to keep the authenticity.
- Steganography is also used by the terrorist for the secret information exchanging.
- Many big terrorist organizations use this technique to carry out their information exchange. Steganography is also popular from the forensics point of view and is widely covered under cyber forensics.



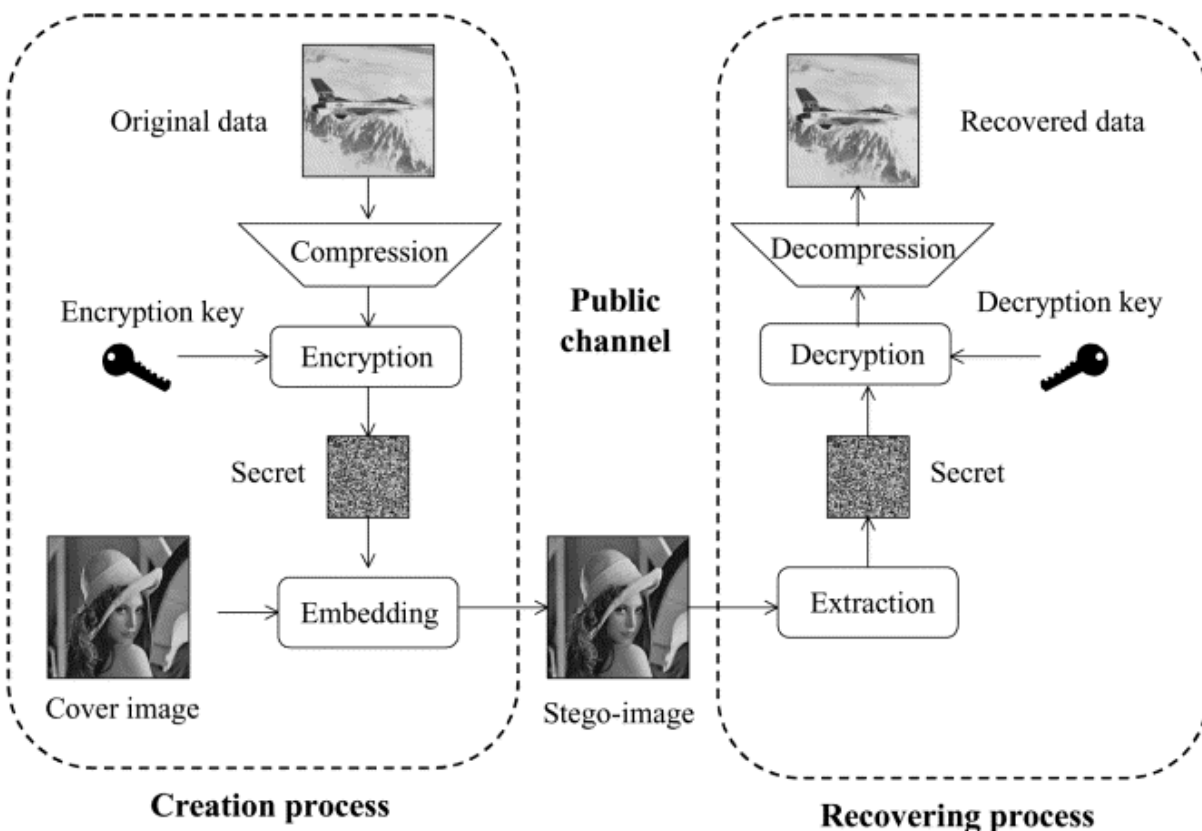
For example:

An attacker hides some confidential information within a picture using the steganography. The new image which contains the information hidden within will be now infected image. Attacker use a brand new car's picture and upload it over the social media to secretly without suspiciousness and the receiver will download the picture and extract the information using the

tools. Now the attacker will remove the picture from social media. In this whole process, attacker pretended to share the pictures of his new car but actually the secret information was shared without knowledge of anyone. The information hidden can be retrieved with the help of steganography analysis tool which is not a difficult task but in case of complex steganography, the process of retrieving the information might be harder.

**Steganography Process :**

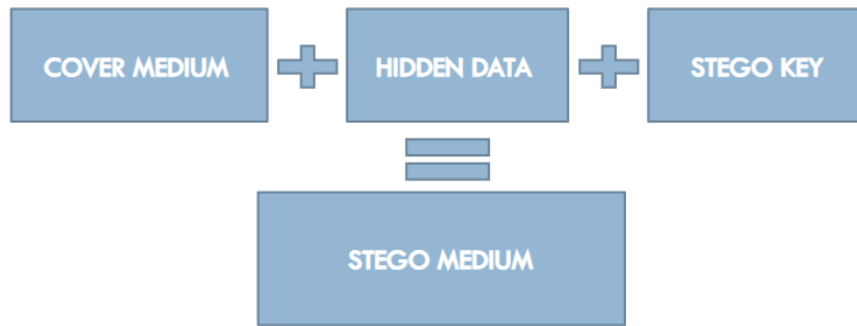
1. The target message is first encrypted and then combined with the target file by the means of special tools which have permissions to modify the files.
2. The encrypted data is appended with the target file by using special algorithms which makes the data hidden into the file and makes it invisible to naked eyes.
3. The information is visible to some special exceptional programs which are designed for steganography analysis.



### **Terms Associated With Steganography :**

#### **1. Cover- Medium :**

The medium in which the information or the target message is to be hidden is known as cover medium. Cover medium is initial phase of deciding where the information should be hidden in the medium.



## 2. Stego-Medium :

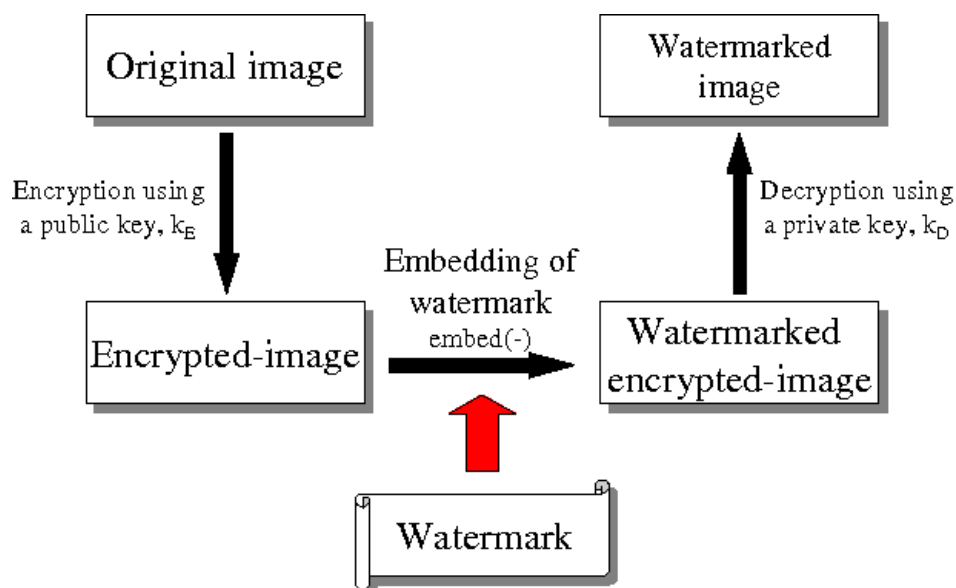
The Medium in which the information or the target message is hidden is known as the stego medium. In the stego medium, the information has been already hidden somewhere into the medium and this is the next phase after cover medium.

## 3. Information :

The plain text or data which is to be hidden within any particular data type is known as information. Everything is performed for the security and confidentiality of information.

Watermarking:

Watermarking Is a similar process to the steganography, which is used for the protection of the documents by keeping a copyright of the owner. Its primary goal is not to be destroyed or extracted. Watermarking is generally used with multimedia files to protect the intellectual property rights. Watermarks are also used with documents which are visible watermarks. It may be used to make information temper proof by using as fingerprint to the information for detection of changes.



## **Steganography Methods:**

### **1. Traditional Methods**

#### **a. Hidden Tattoos**

Hidden Tattoos: This method involves embedding information by slightly altering the pixels of an image. The changes are so subtle that they are not perceptible to the human eye, but they can be detected by steganography software.

#### **b. Using wax paper**

Using Wax Paper: In this method, information is written with invisible ink on a piece of paper, which is then covered with wax. The message becomes visible when the wax is removed.

#### **c. Using the news articles by highlighted text method**

This method involves sending a seemingly innocuous text, like a news article, where certain words or letters are highlighted. When these highlighted portions are combined, they form the hidden message.

#### **d. Microdots and symbolic communication**

Microdots are tiny dots printed with text that are too small to be seen by the naked eye. These microdots can be hidden within printed text or images. Symbolic communication involves using symbols or images to represent letters or words, creating a message that appears innocuous to anyone not familiar with the code.

### **2. Modern Methods**

- a. Plain text
- b. Hyper Text
- c. Image
- d. Video
- e. Audio
- f. Executable
- g. Network Packets

#### **Plain Text:**

In plain text steganography, hidden information is embedded within a regular text document. One of the common methods of steganography is by using plain text. Plain text steganography can be done by using the letters present in a paragraph or sentence. Special hover or text highlighting is used for this method.

For Ex : He Is Good Illusionist and Recon Lover if the first letter of each word is taken, it will look like : HIGIRL and after careful observation it is clear that the message is “ HI GIRL”.

Sometimes some special symbolic or white characters are used which are generally not decoded by normal text viewers and hence are used for steganography.

### **Hyper Text:**

Hyper Text steganography involves hiding data within HTML or XML documents. Generally the message is hidden within the file using the comments which is generally not visible to a normal user and hence can be viewed by the inspection of source code and hence might be used for steganography. In this case the method is not much secure because an advanced user can easily detect this steganography. Sometimes it may present within the phrases, images or any other page content settings.

### **Image:**

Digital images are a common carrier for hidden data. Techniques like LSB (Least Significant Bit) insertion involve altering the least significant bits of the pixel values in an image to encode hidden information without significantly changing the visual appearance of the image.

### **Video:**

Videos can be used to hide information by manipulating frames, changing pixel values, or altering audio frequencies. Video steganography methods aim to embed data within the video frames or audio channels without causing noticeable changes to the video quality or audio playback.

### **Audio:**

Similar to image steganography, audio steganography involves hiding data within audio files. Techniques like LSB manipulation can be applied to audio samples or channels to embed hidden information without perceptible changes to the audio.

### **Executable Files:**

Steganography can be applied to executable files by modifying specific portions of the file without affecting its functionality. This method involves embedding data within the binary code of executable files, making it challenging to detect without specialized tools.

### **Network Packets:**

Steganography in network packets involves concealing data within the headers or payload of network packets. This technique is often used for covert communication over a network, where the hidden information is transmitted within seemingly normal network traffic.

## **Steganalysis:**

Steganalysis is the process of analysing and detecting steganography. Some special techniques and tools are used for steganalysis. Generally the statistical analysis is used for the steganography detection.

## **Steganalysis Attacks:**

### **1. Stego-Only Attack :**

In this type of attack only the stego file is available to the attacker. It means that an attacker can only access the stego file to retrieve the hidden message.

Detecting the presence of hidden information in the stego-object and extracting the hidden data without knowledge of the original cover object present significant challenges, especially if strong steganographic techniques have been employed to ensure the hidden data is imperceptible and difficult to detect.

### **2. Cover Attack :**

In cover attack, an attacker compares the original file with stego file to detect the pattern differences. For ex : an original and stego image is compared to know the pattern variance in that to find whether the steganography is done or not.

### **3. Visual Detection :**

Steganography can also be detected by using visual lookup. Sometimes the unusual variance and patterns can lead to the failure and detection of the steganography. Generally due to lack of proper encrypting within the image, it is detected by viewing the image. Specially, in case when the steganography is done using colour variance.

## **Steganography using tools :**

### **1. NetTools :**

DOWNLOAD :- <http://mabsoft.com/nettools.htm>

Using NetTools :

- NetTools is the all in one solution for beginners as well as intermediate users. It contains more than 100 tools for hacking and it is a complete toolkit package itself.
- It also Contains Steganography toolkit. So We can perform steganography using NetTools.
- Download & Run NetTools. There is drop down menu named tools from there choose steganography.

- Now click on load image option to open a image in which you want to hide a message. In the message box enter message you want to hide and click on hide text. Now save the image, output image will contain your secret message.
- Now if you want to extract message just load the image file and click on extract message. If image contains any message it will get separated and displayed.
- There are more tools present in net tools for steganography , try exploring them.

## 2. QuickStego :

DOWNLOAD :-[www.cybernescence.com/](http://www.cybernescence.com/)

USING QuickStego :

- Firstly download & Run QuickStego. It is very simple to use & have user-friendly interface.
- Click on open image to open the image in which you want to hide a message or text file. Click on Open text to open the text file you want to hide or type new message in message box.
- Click on save image to save . it will contain secret message hidden in it.
- Now To Extract Message , Load image and click on extract message . If the image contains any hidden message , it will be extracted.





## VULNERABILITY

“vulnerability is weakness present in any system. Vulnerability gives attacker advantage to use it to exploit the target system.”

Just like human gets a disease because of deficiency or weakness in immune system, this weakness is actually vulnerability in immune system and a disease uses that weakness to spread into human body. Similarly, Vulnerability is a weakness which leads to the exploitation of the target system.

- Vulnerability is also termed as loophole or bug. A bug is a technical error due to which a system or service became vulnerable.
- Researcher finds the bug and reports them so that the vulnerability might get patched and the security of service increase.
- Vulnerability may be due to human error or due to missing lines of codes or improper development.
- Vulnerability is a sign of danger, more the vulnerability are associated with the system, less security is associated. Vulnerability is of many types.



A Newly discovered vulnerability is known as ZERO-DAY. Zero-day is fresh vulnerability and hence there are high chances that it may be found in all of the application. penetration testing is all dependent upon vulnerability.

If a system is vulnerable, exploitation could be done. In the complete phase of penetration testing, attacker first tries to identify the vulnerability and then exploits the system by taking advantage of the same vulnerability.

Generally the penetration testing and vulnerability assessment is done in following:

1. Web Application Penetration testing
2. Network and Server Side Penetration testing
3. Android Application Penetration testing

#### 4. IOS Application Penetration testing

#### 5. Client Side Penetration testing

Almost every company rewards researchers for finding and reporting the bugs present in their websites or applications. Rewards may be in the form of money or goodies. Researcher also rewarded with their name in company's hall of fame. This became very interesting field due to this is completely white hat and researchers also get rewarded. Many newcomers are directly focusing on disclosure of vulnerability.

- Vulnerabilities are defined on the basis of the threat level. There is a standard who defines the list of top vulnerabilities by effect of every three years.
- Researcher's findings are rewarded according to the type of bug found. Generally, if top bugs are found, high amount is paid to the researchers along with hall of fames and goodies. This is also known as BUG BOUNTY or BUG HUNTING.
- There are many big giant like Microsoft, Google, Facebook, etc. who runs their own bug bounty program every year. Top vulnerability list is defined by the OWASP.

### **THE OPEN WEB APPLICATION SECURITY PROJECT (OWASP)**

OWASP is an international open source foundation. Owasp declares the list of top vulnerabilities on the basis of threat level and risk factor. This list is known as OWASP TOP 10. OWASP Top 10 vulnerabilities are recognized as the standard vulnerability list. Threat from these vulnerabilities is very high and cause potential damage to the web application.

- OWASP also declares the list for Mobile vulnerability with the name of OWASP Mobile Security Project.
- OWASP Zed Attack Proxy (ZAP) is one of the open source tool used for penetration testing.
- OWASP Zap is available online for free. It helps the user to automatically find security vulnerabilities in the target website.

This is mostly useful when you want to test developing web applications. OWASP ZAP is also used for manual penetration testing and generally used by professionals for manual testing. OWASP ZAP comes pre-installed in kali linux.

### **OWASP TOP 10 (2013):**

- OWASP TOP 10 is a flagship project of OWASP foundations. It is the list of 10 most threatening vulnerabilities which are found in web applications.

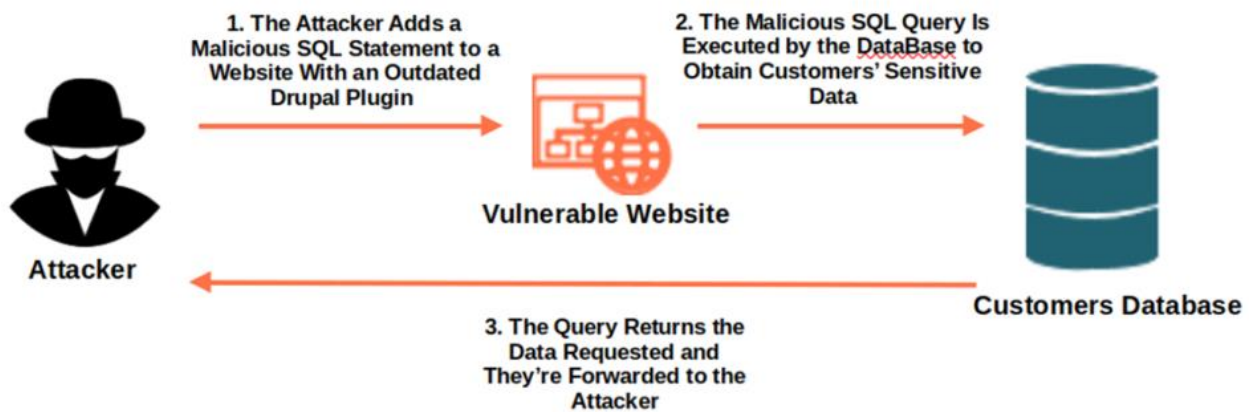
- OWASP redefines TOP 10 list from every three years. Along with the list of TOP 10 Critical vulnerabilities, it provides the whole documentation to learn and test for these security vulnerabilities in web application. This project is completely open source.
- All the penetration tester and bug bounty hunters follows OWASP TOP 10 Vulnerability standard while testing web applications.
- OWASP Projects are open source and for awareness purpose.
- OWASP TOP 10 will be revised By 2016 end or in 2017.

**Following are the top 10 vulnerabilities:**

1. Injection.
2. Broken Authentication and Session Management.
3. Cross-Site Scripting (XSS).
4. Insecure Direct Object References.
5. Security Misconfiguration.
6. Sensitive Data Exposure.
7. Missing Function Level Access Control.
8. Cross-Site Request Forgery (CSRF).
9. Using Components with Known Vulnerability.
10. Un-validated Redirects and Forwards.



1. **Injection:** Injection is at the top of top 10 vulnerability list from 2010. It is easy to exploit using the injections. This involves injecting malicious code (e.g., SQL, OS commands) into input fields or data to manipulate the behavior of the application.



Injections are of many types. Generally SQL Injection, LDAP, Xpath, XML Phrases, SMTP headers, etc. Injection flaws can be easily detected by examining the source code but in the testing it is somewhat tough to find the injection flaws. Generally Fuzzers are used by the attacker to find injection flaws in any web application.

An attacker tries to bypass the security level by using queries. LDAP, OS Command and SQL Injections are mostly seen forms of injection vulnerabilities.

### **Prevention:**

Best practise of preventing the injection flaws to occur in a web application is keeping the untrusted data filtered and keeping separate from command and queries.

- Secure coding is used during the development of web application. By which filters are define within the internal coding so that the injection flaws can be prevented.
- Due to many web application uses sql based databases, it is quite recommended to restrict the code to allow queries.
- If the web application will not be restricted, there are huge chances of compromise into the databases or whole web application.

### **Some of the prevention mechanism (according to owasp) :**

- a) Use of safe API which avoids the use of interpreter completely and restricts the queries to get executed.
- b) 2. Carefully escape special characters using the specific escape syntax should be used so that input can be restricted.

- c) 3. White list input can also be used which deny the unauthorized input and hence less chance of takeover.
- d) 2. Broken Authentication and Session Management : Broken Authentication and Session Management comes after the

## 2. Broken Authentication and Session Management:

- Weaknesses in user authentication and session management can lead to unauthorized access, identity theft, or session hijacking.
- Broken authentication and session management vulnerability leads to takeover of all accounts or sometimes few targeted accounts present in the web application. Once the exploit is done successfully, attacker owns the accounts and has full privileges as of the user.
- Generally the admin or privileged accounts are targeted. According to the corporate point of view, compromising into account may be lead to sensitive information disclosure.

### How to check Broken Authentication and Session Management:

1. Session ID maybe clearly visible in the URL.
2. Session Ids are vulnerable to session time fixation.
3. User authentication and session management tokens are not invalidated during the logout.
4. No Session timeout.
5. Unencrypted network transmissions transmissions are used.
6. Weak credentials are allowed i.e. weak or simple passwords are allowed.
7. Improper encryption algorithms are used to encrypt the user credentials

### Protection (According to OWASP):

- A single and proper set of authentication and session management controls should be used. The interface should be simple for the developers.
  - Precautions should be taken to avoid the XSS flaws which can be used to steal the session ids.
3. **Cross-Site Scripting (XSS):** Attackers inject malicious scripts into web pages viewed by other users. These scripts can steal user data or manipulate the content of the web page. Cross-Site scripting is generally used to steal the session ids. It allows an attacker to inject untrusted javascript codes into the web application without any validation.

## **Cross-Site Scripting is of 3 types:**

### **1. Stored XSS :**

In stored xss, attacker plants an untrusted javascript snippet into the target web application. Once the user visits the targeted web application, stored javascript gets executed and further exploitation is performed.

### **2. Reflected XSS :**

In reflected xss, attacker invites the user to visit a particular targeted web application by sharing the link over chats or e-mails, etc.

### **3. DOM based XSS :**

In DOM based xss, attacker modifies the DOM of the target web application from the client side in the victim browser and hence it gets executed once the user opens the web application in the targeted system.

## **Prevention:**

- There should be proper output encoding which is useful to restrict the cross-site scripting in a web application.
- There should be a proper input validation so that the cross-site scripting can be avoided in the target web application.

### **4. Insecure Direct Object References (IDOR):**

- Occurs when an application provides direct access to objects based on user-supplied input, allowing unauthorized access to data.
- It is simply a flaw in a web application in which the particular database records or directories are not protected completely and can be easily exposed.
- For ex : A person logs in into his e-mail account, due to the insecure direct object references vulnerability is present in the web application, he might be able to see some other person's email address.

### **5. Security Misconfiguration:**

- Improperly configured security settings or default configurations can expose sensitive information or provide unauthorized access.
- Security misconfiguration may be present due to insecure coding of the web application, improper configuration of web server, outdated version of operating system or due to the vulnerable scripts or APIs used. In this case, automated scanners are helpful to detect the unpatched points from which the web application might become vulnerable.

- Security misconfiguration may leads to complete takeover of the web application without the knowledge of users.

#### 6. **Sensitive Data Exposure:**

- Failure to properly protect sensitive data (e.g., credit card numbers, passwords) can lead to data breaches and identity theft.
- Attacker generally perform various kinds of sniffing attacks like man in the middle attack or steals the credentials which are in plain form (unencrypted) or by the cookie stealing, an attacker can take advantage and gets the sensitive information disclosed to him.

#### 7. **Missing Function Level Access Control:**

Attacker tries to change the URL in the browser when trying to get access of the web application to get access to a function which is not accessible by him. An attacker uses Missing Function.

- Failure to enforce proper access controls can allow unauthorized users to access privileged functionality.
- Level Access Control Vulnerability to perform this exploit. Due to the improper checksums or missing function level access control, web application is not able to verify for a specific object or function and hence attacker can access the functions for which he is not having any authority. It is easy to exploit web application using this vulnerability.

#### 8. **Cross-Site Request Forgery (CSRF):**

Cross-Site Request Forgery is widely known as CSRF. CSRF is again one of top listed vulnerability. Using CSRF attacker can create forged http requests. Using the forged http request, attacker tries to trick the user to exploit him.

- Attacker can use xss or any other methods to get access from user. If the user is successfully authenticated, attack completes successfully.
- Browser generally sends credentials in the form of session cookies automatically.
- An attacker can create fake malicious pages and sends forged requests which are not easily differentiated from the original requests. Using the CSRF, once the attack is successfully completed the attacker can perform various activities in the user's account like maintaining the session (login and logout), shopping or even updating the details.



- Cross-Site Request Forgery is generally popular with the spammers and the fraudster. Once the target is exploited, the attacker can make the forged http request in order to get credentials.
- This involves tricking a user's browser to perform an unwanted action on a site where the user is authenticated.

## 9. Using Components with Known Vulnerability:

Web application sometime uses the components which are well known and also their weakness is publicly disclosed. In such cases, the attacker may exploit the web application by exploiting the components with known vulnerability.

- Many plugins and scripts are vulnerable to attack and many web applications use the same components and hence easily get exploited by the attacker.
- Attacker can easily finds the vulnerable and out dated components using the automated scanners. In such cases, automated scanners save the time of the attacker.
- Sometimes it get complicated due to the components used are placed at very lower and deep positions.
- In most cases the development didn't pay much attention to the version of the components and checking whether it is already vulnerable or not. In some cases, the components used are highly vulnerable.
- Applications using outdated or vulnerable components (e.g., libraries, frameworks) are at risk of exploitation.

## 10. Unvalidated Redirects and Forwards:

Generally when users visits a website they are redirected or forwarded to a new page of different web address. Now these forwarding and redirects are changed each and every. If an application allows untrusted input to determine the destination of redirects or forwards, attackers can redirect users to malicious sites.

Generally when users visits a website they are redirected or forwarded to a new page of different web address. Now these forwarding and redirects are changed each and every allowing attacker to choose the destination page.

This vulnerability is generally used to redirect or forward user to an malicious page and attempt to install some Trojans or malwares into the user's system which will ultimately result into takeover of the user's system and disclosure of the sensitive information like bank account details, login credentials, personal information, etc.



## **DAMN VULNERABLE WEB APPLICATION (DVWA):**


Damn Vulnerable Web Application (DVWA) is a specially designed vulnerable web application which is used to learn real time vulnerability assessment.

DVWA contains most of the vulnerabilities. A tester can perform testing on it. It is completely open source project. There are many other web applications which are available to check vulnerability assessment and penetration testing skills and some live bootable image files are also available which can be run as virtual machine.

Download DVWA : <http://www.dvwa.co.uk/>

Installing DVWA on Local Host :

1. Download the DVWA package from its website.
2. Download XAMPP to run DVWA on local host. Download XAMPP : <https://www.apachefriends.org/download.html>
3. Install and Run the XAMPP Control Panel.
4. Install Apache and MySQL Server from XAMPP control panel and allow them through firewall. From the control panel start both servers.
5. Extract the DVWA archive downloaded and put the folder into “ C:\xampp\htdocs”.
6. Now DVWA will run on your local host.
7. Open your browser and type “ 127.0.0.1” or “localhost” to open the local host server. This is generally used for the testing web application on local server.
8. Navigate to “127.0.0.1/dvwa/login.php” or “localhost/dvwa/ login.php”. Username : admin Password : password.
9. A MySQL error will be encountered. Now navigate to : “C:\xampp\htdocs\dvwa\config\config.inc.php”.
10. Open this file using any text editor and find the line : “\$ DVWA[’db password’]=’p@ssw0rd’ “
11. Change this line to the following : “ \$ DVWA[’db password’]= ‘ ’ ” 12. Now again visit to the dvwa login page and this time no error would be encountered.



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

### WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

### Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

### General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

## Testing with DVWA :

### 1. SQL Injection :

SQL injection is one of common and most threatening injection vulnerability. An attacker injects the sql queries into data field like form fields or login page in order to bypass the security and get access to the databases. Some time it leads to the complete host takeover.

1. Run DVWA on local host and Login into it.
2. Click on DVWA security and set it to LOW (for the beginners).
3. Click on Sql injection button in left sidebar.
4. Input any sql queries into the USER ID field to check whether it is working or not. For ex : input ' 3 '. Now If it shows the user details present at id = 3 than its working (shown in screenshot).
5. To see the all users into database database input this query : “ %’ or 0=0 union select null, user() # “ (shown in screenshot).
6. Last detail in which only surname is shown as “root@localhost” indicates the user who injected the query.

7. Download sql cheat sheet from the internet and try to taste different queries and analyse their behaviour.



## 2. XSS :

Cross-Site scripting is already explained above and is the one of the critical vulnerability.

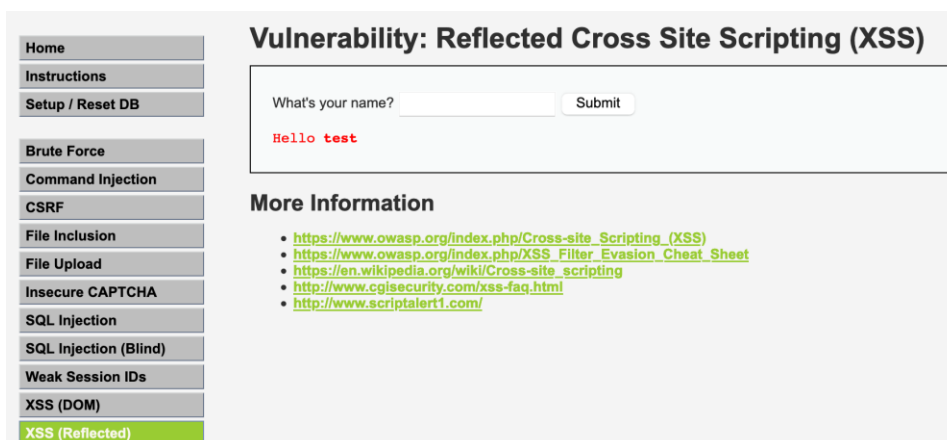
1. Run DVWA on local host and Login into it.

2. Click on DVWA Security in left sidebar and Set DVWA Security to LOW. 3. Click on XSS (stored). For the beginning, start with stored xss.

4. In the Name field input the name (anything) and in message field input javascript. For ex :  
Name : Harsh Message : `<script>alert("Hacked ! ")</script>`

5. Click on Sign Guestbook. The javascript will get stored. Now again input name and message with anything and click on Sign Guestbook. The javascript which was submitted earlier will get executed and a popup will be shown up (shown in screenshot).

6. Download XSS cheat sheet from the internet and try executing different XSS (stored and reflected).



### 3. Cross-Site Request Forgery :

1. Run DVWA on local host and login into it.
2. Click on DVWA Security from the left side bar and set the security as LOW.
3. Click on CSRF from the left side bar.
4. Input the New Password and Confirm New Password with any password and click on Change.  
For ex : harsh@harsh
5. Password Changed message will be shown below the change button.
6. Now Check the URL. There will be two strings which are separated by the "&" :  
password\_new = harsh@harsh password\_conf= harsh@harsh
7. These strings contain the password which has been set as new password.
8. Change the password present in both the strings like : password\_new = xr00t password\_conf= xr00t (shown in screenshot)
8. Now reload the page and the password will be changed again.
9. Now logout from DVWA and try to login with changed password password and login will be successfully (shown in screenshot).
10. Visit [www.owasp.org](http://www.owasp.org) and read about more advanced uses of CSRF.

