Question1:

## *What is ToR and discuss attacks that are possible on it. Install ToR on your system and compare and contrast it with a regular search engine like Google*

***Answer:***

The Tor (the onion routing) browser is a web browser designed for anonymous web surfing and protection against traffic analysis. Although Tor is often associated with the darknet and criminal activity, law enforcement officials, reporters, activists, whistleblowers and ordinary security-conscious individuals often use the browser for legitimate reasons.

The United States Navy originally designed the browser to protect sensitive U.S. government communications. While Tor continues to be used by the government, it is now an Open Source, multi-platform browser that is available to the public. Today, human rights activists and dissidents who need to keep their internet activities private from oppressive governments, law enforcement, intelligence agencies and criminals use Tor, for example.

Law enforcement agencies are able to use various techniques and tools to track down the users of Tor, especially if the sites they visit are not using end-to-end encryption (E2EE). The browser uses exit relays and encrypted tunnels to hide user traffic within a network but leaves the endpoints more easily observable and has no effect beyond the boundaries of the network.

**Tor works :**

The Tor browser works by using a technology known as *onion routing*. The onion router is a peer-to-peer (P2P) overlay network that enables users to browse the internet anonymously. Onion routing uses multiple layers of encryption to conceal both the source and destination of information sent over the network. It is designed so no one can monitor or censor online communication.

Once a user installs Tor, the browser uses Tor servers to send data to an exit node, which is the point at which data leaves the network. Once this data has been sent, it is encrypted multiple times before being sent to the next node. Repeating this process makes it difficult to trace the data back to the original source. In addition to encryption, the Tor browser does not track browsing history or store cookies.

***Levels of security*:**

The Tor browser offers three levels of security, including the default level plus two additional levels. Each level provides a different degree of protection, with the maximum protection found in the highest level.

1. On the **default setting**, the browser is the most user-friendly; however, this setting provides the lowest level of security.
2. The **second level** provides more security but offers a slower experience. For example, JavaScript-enabled sites may run slower as this setting disables JavaScript on non-Hypertext Transfer Protocol Secure (HTTPS) sites.

3. The **third and highest level** of security disables some fonts and images, in addition to JavaScript, on all sites.

## *Tor weaknesses*:

Although Tor is more secure than most commonly used browsers, it isn't impervious to attack. While Tor protects against traffic analysis, it does not prevent end-to-end correlation, which is the process of using more than one data point from a data stream to identify the source and purpose of an attack.

Other Tor browser weaknesses include the following:

- **Consensus blocking.** The Tor exit relay is vulnerable to a class of attacks that enables a malicious user to temporarily block consensus nodes from communicating. This problem is similar to a denial of service (DoS) attack, which blocks access to a website by flooding it with so many requests that it is impossible for the servers to keep up.
- **Eavesdropping.** The Tor exit nodes are vulnerable to eavesdropping, as the traffic passing through does not use E2EE. While this method does not explicitly reveal a user's identity, the interception of traffic can expose information about the source.
- **Traffic analysis attack.** In a passive traffic analysis attack, an intruder extracts information and matches that information to the opposite side of the network. In an active traffic analysis attack, the intruder modifies packets following a pattern to assess their impact on traffic.
- **Tor exit node block.** Websites can block users using the Tor browser from accessing their page.
- **Bad apple attack.** In 2011, a documented attack revealed the exposure of the Internet Protocol (IP) addresses of BitTorrent users on the Tor browser.
- **Sniper attack.** A type of distributed DoS (DDoS) attack, a sniper attack overwhelms exit nodes until they run out of memory. An attacker can reduce the number of functioning exit nodes, increasing the chances of users using exit nodes controlled by the attacker.
- **Relay early traffic confirmation attack.** In 2014, Tor released a security advisory after discovering a deanonymization attempt on the browser's users. Bad actors modified the headers of cells and sent them back to the user. If the entry node was also part of the attack, an attacker could capture the IP address of users by the attacking relays.
- **Mouse fingerprinting.** In 2016, a researcher discovered they could track mouse fingerprinting using a time measurement at the millisecond level. Using this method, third parties could identify users by tracking their mouse movements when using a specific website and comparing their mouse movements on the Tor browser or a regular browser.

## *Access to the dark web :*

The *dark web* refers to the parts of the internet not indexed by search engines. It contains a range of websites, including forums and marketplaces, that require specific software for access. While anyone can surf the public internet, the dark web is a private network where users do not disclose their real IP addresses. This makes it a more secure place to do business on the web but also a place where many illegal activities occur.

Users such as the military, politicians, journalists and criminals use the dark web. The dark web was created to enable individuals or groups to communicate in a way that is, in their view, untraceable. Besides potential illegal uses, the dark web also serves a number of legitimate purposes, including enabling whistleblowers to share information that they might not otherwise be able to share.

The Tor browser enables people to have access to the dark web. While many associate the dark web with illegal activities, the Tor network also has a number of legitimate uses. These include communicating or browsing in countries implementing internet censorship.

***Tor browser: A different way to use the internet*:**

Despite Tor and the dark web being closely linked, using Tor browser doesn't mean involving in illicit activities. It can be very useful software to certain internet users. Because of how it operates, Tor is generally safe to use, and Tor onion browser offer several benefits like heightened safety and privacy. Before using the Tor browser, though, users should be aware of any potential legal issues with Tor in their country, and that they could be flagged for its use.

The differences between the Tor browser, proxy servers, and VPNs:

While the Tor browser, proxy servers, and VPNs all offer some form of anonymity, they differ slightly in how they work and the levels of protection they provide.

Proxy servers essentially function as an intermediary between a user and the websites they access. While they do obscure IP addresses and geographical locations, they do not encrypt data and online activity. Because of this, user data remains exposed and can easily be tracked and hacked. So, is Tor safe compared to proxy servers? Yes, to an extent. Despite the weaknesses outlined above, the Tor browser offers a much higher level of encryption and routing, giving users more anonymity. While using a proxy server alongside the Tor browser can help mask the use of Tor, using both a proxy server and Tor browser will not offer any further protection to users.

Virtual private networks (VPNs) are powerful networks that fully encrypt all web traffic by routing it through different servers, thereby also obscuring the user's IP address. The most significant difference between VPNs and the Tor browser is that VPN is operated by central providers who operate the network, while the latter is a decentralized network managed by volunteers. Additionally, Tor routes data through independent nodes, while VPNs route online traffic through remote servers.

.Question 2:

## *Use the web site http://testphp.vulnweb.com/ for the following. Perform sql injection on it and retrieve the user table and its contents.*

***Answer:***

SQL Injection is a code injection technique where an attacker executes malicious SQL queries that control a web application's database. With the right set of queries, a user can gain access to information stored in databases. SQLMAP tests whether a 'GET' parameter is vulnerable to SQL Injection.

For example, Consider the following php code segment:

$variable = $_POST['input'];

mysql_query("INSERT INTO `table` (`column`) VALUES ('$variable')");

If the user enters "value'); DROP TABLE table;--" as the input, the query becomes

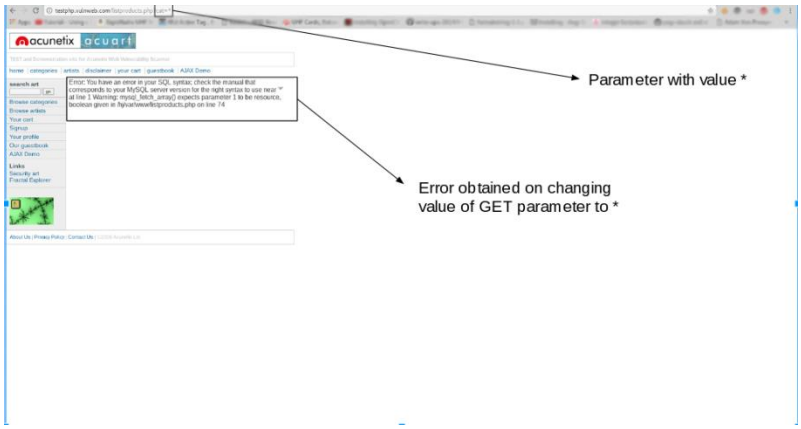
INSERT INTO `table` (`column`) VALUES('value'); DROP TABLE table;--')

which is undesirable for us, as here the user input is directly compiled along with the pre-written sql query. Hence the user will be able to enter an sql query required to manipulate the database.

**cat=1**, where the 'GET' parameter is in bold, then the website may be vulnerable to this mode of SQL injection, and an attacker may be able to gain access to information in the database. Furthermore, SQLMAP works when it is php based.

A simple test to check whether your website is vulnerable would be to replace the value in the get request parameter with an asterisk (*). For example,

http://testphp.vulnweb.com/listproducts.php?cat=*




If this results in an error such as the error given above, then we can conclusively say that the website is vulnerable.

### Installing sqlmap

SQLMAP comes pre-installed with kali Linux, which is the preferred choice of most penetration testers. However, you can install sqlmap on other debian based linux systems using the command

sudo apt-get install sqlmap

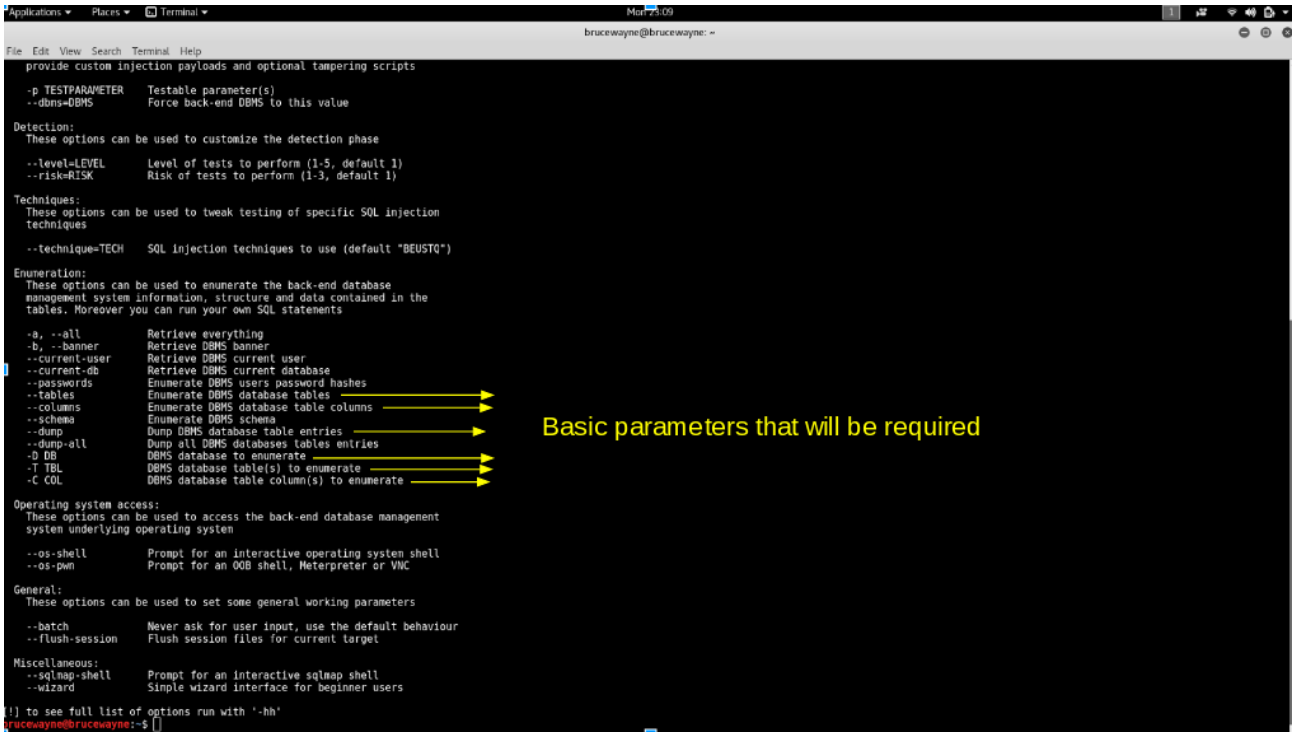
### Usage

In this article, we will make use of a website that is designed with vulnerabilities for demonstration purposes:

http://testphp.vulnweb.com/listproducts.php?cat=1

As you can see, there is a GET request parameter (cat = 1) that can be changed by the user by modifying the value of cat. So this website might be vulnerable to SQL injection of this kind.
To test for this, we use SQLMAP. To look at the set of parameters that can be passed, type in the terminal,

sqlmap -h



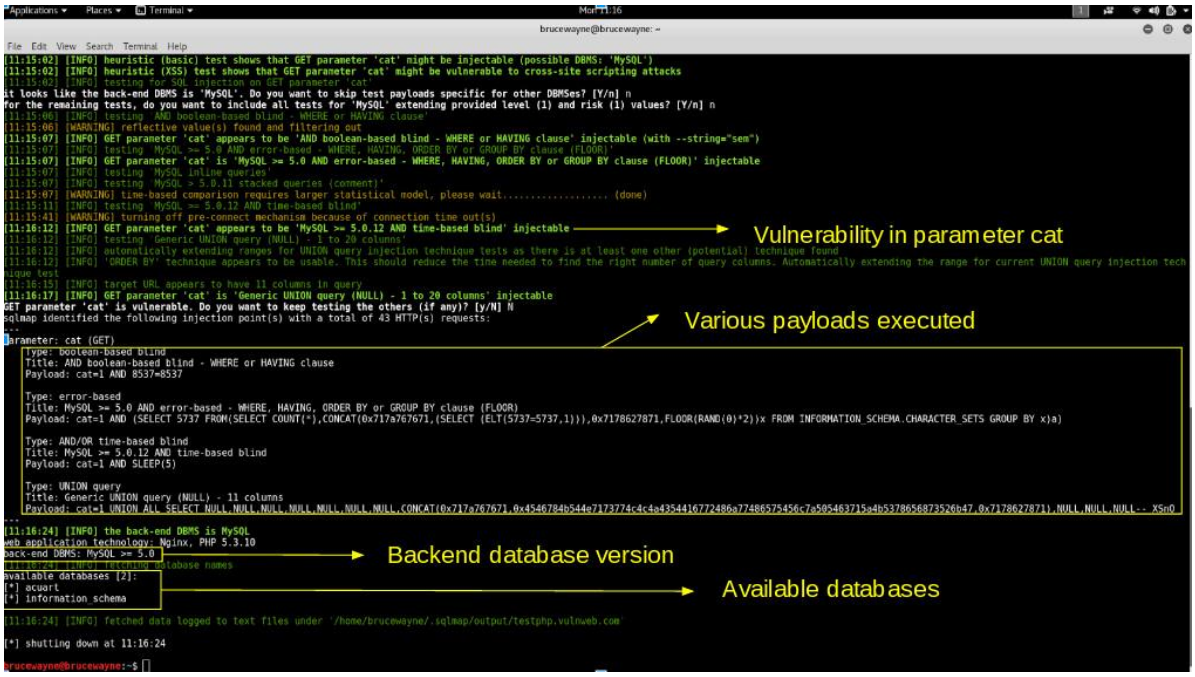

The parameters that we will use for the basic SQL Injection are shown in the above picture. Along with these, we will also use the –dbs and -u parameter, the usage of which has been explained in Step 1.

**Using SQLMAP to test a website for SQL Injection vulnerability:**

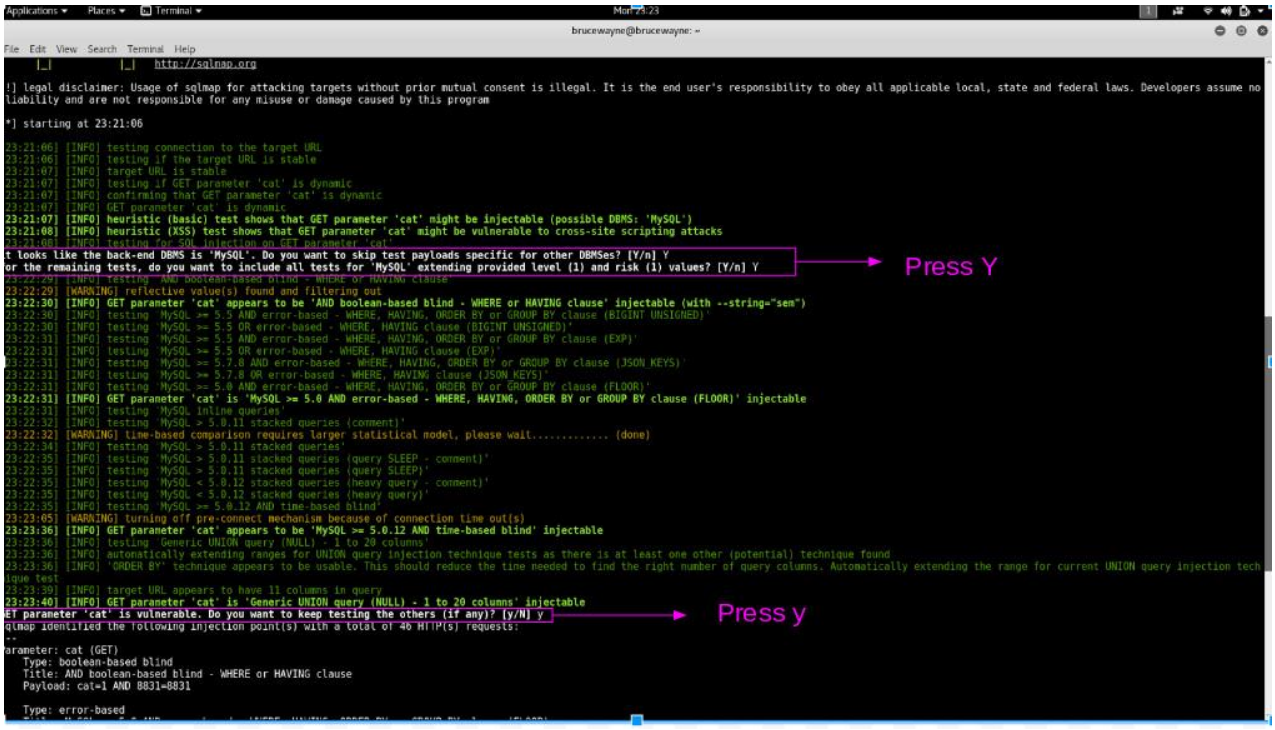
- **Step 1: List information about the existing databases**

  So firstly, we have to enter the web url that we want to check along with the -u parameter. We may also use the –tor parameter if we wish to test the website using proxies. Now typically, we would want to test whether it is possible to gain access to a database. So we use the –dbs option to do so. –dbs lists all the available databases.

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs




- *We get the following output showing us that there are two available databases. Sometimes, the application will tell you that it has identified the database and ask whether you want to test other database types. You can go ahead and type 'Y'. Further, it may ask whether you want to test other parameters for vulnerabilities, type 'Y' over here as we want to thoroughly test the web application.*



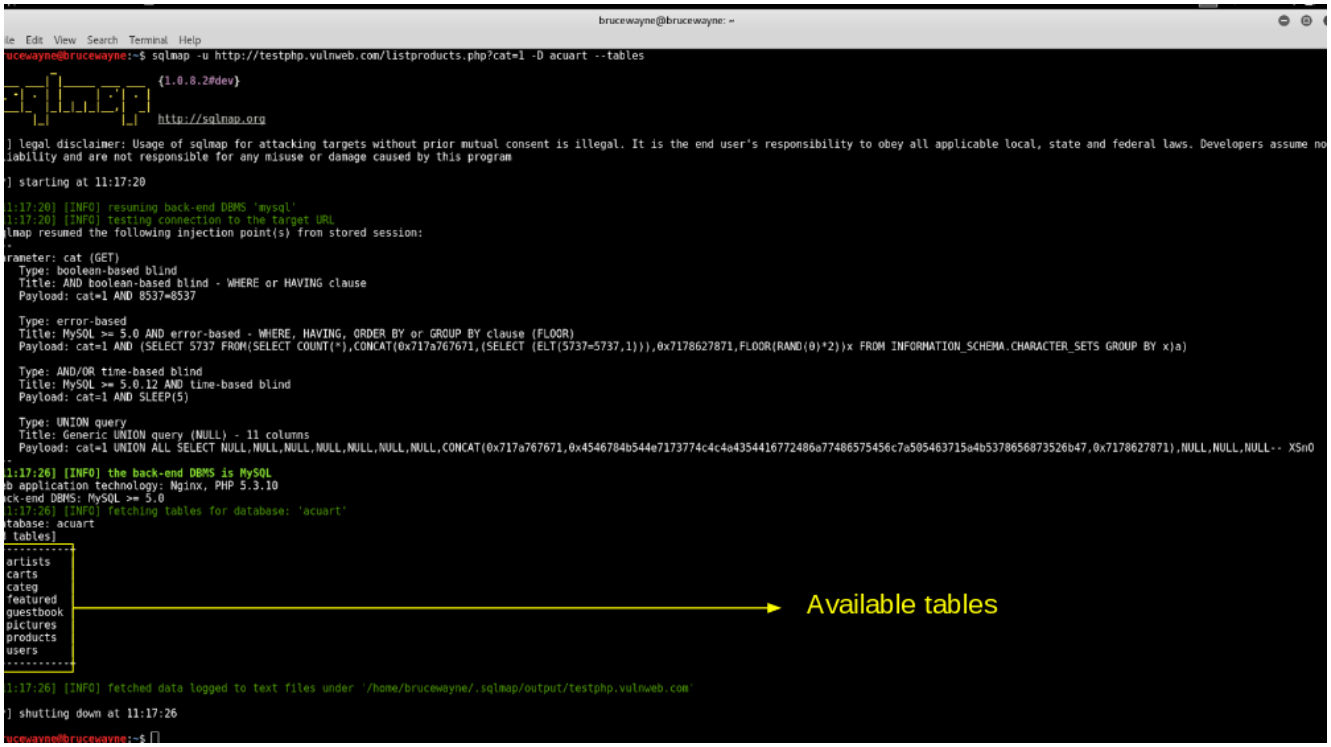

- *We observe that there are two databases, accurate and information_schema*

- **Step 2: List information about Tables present in a particular Database**

  To try and access any of the databases, we have to slightly modify our command. We now use -D to specify the name of the database that we wish to access, and once we have access to the database, we would want to see whether we can access the tables. For this, we use the –tables query. Let us access the accurate database.

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1

-D acuart --tables



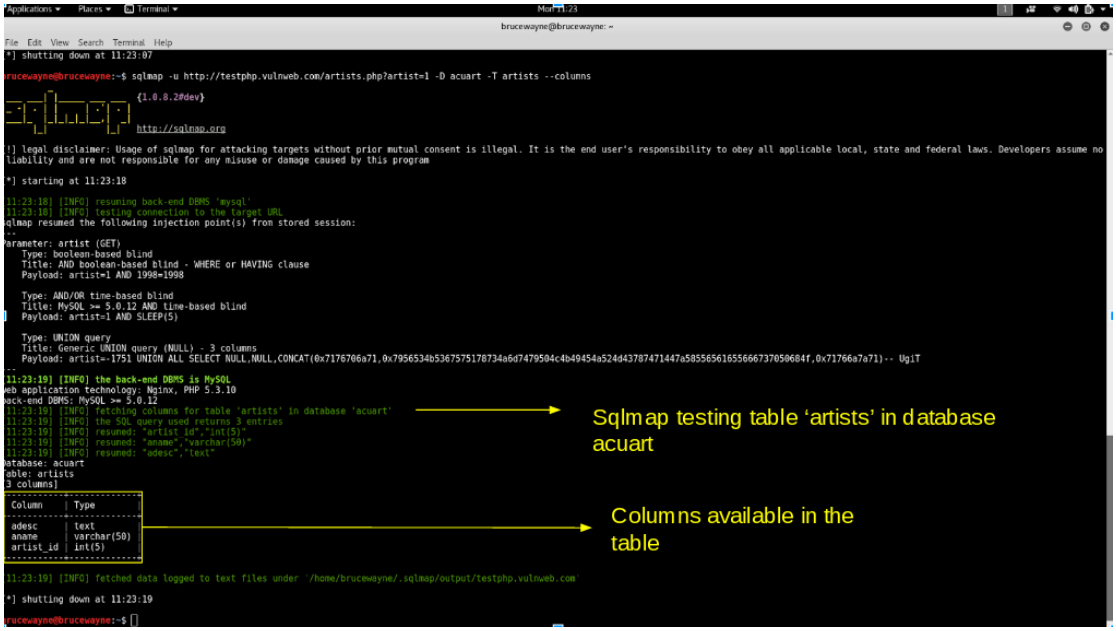

Tables

- In the above picture, we see that 8 tables have been retrieved. So now we definitely know that the website is vulnerable.
- **Step 3: List information about the columns of a particular table**

  If we want to view the columns of a particular table, we can use the following command, in which we use -T to specify the table name, and –columns to query the column names. We will try to access the table 'artists'.

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1

-D acuart -T artists --columns




Columns

- **Step 4: Dump the data from the columns**

  Similarly, we can access the information in a specific column by using the following command, where -C can be used to specify multiple column name separated by a comma, and the –dump query retrieves the data

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1

-D acuart -T artists -C aname --dump

**Question 3** :

## *What are Deepfakes? Discuss how they are being used for Impersonation attacks. Explain how they can be countered.*

***Answer:***

A deepfake is a technology that typically belongs to fraudsters. They create the fake media using machine learning and artificial intelligence algorithms to alter videos, emulate forgeries of people doing or saying malicious things, creating convincing synthetic audio, and other forms of fake content where humans are present. Con artists can even generate deepfakes from existing images to create places, people, and things that are entirely synthetic.

People have used deepfake technology for a variety of purposes from fun to malicious. For example:

- Biometrics like facial expressions are generated and superimposed onto another person's body in fake videos
- Human voices matching the timbre and pitches of celebrities make like Jay-Z singing Billy Joel in deepfake audio recordings
- Politicians saying things they've never said before.

As the technology gets better, fraudsters will likely continue to use malicious deepfakes for cybercrimes and corporate espionage.

The first known deepfakes were likely AI-generated videos published at the start of 2017 by a Reddit user to the platform. Today, the user has been credited as deepfakes' creator, bringing the overall practice into public view.

Deepfake creators often used open-source image libraries like Google image search, social media websites, stock photo databases, tensorflow, and YouTube videos to create a machine-learning algorithm which allowed the user to insert people's faces onto pre-existing videos frame by frame.

Although there are glitches and obvious catches a user can notice, the videos are quite believable and are only getting more convincing as more users continue to experiment. At the time, the deepfake creator even created and released an app called "FakeApp," making it easier for even basic, less tech-savvy users to create fake content from funny videos to those with more malicious aims. Today, there are likely hundreds of deepfake generators.

Deepfake creation doesn't have the lowest bar to entry, but it's not super difficult, either, especially given the proliferation of DIY tools. Bad actors likely have some combination of a super-powered computer, artificial intelligence and machine learning programs, and hundreds of thousands of images of selected people.

***Here's the process for a deepfake video:***

1. First, a user runs thousands of facial pictures of two selected people through an encoder – an artificial intelligence algorithm that uses a deep, machine learning network
2. The encoder compares the images of the two faces, compressing them into shared common features.
3. A second AI algorithm called a decoder recovers the faces from the compressed images. Multiple decoders may be used: one to find and analyze the initial person's face, the other to do same to the second person's face.
4. To perform the face swap, a user feeds the encoded images of person A's face into the decoder trained on person B. The decoder then reconstructs the face of person B with the expressions and orientation of face A and vice versa. For the more convincing fake content (or malicious deepfakes), this will be done on thousands of frames.

Another method to create deepfakes use a generative adversarial network (Gan). The notable difference here is the Gan creates an entirely new image/video that looks incredibly real, but is entirely fake. Here's how it works:

1. A Gan pits two artificial intelligence algorithms against each other. The first algorithm, known as the generator, is fed a noise signal and turns it into a fake image.
2. This synthetic image is added to a discriminator – another algorithm that's being fed a stream of real images

3. The two components (generator and discriminator) are functionally adversarial, and they play two roles against each, like a "forger and a detective" described by Shen et al, students who used a GAN to create deepfakes in a study at UCSD.
4. The process is repeated countless times with the discriminator and generator both improving. After a while, the generator will start producing a realistic image, or deepfake. This could be a person, place, or thing.

To take a deep fake to the next level, Tom Cruise's fake face must have a fake Tom Cruise voice. Layering audio onto deepfakes typically happens in one of three ways.

1. Replay-based deepfakes, which use a microphone recording or cut-and-paste techniques to cobble a new audio string together from existing voice snippets.
2. Speech synthesis, which often uses a text-to-speech system to create real-sounding audio from a written script.
3. Imitation-based voice deepfakes, which transform an actual speech clip from one subject to make it sound as if another subject is saying it

## *Deepfakes be used for fraud:*

Instagram users share more than 1 billion images daily on the platform.Google likely has even more selfies of people in the petabytes it stores. As a result, most people have some type of digital fingerprint – whether that's a LinkedIn account profile picture, or family photos shared on Facebook (these items encompass a behavioral biometric profile). All these pictures are potential inputs for AI to begin creating convincing Deepfakes for deceptive media.

Deepfakes have been used for spoofing famous people, account takeovers, political tricks, extortion, fraud, and revising existing formatting of entertainment and art, and more innocuous meme creation in social media circles. One example, shows how con artists can leverage the technology to blackmail even high-ranking executives.

As the technology improves and becomes commoditized, it could be used for identity-theft and other cybercrimes including fraudulent account opening and account takeover. Bad actors can use deepfakes for various types of fraud, including:

- **New account opening fraud:** Using the methods to create a deepfake described above, a fraudster could look on a social network and collect hundreds of images to create a deepfake image or audio, and add that to a synthetic identity: an amalgamation of stolen identity info. If it's good enough, the fraudster could use the compelling deepfake and identity to open a new account at bank, take out hundreds of thousands in loans, and bust out without paying interest leaving the bank with monetary losses. Tough break.
- **Account takeover fraud:** In 2022 alone, nearly 2,000 data breaches impacted hundreds of millions of individuals.Some of those data breaches might have included Biometrics databases perpetrators can create fakes that mimic biometric data and trick systems that rely on face, voice, vein or gait recognition.
- **Phishing scams:**

  Modern phishing attempts have incorporated fake video messages, which are often personalized and tailored to the target. Using deepfake technology, scammers can generate video clips of trusted figures, celebrities, or even family members, asking the recipient to undertake certain financial actions, making the deceit seem all the more authentic. Like the example of the unwitting CEO and the fake Hungarian

supplier, fraudsters also use voice-imitation techniques to simulate calls from trusted entities. These fake audio calls can be convincing enough to persuade individuals to share sensitive information or transfer funds to unauthorized accounts.

- **Impersonation attacks:**

  Again, the fake Hungarian supplier comes into the spotlight. Like that fraudster, others use deepfakes to mimic corporate executives or even high-ranking government officials. Successful fakes can trick employees into divulging sensitive information or money. In the case of government officials, this information passed to bad actors may even be considered espionage.

- **Synthetic identity theft:**

  Criminals may even create entirely fake personas. They do so by generating entirely new, fictitious identities complete with photos, voiceprints and even background stories by harvesting pieces of legitimate identity information and cobbling them together. These synthetic identities can then be used to open bank accounts, apply for credit cards, or even commit large scale financial fraud, making it hard for authorities to trace back to a real individual.

Scam artists will use these various forms of deepfakes to commit fraudulent financial transactions. By manipulating audio or video to mimic an actual person (or fabricate a new identity), bad actors can forge verbal or visual approvals for everything from a wire transfer to a loan application. They'll use deepfakes and other forms of fraud for financial gain, to damage to reputations or to sabotage a competitive company or even government.

In part two of this blog post, we'll examine how organizations can spot and even set up better safeguards to prevent against deepfakes and other types of fraud.

## The solutions for deepfakes:

Detecting deepfakes is a hard problem. Poorly done or overly simplistic deepfakes can, of course, be detected by the naked eye. Some detection tools can even spot more faulty characteristics. But artificial intelligence that generate deepfakes are getting better all the time, and soon we will have to rely on deepfake detectors to flag them to us.

To counter this threat, it's important to make sure companies and providers use two- or multi-factor authentication. Multi-factor authentication approaches layer various forms of verification on top of one another to create more obstacles for fraudsters. For example, facial authentication software may include certified liveness detection that provides an additional safeguard against deepfakes. And because sophisticated deepfakes can spoof common movements like blinks and nods, authentication processes must evolve to guide users through a less predictable range of live actions.

## *Detecting deepfakes in financial scams:*

In an era where deepfakes are increasingly being used in financial scams, safeguarding against them is increasingly important. Fortunately, as technology advances, methods to detect these scams are also evolving. Organizations can employ the following strategies to detect and counter deepfakes, which will be especially important in the financial services realm.

### Visual analysis:

Deepfakes, while sophisticated, often display inconsistent facial features. AI struggles to replicate minute facial expressions, eye movements, or even the way hair and facial features interact. Algorithms that generate deepfakes can also show unnatural lighting and shadows. Visual analysis may uncover shadows inconsistent with the light source or reflections that do not align correctly.

### Verification:

While deepfakes can replicate voices, they might also contain unnatural intonations, rhythms or subtle distortions that stand out upon close listening. Voice analysis software can help identify voice anomalies to root out deepfakes. Implementing authentication processes that layer codes or follow-up questions on top of voice commands can help ensure the request is genuine. Where files are concerned, automated document-verification systems can analyze documents for inconsistencies, such as altered fonts or layout discrepancies, that might indicate forgery.

### *Multi-factor authentication:*

The name of the game is layered security. Adding facial, voice, or other biometric recognition adds another hoop for a scammer to jump through even if they manage to impersonate a voice or face. Device recognition can help verify that requests are from previously authenticated or recognized devices is also an option for multi-factor authentication.

### Blockchain and digital signatures:

Blockchain technology promises an immutable record of all transactions. By using digital signatures and blockchain ledgers, organizations can implement provenance tracking for financial transactions to ensure the authenticity and integrity of financial instructions. Any unauthorized or tampered transaction would lack the correct signature, flagging it for review.

Whatever approach organizations take, layering various authentication factors on top of one another is paramount for preventing deepfake-enabled fraud. The other key to robust protection against deepfake is to implement continuous verification. Rather than verify identity once at sign up, organizations must integrate verification measures during the entire customer experience, even after their account has been set up. Some companies routinely invoke identity verification (for strong security, it is important to understand authentication vs. verification) whenever a dormant account suddenly becomes active for high-value transactions, or when passive analytics indicate elevated fraud risk.

One way to do this is to request a current selfie, then compare it to the biometric data stored from onboarding (where storage is allowed by regulations and permissioned by the customer). In very risky situations, you could also request a new snapshot of the originally submitted government issued physical ID and take a few seconds to verify the authenticity of the document and compare the photo on the ID against the selfie.

The good news is governments, universities, and tech firms are all funding research to create new deepfake detectors. And recently, a large consortium of tech companies have kicked off the Deepfake Detection Challenge (DFDC) to find better ways to identify manipulated content and build better detection tools.

### *Machine learning and AI automate, strengthen anti-fraud efforts:*

When combining manual scrutiny with automated systems to detect and prevent fraud, AI and machine learning-infused solutions will further bolster anti-fraud efforts. Many authentication systems are trained in pattern recognition and anomaly detection. These solutions are better and more efficient at scanning files and authentication attempts for nuances that humans alone will struggle to recognize. Over time, these tools' detection capabilities should improve as they learn from more data. It's worth diving deeper into how AI and ML impact anti-fraud efforts.

Machine learning has become an indispensable tool in detecting deepfakes. Fraudsters have learned to deceive traditional methods of detection, which often rely on human expertise. Compared to traditional detection methods, however, machine learning models can offer:

1. Automated analysis: Models can quickly analyze vast amounts of video and audio data, identifying anomalies at speeds beyond human capabilities.
2. Pattern recognition: Over time, machine learning models can recognize patterns characteristic of deepfake production algorithms, thus identifying manipulated content.
3. Continuous learning: As new types of deepfakes emerge, machine learning models can be retrained and adapted, ensuring they remain effective over time.

### *AI also helps firms stay ahead of evolving deepfake technologies:*

Unfortunately, criminals' abilities grow as technology capabilities evolve. Investing in AI helps financial institutions develop more advanced detection tools, as well as stay abreast of emerging threats. AI-enabled tools can simulate deepfake attacks and test detection systems, shoring up vulnerabilities and training team members on how to better recognize fraudulent actions.

By collaborating with technology companies offering AI-enabled tools, financial services and other firms can broaden their deepfake knowledge base to spread their anti-fraud blanket even farther. Spreading anti-fraud defenses farther serves a second purpose: educating the public. Firms and technology providers that are well-versed in potential risks of deepfakes can provide PSAs and other collateral to help better inform prospective customers about their own risk.

AI can also train datasets specific to financial fraud and identity theft to really stay a step ahead of bad actors. This means feeding AI algorithms datasets tailored to financial fraud and identity theft scenarios, such as:

1. **Real-world data collection:** Financial institutions can use instances of past fraud attempts to train models on actual threats faced by the industry.
2. **Synthetic data generation:** Creating datasets is a resource-intensive task and not always an easy feat. To bolster real-world datasets, algorithms can drum up synthetic examples of potential fraud scenarios, ensuring a comprehensive training environment for models.

3. **Continuous updating:** As fraud methods evolve, it's essential to continually update the training dataset to reflect new tactics and techniques employed by fraudsters. AI can perform this task much more efficiently than humans alone can.

## *Legal responses to deepfake financial crimes require ethical considerations:*

Some jurisdictions have started drafting or amending legislation to address deepfake-related crimes, especially when they lead to financial fraud. Penalties for creating or disseminating malicious deepfakes can include imprisonment and hefty fines. Elsewhere, legal firms collaborate with tech companies for forensic analysis to verify digital content, and financial services organizations have enhanced their identity-verification protocols with processes like Know Your Customer (KYC).

Though these efforts are aimed at thwarting deepfake and other types of fraud, they carry with them privacy and other ethical concerns. As private and public sector organizations move forward with anti-fraud efforts, they'll have to ensure they maintain strict data privacy and security protocols when they collect data, to avoid unauthorized use of that information, data breaches, anonymity infringement or consent issues.

Regardless of how lawmakers and organizations approach anti-deepfake fraud, there is a need for clear regulations about what constitutes informed consent and correct data usage in the age of deepfakes.

## proceed in the age of deepfakes :

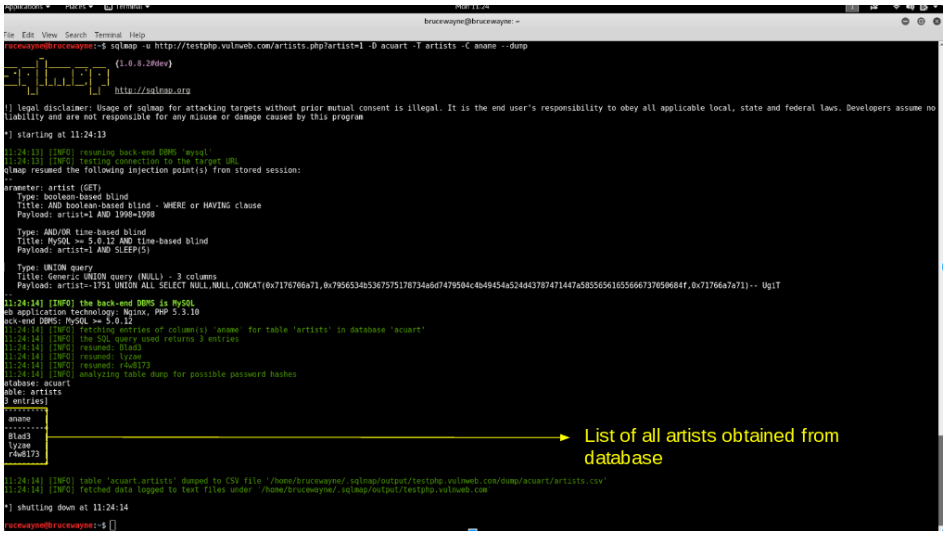
Firms in every industry can take measures to safeguard against deepfake and other types of fraud. Informing employees and customers about risk, implementing ongoing identity verification and constant transaction monitoring are common ways of buttressing security against novel forms of fraud.

Holding awareness sessions, training events with real-world examples and updating employee and customer bases about emerging types of fraud are methods firms can educate employees and individuals linked to their organization about fraud and how to identify it.

Strong authentication methods, such as multi-factor authentication (MFA), biometric verification (whether behavioral, voice, or any other form of biometrics) add layers of security onto every interaction with the firm's apps or services.

Financial services firms must also regularly monitor financial transactions, something they likely do anyway. But monitoring for fraud, such as deepfake fraud, may require additional processes, such as automated alerts, more frequent statement reviews, internal audits and even more regular contact with clients regarding potentially questionable or anomalous transactions.

All of these efforts are simply measures that should augment existing cybersecurity firewalls. Organizations that leverage anti-phishing software and firewall and intrusion detection systems, along with VPNs and regular software updates stand a much better chance should fraudsters come knocking.




- From the above picture, we can see that we have accessed the data from the database. Similarly, in such vulnerable websites, we can literally explore through the databases to extract information

**Prevent SQL Injection :**

SQL injection can be generally prevented by using **Prepared Statements** . When we use a prepared statement, we are basically using a template for the code and analyzing the code and user input separately. It does not mix the user entered query and the code. In the example given at the beginning of this article, the input entered by the user is directly inserted into the code and they are compiled together, and hence we are able to execute malicious code. For prepared statements, we basically send the sql query with a placeholder for the user input and then send the actual user input as a separate command.
Consider the following php code segment.

```
$db = new PDO('connection details');
$stmt = db->prepare("Select name from users where id = :id");
$stmt->execute(array(':id', $data));
```

In this code, the user input is not combined with the prepared statement. They are compiled separately. So even if malicious code is entered as user input, the program will simply treat the malicious part of the code as a string and not a command.

Question 4 :

***Discuss about different types of Cyber crimes. Explain how a person can report to the concerned officials and take protection.***

***Answer:***

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.

Cybercrime can be carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

Types of cybercrime include:

1. Email and internet fraud.
2. Identity fraud (where personal information is stolen and used).
3. Theft of financial or card payment data.
4. Theft and sale of corporate data.
5. Cyberextortion (demanding money to prevent a threatened attack).
6. Ransomware attacks (a type of cyberextortion).
7. Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
8. Cyberespionage (where hackers access government or company data).
9. Interfering with systems in a way that compromises a network.
10. Infringing copyright.
11. Illegal gambling.
12. Selling illegal items online.
13. Soliciting, producing, or possessing child pornography.

Cybercrime involves one or both of the following:

- Criminal activity *targeting* computers using viruses and other types of malware.
- Criminal activity *using* computers to commit other crimes.

**Examples of cybercrime**

Here are some famous examples of different types of cybercrime attack used by cybercriminals:

### 1. Malware attacks

A malware attack is where a computer system or network is infected with a computer virus or other type of malware. A computer compromised by malware could be used by cybercriminals for several purposes. These include stealing confidential data, using the computer to carry out other criminal acts, or causing damage to data.

A famous example of a malware attack was the WannaCry ransomware attack, a global cybercrime committed in May 2017. WannaCry is a type of ransomware, malware used to extort money by holding the victim's data or device to ransom. The ransomware targeted a vulnerability in computers running Microsoft Windows.

When the WannaCry ransomware attack hit, 230,000 computers were affected across 150 countries. Users were locked out of their files and sent a message demanding that they pay a Bitcoin ransom to regain access.

Worldwide, the WannaCry cybercrime is estimated to have caused $4 billion in financial losses. To this day, the attack stands out for its sheer size and impact.

### 2. Phishing

A phishing campaign is when spam emails, or other forms of communication, are sent with the intention of tricking recipients into doing something that undermines their security. Phishing campaign messages may contain infected attachments or links to malicious sites, or they may ask the receiver to respond with confidential information.

A famous example of a phishing scam took place during the World Cup in 2018. According to our report, 2018 Fraud World Cup , the World Cup phishing scam involved emails that were sent to football fans. These spam emails tried to entice fans with fake free trips to Moscow, where the World Cup was being hosted. People who opened and clicked on the links contained in these emails had their personal data stolen.

Another type of phishing campaign is known as spear-phishing. These are targeted phishing campaigns which try to trick specific individuals into jeopardizing the security of the organization they work for.

Unlike mass phishing campaigns, which are very general in style, spear-phishing messages are typically crafted to look like messages from a trusted source. For example, they are made to look like they have come from the CEO or the IT manager. They may not contain any visual clues that they are fake.

### 3. Distributed DoS attacks

Distributed DoS attacks (DDoS) are a type of cybercrime attack that cybercriminals use to bring down a system or network. Sometimes connected IoT (Internet of Things) devices are used to launch DDoS attacks.

A DDoS attack overwhelms a system by using one of the standard communication protocols it uses to spam the system with connection requests. Cybercriminals who are carrying out cyberextortion may use the threat of a DDoS attack to demand money. Alternatively, a DDoS may be used as a distraction tactic while another type of cybercrime takes place.

A famous example of this type of attack is the 2017 DDoS attack on the UK National Lottery website. This brought the lottery's website and mobile app offline, preventing UK citizens from playing. The reason behind the attack remains unknown, however, it is suspected that the attack was an attempt to blackmail the National Lottery.

Cybercriminals that *target* computers may infect them with malware to damage devices or stop them working. They may also use malware to delete or steal data. Or cybercriminals may stop users from using a website or network or prevent a business providing a software service to its customers, which is called a Denial-of-Service (DoS) attack.

Cybercrime that *uses* computers to commit other crimes may involve using computers or networks to spread malware, illegal information or illegal images.

Cybercriminals are often doing both at once. They may target computers with viruses first and then use them to spread malware to other machines or throughout a network. Some jurisdictions recognize a third category of cybercrime which is where a computer is used as an accessory to crime. An example of this is using a computer to store stolen data.

Given its prevalence, you may be wondering how to stop cybercrime? Here are some sensible tips to protect your computer and your personal data from cybercrime:

### 1. Keep software and operating system updated

Keeping your software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.

### 2. Use anti-virus software and keep it updated

Using anti-virus or a comprehensive internet security solution like Kaspersky Premiumis a smart way to protect your system from attacks. Anti-virus software allows you to scan, detect and remove threats before they become a problem. Having this protection in place helps to protect your computer and your data from cybercrime, giving you piece of mind. Keep your antivirus updated to receive the best level of protection.

### 3. Use strong passwords

Be sure to use strong passwords that people will not guess and do not record them anywhere. Or use a reputable password manager to generate strong passwords randomly to make this easier.

### 4. Never open attachments in spam emails

A classic way that computers get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

### 5. Do not click on links in spam emails or untrusted websites

Another way people become victims of cybercrime is by clicking on links in spam emails or other messages, or unfamiliar websites. Avoid doing this to stay safe online.

### 6. Do not give out personal information unless secure

Never give out personal data over the phone or via email unless you are completely sure the line or email is secure. Make certain that you are speaking to the person you think you are.

### 7. Contact companies directly about suspicious requests

If you are asked for personal information or data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them and not a cybercriminal. Ideally, use a different phone because cybercriminals can hold the line open. When you think you've re-dialed, they can pretend to be from the bank or other organization that you think you are speaking to.

### 8. Be mindful of which website URLs you visit

Keep an eye on the URLs you are clicking on. Do they look legitimate? Avoid clicking on links with unfamiliar or URLs that look like spam. If your internet security product includes functionality to secure online transactions, ensure it is enabled before carrying out financial transactions online.

### 9. Keep an eye on your bank statements

Spotting that you have become a victim of cybercrime quickly is important. Keep an eye on your bank statements and query any unfamiliar transactions with the bank. The bank can investigate whether they are fraudulent.

Question 5 :

## *Discuss about various online payment frauds and how can they be prevented*

***Answer:***

Online payment fraud is a serious and growing problem in the digital world. It refers to any fraudulent or unauthorised transaction that occurs online using a payment method such as a credit card, debit card, NetBanking, UPI or wallet. Online payment fraud can occur in various ways, such as phishing, data theft, identity theft or chargeback fraud.

In this article, we will discuss the different types of online payment fraud, their impact on businesses and customers, and the strategies to prevent and mitigate them. But before that, let's dive deep into what payment fraud is.

Table of Contents

## Payment Fraud:

Payment fraud is a type of financial fraud or online payment scam where fraudsters use unauthorised methods to steal money or sensitive financial information. It can happen in various ways, but it often involves scammers stealing credit card / bank details, making fake cheques, or using stolen IDs to make unauthorized purchases.

The following features characterise online payment fraud:

- It is often carried out by organized criminal groups or networks that use sophisticated tools and techniques to steal and use payment information.
- It exploits the vulnerabilities and loopholes in online payment systems and processes, such as weak security measures.
- It targets businesses and customers across various industries and segments such as e-commerce, travel, gaming, education, healthcare, etc.

## 6 Different Types Of Payment Frauds

The most common types of online payment fraud occur via phishing or spoofing, data theft, identity theft and chargeback. We have explained these in detail below.

### 1. Online Phishing or Spoofing

Online phishing involves accessing your personal information through fraudulent emails or websites claiming to be legitimate. This information can include usernames, passwords, credit card numbers, or bank account numbers.

The most widely used method for online phishing is to redirect you from an email or SMS to an 'official' website, where you are asked to update your personal information. Thus, you are tricked into revealing personal information that you would ideally not reveal to anyone. You can also be redirected to make a payment on a website that looks legitimate but is created to capture your card details so they can be used later.

According to reports, India is the third-most targeted country for online phishing attacks, after the US and Russia.

### 2. Data Theft

Data theft is the illegal copying or accessing of digital information, such as personal, financial, or confidential data. Data thieves can use various methods, such as phishing, hacking, or social engineering, to obtain data from individuals or organisations. The stolen data can be used for identity theft, fraud, ransomware, or other malicious purposes. Data theft can cause serious harm to the victims, such as financial loss, reputational damage, legal issues, or emotional distress.

To prevent data theft, it is essential to use strong passwords, encryption, antivirus software, and secure networks. To protect customer data, online platforms use advanced security techniques such as tokenisation and encryption. Razorpay is a leader in data security and has achieved the ISO-27001 certification, which demonstrates adherence to the highest data protection standards.

### 3. Identity Theft

Identity theft is a malicious act where your personal information such as driver's license, PAN or Aadhaar details are illicitly obtained and exploited for fraudulent financial activities. This includes unauthorised transactions and the establishment of counterfeit accounts, thereby inflicting financial and emotional distress. Recovering from identity theft is a burdensome and time-consuming process, often involving legal and financial complexities.

This crime results in financial loss and can even damage your reputation. Identity theft victims are forced to spend significant time and resources rectifying the aftermath, often requiring legal and financial assistance. To combat this issue, it is essential to prioritise personal data security through enhanced awareness and robust security measures.

### 4. Chargeback Fraud or Friendly Fraud

Let's say a customer makes an online purchase. Later, they claim that the purchase was made fraudulently and ask for friendly fraud chargebacks – even though they made it themselves! In simple terms, a friendly fraud chargeback is an order from a bank to a business, asking it to return the amount paid for a possible fraudulent purchase. The business processes the transaction since it seems legitimate, only to be issued with a chargeback later on.

Chargeback online payment frauds cause GMV losses and are a hassle for businesses. Razorpay's Chargeback Guide can help you understand why friendly fraud chargebacks happen and what steps can be taken against these charges.

### 5. Card-not-present (CNP) fraud

Perpetrators exploit stolen cardholder data to make remote online purchases. This is often acquired through phishing, malware, data breaches or social engineering. In this scenario, merchants face chargeback risks.

### 6. Account takeover (ATO) fraud

Fraudsters infiltrate online accounts by stealing credentials or exploiting security weaknesses. They can then enable unauthorised transactions, account modifications and fund transfers, affecting your financial security.

**Prevent Payment Fraud:**

To protect against **online payment frauds**, businesses must implement following effective strategies:

### Transaction Monitoring

1. Continuously employ advanced real-time monitoring techniques like condition monitoring, digital experience monitoring and computational monitoring to scrutinise all transactions, identifying and flagging any irregularities or suspicious patterns.
2. Utilise cutting-edge algorithms like the random forest, support vector machine and logistic regression to analyse transaction data swiftly and accurately. This ensures a proactive approach to fraud detection and risk mitigation.
3. Maintain a vigilant watch over financial activities, leveraging anomaly detection methods like isolation forest and K-means to identify deviations from established norms swiftly. This proactive surveillance allows for timely investigation and intervention, enhancing the security and integrity of the system. It ultimately fosters a safe and trusted transaction environment for all stakeholders involved.

### Restrict Access to Sensitive Data

1. Stringently restrict access to sensitive customer data, employing robust security protocols and access controls.
2. Implement encryption and multi-factor authentication to fortify storage mechanisms. This safeguards customer information from unauthorised access and potential breaches.
3. Adhere to best industry practices like using authentication, authorisation and encryption, along with compliance standards like the Personal Data Protection Act (PDPA) in India to uphold data privacy and security standards. This mitigates risks associated with data leaks or cyber threats.
4. Utilise secure storage solutions and regularly update security measures to adapt to evolving cyber threats. This instils confidence in customers regarding the protection of their private information and reinforces trust in the organisation's commitment to data security and privacy.

### Encryption

1. Encrypt data using industry-leading encryption protocols, including strong encryption algorithms like Transport Layer Security (TLS) or Secure Sockets Layer (SSL), to establish secure communication channels. This ensures the utmost data security during transmission, rendering it unintelligible to unauthorised parties and mitigating the risk of eavesdropping or tampering.
2. Continuously update encryption standards and stay informed about emerging threats to adapt and strengthen encryption methods. This bolsters the overall security posture and guarantees the confidentiality and integrity of data exchanged over networks.

### Authentication Procedures

1. Integrate multi-factor authentication (MFA) as a robust identity verification measure to ensure user security.
2. Mandate users to authenticate their identity using at least two independent factors, such as a password, biometric scan, smart card, or one-time verification code. This dual or multi-step verification process significantly enhances security by adding layers of protection, making it exponentially more difficult for unauthorised individuals to gain access.
3. Regularly update and strengthen MFA mechanisms in response to evolving cyber threats, maintaining a proactive stance in safeguarding user identities and preventing unauthorised access to sensitive systems and information.

## Stay informed about Fraud Trends

1. Stay vigilant by learning about the ever-evolving landscape of fraud and cyber threats.
2. Continuously monitor the latest fraud trends, techniques and tactics employed by malicious actions within the digital realm. This proactive approach allows for the swift adjustment of security measures to stay ahead of potential threats.
3. Collaborate with industry experts, engage in information sharing within cyber security communities and participate in threat intelligence networks to gather insights into emerging fraud patterns. Utilise this knowledge to adapt security protocols, update detection mechanisms, and reinforce protective measures. This will effectively help thwart new and sophisticated fraudulent activities and preserve the trust and integrity of systems.

## The Effect of Payment Fraud on Businesses

As per the current terms and conditions, a credit card issuer (i.e., the bank) does not consider the cardholder liable for any fraudulent activity for both card-present and card-not-present online payment frauds.

Therefore, online payment frauds involving credit cards have a significant effect on the business community and a merchant's bottom line. Every time a customer issues a chargeback, it leads to a loss of both inventory and GMV. This is especially true for retail establishments, where the profit margins are usually small.

The 'subscription' industry continues to have the highest rate of online **payment fraud** for **two main reasons:**

1. Subscriptions are essentially a card-dependent service, wherein the USP of the service is that one does not have to make manual payments. It is easy to claim that one's card was used without knowledge in such a scenario.
2. Hackers use subscription services to 'test' cards. Online subscription services usually provide a one-month free trial, but one needs a credit card to initiate the trial period. Since the value is negligible, such payments usually go unnoticed by the card owner. If the card details are incorrect, the subscription business shares a detailed authorisation error, thus making it easy for the hacker to modify their strategy and continue using the card.

## Affected by Online Payment Fraud:

Payment fraud primarily affects businesses and merchants who bear the financial burden of chargebacks and inventory losses. **Payment fraud** has wide-ranging consequences for businesses, leading to financial losses, damaged reputation, and eroding customer trust. To mitigate these challenges, businesses must invest in robust fraud prevention and detection measures to protect their bottom line and reputation in an environment where online payment fraud remains a significant threat.

Online payment fraud also impacts customers and payment service providers. Customers face wide ranging impacts including financial losses and potential identity theft.

Payment service providers can lose money and credibility, facing compliance challenges under regulations like PSD2. PSD2 introduced Strong Customer Authentication (SCA) and Liability Shift, impacting who covers losses in fraudulent transactions. This has implications for both sellers and payment service providers. Payment fraud's consequences ripple throughout the online payment ecosystem.

### Systems for detecting 'customer fraud'

Our platform employs robust mechanisms to detect suspicious customer behaviour and unauthorised transactions. This includes –

1. **Checking for hotlisted cards:** Every time a card is used for payment, our gateway connects with the card provider to check if the card has been hotlisted. (Hotlisting means that the card has been blocked temporarily / permanently). This is done in real time so that a verified transaction is still completed within seconds, while a suspicious one gets flagged.
2. **Pattern-based transaction monitoring:** We use geographical and pattern-based transaction monitoring to identify suspicious transactions. This helps in preempting and preventing chargeback and other types of fraud. We have a hit ratio of being able to identify 85% of fraudulent cases in advance.

## Online Fraud Prevention: The Present and the Future

Online payment fraud is a growing concern as more transactions are being conducted online. While it is impossible to eliminate fraud completely, there are measures in place to minimise the risk. Here are some current measures being used –

### 3D Secure (3DS) protocol:

VISA developed this protocol to keep its customers safe. It has been adopted by other card companies like American Express, MasterCard and JCB International. It is a more robust, secure and mobile-friendly specification that allows for frictionless transactions. It also mitigates fraud and shifts the liability of chargebacks from businesses to the customer's bank.

### Two-factor authentication (2FA):

This is mandatory for all cardholders and card-issuing banks in India. The Reserve Bank of India (RBI) has mandated online alerts for all card transactions, even those where the cardholder physically swipes their card at a PoS system.

### De-activation request:

You have the option to issue a de-activation request immediately and hotlist your card for all transactions considered suspicious.

### FCORD initiative:

The Indian government has appointed a nodal agency for dealing with phone fraud, called the FCORD initiative. Razorpay is in touch with the Ministry of Home Affairs (MHA), which has designated the FCORD as the nodal agency for reporting and preventing cybercrime frauds in India.

While it will take time to achieve a zero-fraud system, companies are constantly building new processes to minimise online payment fraud risk. It is important to remain vigilant and adopt these measures.

While 3D Secure and 2FA provide vital security measures, innovative techniques like machine learning and link analysis enhance fraud detection. Staying informed about emerging fraud trends and using test rules for scenario simulation further strengthen defense against this persistent threat. Let us understand these innovative solutions in detail –

### Machine learning:

This is a branch of artificial intelligence that enables systems to learn from data and improve their performance. This enables faster and more accurate fraud detection and prevention.

### Link analysis:

This technique uses network history to identify connections and relationships between entities, such as customers, merchants, transactions, devices, etc. This can help uncover hidden patterns and anomalies in data and reveal complex fraud schemes.

### Test rules:

You can create and apply these rules to transactions to simulate different scenarios and outcomes. This can help you evaluate the effectiveness of your fraud prevention measures and optimise them for better results.

### Stay updated about new fraud trends:

As online payments become more popular and diverse, new types of fraud may arise, such as mobile payment fraud, social media payment fraud, cryptocurrency payment fraud, etc. You need to stay aware of these trends and adapt your strategies accordingly.

## Conclusion

Online payment fraud is a pervasive and ever-evolving threat in the digital world. Businesses and individuals must remain vigilant to protect themselves from various types of payment fraud. Razorpay's commitment to fraud prevention, along with the continuous advancement of technology, offers hope for a safer online payment environment in the future.