TASK – 9

DAY – 26

DATE – 22-09-2022

KEY FOBS:-

Many new cars now have keyless entry systems, or can have them added as an upgrade. This allows the driver to open and start the car without using a button or turning a key so long as the fob is nearby.

Thieves are exploiting this, using sophisticated technology to hack into your car's computer, meaning they don't even need a key-fob to start the vehicle and can drive it away in a matter of minutes.

In fact, 96% of motorists are at risk of having their car stolen by criminals using the latest theft technique, according to figures from security company Tracker.

The most at-risk are cars that use keyless fobs, as well as 'connected cars'. In other words those that use internet to access maps, travel info and music – basically anything with an internet-enabled infotainment system.

How does a relay attack work?

A relay attack usually involves two people working together. One stands by the targeted vehicle, while the other stands near the house with a device that can pick up a signal from the key fob. What's more, some devices can pick up a signal from over 100 metres away.

The device then relays the key fob's signal directly to the car, allowing the thieves to get in and drive away immediately. According to the Daily Mail, these hacking devices can be bought for as little as £100 by thieves online.

Testing out devices available from Amazon and eBay, the Mail managed to break in to and 'hack' a Ford Fiesta in less than two minutes. In another test, Germany's ADAC discovered that some brands are more at risk than others, with BMW and Peugeot systems being particularly easy to hack.

But ADAC also managed to unlock a Toyota Prius, Ford Focus and Volkswagen Golf, showing that no one particular manufacturer is immune to this new kind of crime. The video above shows examples of thieves employing the 'relay' technique.

Andy Barrs, head of police liaison at security firm Tracker, said: "As relay attacks become even more prevalent, owners need to protect themselves, particularly since criminal gangs are routinely using relay devices to exploit weaknesses in keyless security systems across a broad range of manufacturers.

"These tools are readily available on the internet for as little as £80 and thefts typically occur in residential areas, where cars are parked relatively close to the house, especially at night.

"It's worth remembering that technology is just one part of vehicle security and more vigilance needs to be taken across the board; this includes car owners, manufacturers, dealers, insurers and the police."

What's being done to stop relay attacks?

Police have made significant in-roads into the criminal gangs and arrests are constantly being made across the UK. Earlier this year, five people in Liverpool were convicted of offences including the theft of keyless cars totalling around £2.6 million.

As for cars themselves, the government released new guidelines for car makers that will soon have to provide more security as cars get ever-more advanced. But it's not just aimed at reducing theft; it's part of the Autonomous and Electric Vehicles Bill, which will create a framework to insure autonomous vehicles.

The stricter guidelines also aim to reduce the risk of hackers accessing personal data or, as we get closer and closer to self-driving cars, take over the vehicle and cause accidents.

With autonomous cars purportedly only a few years away, the government wants to make cars as safe and secure as possible in the face of cyber criminals.

Transport minister Lord Callanan said: "We need to make sure that the designs of the vehicles in the first place are completely cyber secure so that people can't break into them, they can't steal them and more importantly they can't hack them to potentially cause accidents."

He added: "The advice would be treat them as you would your computer; be careful who you give access to, don't plug in devices such as USB sticks that you don't know the origin of."

Ford also recently announced the Fiesta and Focus will be the first models to feature a sleep mode to protect against being hacked by relay car thieves.

Top tips on how to avoid vehicle theft and relay attacks

- **Block electronic key fob signals:** A Faraday-style wallet, as pictured above is the best way to block out any electronic signals, but even your fridge can shield electronic car keys from relay attacks.
- **Check it's locked:** Always double check that your car is physically secure and alarmed when using keyless locking systems.
- **Keep keys out of sight:** Leaving keys in the hallway or on the kitchen worktop means thieves can easily employ the relay technique if it is within proximity or failing that break in and swipe them.
- **Add layers of security:** Physical barriers can be effective in deterring thieves. Consider adding a crook lock or wheel clamp to your car.
- **Install a 'ghost immobiliser':** For another layer of protection, add a secondary barrier to your car's factory fitted immobiliser by having a unique access code to start your car.

- **Invest in a tracking device:** A tracking device won’t stop your vehicle being stolen, but it significantly increases chances of police recovering and returning it.

“It’s clear from our survey that many people are unintentionally leaving themselves vulnerable to these kinds of attack, by putting their keys in easy reach of relay devices”, concluded Barrs.

Further research by Tracker revealed that 50% of those surveyed leave their keys either in the hallway of their house or a key pot elsewhere. Only 4% use a metal container to ensure their car is protected from a relay attack.

What are the most commonly targeted cars?

Recent stats from the car security company Tracker has revealed that 92% of the cars it recovered last year were taken without using the keys. This is an increase from 2018’s figure which stood at 88% and a worrying increase of 26% compared with four years ago. The figure in 2016 stood at 66%.

Tracker’s stats show that it is mainly the more premium manufacturers that are being targeted, with Land Rover models taking six of the top 10 spots. Here are its most stolen and recovered cars during 2020 compared to 2019.

Year	2020	2019
1.	Range Rover Sport	Range Rover Sport
2.	Range Rover Vogue	BMW X5
3.	Range Rover Autobiography	Mercedes-Benz C-Class
4.	BMW X5	Range Rover Vogue
5.	Land Rover Discovery / BMW 3 Series	Land Rover Discovery
6.	Mercedes-Benz C-Class	BMW X6
7.	Range Rover Evoque	Range Rover Evoque
8.	Mercedes C-Class AMG	BMW 3 Series
9.	BMW M3 / Mercedes S-Class	Range Rover Autobiography
10.	Land Rover Defender / Mercedes E-Class / BMW 6 Series	Mercedes-Benz E-Class

The most expensive vehicle recovered by Tracker in 2019 was a Range Rover SV Autobiography, valued at £150,000. A VW Polo valued at £575 was the least expensive car recovered. The total value of recovered vehicles was £13m.

OWASP Top 10 Vulnerabilities 2021

1. Broken Access Control

A flawed access **control** means no verification of proper access checks to the requested object. Unauthenticated privileged functionality of crucial data and information.

A typical example of access control vulnerabilities could be seen when one forces browsers to target URLs.

E.g. As we know, to gain access to an application’s admin dashboard one needs to have admin access right.

http://appwebsite.com/app/getadmininfo

http://appwebsite.com/app/admin_getadmininfo

In the second URL, the parameter is modified to check access. If unverified, the URL could pave the way to unauthorized access, thanks to ‘broken’ control of access to sensitive data.

2. Cryptographic Failures

When one sneaks into sensitive data information in an application, be ready for serious repercussions. At least UBER drivers are aware of this.

Typical example of sensitive information exposure could be any of the following:

- Session tokens,
- login ID and passwords,
- online transactions, and
- personal details (SSN, Health records) etc.

Any unprivileged access to the victim’s accounts is a serious concern. The practice of using Simple hashes to store sensitive data is to be blamed for.

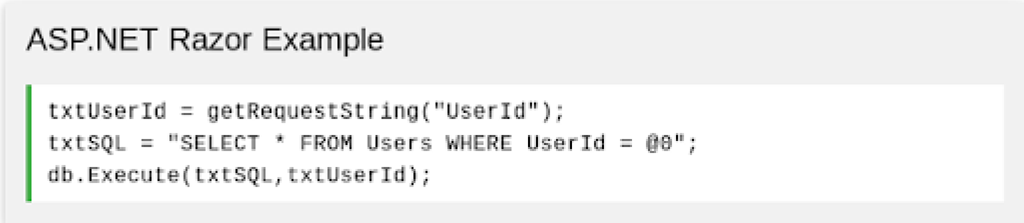
Coupled with absence of encryption of all sensitive data at rest and cashing, the threat is one of the key OWASP top 10 vulnerabilities.

3. Injection

As injection is an attack on a web application’s database using Structured Query Language (SQL) to gain information or execute actions that normally would require an authenticated user account.

A hacker already has your database, and you only just realized it. This is a pretty alarming situation.

A typical example of SQL injection is when “101 OR 1=1” is passed instead of just “101”.



ASP.NET Razor Example

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = @0";
db.Execute(txtSQL,txtUserId);
```

4. Insecure Design

This newest OWASP Top 10 revision talks about risks related to design and architectural flaws, with recommendations for implementing threat modelling, secure design patterns, and reference architectures – from the very beginning of the design process.

5. Security Misconfiguration

OWASP top 10 security misconfiguration vulnerability is an open invite for an attack on an application with poorly configured permissions on servers.

Default configurations, open ports, privileges, incorrect HTTP headers etc. are some common examples that make an application vulnerable to breach.

NB: XML External Entities (XXE) is not part of Security Misconfiguration now.

OWASP XML External Entities attack is occured when an application parses VML*input. This input could be understood as an external entity (let's suppose an external drive) that tries to get into an application tapping security flaws in XML parser.

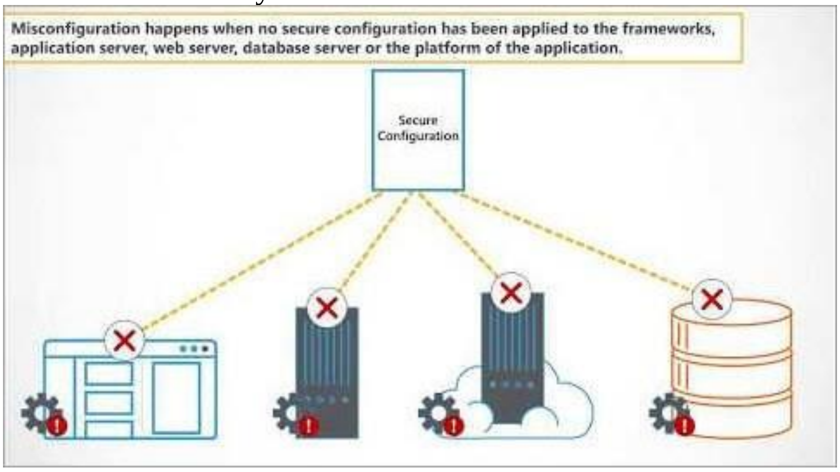
An example of XML external entities attack is when attacker tries to extract data from the server

```
<?xml version=”1.0″ encoding=”ISO-8859-1″?> <!DOCTYPE foo [
 <!ELEMENT foo ANY >
 <!ENTITY xxe SYSTEM “file:///etc/passwd” >]> <foo>&xxe;</foo>
```

Also, the server private network is modified by changing the above ENTITY line to

```
<!ENTITY xxe SYSTEM “https://192.168.1.1/private” >]>
```

Source:HdivSecurity



Misconfiguration happens when no secure configuration has been applied to the frameworks, application server, web server, database server or the platform of the application.

NB: XSS (cross-site scripting) attack now comes under ‘injections’ category.

Affecting many applications, cross-site scripting vulnerability is exploited in the form of malicious Javascript scripts that basically acts to intercept communication between server and a browser.

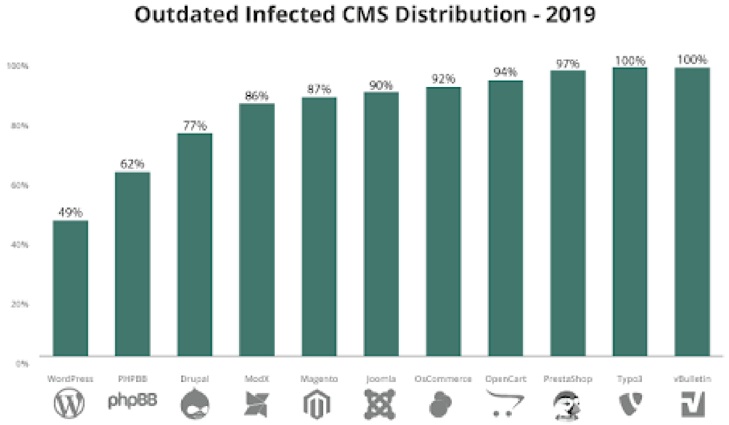
A common Example of XSS Vulnerabilities is when one tries to create a new post on his WordPress admin dashboard.

Exploiting XSS, a hacker could inject and tamper with the admin URL and force the browser to create a new admin. End result? WordPress posts can be edited/changed or all things bad you can imagine on the dashboard.

6. Vulnerable and Outdated Components

Most web applications are developed using special frameworks that are provided by third parties. The ‘Coding’ world is filled with various open-source components and frameworks to build applications, which means there is a huge number of eyes looking at their source codes for any vulnerabilities.

Unknown application codes may cause unlucky consequences and unwanted situations in the form of accent control breach, SQL injections etc.



7. Identification and Authentication Failures

As the name suggests, as **identification and authentication failure** vulnerability is exploited by hackers to get the best of improper authentication. It leads to security risks when an attacker gets hold of user information, password recovery, ID sessions and other login credentials.

Brute force is considered to be the key driver of such broken authentication attack attempts in the form of credential stuffing.

A typical example is when an attempt is made in an online shopping URL.

E.g. An online shopping platform has an application that supports URL rewriting, putting session IDs in the URL.

http://shoppingsitexample.com/products/item;jsessionid=2P0OC4KBIWHYDYIBOME1JV?dest=Nike

8. Software and Data Integrity Failures

For software, data integrity failures are becoming increasingly relevant as sensitive information is increasingly stored in databases, where it is at risk of tampering security.

The section analyzes failures related to software updates (insufficient integrity verification), secure CI/CD pipelines, and the need for sufficient data integrity.

OWASP considers insecure deserialization (conversion of byte strings to objects) vulnerability in data integrity failure now because this weakness breaks logic of an application with the help of invalid data.

An insecure deserialization attack example is an RCE attack (Remote Code Execution)

NB: **– Insecure Deserialization** is now a part of Software and data integrity failure category.

9. Security Logging and Monitoring Failures

A lack of logging in the face of suspicious actions and events can result in growing gaps of time that go unmonitored and allow security breaches to go undetected for longer than they might with better logging in place.

Hacking into a website can be bad, but it’s becoming even worse when web application owners are not monitoring for the identification of suspicious code behavior.

This is where a monitoring system is handy. It will alert you in the event that something happens with your site and instruction on how to address it in a timely manner.

Without having an efficient logging and monitoring process in place, one could be left dealing with the repercussions of a cyber attack without fully understanding what has happened to their system.

Example of Insufficient Logging and Monitoring:

- An attacker or program can scan for users with easily crackable passwords.
- Once this is complete, the attacker only has to try only one of the passwords to login to all accounts with simple passwords.
- The more different passwords are tried, the better it is for the user, because after some time only one false login is left. If an attacker wants to get into more accounts he has to invest more work into that.

10. Server Side Request Forgery (SSRF)

When server-side requests are being made without first validating the user-supplied URL, this is known as Server Side Request Forgery or SSRF attack.

Examples

A web application can be vulnerable to an SSRF attack if it does not validate the remote resource URL supplied by the user.

– A potential remote resource URL could be http://target.example.com/inc/sharefile.asp

– If the web application does not validate the URL, then the user might be able to exploit this to access other internal resources or even internal networks.

10 Types of Social Engineering Attacks

To prevent a social engineering attack, you need to understand what they look like and how you might be targeted. These are the 10 most common types of social engineering attacks to be aware of.

1. Phishing

Phishing is the most common type of social engineering attack, typically using spoofed email addresses and links to trick people into providing login credentials, credit card numbers, or other personal information. Variations of phishing attacks include:

- **Angler phishing –** using spoofed customer service accounts on social media
- **Spear phishing –** phishing attacks that target specific organizations or individuals

2. Whaling

Whaling is another common variation of phishing that specifically targets top-level business executives and the heads of government agencies. Whaling attacks usually spoof the email addresses of other high-ranking people in the company or agency and contain urgent messaging about a fake emergency or time-sensitive opportunity. Successful whaling attacks can expose a lot of confidential, sensitive information due to the high-level network access these executives and directors have.

3. Diversion Theft

In an old-school diversion theft scheme, the thief persuades a delivery driver or courier to travel to the wrong location or hand off a parcel to someone other than the intended recipient. In an online diversion theft scheme, a thief steals sensitive data by tricking the victim into sending it to or sharing it with the wrong person. The thief often accomplishes this by spoofing the email address of someone in the victim’s company—an auditing firm or a financial institution, for example.

4. Baiting

Baiting is a type of social engineering attack that lures victims into providing sensitive information or credentials by promising something of value for free. For example, the victim receives an email that promises a free gift card if they click a link to take a survey. The link might redirect them to a spoofed Office 365 login page that captures their email address and password and sends them to a malicious actor.

5. Honey Trap

In a honey trap attack, the perpetrator pretends to be romantically or sexually interested in the victim and lures them into an online relationship. The attacker then persuades the victim to reveal confidential information or pay them large sums of money.

6. Pretexting

Pretexting is a fairly sophisticated type of social engineering attack in which a scammer creates a pretext or fabricated scenario—pretending to be an IRS auditor, for example—to con someone into providing sensitive personal or financial information, such as their social security number. In this type of attack, someone can also physically acquire access to your data by pretending to be a vendor, delivery driver, or contractor to gain your staff's trust.

7. SMS Phishing

SMS phishing is becoming a much larger problem as more organizations embrace texting as a primary method of communication. In one method of SMS phishing, scammers send text messages that spoof multi-factor authentication requests and redirect victims to malicious web pages that collect their credentials or install malware on their phones.

8. Scareware

Scareware is a form of social engineering in which a scammer inserts malicious code into a webpage that causes pop-up windows with flashing colors and alarming sounds to appear. These pop-up windows will falsely alert you to a virus that's been installed on your system. You'll be told to purchase and download their security software, and the scammers will either steal your credit card information, install real viruses on your system, or (most likely) both.

9. Tailgating/Piggybacking

Tailgating, also known as piggybacking, is a social engineering tactic in which an attacker physically follows someone into a secure or restricted area. Sometimes the scammer will pretend they forgot their access card, or they'll engage someone in an animated conversation on their way into the area so their lack of authorized identification goes unnoticed.

10. Watering Hole

In a watering hole attack, a hacker infects a legitimate website that their targets are known to visit. Then, when their chosen victims log into the site, the hacker either captures their credentials and uses them to breach the target's network, or they install a backdoor trojan to access the network.

How to Prevent a Social Engineering Attack

Social engineering represents a critical threat to your organization's security, so you must prioritize the prevention and mitigation of these attacks as a core part of your cybersecurity strategy. Preventing a social engineering attack requires a holistic approach to security that combines technological security tools with comprehensive training for staff and executives.

Your first line of defense against a social engineering attack is training. Everyone in your organization should know how to spot the most common social engineering tactics, and they should understand the psychological triggers that scammers use to take advantage of people. A comprehensive social engineering and security awareness training course should teach staff to:

- **Determine** whether an email has been spoofed by hovering over the sender's name to make sure it matches the email address and checking the email address for spelling errors and other common giveaways.
- **Be suspicious** of any unsolicited communication, especially from someone they don't know.
- **Avoid** downloading suspicious email attachments.
- **Hover** over links in emails to make sure the website URL is valid.
- **Verify** someone's identity through an alternate contact method (e.g. in person or by calling them directly) before providing any sensitive information.

You also need to follow up your security awareness training with periodic tests to ensure your staff hasn’t become complacent. Many training programs allow for the administration of simulated phishing tests in which fake phishing emails are sent to staff members to gauge how many people fall for the social engineering tactics. Those staff members can then be retrained as needed.

Creating a positive security culture within your organization is critical for containing a social engineering attack that’s already happened. Your staff needs to feel comfortable self-reporting if they believe they’ve fallen victim to a social engineering attack, which they won’t do if they’re concerned about facing punishment or public humiliation. If these issues are reported as soon as they occur, the threat can be mitigated quickly before too much damage has occurred.

Finally, you need to implement technological security tools to prevent attacks on your organization and minimize the damage from any successful breaches. These tools should include firewalls, email spam filters, antivirus and anti-malware software, network monitoring tools, and patch management.