NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

---

1. Kevin Mitnick:

- Kevin Mitnick is a former computer hacker who turned his life around to become a cybersecurity consultant and author.
- He gained notoriety in the 1990s for his high-profile computer intrusions into several major corporations.
- After serving time in prison, Mitnick founded Mitnick Security Consulting, which provides cybersecurity services to businesses.
- He is also the author of books like "The Art of Deception" and "Ghost in the Wires," which delve into social engineering and hacking exploits.

2. Anonymous:

- Anonymous is a loosely organized international collective of hackers and activists.
- They are known for various cyberattacks and protests against governments, corporations, and organizations.
- Anonymous often uses the Guy Fawkes mask as a symbol and has participated in several high-profile operations, including attacks on government websites and social justice campaigns.

3. Adrian Lamo:

- Adrian Lamo was a well-known computer hacker and security analyst.
- He gained fame for turning in Chelsea Manning (formerly Bradley Manning), a U.S. Army intelligence analyst who leaked classified information to WikiLeaks.
- Lamo passed away in 2018, but his actions regarding the Manning case remain a significant part of his legacy.

4. Albert Gonzales:

- Albert Gonzales was a notorious cybercriminal known for leading a group that carried out significant data breaches.
- He was responsible for stealing millions of credit card numbers from various companies, including TJX Companies and Heartland Payment Systems.
- Gonzales was eventually arrested and sentenced to prison.

5. Mathew Bevan and Richard Pryce:

- Mathew Bevan and Richard Pryce are two British hackers who gained attention in the 1990s.
- They were accused of hacking into U.S. military systems, including NASA and the Pentagon.
- Their activities raised concerns about the vulnerability of military and government computer networks.

NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

---

6. Jeanson James Ancheta:

- Jeanson James Ancheta, also known as "Resilient," was a hacker who created a botnet known as "rxbot" or "rbot."
- He used this botnet to carry out various cyberattacks and distribute malware.
- Ancheta was arrested and sentenced to prison for his cybercrimes.

7. Michael Calce (Mafiaboy):

- Michael Calce, also known as "Mafiaboy," is a Canadian hacker known for launching a series of high-profile distributed denial-of-service (DDoS) attacks in 2000.
- His attacks temporarily shut down major websites, including Yahoo!, eBay, and Amazon.
- Calce was arrested and later became a cybersecurity consultant.

8. Kevin Poulsen:

- Kevin Poulsen, also known as "Dark Dante," is a former hacker who was involved in various cybercrimes.
- He gained notoriety for hacking into phone systems and winning a Porsche in a radio contest.
- Poulsen was arrested, served a prison sentence, and later became a journalist specializing in cybersecurity.

9. Jonathan James (c0mrade):

- Jonathan James was a hacker who gained fame for being the first juvenile to be imprisoned for cybercrimes in the United States.
- He was involved in various cyberattacks, including intrusions into NASA and the theft of software from a defense contractor.
- Tragically, James took his own life in 2008.

10. ASTRA (Anti-Sec Tech Rebellion Army):

- ASTRA was a hacking group associated with the hacktivist movement.
- They claimed responsibility for various cyberattacks and data breaches in protest against perceived injustices.
- The group's activities often aligned with the broader Anonymous collective and its goals.

OWASP Vulnerabilities

NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

The Open Web Application Security Project (OWASP) is a nonprofit organization focused on improving the security of software. They provide valuable resources and guidance on web application security vulnerabilities. Here are some common OWASP vulnerabilities:

1. Injection: This includes SQL injection, where an attacker can manipulate an SQL query to gain unauthorized access to a database, and Command injection, where an attacker can execute arbitrary commands on a system.

2. Broken Authentication: This vulnerability occurs when authentication mechanisms are not properly implemented, leading to unauthorized access to user accounts.

3. Sensitive Data Exposure: Inadequate protection of sensitive data, such as passwords or credit card numbers, can lead to data breaches.

4. XML External Entity (XXE) Injection: Attackers can exploit this vulnerability to disclose internal files, execute remote code, or perform other malicious actions.

5. Broken Access Control: When access controls are not properly enforced, users may be able to access unauthorized resources or perform unauthorized actions.

6. Security Misconfiguration: This includes leaving default credentials, misconfigured security headers, or unnecessary services exposed, which can be exploited by attackers.

7. Cross-Site Scripting (XSS): Attackers inject malicious scripts into web pages viewed by other users. This can lead to the theft of session cookies or other sensitive information.

8. Insecure Deserialization: Improper deserialization of untrusted data can lead to remote code execution or other security issues.

9. Using Components with Known Vulnerabilities: If you use outdated or vulnerable components (e.g., libraries or plugins), attackers can exploit known vulnerabilities.

10. Insufficient Logging and Monitoring: Without proper logging and monitoring, it's challenging to detect and respond to security incidents in a timely manner.

NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

OWASP provides extensive documentation, tools, and resources to help developers and security professionals understand and mitigate these vulnerabilities. It's crucial to follow best practices in application development and security to protect against these common threats.