Security Testing

INFO6255 Software Quality Control & Management

Medi Servattalab

M.Servattalab@northeastern.edu

What is Security Testing?

定义

- **Security Testing** is defined as a type of Software Testing that ensures software systems and applications are free from any
  - Vulnerabilities
  - Threats
  - Risks

  that may **cause a big loss.**

目的/意义

- **Security testing** of any system is about finding all possible **loopholes and weaknesses** of the system which might result into
  - Loss of information
  - Loss of revenue

Security testing – Guru99.com

Security Testing Goals

To **identify the threats** in the system and measure its potential vulnerabilities, so the system does not **stop functioning** or **is exploited**

It also helps in **detecting** all possible security risks in the system and help developers in **fixing these** problems through coding

It’s a nasty world out there!!!

- **Security testing** is the most important testing for an application and **checks whether confidential data stays confidential**.

- In this type of testing, tester plays a role of the **attacker** and plays around the system to find **security-related bugs**.

- **Security Testing** is very important in Software Engineering to **protect data** by all means.

Security Testing Types

- Vulnerability Scanning
- Security Scanning
- Penetration testing
- Risk Assessment
- Security Auditing
- Posture Assessment
- Ethical hacking

Security Testing Definitions

1. **Vulnerability Scanning** 搜索已知签名

This is done through automated software to scan a system against known vulnerability signatures.

2. **Security Scanning** 网络和系统，提供solutions

It involves identifying network and system weaknesses, and later provides solutions for reducing these risks. This scanning can be performed for both Manual and Automated scanning.

3. **Penetration testing** 模拟攻击

This kind of testing simulates an attack from a malicious hacker. This testing involves analysis of a particular system to check for potential vulnerabilities to an external hacking attempt.

Security Testing Definitions...

4. Risk Assessment

This testing involves analysis of security risks observed in the organization. Risks are classified as Low, Medium and High.

5. Security Auditing 代码逐行审查

This is an internal inspection of Applications and Operating systems for security flaws. Audit can also be done via line by line inspection of code.

Security Testing Definitions...

6. Ethical hacking 白客

It's hacking an Organization Software systems. Unlike malicious hackers, who steal for their own gains, the intent is to expose security flaws in the system.

7. Posture Assessment

This combines Security scanning, Ethical Hacking and Risk Assessments to show an overall security posture of an organization.

sdlc不同阶段的安全测试活动

When to do Security Testing

SDLC Phases	Security Processes
Requirements	Security analysis for requirements and check abuse/misuse cases
Design	Security risks analysis for designing. Development of Test Plan including security tests
Coding and Unit Testing • Involve Security Testing in the SDLC in the earlier phases	Static and Dynamic Testing and Security White Box Testing
Integration Testing	Black Box Testing
System Testing	Black Box Testing and Vulnerability scanning
Guru99 Implementation	Penetration Testing, Vulnerability Scanning

Security Testing Roles

- **Hackers** - Access computer system or network without authorization.
- **Crackers** - Break into the systems to steal or destroy data.
- **Ethical Hacker** - Performs most of the breaking activities but with permission from the owner.
- **Script Kiddies or packet monkeys** - Inexperienced Hackers with programming language skill.

Techniques for Security Testing (Methodologies)

Tiger Box: This hacking is usually done **on a laptop** which has a collection of Operating Systems and hacking tools.

This testing helps **penetration testers and security testers to conduct vulnerabilities assessment and attacks**.

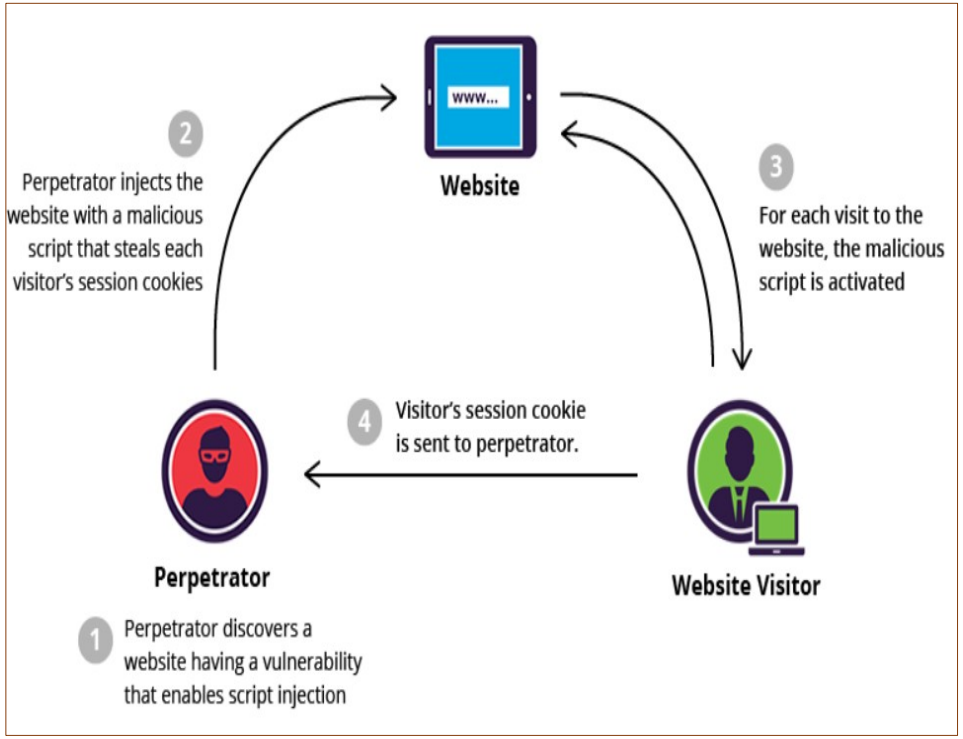
Black Box: Tester **is authorized to do testing** on everything about the network topology and the technology.

Grey Box: **Partial information is given to the tester** about the system, and it is a hybrid of white and black box models.

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of software testing that tests internal structures or workings of an application, as opposed to its functionality.

What is Cross Site Scripting (XSS)?

- **XSS enables attackers** to inject client-side scripts into web pages viewed by other users.



- A **cross-site scripting** vulnerability may be used by attackers to bypass **Access Controls** such as the same-origin policy.

Under the policy, a web browser permits scripts contained in a first web page to access data in a second web page, but only if both web pages have the same origin.

What is SQL Injection?

- **SQL injection** attacks are used to steal information from **databases.**

- A SQL injection attack happens when SQL code is **injected** into forms, cookies, or http headers that do not use **data sanitizing or validation methods** to verify the request.

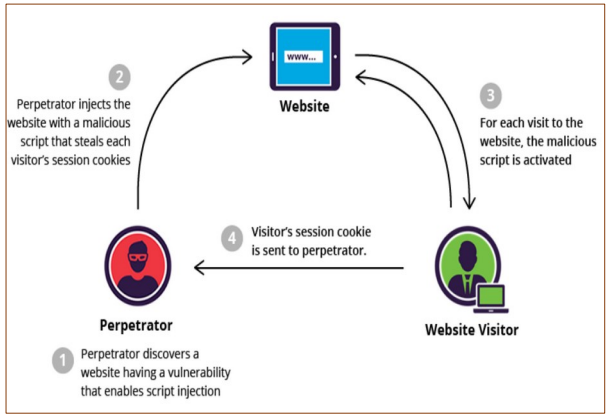
https://scotch.io/@PratyushB/sql-injection-and-xss-security-threats

SQL Injection vs. XSS

- **SQL injection** attacks are used to steal information from **databases.**

- **XSS** attacks are used to **redirect users** to **websites** where attackers can steal data from them.

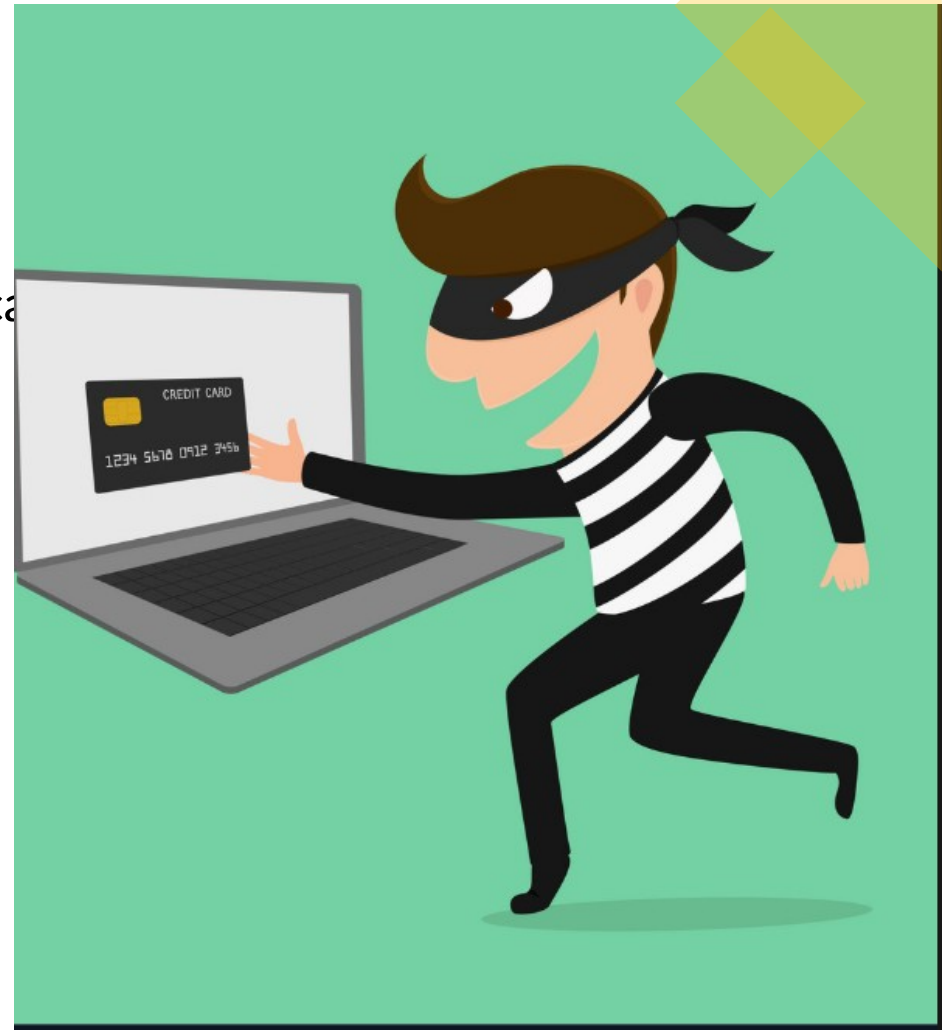
SQL injection is **data-base focused** whereas **XSS is** geared towards attacking **end users**.



https://scotch.io/@PratyushB/sql-injection-and-xss-security-threats

Sample Security Testing Test Scenarios

- A password should be in **encrypted** format.
- Application or System should not allow **invalid** users.
- Check **cookies** and **session time** for application.
- For financial sites, the **Browser back** button should not work.
- A Student Management System is insecure if 'Admission' branch ca edit the data of 'Exam' branch – **User Roles.**
- An ERP system is not secure if DEO (data entry operator) can generate 'Reports' – **User Roles.**
- An online Shopping Mall has no security if the customer's Credit Card Detail **is not encrypted.**
- A custom software possess inadequate security if an SQL query retrieves actual **passwords** of its users.



•Guru99.com and SoftwareTestingHelp.com

应用中可能的漏洞及如何处理

Examples of Security Flaws in an Application

8 Top Security Testing Techniques

1. Access to Application – Roles and Rights Management should be tested.
2. Data Protection – The user can only view the data that he/she is entitled to.
3. Brute-Force Attack – Software attempts to guess passwords and tries to login again & again.
4. SQL Injection and XSS (cross-site scripting) – Malicious script is used by hackers in order to manipulate a web site.
5. Service Access Points (Sealed and Secure Open) – Application to Application Access points should be protected and sealed.

Examples of Security Flaws in an Application

6. Session Management – Test for
   - Session expiry after a particular idle time
   - Session termination after maximum lifetime
   - Session termination after log out
   - Check for session cookie scope and duration
   - Testing if a single user can have multiple simultaneous sessions, etc.
7. Error handling – Test these by making certain requests to the page such that these error codes are returned
   - 408 request time-out
   - 400 bad requests
   - 404 not found, etc..
8. Specific Risky functionalities - two risky functionalities are
   - Payments
   - File uploads – Test for any unwanted malicious file upload is restricted

Security Testing Tools for Web Applications

- There are many **free web application testing tools** available in the market. Here are **12 open source security testing tools**:

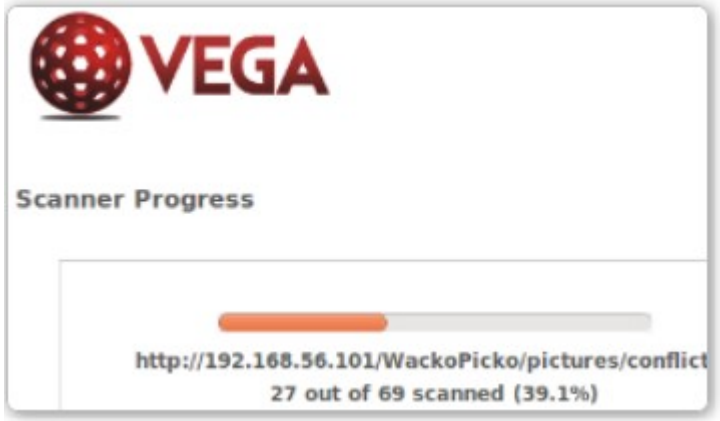
1. Zed Attack Proxy
2. Wfuzz
3. Wapiti
4. W3af
5. Vega
6. SQLMap
7. SonarQube
8. Nogotofail
9. Grabber
10. Arachni
11. Skipfish
12. Ratproxy

https://www.softwaretestingmaterial.com/open-source-security-testing-tools/

Example of a Security Testing Tools for Web Applications

Vega

- It is written in Java, with a great GUI, and runs on Linux, and Windows. It exposes vulnerabilities including:
  - Find and validate SQL injection
  - Cross-Site Scripting (XSS) injection
  - Blind SQL injection
  - Header injection
  - Remote file include
  - Shell injection



- **Website Link:** https://subgraph.com/vega/
- **Source Code Download Link:** https://github.com/subgraph/Vega

Security Testing References

https://www.guru99.com/what-is-security-testing.html

https://insights.sei.cmu.edu/sei_blog/2018/07/10-types-of-application-security-testing-tools-when-and-how-to-use-them.html

https://www.tutorialspoint.com/software_testing_dictionary/security_testing.htm

https://www.softwaretestinghelp.com/how-to-test-application-security-web-and-desktop-application-security-testing-techniques/

https://www.softwaretestingmaterial.com/open-source-security-testing-tools/

Cybersecurity

INFO6255 Software Quality Control & Management

Medi Servattalab

M.Servattalab@northeastern.edu

What is Cybersecurity?

Cybersecurity refers to a set of techniques used to protect the integrity of **networks, programs and data from attack**, damage or unauthorized access.

According to Forbes, the global cybersecurity market is expected to reach 170 billion by 2020.

The rapid market growth BYOD, IoT, The Cloud Based applications and Workloads.

Cybersecurity Vs. Application Security

Software Application Security refers to the **prevention of writing vulnerable code** and to create processes for **secure development**.

Cybersecurity is to protect more than just the software application. It refers to the entire infrastructure of a company:

- **Hardware**
- **Network Switches**
- **Wireless Devices**
- **Firewalls**
- **Databases**

Cybersecurity

- Protecting Information and systems from **Major cyberattacks:**
  - Application attacks
  - Malware
  - Ransomware
  - Phishing
  - Exploit kits
- Keeping pace with the **sophisticated attacks** has been becoming more challenging.
- **Cyberthreats** are now taking aim at: **political, military, governments, infrastructures of nations.**

Cybersecurity glossary

- **Botnet**
  Multiple computers on a network that are infected with a program that can be controlled remotely.
    - The infected computers are usually used to cause damage that couldn't be achieved with a single computer.
- **DDoS**
  A **distributed denial of service** attack attempts to make an online service, like a website, unavailable by overwhelming it with a **flood of traffic** from a team of computers.
- **Spam**
  Unsolicited emails sent to many addresses. The purpose of most spam is to make money through advertising or identity theft.

Cybersecurity glossary…

- **Hacktivist**
  Someone who uses computers and computer networks to **disrupt services** or share secret information in an effort to draw attention to political or social issues.

- **Keylogger malware**
  A program that **records every key struck** on a keyboard and sends that information to an attacker.

Cybersecurity glossary...

- **Malware**
  Software that harms **computers, networks,** or people. Includes viruses, worms, ransomware, and other computer programs.
- **Phishing**
  Attempting to trick people into **revealing sensitive** information, such as passwords and credit card numbers, often by using **emails or fake websites** that look like they are from trusted organizations.
- **Ransomware**
  A type of malware that holds **victims' computer files hostage** by locking access to them or encrypting them. It then demands a ransom if the victim wants his or her files back.

bersecurity Facts

- Two years ago, Ginni Rometty, IBM's chairman, president and CEO, said: **"Cybercrime is the greatest threat to every company in the world."** And she was right.

During the next five years, cybercrime might become the greatest threat to every person, place and thing in the world.

- **The average cost of a data breach in 2020 will exceed $150 million**
  - As more business infrastructure gets connected, cybercrime will cost businesses over $2 trillion total in 2019 (Juniper Research data).
- **Since 2013 there are**
  - 3,809,448 records stolen from breaches every day, 158,727 per hour, 2,645 per minute and 44 every second of every day (Cybersecurity Ventures.)

https://www.cybintsolutions.com/cyber-security-facts-stats/

Cybersecurity Facts

- **Over 75% of healthcare industry has been infected with malware over last year**
  - The study examined **700 healthcare organizations** including medical treatment facilities, health insurance agencies and healthcare manufacturing companies.
- **Large-scale DDoS attacks increase in size by 500%**
  - According to the Q2 2018 Threat Report, Nexusguard's quarterly report, the average **distributed denial-of-service (DDoS)** attack grew to more than 26Gbps, increasing in size by 500%.
- **Unfilled cybersecurity jobs worldwide will reach $3.5 million by 2021**
  - More than 300,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past five years.

https://www.cybintsolutions.com/cyber-security-facts-stats/

Facts about Cybersecurity

- **95% of breached records came from only three industries in 2016**
  - Government, retail, and technology. Why? Because of popularity, high traffic with personal information.
- **There is a hacker attack every 39 seconds.**
  - **From the Univ of Maryland:** affecting one in three Americans every year —and the **non-secure usernames and passwords** we use that give attackers more chance of success.
- **43% of cyber attacks target small business**
  - 64% of companies have experienced web-based attacks.
  - 62% experienced **phishing & social engineering** attacks.
  - 59% of companies experienced **malicious code and botnets.**
  - 51% experienced **denial of service** attacks.

https://www.cybintsolutions.com/cyber-security-facts-stats/

Cybersecurity Facts

- 95% of cybersecurity breaches are due to human error:
  - Cyber-criminals and hackers will infiltrate your company through your weakest link.
- Only 38% of global organizations claim they are prepared to handle a sophisticated cyber attack
- What's worse? An estimated 54 percent of companies say they have experienced one or more attacks in the last 12 months.

https://www.cybintsolutions.com/cyber-security-facts-stats/

Cybersecurity Facts

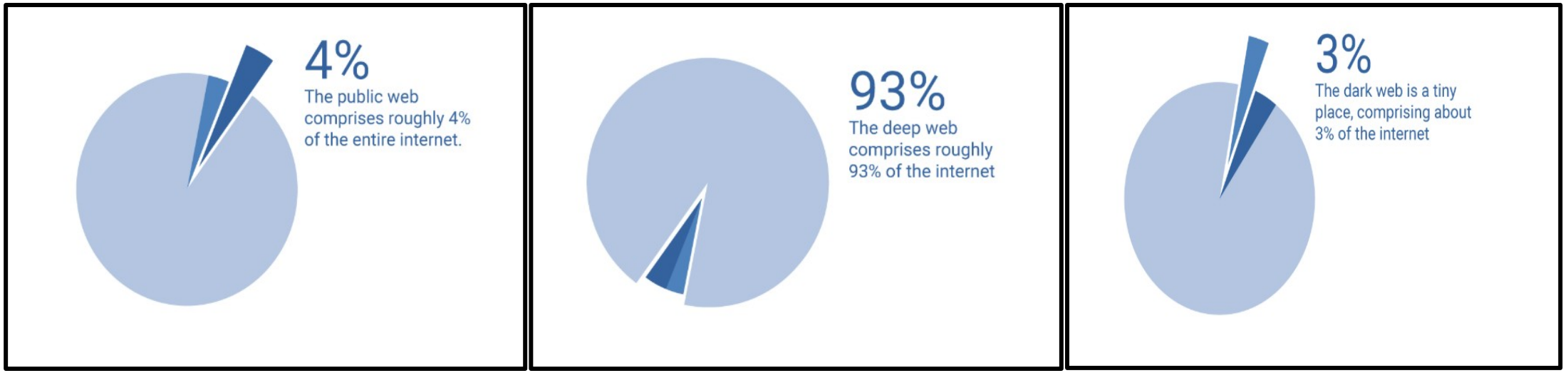
- **Total cost for cybercrime committed globally has added up to over $1 trillion dollars in 2018.**

  - Don’t think that all that money comes from hackers targeting corporations, banks or wealthy celebrities.
  - Individual users like you and me are also targets.

  - **As long as you’re connected to the Internet, you can become a victim of cyber attacks.**

What are the Web Types?

- **Public Web:** Information you **normally** find on the search engines.
- **Deep Web:** Information that is **not indexed** by the search engines and does not require Authentication (School, Internal company sites).
- **Dark Web:** Information that is not accessible by normal internet browsers.



https://www.experian.com

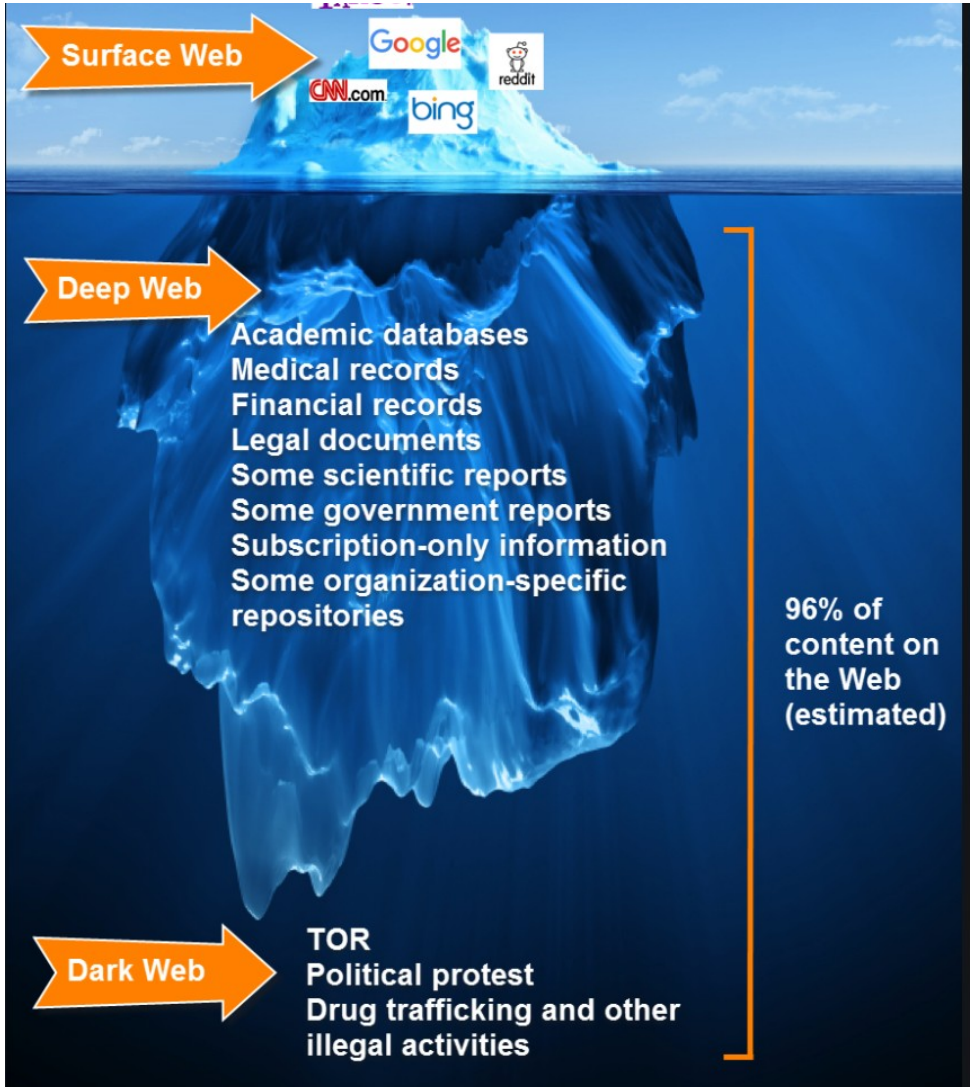
The Dark Web

- **The Dark Web**, a seemingly hidden world a far-cry from the internet we know, love and have become accustomed too.

- A place <u>shrouded in mystery</u> for some and wonder for others.

- All the criminal activity that takes place. The user is able to surf the **<u>internet anonymously</u>**.

- This means hackers, governments, and even internet service providers and the websites you're visiting **<u>won't be able to tell who you are</u>**.



The Dark Web…

- **Internet:** when you visit a website on the WWW, IP addresses trace online activity on your computer.
- **Dark Web:** with the **masking software** activated, a computer takes a randomized path to its file destination, bouncing around a number of encrypted connections to ultimately mask both **location and identity**.
- In 2017, Experian found the going rates for some dark web sites:
  - Social Security number: $1
  - General login: $1
  - Credit card number with CV: $5
  - Debit card number with bank info: $15
  - Driver's license: $20

•https://www.makechange.aspiration.com; https://www.experian.com; https://www.sys-corp.net/darkweb/

8 Best Dark / Deep Web Browsers in 2019

- The Tor Browser
- Subgraph OS
- Firefox
- Waterfox
- ISP - Invisible Internet Project
- Tails - The Amnesic Incognito Live System
- Opera
- Whonix

https://drfone.wondershare.com/dark-web/dark-web-browser.html

How Can You Protect Yourself from the Dark Web?

Monitor	Monitor your accounts and statements for any information that looks off
Check	Check your credit report regularly to see if inquiries or new accounts appear that you don't recognize
Use	Use strong passwords, and change them often
Consider	Consider an online product to help you protect your identity and monitor your credit.
Know	Know how to respond immediately to suspicious activity
Use	Use Experian's Free Dark Web Scan to see if your Social Security number, phone number, or email address is on the dark web.

Cybersecurity Tools

- **Metasploit -** is a very popular collection of various penetration tools.
  - It is used for years to accomplish various objectives, including discovering vulnerabilities, managing security evaluations, and formulating defense methodologies.
- **Nmap -** also known as **network mapper**, is a free and open source tool for scanning your systems or networks for vulnerabilities

https://www.cybrary.it/0p3n/7-cyber-security-pentesting-tools/

Cybersecurity Tools…

- **Wireshark -** is a handy tool that can assist you to see the **minutest details** of the activities taking place in your network.

- **John the Ripper -** free tool that blends different password crackers into a single package, automatically identifies different types of **password hashes**, and comes with a **customizable cracker**

https://www.cybrary.it/0p3n/7-cyber-security-pentesting-tools/

The Cybersecurity video

- https://www.khanacademy.org/partner-content/nova/cybersecurity/cyber/v/cybersecurity-101

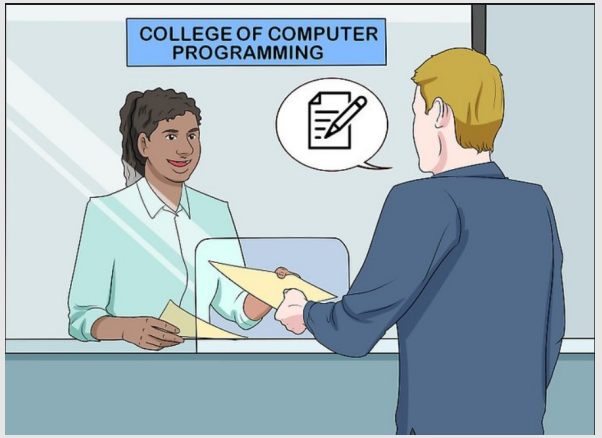
Cyber Security Certifications

- 1. CEH: Certified Ethical Hacker
- 2. CISM: Certified Information Security Manager
- 3. CompTIA Security+
- 4. CISSP: Certified Information Systems Security Professional
- 5. GSEC: GIAC Security Essentials
- 6. ECSA: EC-Council Certified Security Analyst
- 7. GPEN: GIAC Penetration Tester
- 8. SSCP: Systems Security Certified Practitioner
- 9. CRISC: Certified in Risk and Information System Control
- 10. CISA: Certified Information Systems Auditor

https://www.businessnewsdaily.com/10708-information-security-certifications.html#CEH

CYBER SECURITY DEGREES & CAREERS

- Bachelor's Degree in Cyber Security
- Master's Degree in Cyber Security
  - **PENETRATION TESTING AND VULNERABILITY ANALYSIS -** Introduces **methodologies, techniques and tools** to analyze and identify vulnerabilities in stand-alone and networked applications.
  - **APPLIED CRYPTOGRAPHY -** Examines **Modern Cryptography** from both a theoretical and applied perspective; emphasis is on provable security and application case studies.
  - **DIGITAL FORENSICS -** Instruction in the application of forensic science principles and practices for **collecting, preserving, analyzing and presenting digital evidence;** covers topics from legal, forensic, and information-technology domains.



- https://www.learnhowtobecome.org/computer-careers/cyber-security/

Cyber Security Testing - Courses

- **INTRODUCTION TO PENETRATION TESTING -** Lab-based course providing students with an understanding of the threat vectors and exploitation techniques used to penetrate systems and networks.
  - **Skills Gained:**
    - Assessment
    - Exploitation
    - Remediation techniques
- **FULL SCOPE SECURITY TESTING -** Review of the tools, techniques, and sources of digital information and its role in attacking and defending software systems and network environments.
  - **Skills Gained:**
    - Penetration testing processes
    - Exploitation
- **ADVANCED MALWARE ANALYSIS -** Covers advanced techniques used in malware analysis; focuses heavily on static analysis of unknown binaries utilizing reverse engineering tools and procedures.
  - **Skills Gained:**
    - Anti-debugging processes
    - x86 assembly language
    - IDA pro

•https://www.learnhowtobecome.org/computer-careers/cyber-security/

CYBER SECURITY JOB GROWTH & OUTLOOK

According to Cisco Systems, Inc., there is a **distinct shortage of cyber security professionals**, particularly those with data science skills. As a result of this scarcity, many computer science workers, particularly those currently in the IT field, are eyeing employment in cyber security.

Indeed, as job growth goes, it's hard to find a profession that outpaces cyber security. According to the U.S. Bureau of Labor Statistics, for example, job growth from 2012 to 2022 is projected to be:

- **37 percent for the Information Security Analysts**
- **18 percent for all computer occupations**
- **11 percent for all occupations**

Top-Paying Cybersecurity jobs By Indeed.com

- The Cybersecurity engineers who review and test the security of code in apps also made our list of 2018's hottest cybersecurity roles.

- Given that the average smartphone user has 80 apps on their phone, this role will likely remain in high demand

List of Top cybersecurity job titles and salaries (Indeed.com)

- $127,855 - Director of Information Security
- $126,628 - Senior Security Consultant
- $126,365 - Cloud Engineer
- $117,633 - Software Architect (is this really a security role as listed by Indeed?)
- $114,431 – Penetration Tester
- $108,465 - Risk Manager
- $103,690 - Chief Information Officer
- $101,808 - Security Engineer
- $99,930 - Information Manager

https://www.secureworldexpo.com/industry-news/top-10-highest-paying-cybersecurity-jobs-2019

So why is job growth in Cybersecurity expected to be so robust?

Cyber crime continues to be a significant and growing problem, both in the United States and around the world.

For example, a record 79 percent of respondents to a recent PricewaterhouseCooper's study reported that they had detected a security incident within the past 12 months.

References

- https://www.cybintsolutions.com/cyber-security-facts-stats/
- https://www.businessnewsdaily.com/
- https://www.khanacademy.org/partner-content/nova/cybersecurity/cyber/e/cybersecurity-101-quiz
- https://www.learnhowtobecome.org/computer-careers/cyber-security/

The Social Dilemma!!!

The Social Dilemma is a 2020 American docudrama film directed by Jeff Orlowski and written by Orlowski, Davis Coombe, and Vickie Curtis.

The film explores the rise of social media and the damage it has caused to society, focusing on its exploitation of its users for financial gain through surveillance capitalism and data mining, how its design is meant to nurture an addiction, its use in politics, its effect on mental health (including the mental health of adolescents and rising teen suicide rates), and its role in spreading conspiracy theories such as Pizzagate and aiding groups such as flat-earthers.

- https://www.thesocialdilemma.com/
- https://www.newsweek.com/facebook-calls-social-dilemma-conspiracy-documentary-rejects-hate-speech-claims-1536643
- In a rebuttal, Facebook has branded the film a "conspiracy documentary," and said it does not deliberately allow misinformation and hate speech to "fester" on its platform and works to remove it, "despite what the film says."

https://www.newsweek.com/facebook-calls-social-dilemma-conspiracy-documentary-rejects-hate-speech-claims-1536643