Assessment Task 3 - Assignment 1

Task 1: Use CSS to display the following information

9411682 Sujeet Shukla

COMP804: Web Security

Assignment 1, due at the end of Week 5

Task 2: Use CSS to style a table

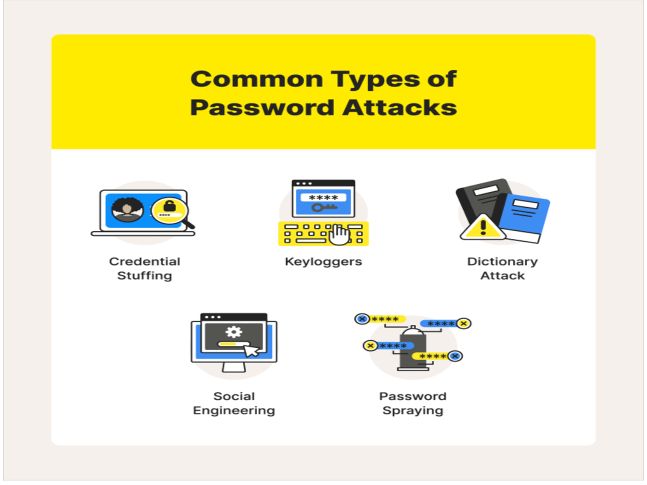
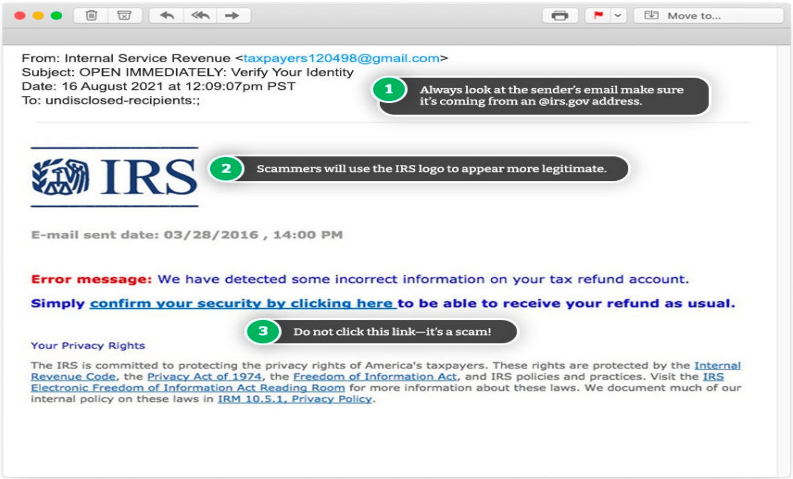
Key dates - University of Wollongong - UOW

18 Jul 2023

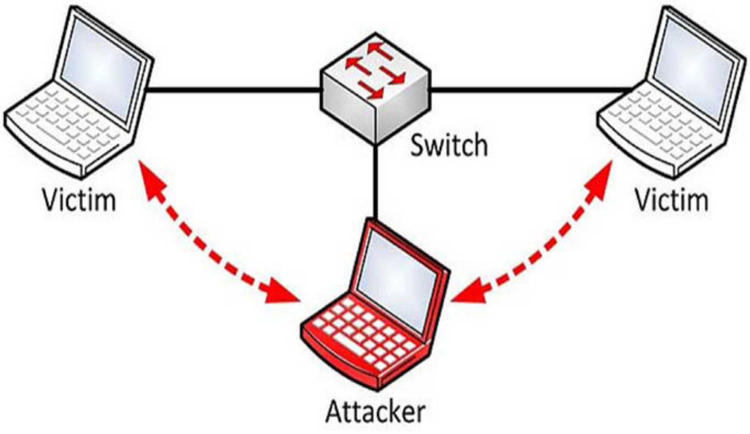
Activity	Date
First day to enrol for re-enrolling (continuing students)	21 Nov 2022
Orientation	18 Jul 2023
Lectures Commence (weeks 1-9)	24 Jul - 22 Sep 2023
Last day to enrol / add subjects yourself	04 Aug 2023
Last day to enrol / add subjects with Head of Students approval	11 Aug 2023
CENSUS DATE • Fees due Last day to withdraw from subject/s without paying for them • HECS / FEE HELP debt reporting date • Last day to change HECS / FEE HELP billing option Learn more about Census date	31 Aug 2023
Student Services and Amenities Fees Due	
Last day to withdraw without academic penalty - subject deleted from record Fail grade recorded if subject withdrawn after this date	22 Sep 2023
Mid-Session Recess (1 week)	25 Sep - 29 Sep

	20233
Lectures Recommence (weeks 10-13)	02 Oct - 27 Oct 2023
Study Recess (1 week)	30 Oct - 03 Nov 2023
Exams (2 weeks)	04 Nov - 16 Nov 2023
Release of Results	30 Nov 2023

Task 3: HTML & CSS

Web Attack Name	Web Attacks - Explanation
A. Password Attacks  Common Types of Password Attacks Credential Stuffing Keyloggers Dictionary Attack Social Engineering Password Spraying https://us.norton.com/	1. These occurs when a hacker tries to steal a user password using a number of methods using a web application. 2. Some of the tactics include phishing, Man-in-the-Middle attack, password spraying, brute force, dictionary attacks, social engineering, credential stuffing and dumping, Pass the Hash technique and keyloggers. 3. Such attacks can be prevented by having MFA authentication (using physical tokens), using strong passwords, regularly changing passwords and using biometrics. https://www.onelogin.com/ https://www.tripwire.com/
B. Phishing attacks - spear phishing, and whaling.  From: Internal Service Revenue <taxpayers120498@gmail.com> Subject: OPEN IMMEDIATELY: Verify Your Identity Date: 16 August 2021 at 12:09:07pm PST To: undisclosed-recipients:; 1 Always look at the sender's email make sure it's coming from an @irs.gov address. 2 Scammers will use the IRS logo to appear more legitimate. E-mail sent date: 03/28/2016 , 14:00 PM **Error message:** We have detected some incorrect information on your tax refund account. **Simply confirm your security by clicking here to be able to receive your refund as usual.** 3 Do not click this link—it's a scam! Your Privacy Rights The IRS is committed to protecting the privacy rights of America's taxpayers. These rights are protected by the Internal Revenue Code, the Privacy Act of 1974, the Freedom of Information Act, and IRS policies and practices. Visit the IRS Electronic Freedom of Information Act Reading Room for more information about these laws. We document much of our internal policy on these laws in IRM 10.5.1, Privacy Policy. https://www.aura.com/learn/types-of-cyber-attacks	1. A cybercriminal masquerading (imposter) as a trusted source sends a fradulent email, text or phone call and collects data. 2. *Spear phishing attacks* are designed to target specific individuals to coerce the victim to comply. 3. A *whaling* phishing attack targets high profile individuals for access to data and corporate resources. 4. *Angler phishing atacks* is used to 'bait' victims on social media and scam users in believing it is a legitimate source. 5. The threat actor uses email/SMS to guide the victim to click a web link, directing them to their webpage where they harvest personal data. https://www.aura.com/

C. Man-in-the-Middle (MitM) Attacks



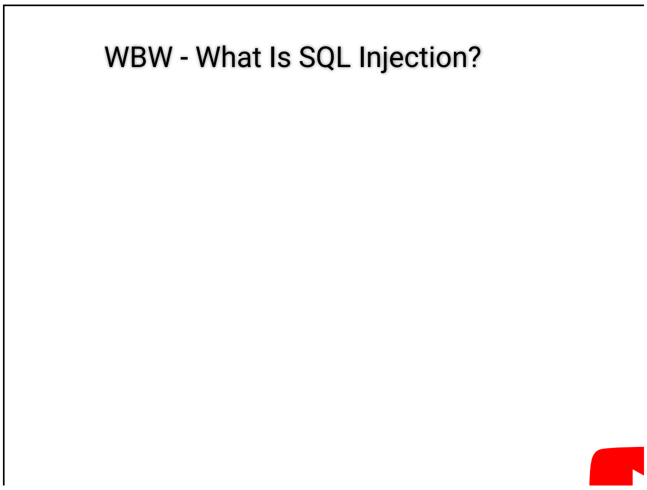
https://www.datto.com/

1. The threat actor intercepts a two way transaction and inserts themselves in the middle intercerpting and spoofing traffic data.
2. Taking advantage of security vulnerabilities in a network such as unsecured public network, the cybercriminal acts a middleman stealing data.
3. Also known as eavsdropping attack, the attacker can traffic information to deploy malware on device and gain access to all of victim's information.

https://www.datto.com/

https://www.cisco.com/

D. SQL Injection


WBW - What Is SQL Injection?

https://www.rapid7.com/

https://youtu.be

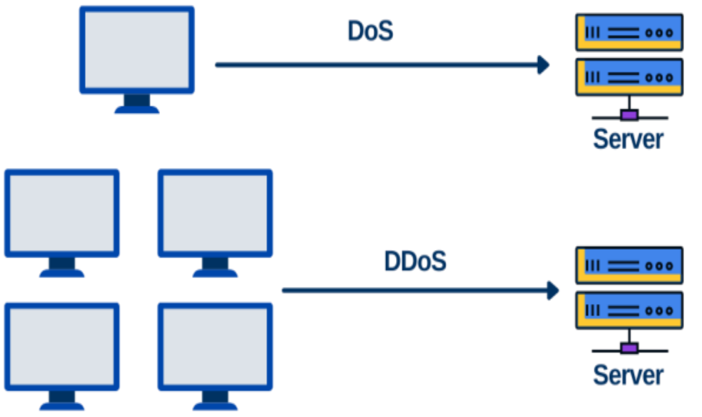
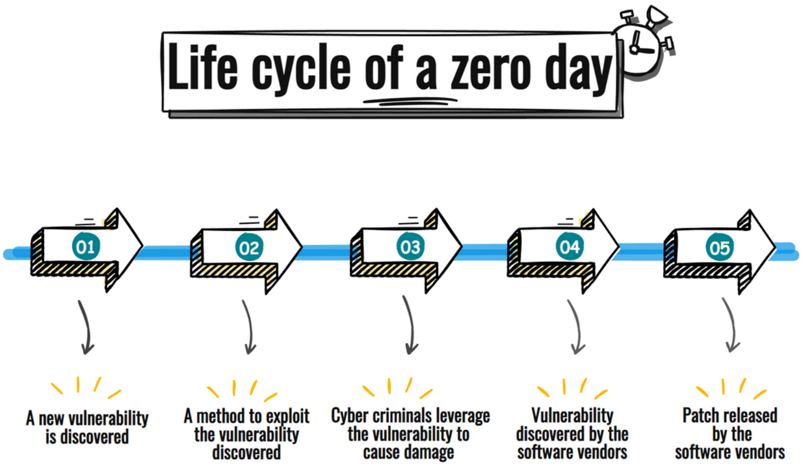
1. SQL injection attacks manipulate input fields with malicious scripts to compromise servers and access sensitive database data.
2. The attack targets vulnerable SQL databases, altering and manipulating data using crafted SQL statements to compromise data integrity and behaviour.
3. Potential entry points for the attack include applications, websites and directly targeting databases. Such attacks pose a high risk as it can be hard to recover fully.
4. Some of types of the SQL Injection attack are as follows:
   - Unsanitised input - user input is not sanitised or validated properly leading to data display
   - Blind SQL injection - the attacker examines the database behaviour using http response and page load times
   - Out-of-Band Injection - forcing the database to create an external connection to the hacker's server and harvest data

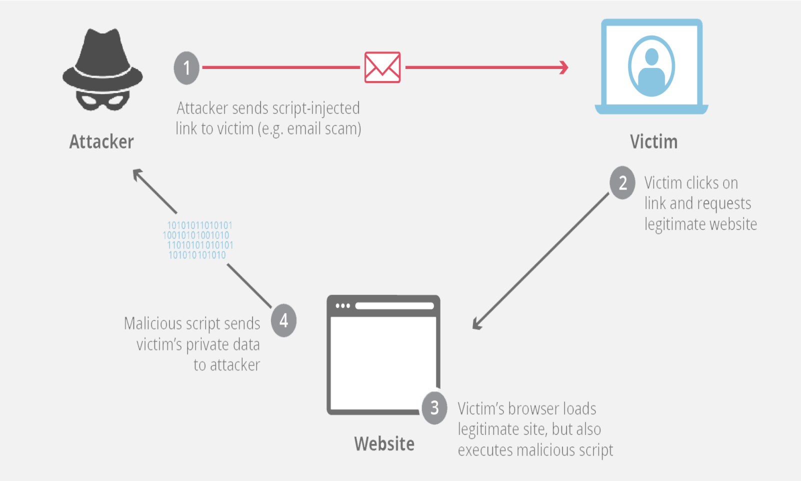
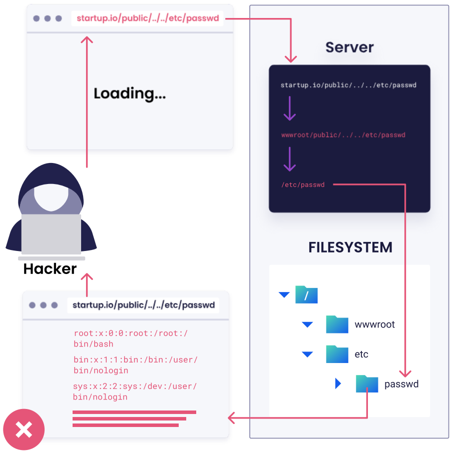
https://www.tripwire.com/

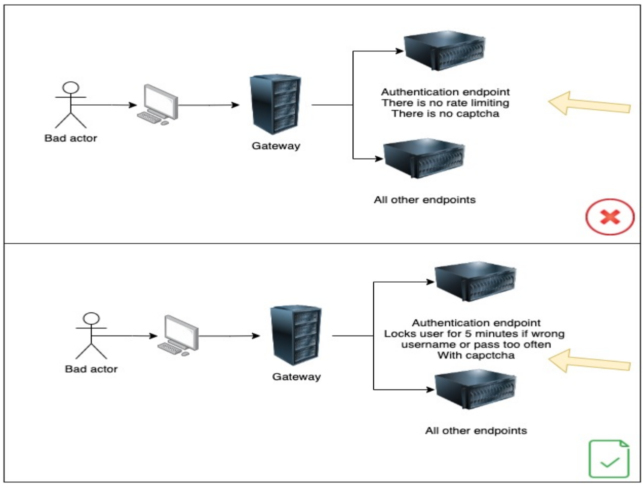
https://www.rapid7.com/

E. Denial of Service (DOS) and Distributed Denial of Service (DDoS)

1. DoS - hackers force false request and traffic to overwhelm and flood a system and shut it down. In DDoS, DoS is used to breach and disrupt multiple systems or devices.
2. Taking advantage of security vulnerabilities in a network such

 https://www.cobalt.io/	as unsecured public network, the cybercriminal acts a middleman stealing data. 3. The following lists the common DoS execution methods: - UDP flooding - overwhelm UDP packets causing it to crash - TCP SYNC floods - disrupt the three way handshake process by not responding and keeping connection open for a long time - HTTP flood - overwhelm Web Servers with http requests - Ping flood - send ICMP requests to consume bandwith and slow down legitimate traffic https://www.aura.com/ https://www.byos.io/
F. Zero-day exploits and attacks  Life cycle of a zero day 01 02 03 04 05 A new vulnerability is discovered A method to exploit the vulnerability discovered Cyber criminals leverage the vulnerability to cause damage Vulnerability discovered by the software vendors Patch released by the software vendors https://www.balbix.com/	1. These refer software vulnerabilities that exist in software and infrastructure that the manufacturer is not aware of. As these vulnerabilities have no fix, the victim company has 'zero days' to fix it. 2. In a zero-day attack or exploit, cybercriminals are able to identify and use these system flaws to access systems and steal data or cause malicious damage. 3. Some examples of significant zero-day attacks are: - "Log4J" (2021) - discovered in widely used Java-based utility including Apple's iCloud, Amazon Web Service, Microsoft, Cisco, Google Cloud and Mars Rover. - Stuxnet (2010) - a worm that exploited PLC vulnerability running on Mircosoft Windows OS infecting Siemens 7 software sabotaging centrifuges used to separate nuclear material - LinkedIn (2021) - a hacker scraped and harvested user data by exploiting the site's API https://www.aura.com/ https://www.imperva.com/

	https://cybriant.com/
G. Cross-site Scripting (XSS)  Attacker 1 Attacker sends script-injected link to victim (e.g. email scam) Victim 2 Victim clicks on link and requests legitimate website 10101011010101 10010101001010 11010101010101 10101010101010 4 Malicious script sends victim's private data to attacker Website 3 Victim's browser loads legitimate site, but also executes malicious script https://www.cloudflare.com/	1. This is an attack where an attacker injects malicious code into a legitimate website, which then executes when users load the site.. 2. It is a client-side code injection attack and the code is typically added to URLs or user-generated content. 3. The attack attacks involve delivering malicious scripts to a victim's browser, which can exfiltrate data, install malware, or redirect the user to malicious sites. 4. Sanitising and validating user input data can help prevent such attacks. https://www.cloudflare.com/ https://www.tripwire.com/
H. Directory Traversal  startup.io/public/../../etc/passwd Loading... Server startup.io/public/../../etc/passwd wwwroot/public/../../etc/passwd /etc/passwd FILESYSTEM / wwwroot etc passwd Hacker startup.io/public/../../etc/passwd root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/user/bin/nologin sys:x:2:2:sys:/dev:/user/bin/nologin https://learn.snyk.io/	1. Directory or path traversal, an HTTP exploit, targets web servers with security misconfigurations to access data outside the server's root directory, allowing attackers to view restricted files and potentially execute commands. 2. This attack mainly affects servers accepting unvalidated input from web browsers, with threat actors scanning directory trees to find paths to restricted files.. 3. To prevent path traversal and enhance web server security, normalise file paths, avoid using lower-privilege users, regularly update programming language and web server versions, and avoid using user-supplied file paths. https://brightsec.com/ https://www.stackhawk.com/
I. Broken Authentication (Vulnerabilities)	1. Broken Authentication is a security risk that can enable attackers to compromise user credentials and gain control over a system, posing a significant threat to data and system integrity. 2. It allows a hacker to bypass the application's authentication mechanism due to software misconfigurations, logic errors, or bugs, enabling unauthorised access .



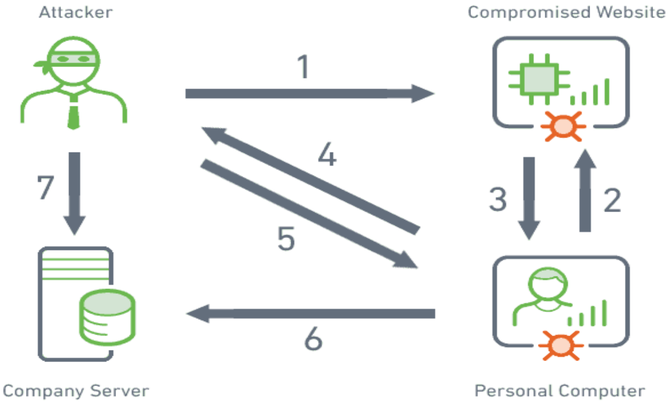
https://www.wallarm.com/

3. Attackers don't need advanced technical skills to exploit this vulnerability, particularly when access controls are poorly implemented or nonexistent: is has been a critical risk in web applications on the OWASP Top 10 since 2013.
4. Such attacks can be prevented by creating strong passwords and using token-based Multi-Factor Authentication (MFA) for authentication.

https://knowledge-base.secureflag.com/

https://www.tripwire.com/

J. Drive-by download Attack



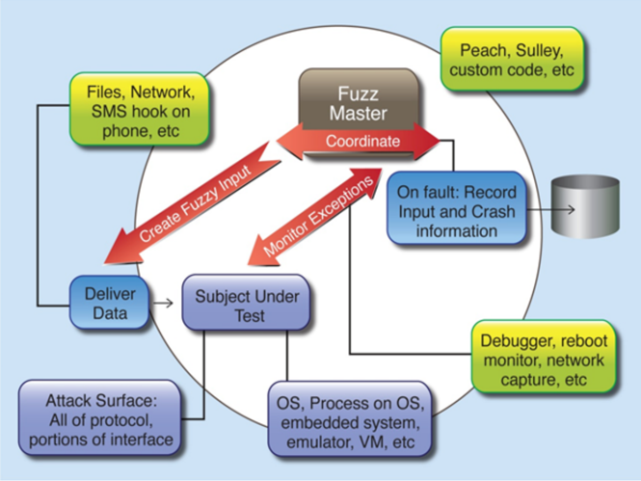
https://www.exabeam.com/

1. It refers to unauthorized, automatic and unnoticed downloading of software onto a user's device while browsing legitimate websites or via malicious advertisement, often exploiting vulnerabilities in web browsers operating systems, Java, file editors and viewers.
2. The aim of the hacker is to ultimately compromise the device and enlist it into botnet as follows:
    - Injection of malicious code in compromised web page via Javascript code, an iFrame, a link, a redirect, a malivertisment and XSS.
    - Vulnerability exploits - user triggers the code by viewing or clicking web-element that exploits a software vulnerability on the device.
    - The code is downloaded and executed silently on user device giving control to the threat actor.
    - The hacker remote accesses the device and harvests sensitive data to access other larger systems.
3. The risk of this attack can be minimised by having a robust software update and patching procedure, enabling a principle of least priviledge and using SIEM-integrated endpoint protection.

https://www.exabeam.com/

K. Fuzzing

1. This 'black box' technique works by inputting a large amount of random data into an application to induce crashes, followed by


Peach, Sulley, custom code, etc
Files, Network, SMS hook on phone, etc
Fuzz Master
Coordinate
Create Fuzzy Input
Monitor Exceptions
On fault: Record Input and Crash information
Deliver Data
Subject Under Test
Debugger, reboot monitor, network capture, etc
Attack Surface: All of protocol, portions of interface
OS, Process on OS, embedded system, emulator, VM, etc

https://bromiumlabs.wordpress.com/

the use of a fuzzer software to identify vulnerabilities.

2. It is used for discovering software bugs by stressing applications with unexpected inputs to trigger crashes or vulnerabilities.
3. There are two main categories for http(s) fuzzing:
    - Recursive - involves fuzzing a part of a request by iterating through all possible combinations of a set alphabet. For example, fuzzing the "8302fa3b" part of a URL against the hexadecimal alphabet (0-9, a-f) generates multiple requests, one for each possible combination. This results in a large number of requests with variations of the fuzzed part.
    - Replacive - a part of the request is fuzzed by replacing it with a set value known as a fuzz vector. For instance, testing for XSS by sending different fuzz vectors to a URL involves replacing a part of the URL with these vectors. The total number of requests depends on the number of fuzz vectors used.

https://owasp.org/

https://www.tripwire.com/

Task 4: Javascript with button

Cat Dog Frog

User clicks Dog

Dog is clicked

Task 5: Gihub repository

Click here to view the Report

Click here to view Report