Netaji Subhas University of Technology

A STATE UNIVERSITY UNDER DELHI ACT 06 OF 2018, GOVT. OF NCT OF DELHI

Azad Hind Fauj Marg, Sector-3, Dwarka, New Delhi-110078

Project Report

COCSC22 : Project-1

Fortifying Web Applications:

End-to-End Prevention and Solutions for Web Attacks

Supervisor : Dr. Vipin Pal

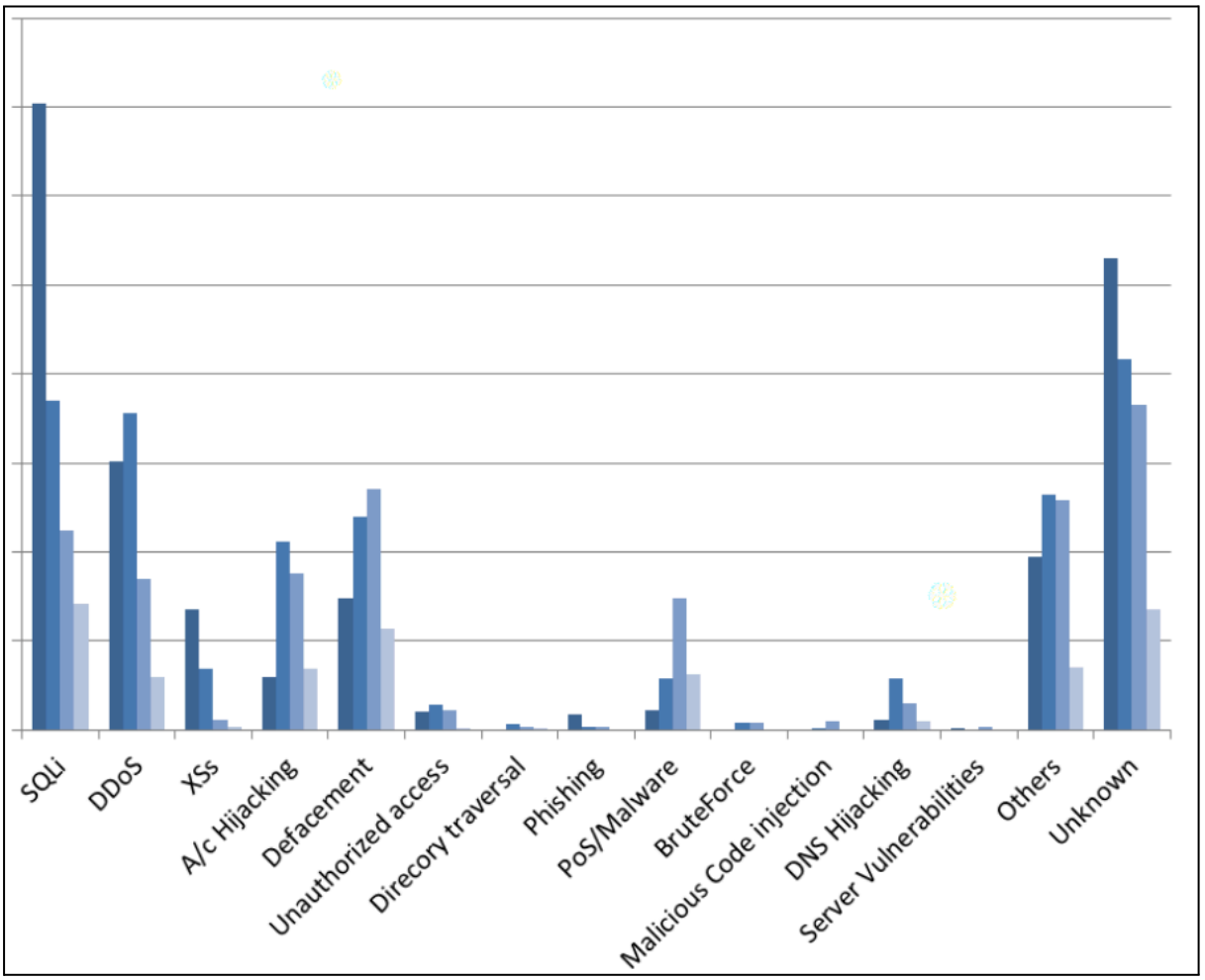
Submitted By: Group-131

Shobhit - **2021UCS1618**

Yash Gautam - **2021UCS1690**

Prachi Sah - **2021UCS1702**

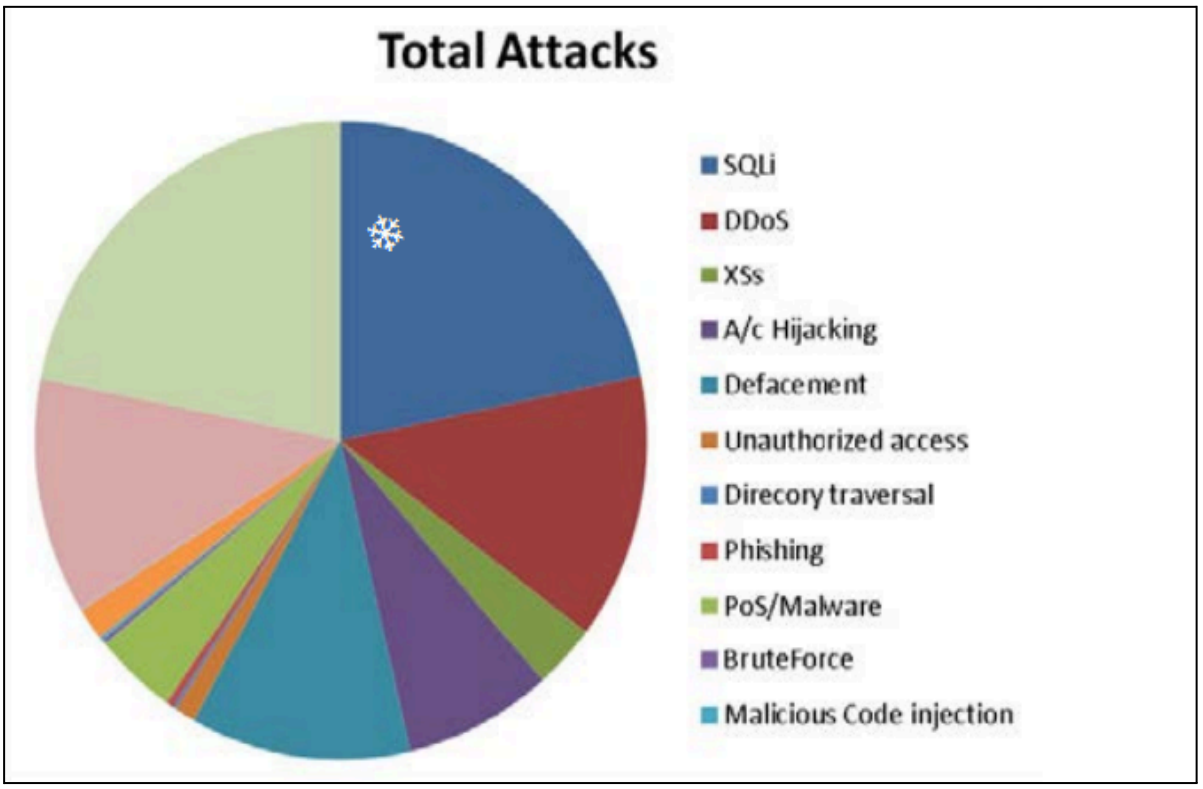
Based on type of attacks and their number we can deduce this bar graph.



D. Kaur and P. Kaur, "A Study of Web Application Security and Vulnerabilities," Procedia Computer Science, vol. 78, pp. 298-306, 2016.

The top five categories of the web attacks are **SQLi (SQL Injection) , DDoS (Distributed Denial of Service), Defacement, Account Hijacking and Malware**.

Many attacks are popular among hackers for a particular set of web applications depending on the services provided by it. Next section identifies various categories of web applications and attack trends on them.

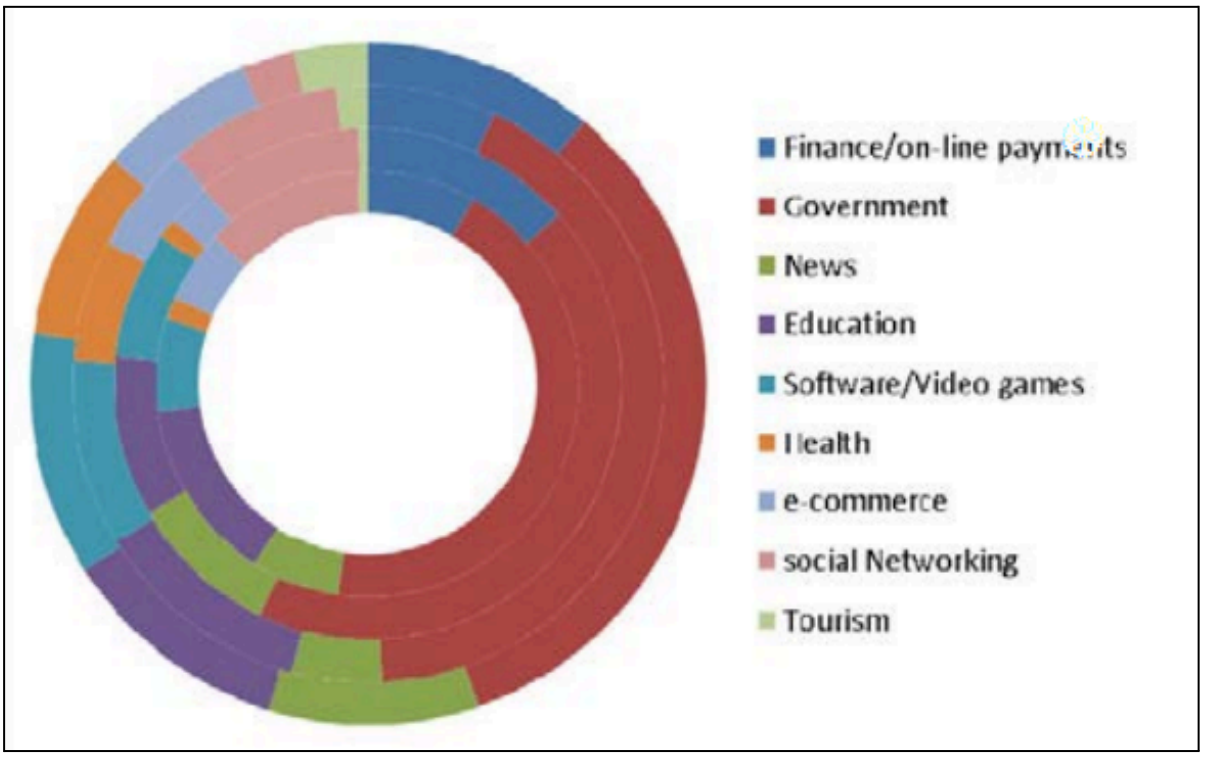


D. Kaur and P. Kaur, "A Study of Web Application Security and Vulnerabilities," Procedia Computer Science, vol. 78, pp. 298-306, 2016.

b) Web Application Categories:

Every web application that we see falls into a web category and here we have identified the major ten categories of the web applications and these include financial, government, education, news, tourism, entertainment, health, social networking, ecommerce and software/video games. Then we have analysed the identified attacks in the previous year.We also found out government sites are maximum vulnerable to attacks.

The other web applications that have significant number of attacks in the previous three years are Educational, Social Networking, Finance and the web sites that provide software to download, use or video games. Tourism related web applications have faced least number of attacks, as shown in Table

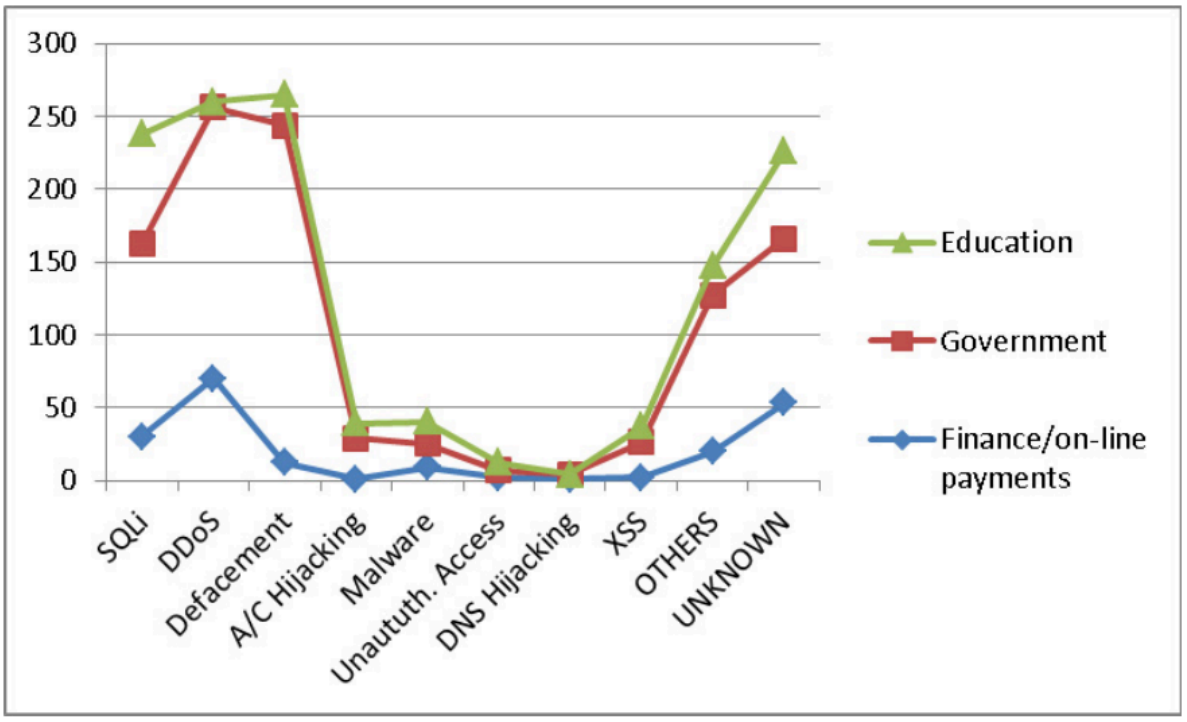


D. Kaur and P. Kaur, "A Study of Web Application Security and Vulnerabilities," Procedia Computer Science, vol. 78, pp. 298-306, 2016.

Web Application Categories	2012 Attacks	2013 Attacks	2014 Attacks	2015 Attacks	Total Attacks
Finance/on-line payments	47	98	33	22	200
Government	248	315	197	67	827
News	38	69	23	20	150
Education	78	73	56	22	229
Software/Video games	40	59	47	23	169
Health	9	9	31	18	57
e-commerce	31	20	28	15	94
social Networking	69	77	44	5	195
Tourism	4	4	8	7	23
On-line entertainment	31	17	9	10	67

D. Kaur and P. Kaur, "A Study of Web Application Security and Vulnerabilities," Procedia Computer Science, vol. 78, pp. 298-306, 2016.

Maximum attacks on **government sites** are Defacement attacks followed by DDoS, SQLi, XSS and others. Educational web sites have maximum SQLi attacks followed by DNS Hijacking, Defacement and Malware attacks. Government websites have least attacks of type DNS Hijacking and Unauthorized Access. Different web sites categories have different types of attacks distribution. We have identified the top attacks on each category as shown in Table.



D. Kaur and P. Kaur, "A Study of Web Application Security and Vulnerabilities," Procedia Computer Science, vol. 78, pp. 298-306, 2016.

So, in order to develop a web site we can see the attack trends and make it more secure just by following the countermeasures of the vulnerabilities that are making those attacks successful. We have researched about the preventive measure against some common attacks. Developers may follow those preventive actions during development life cycle of web applications and avoid dangerous attacks. Different web applications need different level of security and there is no need to spend more efforts than they deserve. It may save development time, cost and still more secure.

VIII. Attacks:

a) Sql Injection / SQLI

SQL Injection (SQLI) is a prevalent and critical security vulnerability that affects web applications interacting with SQL databases. This attack exploits flaws in the application's SQL query handling, allowing attackers to inject malicious SQL code into input fields, leading to unauthorized access to sensitive data, authentication bypass, data modification, or even database deletion. SQLI attacks pose significant threats to key security principles, including confidentiality, integrity, and authentication, as they can expose sensitive information, alter data, and enable unauthorized access to restricted areas. Despite being known for over two decades, SQLI remains a major concern, particularly in poorly designed web applications. Common prevention