WEB APPLICATION SECURITY

Submitted in partial fulfillment of
the requirement for the award of the
Degree of

Bachelor of Technology

In

Information Technology

University School of Information and
Communication technology
GGSIPU
New Delhi-78
2017-18

Submitted By:

Deepak (014)

CERTIFICATE

This is to certify that the Dissertation entitled "ETHICAL WEB HACKING" submitted by Deepak (014) is in partial fulfillment of the requirement for the award of degree B. Tech in stream Information Technology to USICT, GGSIP University, Dwarka, Delhi. It is a record of the candidate's own work carried out by them under my supervision. The matter embodied in this Report is original to the best of my knowledge and has not been submitted for the award of any other degree.

Date: 09-11-2017

Dr. Anju Saha

Professor

USICT, GGSIPU

DECLARATION

I Deepak, enrollment number 01416401514, student of B. Tech (IT), University School of Information and Communication Technology, Guru Gobind Singh Indraprastha University, Delhi hereby declare that this project report on 'WEB APPLICATION SECURITY' is submitted in partial fulfillment of requirements for the award of the degree of Bachelors of Technology (Information Technology). The project team comprised of two members:

1. Deepak **Enroll. No. 01416401514**

My Minor Project work term was done under the mentor-ship of Dr. Anju Saha, Professor, USICT, GGSIPU. The project has never been used for award of any degree/diploma to the best of my knowledge.

Deepak

01416401514

B. Tech (IT)

ACKNOWLEDGEMENT

I am using this opportunity to express my gratitude to everyone who supported me throughout the courses of this project. I am thankful for their aspiring guidance, invaluably constructive criticism and friendly advice during the project work. I am sincerely grateful to them for sharing their truthful and illuminating reviews on the number of issues related to the project. I express my warm thanks to Dr. Anju Saha for her support and guidance.

I would also like to thank all those people who provided me with the facilities being required and conductive conditions for my project.

Thank you,

Deepak (014)

TABLE OF CONTENTS

TOPIC PAGE

ABSTRACT

This project is to implement the famous hacking attacks on a self-made vulnerable website. Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering them. Hacking is usually done to gain unauthorized access to computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

The website is build using Asp.Net, C#, Sql-Server, JavaScript, Bootstrap, Ajax. The website has several vulnerabilities and following attacks and testing is done on this website -

1) Denial of Service attack (DoS/DDoS)
2) Phishing
3) Sql Injection
4) Cross-site scripting (XSS)
5) Pen testing

After implementation of these attacks we will present the code due to which the attack was successful.

OBJECTIVE OF THE PROJECT

The purpose of this project is to implement the famous hacking attacks on a self-made vulnerable website. Ethical hacking offers an objective analysis of an organization's information security posture for organizations of any level of security expertise. The ethical hacking organization has no knowledge of the company's systems other than what they can gather. Hackers must scan for weaknesses, test entry points, priorities targets, and develop a strategy that best leverages their resources.

The objectiveness of this kind of security assessment has a direct impact on the value of the whole evaluation. The need for more effective information security practices is increasingly evident with each security breach reported in the media. When adopting new technologies like cloud computing, virtualization, or IT outsourcing, enterprises are facing imminent security threats and must adjust their security processes, policies, and architectures accordingly. Among the many options available to help customers to achieve this goal, organizations should consider the value of ethical hacking services, which are rapidly gaining attention as an essential security practice that should be performed on a regular basis.

INTRODUCTION

1.1 Hacking

Definition: Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose.

Hacking can also be defined as the act of finding the possible entry points that exist in a computer system or a computer network and finally entering them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Types of Hacking

We can divide hacking into different categories, based on what is being hacked. Here is a set of examples −

- **Website Hacking** − Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
- **Network Hacking** − Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
- **Email Hacking** − It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.
- **Ethical Hacking** − Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
- **Password Hacking** − This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- **Computer Hacking** − This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

1.2 Ethical Hacking

Ethical hacking also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use, but with one major difference that Ethical hacking is legal. Ethical hacking is performed with the target's permission. The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. It's part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

Security:

Security is the condition of being protected against danger or loss. In the general sense, security is a concept like safety. In the case of networks the security is also called the information security. Information security means protecting information and information Systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Need for Security:

Computer security is required because most organizations can be damaged by hostile software or intruders. There may be several forms of damage which are obviously interrelated which are produced by the intruders.

These include:

- Lose of confidential data
- Damage or destruction of data
- Damage or destruction of computer system

1.3 History of Hacking

Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated.

1) Jonathan James

Jonathan James was an American hacker, infamous as the first juvenile sent to prison for cyber crime in United States. He committed suicide in 2008 of a self-inflicted gunshot wound. In 1999, at the age of 16, he gained access to several computers by breaking the password of a server that belonged to NASA and stole the source code of the International Space Station among other sensitive information.

2) Mark Abene

Mark Abene, known around the world by his pseudonym Phiber Optik, is an information security expert and entrepreneur. He was a high-profile hacker in the 1980s and early 1990s. He was one of the first hackers to openly debate and defend the positive merits of ethical hacking as a beneficial tool to industry.

Advantages of hacking

Hacking is not only done for illicit purposes there are some good purposes for which hacking can be used. Some of the uses of hacking can be:

i. To put adequate preventative measures in place to prevent security breaches.
ii. To recover the lost information for example in case you lost your password.
iii. To perform penetration testing to check the strength and security levels of the system and then making the system more secure.
iv. To have a computer system that prevents malicious hackers from gaining access.

TOOLS/TECHNOLOGIES USED

- **IDE: Visual Studio**

Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs for Microsoft Windows, as well as web sites, web apps, web services and mobile apps. It can produce both native code and managed code.

- **Technology Asp.Net(c#)**

ASP.NET is an open-source [2] server-side web application framework designed for web development to produce dynamic web pages. It was developed by Microsoft to allow programmers to build dynamic web sites, web applications and web services.
It was first released in January 2002 with version 1.0 of the .NET Framework.

- **DBMS: Sql Server**

SQL is a domain-specific language used in programming and designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS).

- **Operating System: Windows**

Microsoft Windows, or Windows, is a metfamily of graphical operating systems. Microsoft introduced an operating environment named Windows on November 20, 1985, as a graphical operating system shell for MS-DOS in response to the growing interest in graphical user interfaces (GUIs).

- **Web Browser: Chrome, Mozilla or any Modern browser**

Web browser, used to access the World Wide Web.

PHASES OF HACKING

There are 5 phases of Hacking.

1. **Reconnaissance:** This is the first phase where the Hacker tries to collect information about the target. It may include Identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc.
2. **Scanning:** This phase includes usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data. Hackers are now probably seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts. Now that the hacker has some basic information, the hacker now moves to the next phase and begins to test the network for other avenues of attacks.

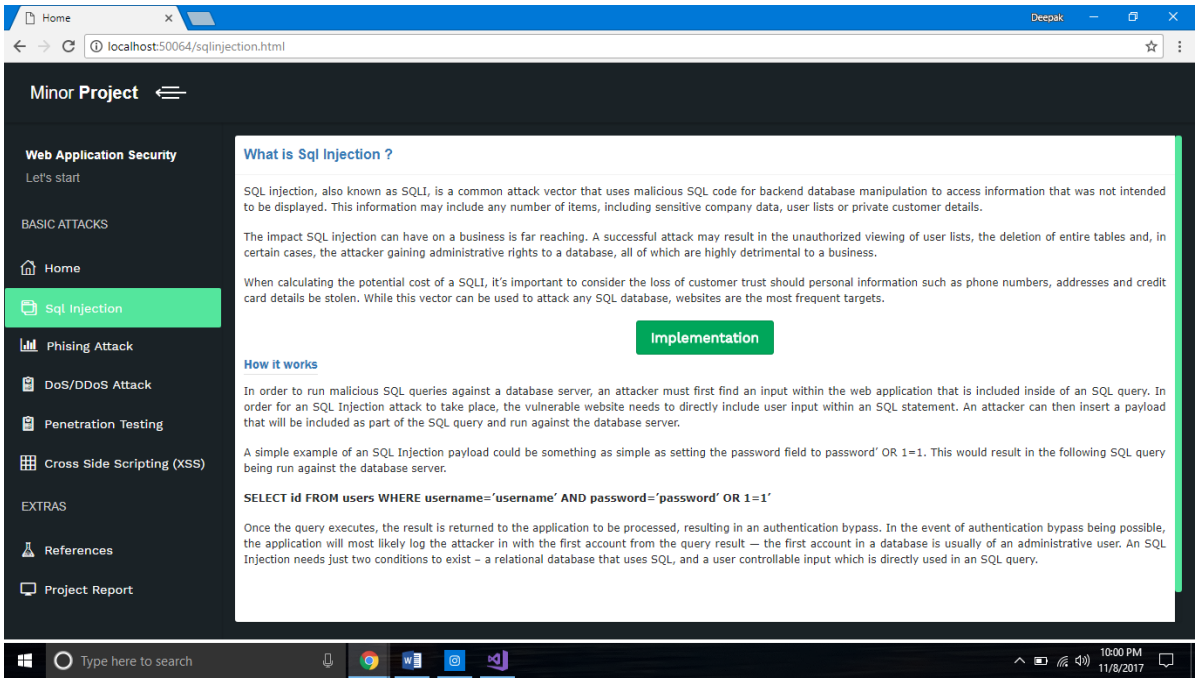
3. **Gaining Access:** In this phase, hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. The hacker has finished enumerating and scanning the network and now decide that they have some options to gain access to the network. An variant of Denial of Service attack, stack based buffer overflows, and session hijacking may prove to be great.
4. **Maintaining Access:** Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system**.**
5. **Clearing Tracks (so no one can reach them):** Prior to the attack, the attacker would change their MAC address and run the attacking machine through at least one VPN to help cover their identity. They will not deliver a direct attack or any scanning technique that would be deemed “noisy”. Once access is gained and privileges have been escalated, the hacker seek to cover their tracks. This includes clearing out Sent emails, clearing server logs, temp files, etc.

PROCEDURE

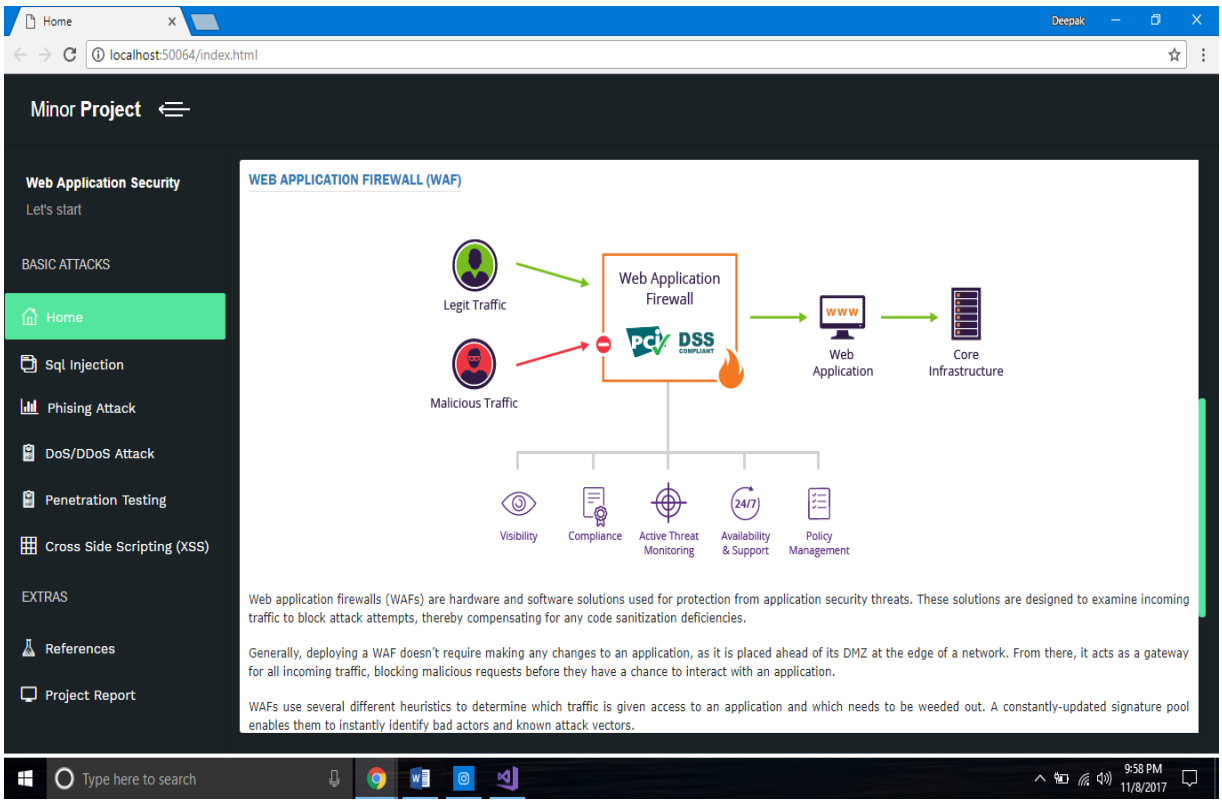
1) **Add a project in Visual Studio**
2) **Prepare the solution for the project.**
3) **Add the necessary configuration files.**
4) **Create Html/ASPX pages from the solution Explorer.**
5) **Design the webpage.**
6) **Logic for the implementation is written in .cs file.**
7) **Create a database in the visual studio in SQL Server Object Explorer.**
8) **Create a connection on the .cs page and write the query to insert the data or to retrieve it from the database.**
9) **Finally set a start page for the project and press F5.**
10) **The project will run in the default browser on localhost i.e. 127.0.0.1 and on a specific port.**
11) **Navigate through the project on chrome through the side navigation bar and the implementation button on some pages.**
12) **Enter the necessary details to enjoy the functionalities.**
13) **For making changes in the front end will not require the debugging to stop, just make the changes and refresh the browser, the changes will be reflected but if the changes are made in the .cs file then we must restart the project because the c sharp code should be compiled.**

SCREEN SHOTS

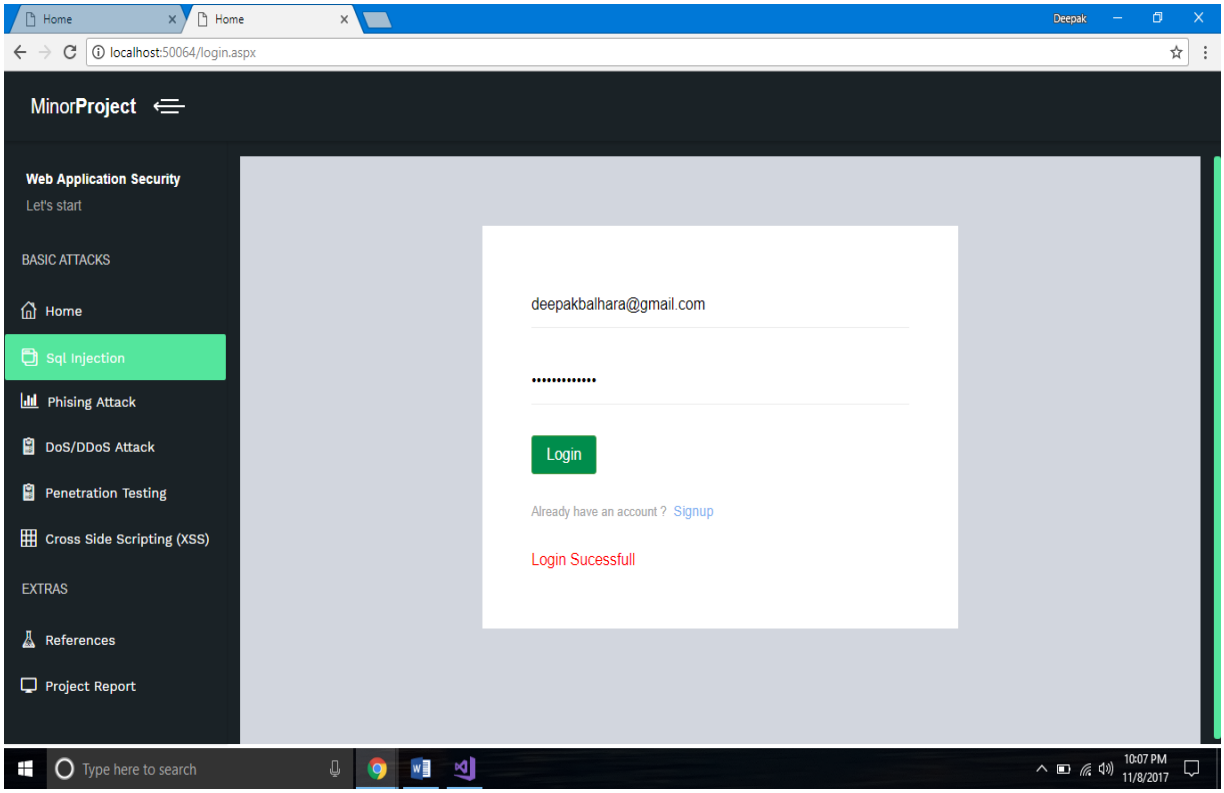
Home Page



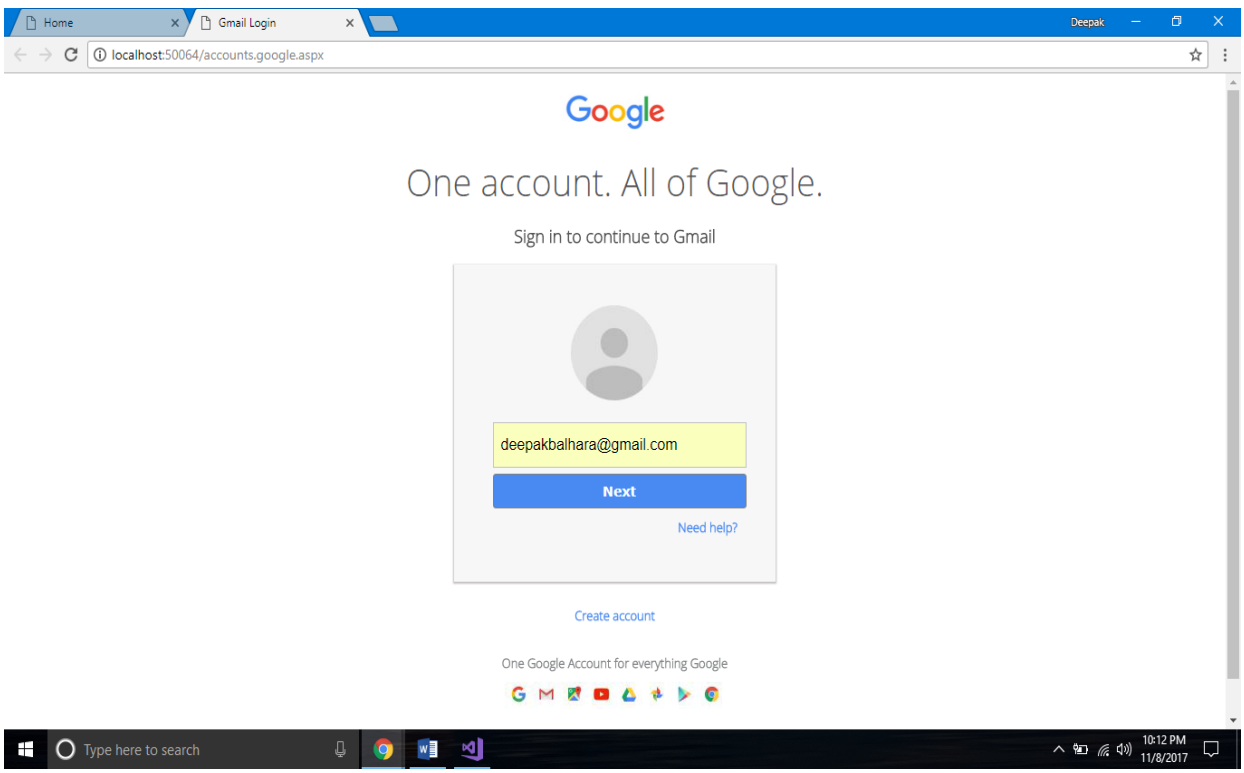
Sql Injection Introduction



Sql Injection Implementation



Phishing Attack Implementation



Cross Side Scripting Implementation