# ETHICAL WEB HACKING

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

**Bachelor of Technology**
**In**
**Information Technology**

Supervisor
Dr. Anju Saha

Submitted by:
Deepak (0**14**16410514)
Gaurav Baisoya (0**57**16410514)

**University School of Information and Communication Technology**
**GGSIPU, Delhi-78**

2014-2018

# CONTENTS

# INTRODUCTION

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 similar to 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
- Loss of reputation of a company

# OBJECTIVE OF 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.

# PROJECT REQUIREMENTS

- IDE :  Visual Studio
- Technology : Asp.Net (C#)
- DBMS : Sql Server
- Operating System : Windows
- Web Browser : Chrome, Mozilla or any Modern Browser

# PROJECT DESCRIPTION

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 into 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.

The website is to be build using Asp.Net, C#, Sql-Server, JavaScript, Bootstrap, Ajax. The website will have several vulnerabilities and following attacks and testing can be 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 the these attacks we will present the code due to which the attack was successful.

# TIMELINE

Phase 1 – Configure all the software’s required.
Phase 2 – Design the database scheme.
Phase 3 – Build a vulnerable website.
Phase 4 – Implementation of famous attacks on the website.
Phase 5 – Visualization of the effects of the attacks.
Phase 6 – Measures to avoid such attacks.
Phase 7 – Documentation.

# FUTURE SCOPE OF THE PROJECT

Daily thousands of websites are being developed and deployed on the web which are not secure and vulnerable to attacks and thus their data can be stolen easily by the hackers.
The project is going to help many web developer's aspirants who are not aware of such attacks and will help them in knowing how they can make their websites more secure and thus preventing the attacks.

# REFERENCES

- Tutorials Point(https://www.tutorialspoint.com).
- The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy
- Google (www.google.com).
- YouTube (https://www.youtube.com)