

NAME - ADITYA RAWAT

ROLL NO - 1022714

SUBJECT - INFORMATION CYBER LAB

Answer 1 \Rightarrow Any flaw in a website that can be exploited by a hacker is called website vulnerabilities. though the website uses many security systems but if hacker utilises manager to find a security breach and break the security window he can gain access to admin panel.

There are many vulnerabilities which would lend a helping hand to hackers

i) XSS Cross site scripting \Rightarrow It is a kind of code injection attack. Basically the malicious code is injected in website and is executed in a browser. Website using user's input with output without any validation and encryption are always prone to XSS. In this attack the browser is target indirectly. When the victim visits infected page the Java script code is delivered to browser and once the code gets executed attacker can access objects.

Sign Aditya

NAME - ADITYA RAWAT

Roll NO - 1022714

ii) ~~Wrong~~ Wrong Security Configuration: Insecure configurations can be components of a web application and can invite great security threats. An attacker can easily enjoy the privilege of the admin if we stick with the default configuration like using default username and password.

iii) SQL Injection \Rightarrow Injection is a security vulnerability that allows an attacker to alter backend SQL statements by manipulating the user supplied data.

Implications \Rightarrow

- i) It can inject malicious content in fields.
- ii) Sensitive data like user name can be read from database.

iv) Insecure Direct Object References \Rightarrow It occurs when a developer exposes a reference to an internal implementation object, such as a file, directory or database key in a URL or as a form parameter.

Implication \Rightarrow

Using this vulnerability, an attacker can gain access to unauthorized internal objects, can modify data or applications.

Sign Aditya