eCore Techno Solutions

eCore Techno Solutions Pvt Ltd

www.eCoreTechnoS.com

HackingTechnologies Powered by eCore

www.HackingTechnologies.com

SCO 62-63, 3rd floor, Opposite Hotel Taj, Sector 17-A, Chandigarh - 160017 India

+91 (172) 461 0064 | +91 (172) 400 9111

www.eCoreTechnoS.com | info@eCoreTechnoS.com

Website Threats

Attack Type	Explanation	Business Impact
Malware	Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.	**Worst anyone can think of. It can lead to complete website hijack with NO Control over it.**
SQL Injection	SQL Injection is a Web attack mechanism used by hackers to steal data from an organization. Hacker can get access to Website and change/delete Website Data.	Your own/clients Sensitive and Confidential Data is at risk. **Legal implications***.
XSS – Cross Site Scripting	Hacker can access your Live/Active session and log in as you to your website.	Website info is at risk – It can even hit your business and its reputation and can even result in **Legal implications***.
CSRF (Cross-Site Request Forgery)	CSRF is an attack which forces an end user to execute unwanted scripts/actions embedded by Hackers. It can then result in gaining illegal access to your credentials (Cross-Site Scripting). If a user is logged into the site and an attacker tricks their browser into making a request to one of these malicious url's, then the script is executed and hacker logs in as the authenticated user.	Website info is at risk – It can even hit your business and its reputation and can even result in **Legal implications***.
Path Traversal	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal.	Website info is at risk – It can even hit your business and its reputation and can even result in **Legal implications***.
Broken Authentication and Session Management	Allows Hackers to hijack user accounts or administrative accounts, authorizations and accountability controls and cause privacy violations. Authentication is a critical aspect of this process, but even solid authentication mechanisms can be undermined by flawed credential management functions, including password change, forgot my password, remember my password, account update etc.	User credentials are hijacked - Hackers can pose as a genuine user, abuse the system and malign your brand.
Insecure Direct Object References	Direct object references expose website or account-specific details, such as account numbers, file names, directories, or database keys, in the URL or other accessible sources. It happens when the web application exposes an internal implementation object to the user. An attacker can modify the internal implementation object in an attempt to abuse the access controls on this object.	Expose Credit card details, Sensitive Website Data. It can even hit your business and its reputation and can even result in **Legal implications***.
Security Misconfiguration	Security mis-configuration, or poorly configured security controls, could allow malicious users to change your website, obtain unauthorized access, compromise files, or perform other unintended actions. Attacker accesses default accounts, unused pages, un-patched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the system.	Expose Organizations Security Weakness /Vulnerabilities. Hacker can do Reconnaissance and get company assets information
Failure to Restrict URL Access	An attacker/Hacker tries to gather sensitive data through a Web browser by requesting specific pages, or data files with Forced Browsing technique. Forced browsing attacks can take place when an attacker is able to correctly guess the URL of or use brute force to access an unprotected page.	Gain illegal access to Sensitive Website Data and even Destroy Website Data files bringing the entire site down.
Invalidated Redirects and Forwards	An attacker uses your Website to redirect the victim to a malicious site. This Vulnerability allows attacker to bypass the login page and get access as an authorized user. An attacker can change the destination address to send visitors to a malicious site that appears to be part of the original location. Phishing schemes often exploit invalidated redirects and forwards.	Hackers can Access Website data as an Authenticated and Authorized User (Can delete website data, affect websites with malicious codes)
Insecure Cryptographic Storage	Usernames, passwords or other personal details, must use strong encryption to secure the data. Insecure cryptographic storage means sensitive data isn't stored securely	Expose Organization personal details such as Usernames, passwords etc. It can even result in trading and/or loss of trade secrets.
Insufficient Transport Layer Protection	Insufficient transport layer protection allows communication to be exposed to un-trusted third-parties, providing an attack vector to compromise a web application and/or steal sensitive information. It is a security weakness caused by applications not taking any measures to protect network traffic.	Hackers Intercept or sniff Website personal data and related information. In case of dedicated web-servers it can even result in hacking of the internal Network
DOS Attack	A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users.	Complete/Partial Server and/or Network Shutdown. Resulting in loss of productivity.

SCO 62-63, 3rd Floor, Sector – 17 A, Chandigarh | 0172-4009111 | 0172-4610064

We would like to draw your kind attention to some provisions of the Information Technology Act that impose stringent liabilities upon organizations **handling sensitive personal data or information**.

Sensitive personal data or information has been defined by the Central Government in exercise of the powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), to include information relating to:

- password
- financial information such as Bank account or credit card or debit card or other payment instrument details
- physical, physiological and mental health condition
- sexual orientation
- medical records and history
- Biometric information
- any detail relating to the above clauses as provided to body corporate for providing service and
- any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise

***Legal implications – Please read below**

Section 43 A	Section 72 A
Compensation for failure to protect data	**Punishment for disclosure of information in breach of lawful contract**
Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.	Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lac rupees, or with both.

Tips

1. Don't leave important ,sensitive, or confidential material lying around the office
2. Always Verify your Credentials
3. Keep your password secret
4. If you print it, go get it right away!
5. Use Google's cached mode to avoid spyware
6. Read error messages and checkboxes
7. Look before you click
8. Just don't Format data, Wipe it!
9. Update your software
10.Protect your PC, Phone, Emails data with backups
11.Use a firewall always
12.Install and update anti-virus software
13.Install and run anti-spyware software
14.Strengthen your web browser security
15. Install the latest OS service pack

Thank you for your business!

Our Portals

www.eCoreTechnoS.com

www.HackingTechnologies.com

www.LearnHackingSecurity.com

SCO 62-63, 3rd Floor, Sector – 17 A, Chandigarh | 0172-4009111 | 0172-4610064