# Chapter 57
# A Resourceful Approach in Security Testing to Protect Electronic Payment System Against Unforeseen Attack

**Rajat Kumar Behera**
*KIIT University, Bhubaneswar, India*

**Abhaya Kumar Sahoo**
*KIIT University, Bhubaneswar, India*

**Ajay Jena**
*KIIT University, Bhubaneswar, India*

## ABSTRACT

*This article describes how electronic payments are financial transactions made over the internet for goods or services. In the digital era, the e-commerce industry has gone beyond the traditional in-store service due to the wide spread of internet-based shopping. Developed countries are greatly relying on e-commerce business and a sizable number of countries have shown concern in regard to the online payment cards such as credit cards, debit cards, e-cash, e-cheques, e-wallets and smart card security. The main downsides are concerns over privacy or a malicious attack and hence safeguard mechanisms are required to protect personal information from falling into the hands of intruders. Before commercializing electronic payment systems (EPS), security tests play a significant role in the software development life cycle to check whether the system is secure and it is safe to use. A resourceful approach covering security policies, secure coding, security attack prevention methodology, security testing tool, security testing metrics, security test case prioritization techniques and a model for effective project management methodology are presented in this article. Early detection and resolution of security weaknesses can be achieved with the authors' proposed approach and would certainly reduce the time, effort and cost of a project. The proposed approach is likely the best-fit implementation of the payment industry, covering channels like B2C (Business to Consumer), C2C (Consumer to Consumer), C2B (Consumer to Business), B2B (Business to Business), People to People (P2P), G2C (Government to Citizen) and C2G (Citizen to Government).*

DOI: 10.4018/978-1-7998-7705-9.ch057

## INTRODUCTION

In current scenario, security of the online payment website is very important because activities like online banking, utility bill payment and e-commerce etc. are made through the internet, which demands security. Singh et al. (2014) past history like Citigroup, Sony, ADP (Automatic Data Processing) and others suffered from major breaches in the year 2012 and in the recent times, security has taken a major role.

The most common types of attacks that a malicious user can use to exploit EPS security are: SQL injection attack (SQLI), XSS (Cross Site Scripting) attack, URL manipulation, Brute Force attack (BF), Denial of Service (DoS)/Distributed Denial of Service (DDoS), Identity Spoofing, Malware, Malvertising, Session hijacking (SH), etc.

Laverty et al. (2009) standard network security practices attempt to avert unauthorized access to network resources or interrupt the content of network messages before a destructive user has the option to do any potential damage. Still, easy accessibility of internet has led to increase in new web security attack. MacDonald et al. (2009) Intrusion-detection systems and firewalls do not defend web based system from SQL injection attack and Cross Site Scripting. WASC (2005) as per Web Application Security Consortium, XSS, SQLI and DoS are the most frequently attacked the web application. As per 2016 statistics, % wise attack is presented in Table 1 (cyber attack statistics, 2017).

*Table 1. Percentage wise attack on EPS*

| Sr# | Attack Type | Attack Percentage |
|---|---|---|
| 1 | Unknown | 33.1 |
| 2 | Account Hacking | 15.1 |
| 3 | Targeted Attack | 11.6 |
| 4 | DOS/DDOS | 11.3 |
| 5 | SQLI | 8.4 |
| 6 | Malware | 8.0 |
| 7 | Defacement | 4.9 |
| 8 | Others | 7.6 |

2016 Cyber Attacks Statistics. (2017) within industry, e-Commerce was ranked at number one in 2015, slides to number four in 2016 and soar to number two till 2017 March. March 2017 cyber-attack statistics. (2017) as per the available statistics, malware was on top with 26.2%, followed by unknown with 26.1% till March 2017.

The current trend of attack methods targeting EPS cannot be prevented by conventional security actions like network and host layer security. EPS requires a strapping resistance to resist every malicious attack. Failure to build such defense system can cause key damages to the business in terms of legal regulations, identity theft, loss of consumer confidence, financial fraud, etc. An approach to build such defense system is proposed and the payment industries can adopt the proposed approaches to build the robust system.