**Magecart attack**

Magecart is a data skimming type. Attackers use the skimming method to capture the sensitive information of the target from the online payment forms like credit card numbers, debit card numbers, email id, passwords, etc. To steal the information of credit cards, hackers enter harmful code into the website. On the checkout page, the users enter the card information, and the hackers capture it. Shopping cards are really attractive for hackers because it is used to collect the customer's payment information.

**Working of Magecart**

Magecart is a type of data skimming attack which follows a well-established pattern. For their success, they have to achieve the following things:

**Gain access to the website**

The hacker can place skimming code and gain access to the website using two ways. The first one is hackers can either break our server or our infrastructure and place skimming code. The second one is hackers can go to one of our third-party vendors, and when the user calls it in their browser, they will add a malicious script on our website.

**Skim information from a form**

Groups can capture the data in a lot of different ways, but skimming code is always better because it is a type of [JavaScript](https://www.javatpoint.com/javascript-tutorial) that is used to listen to the personal information of users and collect it. We know the hacking approach in which hackers monitor all the keypresses on a page or observe the specific part of a webform and intercept the input like credit card or debit card information and CVV field. Generally, hackers use the other code to hide the malicious code and to avoid detection.

**Send information back to server**

In the whole process, this part is very simple. The game will be over when the attackers gain access to our website and get sensitive data about users which they want. Now they can use the end user's browsers and send the information to any location on the Internet.

**Prevention from Magecart attack**

Preventing access provides the best defense against Magecart. Online companies need a system that can intercept all APT calls made by our website to the browser and block access to sensitive data that we have not authorized previously. Due to this, we can prevent the access of customer's sensitive information from non-critical third-party scripts or any malicious scripts. When the attacker tries to access sensitive information, this system will monitor it and alert the companies.

The attacks against websites continue upticks. The attacker takes the payment information from customers, just like the Magecart attacks that are used to steal sensitive information directly from the customers or end-users. There is a sophisticated botnet attack that uses the data found on other websites and leverages stolen credit card information and credentials of users to commit fraud. Now this time, many brands think about the attacks and provide end-to-end web security. By using this security, the backend infrastructure can be protected, Magecart attacks in the browser can be mitigated, and sophisticated botnet attacks can be stooped.