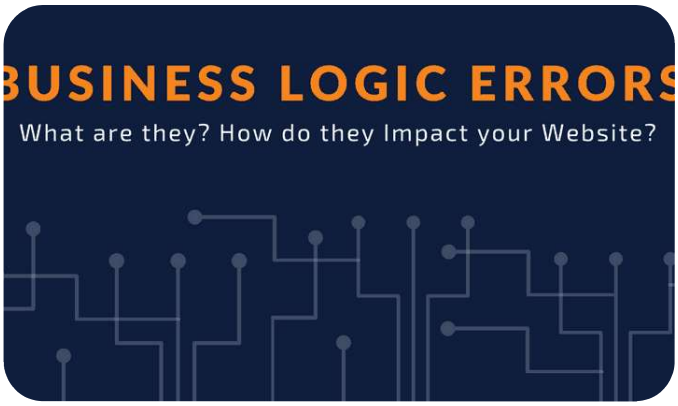
Knowledge Base

Business Logic Errors: All You Need To Know



Updated on: March 29, 2020


Ananda Krishna

4 mins read

Business logic or application login is the core logic of your website. Business logic defines how data can be created, stored and modified. It is the features that are specific to your business and usually developed for you.

This Blog Includes [show]

For example, e-commerce websites allow visitors to add products to a shopping cart, specify the quantity, delivery address, and payment information. **The business logic of the e-commerce store when you checkout can be the following:**

- Forms which first asks for the shipping address, then for the billing address

- Next page will contain the payment details,
- Payment is processed through a payment gateway
- On Successful transaction a page will show congratulations

There will be also business rules of the website:

- When an item is added more than once from a product page, the quantity of the product should be increased in the cart.
- Information provided by the user like visitor's address, email address, and credit card information must follow their respective formats.
- Integration with Payment Gateway to process the payment and receive confirmation of payment

Now that we've talked about business logic and business rules, let us talk about Business Logic Errors.

Example of Business Logic Errors

Business Logic Errors are ways of using the legitimate processing flow of an application in a way that results in a negative consequence to the organization. There are various cases where these errors can result in enormous business losses. **A few notable test cases are mentioned below:**

1. **Business logic flaw in blogging:** A blogging portal was designed to ensure that initial posts do not contain profanity based on a list that the post is compared against. If a word on the profanity list is found, the blog post submission is not accepted. But, once a submission has been accepted, the user can edit the article and update its contents. When saving this edited article, the blog post is not checked against the profanity list. As a result, the original business rule has been bypassed and posts can contain profanity
2. **Exploiting an e-commerce store:** A broken session management can be extremely harmful, in a particular scenario when an attacker is checking out of

cart, he can inject lower costs then the actual calculated by the application logic. In such scenarios attacker causes a lot of damage to the application.

3. **The loyalty program hack:** In another typical scenario, if a loyalty program is in existence with purchases, as soon as the attacker makes a purchase the points get added to their account but if he cancels the purchase the points does not get deducted.

Is my OpenCart, Magento or WordPress Website Vulnerable to Business Login Errors?

Yes, most probably. While CMSs like OpenCart, Magento & WordPress are inherently secure nowadays, the plugins & themes may contain vulnerabilities putting your website at risk.

A vulnerability found in a single plugin or theme can result in thousands of websites being vulnerable. The reason is simple: a plugin is written with general scenarios in mind and some business rules may be missing or not applicable for your website.

We commonly find vulnerabilities in custom code written on top of your OpenCart (vQmod/OCMOD), Magento (local extensions) or WordPress (Plugins & Child Themes) websites.

Consequences of Business Logic Errors

We have seen many cases where companies end up losing important customer data in cyber thefts. The consequences vary depending on the nature of the web application. Due to existence of flaws in the business logic, hackers have managed to buy products from e-commerce stores at lower prices than originally they were listed for.

- User Privilege Escalation
- Access to Unauthorized Information

- Identity Extraction
- Overwrite records in the Database
- Manipulating Shopping Cart & Payment Systems
- Getting More Discounts
- Extending Subscription
- Downloading Data of other Users
- Bypass Security Restrictions
- Circumvent Captcha Codes
- Denial of Service

Why are Business Logic errors difficult to find?

As the name suggests, Business Logic Errors are logical errors requiring sophisticated testing mechanisms to uncover these issues. They are difficult to uncover because:

- **Security Scanners can not identify them.** Security Scanners find known security vulnerabilities and Weak Development Practices, however they may not understand the business rules while testing
- **Intrusion Detection Systems and Web Application Firewalls cannot detect Business Logic Errors.** These systems are designed to identify known malicious attacks like SQLi, XSS, Bad Bots. However, business logic errors are logic leaks and legitimate looking. They may not be detected by WAFs in some cases.
- **Application Specific Knowledge is Required** as what may be a security flaw in one application may not be in another. The business rules vary with the web application.

How can Astra Help Your Website be Secure

In this world of ever increasing threats, it is critical to secure your web application from hackers. Astra offers a comprehensive Vulnerability Assessment & Penetration Testing (VAPT) security scan with 120+ active tests to find any application weaknesses, technical flaws, or vulnerabilities including **Business Logic Errors**. We adhere to the OWASP Guidelines for Business Logic Testing.

If you are an online business handling payments, storing sensitive information or facing targeted hacks get a security scan. If you have any questions, our experts will be happy to assist you in this journey of web security. Contact us.

Tags: Web Security

Share this...

Ananda Krishna

Ananda Krishna is the co-founder & CTO of Astra Security, a SaaS suite that secures businesses from cyber threats. He has been acknowledged by the Indian Navy, Microsoft, United Airlines, etc. for finding critical security vulnerabilities in their systems. Winner of the Best Security Product at Global Conference on Cyberspace 2017 (awarded by Narendra Modi, Prime Minister of India) & French Tech Ticket, Paris (awarded by François

Hollande, former President of France). At Astra he's building an intelligent security ecosystem - web application firewall (WAF), malware detection & analysis, large scale SaaS applications, APIs & more. He's actively involved in the cybersecurity community and shared his knowledge at various forums & invited talks.

5 years ago

[...] due to some vulnerability in these plug-ins hackers can target your shop. The following types of business logic hacks are direct cause of such [...]

0 Reply

Related Articles

Knowledge Base

7 Web Security Mistakes to Avoid (And How to Do So)

Knowledge Base

Choosing a SaaS Product for your Business? 4 Things To Check Before Buying

Knowledge Base

Blockchain Security Issues – A Complete Guide

Psst! Hi there. We're Astra.

We make security simple and hassle-free for thousands of websites & businesses worldwide.

See our glowing reviews on

Trustpilot Capterra

+ Pentest

+ Website Protection

+ Company

+ Resources

Made with ❤️ in

Privacy Policy | **Terms of Service** | **Report a vulnerability**