ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/tanmaya-gaur/328

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 2 & Iss: 1

Research Article

Enterprise Web Application Security and Its Overlap with Fraud Controls: Understanding the Intersections and Divergences

Tanmaya Gaur*

Tanmaya Gaur, Bachelor of Engineering (Electronics and Telecommunication), Birla Institute of Applied Sciences, USA

Citation: Gaur T. Enterprise Web Application Security and Its Overlap with Fraud Controls: Understanding the Intersections and Divergences. *J Artif Intell Mach Learn & Data Sci 2024*, 2(1), 1446-1451. DOI: doi.org/10.51219/JAIMLD/tanmaya-gaur/328

Received: 03 February, 2024; **Accepted:** 26 February, 2024; **Published:** 28 February, 2024

***Corresponding author:** Tanmaya Gaur, Bachelor of Engineering (Electronics and Telecommunication), Birla Institute of Applied Sciences, USA, E-mail: tanmay.gaur@gmail.com

ABSTRACT

This paper discusses modern security practices for web applications developed by enterprises and common attack vectors. This paper will discuss the common attack vectors that are implemented to protect web resources. Fraud is often confused with security which this manuscript will untangle. This paper will go over some of the fraud attack vectors and discuss how they overlap or diverge from security practices for webapps. The goal is not to be an exhaustive manuscript in security and fraud practices but to present a point of view on how to approach these concerns in a real-world environment. The paper will dive into the essential security measures, such as encryption, authentication and access control, without going into significant detail but to try and highlights the distinctions between security and fraud prevention for such controls. The paper will use telecom attach vectors as example to showcase the distinction. The paper emphasizes the importance of taking a holistic approach to protect an enterprise's assets, ensuring confidentiality, integrity and availability of data while preventing fraudulent activities.

Keywords: Web Development, Security, Architecture, Fraud, Enterprise

1. Introduction

In the digital age, enterprise web applications are integral to the operations of organizations. These applications facilitate a range of activities, from data management to customer service, making them prime targets for security breaches and fraud.

Web application security refers to the strategies implemented for hardening websites, applications and APIs against security attacks. The ultimate aim is keeping web applications and its backing dependencies functioning smoothly and securely, protecting business from threats like cyber vandalism, data breach, unethical competition and other negative consequences. The global nature of the Internet exposes web applications and APIs to attacks from many locations and various levels of scale and complexity. As such, web application security encompasses a variety of strategies and covers many parts of the software supply chain. A 2023 recent study estimated cyber-attack losses for US Companies at around 207 billion which would make it roughly .8 to 1 percent of total U.S. GDP.

Apart from threats from bad actors exploiting security weaknesses, Fraud continues to be a completely different adversary for enterprises. A report by the Association of Certified Fraud Examiners revealed that organizations lose roughly 5% of their annual revenues to fraud. Globally in 2024, this translates to $4.7 trillion in losses.

So how is fraud and security related? Fraudsters can at times be taking advantage of security vulnerabilities in an enterprise's software to perpetuate fraudulent activities. That however is not always be the case. Quite often, this corruption is carried out by individuals or groups with legitimate access to data and underlying resources. As such, security protection alone is not enough to protect against Fraud.

This paper will explore common attack vectors and strategies employed to protect against security and fraud and try to untangle overlaps and divergences. We will then take the example of a telecom CRM and see how these concepts apply to a real-world enterprise scenario.

2. Security

Security in the context of web applications refers to the measures and protocols put in place to protect data, systems and networks from unauthorized access, attacks and breaches. This encompasses a wide range of practices, including encryption, authentication, access control and regular security assessments. The primary goal is to ensure the confidentiality, integrity and availability of data and services.

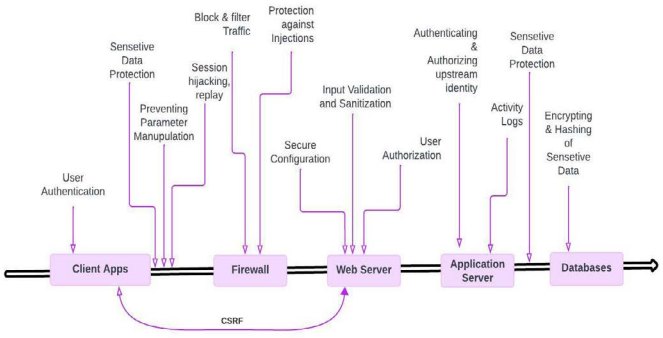

Figure 1 Sample web application security architecture

The next section will discuss the factors contributing to the significant increase in cyber-attack threats. Security Attack vectors and strategies used to secure against these cyber-attacks. In cybersecurity, an attack vector is a method of achieving unauthorized network access to launch a cyber-attack. Attack vectors allow bad actors to exploit system vulnerabilities and gain access to sensitive data, personally identifiable information (PII) and other valuable information accessible after a data breach. The subsequent section will discuss web application attack vectors and mitigation strategies.

2.1. Why are cyber-attacks a problem

In recent years, we keep hearing of high-profile cyber-attacks including ransom ware attacks against organizations. There are quite a few reasons cyber-attacks have become a prevalent problem for enterprises. Recent studies claim cyberattacks have increased up to 30% quarter over quarter between Q1 and Q2 of 2024. Below are some common reasons fuelling this increase.

- **Global Digitization:** As more and more processes, practices and real-world interactions digitize, the surface area prone to cyber-attacks is increasing. Also, the amount of exposure with cyber-attacks is increasing as well.
- **Sophisticated techniques:** Modern increases in technology, such as AI, ML, IoT amongst other things is opening the doors for better and powerful methodologies as well as exploiting previously unexploitable attack vectors.
- **Economic motivation:** This is often the driving factor, especially for attack vectors like Phishing and Ransomware which we will talk about in subsequent section
- **Geo-politics:** Not just economic, some recent high-profile cyber-attacks have been driven due to political tensions between nations or groups.
- **Work-from-home:** This may be a controversial topic at many organizations. Rise in work from home has opened door to new access points and attack vectors often exposed by bad actors. This has also led to a whole new suite of security focused products to solve for niche use-cases.
- **Lack of Security Awareness:** This overlaps with the economic motivations. Often a lack of awareness provides easy opportunities for bad actors to make quick money. Some recent attacks were not targeting the technology but instead focused on social engineering and phishing to gain access.
- **Competitive Advantages:** The repercussions of cyber-attacks can be far-reaching beyond just financials and can include reputational damage and compromised sensitive data used for malicious motives. As such, there can also be non-economic drivers.

2.2. Top security attack prevention methodologies

Before we dive into specificities with web applications, let's take a moment to go over common prevention methodologies.

- **Security Posture:** Significant investment into overall security posture across infrastructure and access controls like firewall protections and software systems like updates and patching vulnerabilities.
- **Investments in Employees:** Educating employees about the latest cyber threats and tactics and fostering a security alert culture.
- **Advanced Security Methods:** Capabilities like browser sandboxing and implementation of targeted access controls.
- **Active Security Testing:** Conducting regular vulnerability assessments and penetration testing and ensuring remediation is high priority across the enterprise.
- **Zero Trust Architecture:** Practices by top hyperscalers like google, amazon, this relies on Implementing strict authentication and authorization for network resources at every tier.
- **Backups and Disaster recovery strategies:** Having a comprehensive incident and disaster recovery response strategy.
- **Network Segmentation:** This is a modern approach practiced at enterprises. It is critical to isolate critical systems to limit attacks even if a portion of the enterprise gets compromised.
- **Third Party Risk management:** Being secure does not apply to ensuring and validating your own systems but ensuring all third-party integrations are also compliant with strict security practices,
- **Access control:** In addition to network and data segmentation, it is essential to restrict data and system access. This often requires building strong authentication and authorization policies.
- **Data Encryption:** While seeming like a minor callout, Strong data encryption practices at rest and in transit are strong deterrents against major attack vectors.

2.3. Major Cyber-attack types

Most cyberattacks can be categorized under broad buckets, below are some major attack types

- Malware or malicious refers to harmful software like viruses, worms and trojan horses. which infiltrate, damage or disrupt computer systems, steal sensitive data and may allow hackers to gain unauthorized access to an enterprises' network.
- Ransomware is a specific type of malware that encrypts a victim's data, rendering it inaccessible until a ransom is paid. These attacks have been on the rise and not just against large enterprises but also against smaller school districts, hospitals etc.
- Phishing is a specific social engineering attack vector where a malicious emails, text or network links tricks and compromises users. This information gained is subsequently used for fraud, identity theft or gaining unauthorized access to an enterprises' systems.
- DDoS or distributed denial-of-service attack is a malicious attempt to overwhelm a target's infrastructure by flooding it with traffic. The goal is to disrupt the normal traffic to a targeted server or service.

2.4. Common Security Attack Vectors and Strategies for web applications

Listed below are common attack vectors employed against web applications and high-level strategies that can be employed to safeguard against them. The protection strategies that work best depends on multiple other factors depending on the enterprise and the application. It would be remiss to not highlight the great work done by The Open Worldwide Application Security Project (OWASP), which is a nonprofit foundation that works to improve the security of software. The OWASP top 10 is always a great resource to keep track of new and emerging threats in this area.

- Cross-Site Scripting (XSS) attacks are a type of injection attack, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. For an XSS attack to be successful, an attacker needs to insert and execute malicious content in a webpage. Thus, all variables in a web application needs to be protected to prevent XSS style attacks. Key safeguards for teams to focus on include ensuring HTML sanitization and output encoding and having a restrictive content security policy in place. Most modern firewalls also provide security mechanisms against XSS.
- Cross-Site Request Forgery (CSRF) is an attack that forces an application user execute unwanted actions on a web application in which they're currently authenticated. Generally, accompanies with social engineering vector (such as a malicious web link via email), an attacker tricks the users into executing actions of the attacker's choosing. Synchronizer tokens and signed double submit cookies are two well-known prevention methods.
- Injection Attacks is an attacker's attempt to send data to an application in a way that will change the meaning of commands being sent to an interpreter. For example, the most common example is SQL injection, where an attacker sends "101 OR 1=1" instead of just "101". Besides SQL injection, attackers can inject commands or code to execute arbitrary actions on the server. Traditionally, input validation has been the preferred approach for handling untrusted data. While input validation is important, it is not a foolproof solution against injection attacks. It's better to also use escaping, a technique used to ensure that characters are treated as data, not as characters.
- **Broken Access controls:** Access control enforces policy making sure users cannot perform actions not allowed by their permissions. If broken, this can lead to unauthorized information disclosure, modification or destruction of all data or performing a business function outside the user's limits. Ensuring a secure access control methodology and keeping it up to date is crucial to prevent such attacks. Frameworks like oAuth2 and proof of possession tokens, if implemented properly can provide good starting strategies for most enterprises.
- Sensitive Data Exposure also known as Cryptographic Failures focuses on failures when cryptographic algorithms, protocols or key management practices are used incorrectly or implemented poorly, leading to exposure of sensitive data. While there is no single protection, ensuring good data protection and processing practices, encryptions with strong and up to date algorithms etc. are measures which help. OWASP keeps its data up to date with emerging sub-vectors and methodologies in this space.
- Security Misconfigurations refers to Vulnerable configurations which expose sensitive information and provide unauthorized access, often due to default credentials, open ports or unnecessary services. Secure installation and regular hardening processes and segmented architecture practices are recommended for all applications to prevent against this vector.
- Vulnerable and Outdated Components is a known issue that refers to when open-source or proprietary code used by an application contains software vulnerabilities or is no longer maintained. A key element here apart from end-of-life software is Zero-day vulnerabilities that do pop up from time to time. Keeping your systems up to date with regular updates and patching to reduce the risk of vulnerable and outdated components is crucial.
- Broken Authentication which somewhat overlaps with the broken access control once exploited, refers to gaps in the way applications confirm of the user's identity, authentication and apply session management. Multi-factor authentication is a key area to focus on, even if you have strong authentication controls. This approach also helps against automated credential stuffing, brute force and stolen credential reuse
- Software and Data Integrity Failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries or modules from untrusted sources, repositories and content delivery networks (CDNs). An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations. Hygienic practices like using only trusted repositories or validating digital signatures in CI/CD pipelines is crucial in mitigating such attack vectors.

- Security logging and monitoring failures are security vulnerabilities that can occur when a system or application fails to log or monitor security events properly. This can allow attackers to gain unauthorized access to systems and data without detection. The key to protecting against security logging and monitoring failures is to log all critical security events and monitor them for suspicious activity. Apart from ensuring a comprehensive logging strategy, it is also paramount to Securely store and protect log files to ensure their reliability, including measures to prevent tampering and unauthorized access.
- Server-Side Request Forgery (SSRF) is an attack vector where Web applications are made to make requests to internal resources or external services, potentially exposing sensitive data or targeting other servers. SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN or another type of network access control list (ACL).
- Some other well-known callouts which no longer make the OWASP top 10 but are well known attack vectors include XML External Entity (XXE) Attacks which targets Vulnerabilities in XML data processing allow attackers to manipulate input for purposes such as accessing local files or initiating denial-of-service attacks. Clickjacking which Deceiving users into unintended actions by tricking them into clicking on something other than what they perceive and Brute Force Attacks, where Attackers use brute force methods to guess usernames and passwords, gaining unauthorized access to web applications. There are many other attack vectors like Server-Side Template Injection, Directory Traversal, Insecure Deserialization and File Upload Vulnerabilities which all application development teams need to stay aware of.

3. Fraud

Fraud involves deceitful practices aimed at gaining an unfair advantage or causing financial loss. In the realm of web applications, fraud manifests in various forms, such as identity theft, transaction fraud and phishing attacks. While security measures aim to prevent unauthorized access and breaches, fraud controls are designed to detect and prevent fraudulent activities that exploit vulnerabilities within the system.

3.1. Why is Fraud a problem

As mentioned earlier, based on recent studies, fraud on an average, accounts for losses to the tune of 5% of an organization's annual revenue. Shift in various technologies and processes post pandemic has only served to magnify the risks associated with fraud.

3.2. Top Fraud attack prevention methodologies

Unlike Security, fraud prevention does not have a specific cheat-sheet. Most enterprises are now setting up Fraud Management practices whose sole focus is to drive comprehensive approaches to detecting, preventing, monitoring and managing fraud for the organization.

- A recommended approach for fraud management is leveraging centralized system that integrates various data sources, such as user, account and device information, analytics and real-time monitoring, to identify potentially fraudulent activities, corruption and criminal behaviors.
- It is important to understand and solve for the fraud attack vectors based on specificities of the businesses. As an example, financial institutions like banks and insurances rely heavily on anomaly detection in data such as unusual spending patterns or charges from a foreign country which trigger alerts or denials. Ecommerce enterprises on the other hand, can rely on suspicious activities such as high-value purchases from newly created accounts.
- Most fraud solutions are multi-layered and include a combination of authentication, authorization-based access control of end users, anomaly detection of the user's activities etc. to determine and flag fraudulent activities. Modern AI practices are widely used in fraud and risk management to look at large sets of data available and flag for fraud.

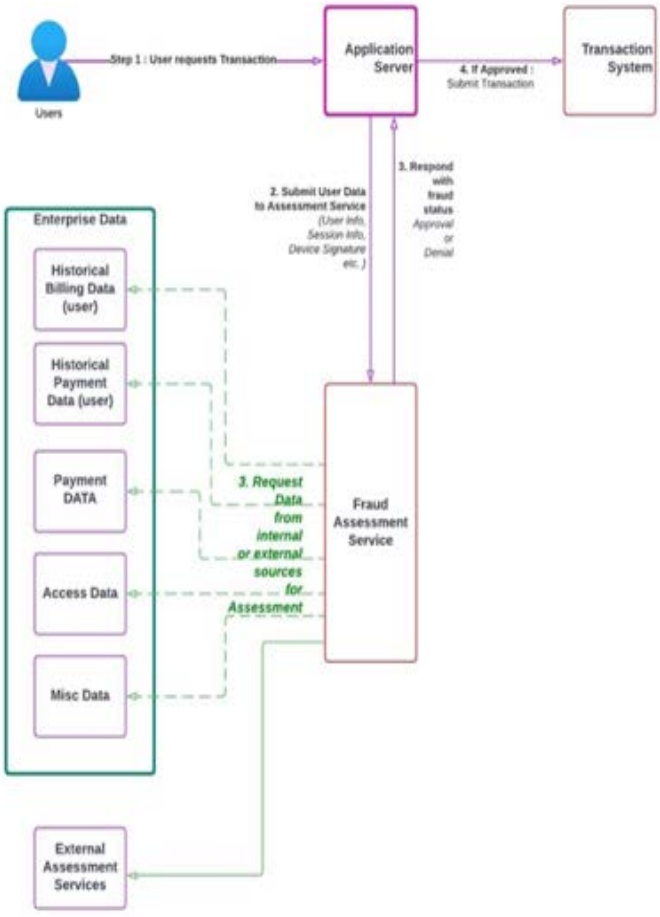

Figure 2 Sample Fraud Assessment Service

3.3. Major Fraud vectors and remediations

While not as structured and methodical as the OWASP list, fraud can generally be categorized into few major buckets.

- Transaction Fraud occurs when unauthorized purchases are made using stolen payment information, leading to chargebacks. This type of fraud is highly common for eCommerce platforms, where these Chargebacks not only result in lost revenue but also incur additional fees and can cause harm to a business's reputation. To prevent against this vector, Companies have started using AI/ML models to analyze and flag potentially fraudulent activity. There

may be additional protection in the forms of additional user challenges like MFA for higher risk activities.

- Account Takeover are a form of identity theft where fraudsters gain unauthorized access to a legitimate user's account, often executed through security vectors discussed in the earlier section. Most common vectors exploited include phishing, credential stuffing or malware injection to harvest login details. Once these bad actors have access to the account, they can place unauthorized transactions or perform malicious account activity. These attacks, just like transaction fraud, lead to both financial losses as well as reputational, as they erode customer trust.
- Fake Accounts from Stolen IDs are often used to exploit businesses, especially financial institutions. These stolen IDs may be procured from earlier security data breaches. There is also a new vector where real data is combined with some fake data to create a so called 'synthetic ID'. Effective prevention relies on systems that can cross-check user-provided information against various data sources, including social signals, digital footprints and device intelligence. Machine learning models are commonly used to identify and flag transactions for review.
- Multi-Accounting is when an individual or group creates multiple accounts to exploit bonuses, promotions or referral programs, common in industries like gaming, online lending and ecommerce, where welcome bonuses and promotional offers are used to attract new customers. Fraudsters take advantage of these programs by creating multiple accounts using different identities or fake credentials to claim offers multiple times, leading to revenue losses and distorted customer data. Like other vectors, AI Models are used to detect this fraud, often by cross-referencing request information such as IP Addresses and payment details. Modern vendor solutions have crept up which create large databases of activity across multiple organizations to analyze and do this at a larger scale to identify fraud rings.

4. Security and Fraud in a Telecom organization

Telcos have some unique characteristics which make them prime targets for both security and fraud. Given the rapid shift to higher levels of digitization means they have much more data to protect. This digitization does not look to be slowing down, as advances in technologies like 5G, IoT, cloud, AI and edge computing, are paving newer business models and services around the telecommunications industry. This puts Telecom organizations at a focal point of how customers interact with these businesses and share, receive data and services. Telcos also have an important place in ensuring connectivity, so much so, that Federal Communications Commission has setup a division known as Cybersecurity and Communications Reliability Division (CCR) helps ensure that the nation's communications networks are reliable and secure so that the public can communicate, especially during emergencies.

Telcos are also prime targets for bad actors given its focal point in ability to deliver ransomware or malicious software for tasks like bitcoin mining or its access to PII and PCI information. Another large fraud vector is due to Telco provided capabilities like SMS services being used as an authentication factor by end customers to their other businesses and their services. This vector, as well as social engineering attack vectors lead to telcos having a central place in protecting their customers. Let's look at some common security and fraud vectors impacting telcos, especially via their web applications.

4.1. Security Vectors impacting Telcos

While most Cyber security attack vectors for telcos follow the OWASP list, below few are more concerning compared to other industries, especially in the CRM application space

- Phishing attacks are commonly used by bac actors to steal data. This involves sending fake links via methods like emails to trick users into giving away their login details. This allows bac actors access sensitive information.
- Malware is another threat. Bac actors try to compromise telecom systems through infected files or websites. Once inside, this attack vector can steal or damage data.
- Telcos have been consistently exploited via data breaches, within their own systems or at times, third party vendors like payment processors.
- All the security remediations mentioned in the earlier section apply to Telcos, who are starting to also place heavy emphasis on both educating their end customers as well as employees against social engineering attack vectors. AI is being used to find and stop threats faster.
- Telcos also see significant impact from insider bad actors. Attack vectors like credential misuse are more prevalent than in other industries.
- While not directly web application vectors, Telecom organizations are seeing large impact from other telco specific attack vectors, like infected UE, swapped radio networks or infected network nodes and other covert channels.

4.2. Fraud Vectors impacting Telcos

Listed below are some specificities to consider for Telco fraud vectors exploited through external or CRM web applications

- Account Takeover in Telcos can result in transactions like Sim swap or identity thefts, this is because the telco connections and capabilities like SMS are often used as an authentication security methods for financial and other institutions including bitcoin wallets.
- Often impersonation and lack of systematic access control protocols are exploited by bad actors calling customer support employees to initiate transaction or account takeover fraud. These attacks are not always rooted in technology, Social Engineering attacks engineered for customer support or end customers are also on the rise.
- SMS or other means of Phishing are often employed by bad actors to maliciously initiate account takeovers.
- Insider threat is just as severe with bad actors often colluding with company insiders to initiate fraud attacks.

5. Conclusion

The intersection of enterprise web application security and fraud controls underscores the necessity of a holistic approach to safeguarding digital assets. The overlap between these two domains highlights the importance of implementing comprehensive strategies that address both security and fraud prevention. By adopting robust security protocols, such as encryption, authentication and access control and integrating

fraud detection mechanisms organizations can effectively mitigate risks and protect their web applications. Additionally, staying vigilant against emerging threats and continuously updating security and fraud prevention measures are crucial for maintaining the trust of users and stakeholders. A good security posture however cannot be the only deterrent against fraud and needs additional safeguards. Ultimately, a well-rounded approach to web application security and fraud controls ensures the confidentiality, integrity and availability of data while preventing fraudulent activities.

References

1. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
2. https://seon.io/resources/the-101-guide-to-enterprise-fraud-management/#:~:text=Enterprise%20Fraud%20Management%20(EFM)%20refers,fraud%20across%20their%20entire%20operations.
3. https://www.cloudflare.com/learning/security/what-is-web-application-security/
4. https://thehill.com/opinion/cybersecurity/4641199-cyberattack-businesses-money-loss-malicious-cybersecurity/
5. https://www.gradwell.com/guides/a-guide-to-telecoms-fraud/
6. https://larbi-ouiyzme.medium.com/a-comprehensive-guide-to-web-application-attacks-b74d0f2cc577
7. https://owasp.org/www-project-top-ten/
8. https://foresite.com/blog/owasp-top-10-vulnerable-and-outdated-components/
9. https://www.securityjourney.com/post/owasp-top-10-security-logging-and-monitoring-failures-explained
10. https://ashwinisp.medium.com/introduction-to-security-architecture-review-20939ce80467