Castellum Labs

WHITE PAPER 2021

App Security... Still the Achilles Heel !

A CISOs world of concern, worry and planning is wide ranging and spans various portions and sections of IT infrastructure and its usage. From securing periphery to changing user habits to ever releasing patches, it is a never ending world of challenges and daily rigors.

Following are some of the key security priorities as they are generally defined and followed in organizations. Mostly in that order.

- Security policy formulations and adoptions
- Peripheral security technology structure and pieces
- Endpoint security and threat protections
- Exploits and vulnerability detections
- Patching and upgrades for security
- Web infrastructure security
- Host and storage security management
- Identity and its life-cycle management
- User behavior and internal threat management
- Data security for data in motion and data at rest
- Application security

In quite a many of my recent discussions and interactions, I discovered that in quite a many organizations, the aspect of security, which is largely neglected and has least security focus or concern is, 'Application'. 'Applications' and 'its security' are still at the tail end of the pecking order of security concern in organizations.

For most of the organization application security still means, conducting regular vulnerability detection and penetration testing, to identify potential issues which might be there. And, then, come up with an action plan to plug the gaps, which are detected by such a test. Even this exercise, is only a cursory routine towards application security, given the fact that most of these vulnerability and pen tests are conducted using standard off the shelf tools available in the market. Most of these vulnerability and pen testing engagements do not have wherewithal of genuine security experts spending time on designing the testing and analyzing the results, and, hence they are mostly rendered an exercise in vain.

If one starts thinking, 'why is this space left largely uncared for or else is left to routine process' by security owners in the organization, following are some of the reasons, which come to mind.

- Applications are perceived to be behind a layer of security walls, and hence, not that exposed to threats
- Application security is something which has to be start at the time of software engineering or software adoption, hence, it has much longer time to realization and recognition
- Application security is complex, because it is not driven or monitored by straight observation of communication or transactional flows or events
- Most of the application security does not entail the adoption of new technology or new software solution, and hence, is not on the forefront of budgetary planning
- Application security is less sexy as compared to some of the other newly coined or adopted trendy security areas such as security analytic of threat intelligence, etc.

If one comes to think about applications and their security, or lack thereof, it probably is one of the most critical areas of security operations and management for an organization. An organization can never adopt a proper security posture if it does not adopt thorough and thought through approach to securing its applications all across the board.

One can protect its periphery or hosts or users identities as much as one wants, but, without a mature approach to its application security, one would always be vulnerable to threats and compromises of worst kind !

After all, applications contain the most important assets of the organization, the information about their business.

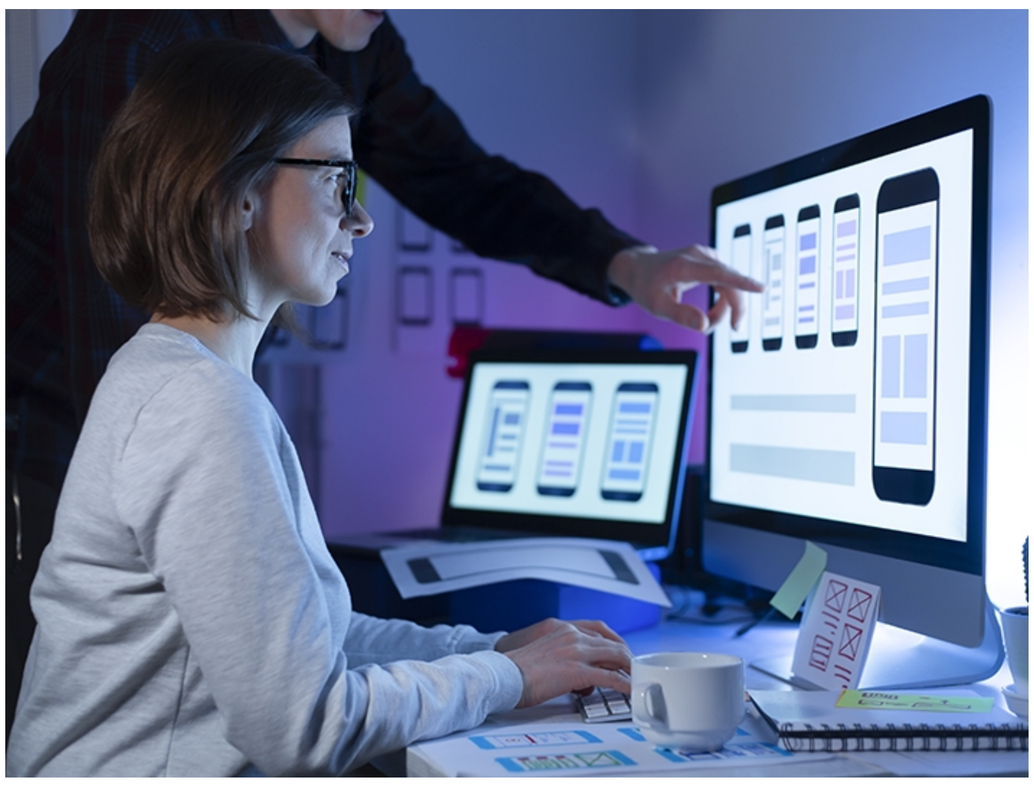
Though a lot of application security software and solutions options are available in the industry, I came up with following list of key concern areas of application security.

Castellum Labs

WHITE PAPER 2021

Design for it

Application security is not only about secure coding or protecting application infrastructure. Genuine application security starts with design of application to be secure. Most of the major security issues are introduced in the application software during the design phase. And, security design of application is different than general software design. So, please spend money on hiring a security expert who can help you design security in applications.



Commonality and Standardization of Security Modules

On a proper inspection, one would find that different applications within the same organization, have completely different approaches to security modules of applications, such as authentication module or authorization module. A proper and common architectural and approach framework for security modules of all applications need to be adopted.

Application Firewalls.. They Work!

Quite a many organizations are happy with firewall word being mostly associated with peripheral security. It is difficult to find a proper adoption of application layer firewall in majority of organizations, even today. This is even more true in emerging and developing economies. Adoption of application firewalls after careful consideration of application nature and its sprawl and its access patterns, can really help in maintaining application security.

Logging of Security Events in Applications

Since application logging is designed by functional designer of applications, and, most of the logging in applications is done for debugging or for support provisions, one would find that security related events and entries in application logs are not given the due treatment. Proper security context is not captured in the security specific events in most of the applications in organizations.

Lack of proper information in the logs of application leads to two major issues.

- Nailing down the security issue when a problem occurs or is detected
- Lack of security context making it impossible to do proper forensic in the event of an issue
- Application specific events not being collected by SIEM tools and hence limited of no monitoring of 'application security happenings'

Built-In Security...

In DevOps

The need of code related security concerns and corrections is to be taken care of during the development cycle. Quite a many organization employ the VPAT teams to conduct special suite of test cases on certain critical builds during the release cycle. But, this is not good enough.

A genuine and complete approach to coding/engineering related security needs to be built into your DevOps practices, process and tool. And, this needs considerable amount of thinking, planning and then resourcing of both tools and skills as part of engineering process establishment.

Monitoring of Application Security

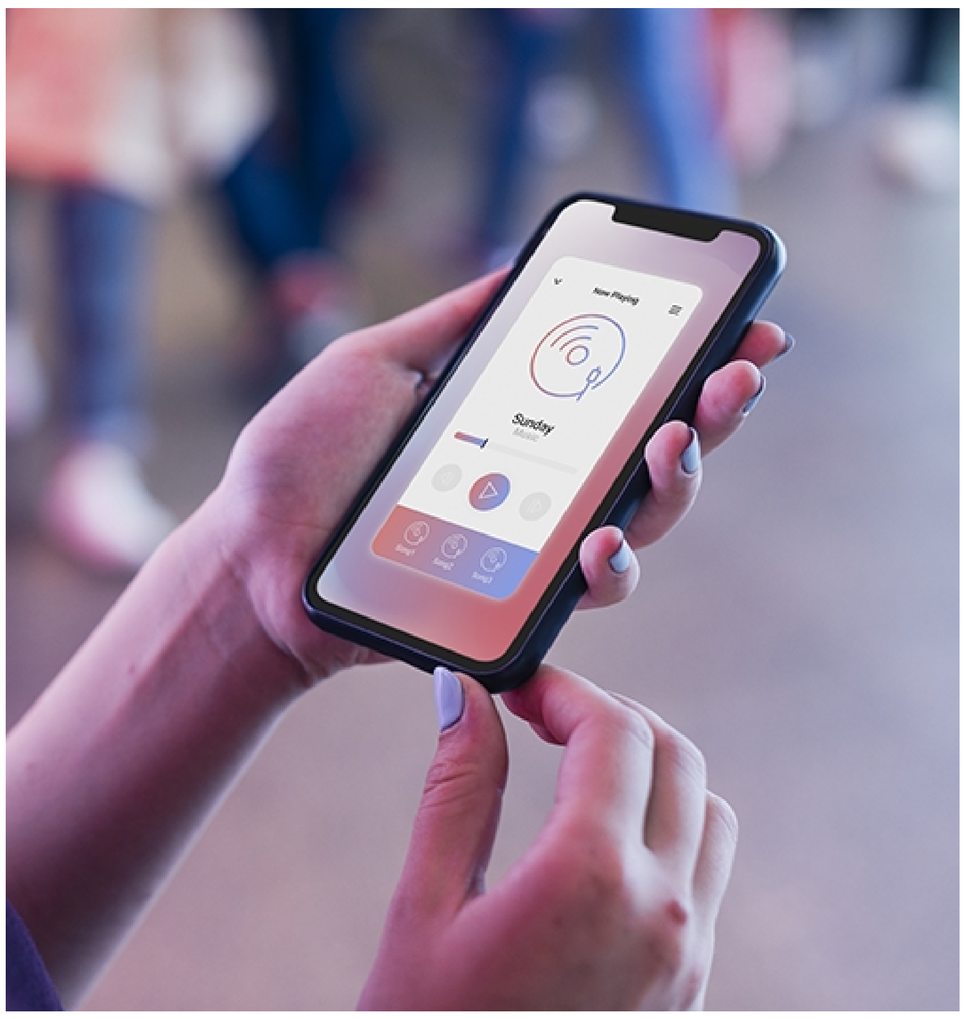
Since it is difficult to identify, detect, collect and map security events from application logs, majority of organizations completely bypass their application security monitoring. Most of the SIEM or monitoring tools in organizations are picking logs from security devices, security software and identity stores.

Though it is a difficult thing to achieve, but, application security monitoring will provide organization with a better response mechanism, in the event of a security issue occurrence. A security event taking place in application has more possibilities of causing immediate damage or compromise to organization, and hence, its detection and corresponding protection needs to be prioritized. This prioritization is possible only when a proper application security monitoring stance is taken and corresponding solution is adopted.

Castellum Labs

WHITE PAPER 2021

Building Threat Data Aware Applications



And, if one is keen on adopting advance security postures in organization, one can get into areas of building advance capabilities within security modules of applications.

Applications security modules, today, can be made aware of and capable of threat data elements. And, application security module themselves can protect the application infra and data from the invalid of threat-ful connection requests and access requests.

The Last .. But .. Not the Least... Vuln & Pen Testing

The age old, tried and tested approach to subject your web application to routine vuln and pen testing, will never go out of fashion. And, it should not.

Though, adopting a practice of doing vulnerability and pen testing before an application is released in production environment would be ideal. Building a specific sandboxed pre-production environment for such testing would be ideal and would enforce the practice of every application going through a standard vuln and pen testing in pre-production environment before it is released in production environment.

In a world where we see web infrastructures and web applications being compromised on a daily basis, organizations need to start thinking of fortifying their most important and critical assets, 'Applications' and 'Data', by adopting a proper and comprehensive approach to 'Application Security'. CISOs need to go way beyond convention models of layered security structures to be able to genuinely protect the real assets, 'Applications'.

Castellum Labs

+91 97009 70397 info@castellumalbs.com www.castellumlabs.com

WHITE PAPER 2021