



Consolidated Project Issue Tracker

Application Security is critical, when your security perimeter has shifted from usual servers behind DMZ and Firewall to web, mobile & cloud!

Go Beyond VAPT



Web Security

Ensuring that your website or open web application is secure.



Mobile Security

Without mobile device security measures, organizations can be vulnerable to malicious software.

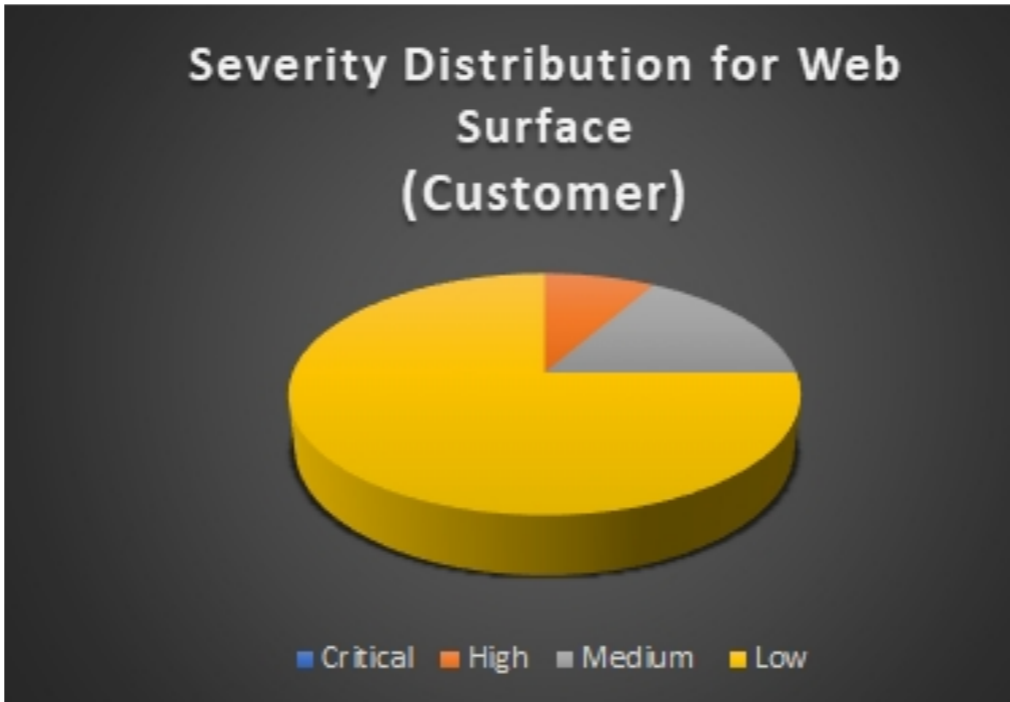
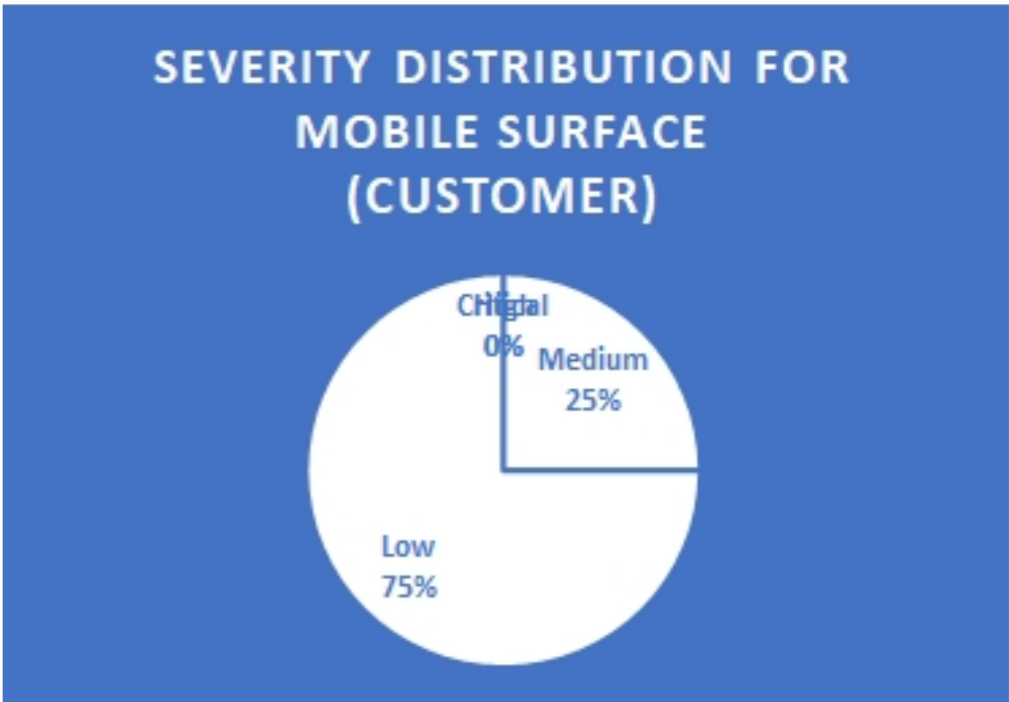


API's Security

Focuses on strategies and solutions to understand and mitigate the unique vulnerabilities and security risks of an Application Programming Interface.

https://*.custname.net
 from 13th Oct 2019
 to 10th Dec 2019
 Web/Mobile/API

SUMMARY

Customer AppSec Summary		Web Surface Total Issues		API Surface Total Issues	
Total Issues Detected	20	12		8	
General Areas Where... Security Issues Detected		Critical	0	Critical	0
Rate Limiting		High	1	High	0
Security Misconfiguration		Medium	2	Medium	2
Session Management		Low	9	Low	6
File Upload		<div style="display: flex; justify-content: space-around;"> <div style="width: 45%;"> <p>Severity Distribution for Web Surface (Customer)</p>  <p>■ Critical ■ High ■ Medium ■ Low</p> </div> <div style="width: 45%;"> <p>SEVERITY DISTRIBUTION FOR MOBILE SURFACE (CUSTOMER)</p>  <p>Low 75% Medium 25% Critical 0%</p> </div> </div>			
Enumeration					
Cryptography					
Input Validation					
Authentication					
Cryptography					

Overall Criticality Distribution	
Critical	0
High	1
Medium	4
Low	15

OWASP Top 10
Injection
Broken Authentication
Sensitive data exposure
XML External Entities (XXE)
Broken Access control
Security misconfigurations
Cross Site Scripting (XSS)
Insecure Deserialization

WEB SURFACE

Issue ID	Issue	Category	Criticality	Business Impact
SAMCUS0012/AC/SAMCUS/WEB/App001/012	Bearer Token Expiry	Session Management	High	High
SAMCUS0012/AC/SAMCUS/WEB/APP001/006	Testing for Ratelimiting on email triggering	Rate limiting	MEDIUM	MEDIUM
SAMCUS0012/AC/SAMCUS/WEB/APP001/005	Testing for Rate Limiting by Brute-forcing	Rate limiting	MEDIUM	MEDIUM
SAMCUS0012/AC/SAMCUS/WEB/App001/003	Missing Secure Flag	Security Misconfiguration	LOW	LOW
SAMCUS0012/AC/SAMCUS/WEB/App001/002	Missing http only	Security Misconfiguration	LOW	LOW
SAMCUS0012/AC/SAMCUS/WEB/App001/001	concurrent logins	Session Management	LOW	LOW
SAMCUS0012/AC/SAMCUS/WEB/App001/011	Malicious File upload	File upload	LOW	LOW
SAMCUS0012/AC/SAMCUS/WEB/App001/004	User Enumeration	enumeration	LOW	LOW
SAMCUS0012/AC/SAMCUS/WEB/App001/010	Weak Encode of password	cryptography	LOW	LOW
SAMCUS0012/AC/SAMCUS/WEB/App001/007	No session Expiration	Session Management	LOW	LOW
SAMCUS0012/AC/SAMCUS/WEB/App001/009	Input value Sanitization	Input Validation	LOW	LOW
SAMCUS0012/AC/SAMCUS/WEB/App001/008	Test account suspension/resumption process	Authentication	LOW	LOW

API's SURFACE

Issue ID	Issue	Category	Criticality	Business Impact
SAMCUS0012/AC/SAMCUS/API/App002/005	Session Invalidation	Session Management	MEDIUM	MEDIUM
SAMCUS0012/AC/SAMCUS/API/App002/006	Session Expiration	Session Management	MEDIUM	MEDIUM
SAMCUS0012/AC/SAMCUS/API/App002/001	Checking For Banner, platform information	Information Disclosure	LOW	LOW
SAMCUS0012/AC/SAMCUS/API/App002/002	Stack trace by inputting random values	Information Disclosure	LOW	LOW
SAMCUS0012/AC/SAMCUS/API/App002/003	Rate Limiting for authenticated and non auth	Rate Limiting	LOW	LOW
SAMCUS0012/AC/SAMCUS/API/App002/004	Input Validation	Input Validation	LOW	LOW
SAMCUS0012/AC/SAMCUS/API/App002/008	Base 64 Encoding	Cryptography	LOW	LOW
SAMCUS0012/AC/SAMCUS/API/App002/007	Rate Limiting Headers	Rate Limiting	LOW	LOW

**Secure applications need big budgets,
AppSec experts and more time - always in short supply.
We deliver everything on a platter!**



Continuous Application Security



Darkweb Monitoring



Next Gen SOC Monitoring



3rd Floor, NYN Arcade,
Lumbini Avenue, Gachibowli,
Hyderabad, India

+91 97009 70397

reach@castellumlabs.com

www.castellumlabs.com