Application Security Program for TechMantra Client

Process Overview and Case study

We have been helping companies across different industries uncover critical bugs.

Share your website/application with us & your security concerns.
Our consultants will perform a pilot scan and will get back to you with minimum 2 critical security gaps -> **www.tftus.com**

About

Indian based client develops applications and software for banks to make their internal processes easier and faster.
We were approached to help secure an application that analyses and integrates bank statements and makes them retrievable instantaneously

Challenges

- Client was in talks with largest bank in Australia to get their application implemented for the bank's processes.
- They had extremely strict standards for security and compliance.
- They had multiple portals inside the same webapp and roles

Key Highlights

5000
Lines of code reviewed

4 Weeks
Time allotted to complete the audit

1 Side
Performing penetration testing for the web app

14
Vulnerabilities pointed out by us in with no any addition uncovered by client

1 Hour
Maximum time taken to fix a bug once it was identified

4 <
White hat hackers assigned to test each module

Categorical Effort Estimation of All 100+ OWASP Attacks for a Single Web Project

Test ID	Test Case	Priority	Time to complete the Test Case with 1 resource
1	Test Application Platform Configuration	P3	8
2	Test Content Security Policy	P3	1
3	Test HTTP Strict Transport Security	P2	1
4	Test RIA cross domain policy	P2	1
5	Test time synchronisation	P2	1
6	Test user-viewable log of authentication/transactions events	P2	1
7	Test Upload of Malicious Files	P2	1
8	Test Upload of Unexpected File Types	P2	1
9	Test Defenses Against Application Mis-use	P3	1
10	Test Integrity Checks	P1	15
11	Test Ability to Forge Requests	P1	15
12	Testing for Session puzzling	P2	2
13	Test multiple concurrent sessions	P2	1
14	Test Session Timeout	P2	1
15	Testing for logout functionality	P2	1
16	Test for Bypassing Session Management Schema / Session Token Strength 1 In cookies check for path, domain and expires attribute 2 Check Session cookies reuseability, Session token should be changed after successful login, Check is it possible to send session id in get request by changing post request.	P1	15
17	Testing for Cross Site Request Forgery	P1	16
18	Role Level Bypass Business logic break Server side validation Privilege Escalation	P1	90
19	Testing for Injections	P1	30
20	Test Role Definitions	P1	8

Test ID	Test Case	Priority	Time to complete the Test Case with 1 resource
21	Test Unique User Registration Process	P1	4
22	Testing for Weak or unenforced username policy	P3	2
23	Test Account Suspension/Weak lock out mechanism	P3	1
24	Testing for Browser cache weakness	P3	3
25	Testing Man in the middle Attack and Testing for Credentials Transported over an Encrypted Channel	P2	2
26	Testing for Weak password policy	P1	1
27	Testing for Weak security question/answer	P2	1
28	Testing for weak password change or reset functionalities	P1	1
29	Testing for Emergency access in case of lost of account	P2	1
30	Redirected file download without upload (Hacking Json Data)	P1	4
31	HTTP Parameter Pollution	P1	1
32	Test Cross Origin Resource Sharing	P1	1
33	Test X-XSS-Protection	P2	1
34	Test X-Content-Type	P2	1
35	Test File Extensions Handling for Sensitive Information	P1	1
36	Testing for Insecure Direct Object References	P1	4
37	Testing for Reconnaissance(Passively)	P3	4
38	Testing for the content of authentication cookies	P1	4
39	Testing for Server-Side Template Injection	P1	6
40	Testing for Data Validation	P1	6

This effort estimation is specific to Web App. For android and IOS app addtional 40 hours efforts would be require for each platform.

Total: 259 Hours

Share your website/application with us & your security concerns.

Our consultants will perform a pilot scan and will get back to you with minimum 2 critical security gaps. -> **www.tftus.com**