Conducting Application Security assignment for a large organization

Background

The Client is alarge organization based in Dubai, with over 15,000 employees, providing services in 10 countries across four sectors.

MIEL e-Security Pvt. Ltd. (MIEL)is one of the largest Information Security services and solutions Company in India. Today, MIEL is a trusted Information Security company which provide services to various business verticals in India and abroad with more than 6 years track record of security services & solutions to more than 500 satisfied clients including some of the leading names in domain of IT, ITES, manufacturing , Banking, Financial Services, Insurance & more. These services include information security audit, consultancy, implementation and training.

Objectiveof the Client

The client approached MIEL for an Application Penetration Testing. The client wanted to understand the risk posed by complete outsiders as well as existing users of the application who have login accounts.

Based on the client's requirements MIEL proposed an initial Black box assessment which is conducted with no prior knowledge of the application apart from the URL of the website on which the application is hosted. The black box assessment would be followed by a grey box approach where the penetration testers would be provided test login accounts.

The application contained both Intranet and internet facing modules which were developed by a third party vendor. The internet facing modules were subject to the assessment.

Most organisations have their web applications developed and maintained by third-party vendors. These applications could be vulnerable to multitude of attacks and since every application is custom built the only way to identify the vulnerabilities in these applications is to have anApplication Penetration Test done.

Approach

Black Box

MIEL's consultants started the assessment with a black box approach. The only pages available to outsiders were a 'login' page and a 'forgot password' page. Both the pages were resistant to injection attacks and other common enumeration vulnerabilities. But on deeper probing, by carrying out resource prediction the consultants found an admin login page which would otherwise never be available to normal users. This page was found to have SQL injection vulnerability. On exploiting the vulnerability it was possible to gain access to the administrative panel of the entire application. It was now possible to view the names of the user's folders, add new users, elevate the privileges of existing users and remove existing users from the application.

The administrative panel was also found to contain multiple cross site scripting vulnerabilities. Exploiting this vulnerability could lead to the theft of the session ID of the user logged as the administrator.

The findings from the Black box test were significant as it showed that the application was susceptible to complete compromise by any external attacker.

Grey Box

After the black box, the application was to be tested after logging in with the test logins provided by the client for the assessment. The consultants first tested all the internal form fields for injection and input validation based vulnerabilities. Again SQL injection and cross site scripting were found in the some internal pages. As the severity of these vulnerabilities were already established in the black box phase, the testers pushed forward to look for logic level vulnerabilities as the time available for the assessment is very limited.

On understanding the logic behind the way in which session and access control is maintained by the application it was discovered that too much trust is placed on the information stored in cookies maintained on the client side. By manipulating the field called 'LoggedIn' in the cookies it was possible to access the internal pages of the application without even the knowledge of a valid username and password. Further it was found that the access control is based on a field called 'userid' which is again maintained on the client side in cookies. The access level of the users fell in to user, manager and administrative levels. It was possible to perform horizontal privilege escalation i.e., accessing the application as any user of any access level by sending a carefully crafted request.

To prove the severity of the vulnerabilities discovered the testers wrote a custom script which identified valid accounts by brute forcing the 'userid' value and then collected sensitive personal information of the users from their private page without the credentials. The script was run for a short duration and was successful in discovering over 350 valid accounts and their personal data in a few minutes.

Solution Proposed

The vulnerabilities and their severities were reported to the client along with detailed mitigation steps. As there were vulnerabilities embedded in the application logic MIEL recommended reviewing and modifying the application logic. MIEL's consultants extended their support to the application developers to mitigate the vulnerabilities by following secure coding practices.

The client had been initially informed by the application vendor that the application went through standard in-house security testing and is secure; therefore the findings of the assessment were largely surprising to them.