

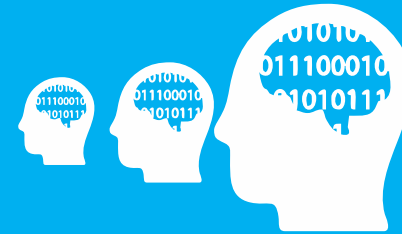
DESKTOP APPLICATION SECURITY

Have you ever heard about zero-day attack? Or people talk about malware that exploits zero-day vulnerability to bring chaos into company's network and system? Do you have any in-house desktop applications or products which are running on desktop but you have no clue whether they are exploitable or not?



At Authscore, we also provide security testing against desktop applications, either it is Windows based or Linux/UNIX based, to search for any vulnerabilities or bugs that could lead to public exploitation.

Our Desktop Application Security services help product owner or user to find any security vulnerability hiding inside the application so that both owner and user could avoid further risk and damage (loss) to the business.



Today, there are so many desktop applications released into the market that have been found to be affected by high risk vulnerability which was later used by hackers to hack into the system or gain advantage through the bugs. Some of applications that are widely used by computer users and usually affected by zero-day attack are;

- Offices Application
- Services Application
- Software Multimedia
- Driver Operating System





METHODOLOGY DESKTOP APPLICATION SECURITY TESTING



At Authscore, our application penetration testing process will targets the entire range of vulnerabilities in your desktop apps. Using the same techniques as sophisticated hackers, we providing unique visibility into security risks automated tools often miss. To ensure high quality and repeatable engagements, our penetration testing methodology will follows these steps:

