

Internet Security



Yousif Yaldo
June 2008

Hi, my name is Yousif Yaldo. I am the CEO, Founder of V.A.P.T. Our company specializes in Web Application Security & Penetration Testing. The reason I started V.A.P.T. was to remediate a precise business and web security solution combined to increase consumer awareness and to help prevent the increasing threat rate to businesses and enterprises throughout the digital world. The main goal V.A.P.T. is striving for, is to complete website vulnerability management provided via our out-source service. V.A.P.T. unites rigorous scanning methodologies and human analysis processes to strictly eliminate all false positives. The scanning procedures we employ operate in a safe manner and involve the most up-to-date tools and resources. Here at V.A.P.T., we believe in ethical practices that surely engage us in securing manually to eliminate any falsified data within searches and to test for business logic flaws. We've had many strong relationships with customers over the time of our launch, and it's been quite interesting to see the types of industries that take security in consideration to operating their businesses. We've worked diligently with health care providers, construction-engineered companies, mining corporations, e-commerce shops, web design firms, and hospitality institutions. V.A.P.T. approaches a unique business model of strategic planning to assemble in its security services, which include:

Assess vulnerabilities in your present security routines

Create an enterprise-wide curriculum customized to your absolute needs

Provide visibility into your system of structure so you can see what's going on instantaneously

Secure internal and external infrastructures

Identify logical flaws

Develop a proactive response plan in the rare incident that your security is seized

Reduce costs by professional consultation depending on type of service

Automate compliance standards so they operate in a routine form

I believe security is going to head in the path of failure for quit some time until media starts playing a more notable role in discussing such topics such as web application security and the dangers of dismissing it as an IT operation. Often the people who you end up communicating with; CTO, IT staff, or perhaps even an administrator seems to be a shot in the dark. From experience in sales and technology combined, you would know that the CTO, IT department, and even the administrator are people you should be talking to, but even they fail to understand the need for security. Businesses spend thousands of dollars every year alone on technologies that don't work well with the mind of a hacker. They often purchase extensive licenses for applications such as firewalls, or even install a SSL certificate to "defend" against attackers. All of these programs fail tremendously when it comes to the attacker's point of view. Insecurity lies within firewalls in many fashions that an attacker effectively takes advantage of, thus assisting the attacker in escalating his/her attack to a more profitable level. SSL certificates however are used today to "protect" against attacks. SSL certificates are used to establish a secure encrypted connection between the client and the server, but in no means does it "block" any types of attacks performed by an attacker. Also, the reason security will head off down the drain is because of programming languages being developed with high amounts of privilege and powerful dynamic behaviors, such as AJAX. Web applications' features are becoming more invisible as this type of technology expands. I like to compare CSS (Cascading Style Sheets) with AJAX because it works in a similar fashion. AJAX introduces features that work when you don't notice. For example, if you send an e-mail to an electronics store describing an incident that had occurred with your specific device, and you want to exchange it for a newer model. You then decide to delete the second sentence in your message, but it's TOO LATE! If the web site uses AJAX, your

message may already been sent. The problem with this is that AJAX is using functionality enabling execution of the users' environment without visual notice, but rather via an XMLHttpRequest. As I have described before, Web 2.0 is not secure, and may be in various ways, violating security policies, surely described in my security-related blog found here: [Web 2.0 Issue](#). Amazingly, there has been an organization dedicated to introducing a care cycle for security within customers and businesses. AVDL (Application Vulnerability Description Language) is pioneering highly valuable and efficient means of dealing with vulnerabilities in a brisk pace. Problems as such arise often, occurring continuously without the sufficient options needed to mitigate security flaws without the business being threatened or at stake. The average company will sort out the following options they are most immune to: Allow exposure, upgrade/downgrade to a secure patch, or simply remove the website. These methods frequently do not work well because allowing exposure is solely doing nothing about the matter. Upgrading or downgrading to a patch for the software then might decrease the functionalities your site depends on, and may just produce even more bugs to deal with. Additionally, removing the site will merely hurt your brand, service, and dramatically hurt your credibility. In addition to the services V.A.P.T. provides, we decided to affiliate with company's that will add value to our clients' needs and initiate a more equipped balance of integrity within the work we tailor. This purely adds core significance, expressing widely-assembled security adjusted to administrate website vulnerability management.