Web Application Vulnerability Assessments

What we did

We used a proven automated tool to scan government owned, internet facing websites (web applications) for vulnerabilities. We reviewed the results from the tool and eliminated as many false positives as possible to provide application owners with valuable results so that they could focus their efforts on correcting vulnerabilities. We reported our findings to application owners, who in some cases had already remediated the vulnerabilities we found. Once the web application owners remediated the vulnerabilities, we rescanned the websites to confirm the vulnerabilities no longer existed.

Why we did this work

Web applications are a common way organizations share information or provide services to the public. For example, the Government of Alberta uses web applications to inform the public about health issues, register vehicles or reserve campsites. Web applications rely on the internet, which means they are accessible by everyone, anywhere in the world. Most people who use a web application do so for legitimate purposes. As with all computer systems, web applications have weaknesses that can be exploited to compromise the security of information or subvert the system to make it do things the developers did not intend.

It is the nature of modern technology that all systems on a network are connected. There are controls in place to limit some of those connections. But hackers take advantage of that inherent interconnectedness and will attack an easy target first and use that to get access to more valuable, and highly secured, targets. Web applications with weak security are easy targets. Therefore, it is important to secure all web applications, not just ones that can be used to access personal information. Even for a simple web application with no personal information, weaknesses in the system could be abused to gain a toe-hold and then gain access to other, more sensitive systems.

For example, one type of vulnerability allows an attacker to trick a user into entering data into a form on a web page, in such a way that an attacker can inject special code into the web application and cause it to behave in a way not intended by the developer. Using this method, the attacker could steal information entered by the user, such as usernames and passwords. The attacker would then use those credentials to try and exploit other vulnerabilities to gain greater privileges, install software and begin attacking other systems.

What we found

We are not publicly reporting details of the vulnerablilities we found and reported to management because public disclosure would increase the risk to the organizations we audited.

We found fewer vulnerabilities than during our audit in 2008, but we found that the government, which includes departments, agencies, boards, commissions and post-secondary institutions, has not consistently applied a process to regularly review the security of web applications. Some organizations have a process to regularly review the security of their web applications, and we found fewer vulnerabilities in the web applications belonging to those organizations. Also, they more promptly remediated the vulnerabilities we did find.

At the organizations that did not have a process to regularly review web applications for security, we found web applications with multiple critical vulnerabilities. These vulnerabilities were well known vulnerabilities, which the organization should have detected and corrected prior to our audit.