

INSERT Ethics INTO Public Web App Testing

By Michael Starks – ISSA member, Fort Worth, USA Chapter

The ISSA Code of Ethics charges us to obey the law, promote best practices, and avoid conflicts of interest. It was designed to keep us out of trouble. It is simple to read and seems pretty straight-forward, but understanding and practicing the code on a daily basis can be another story altogether. Subtle nuances work their way into our professional lives as we weigh options, consider consequences, and look to our peers in an ongoing process of careful consideration.

It is with such consideration that I have been observing an interesting trend lately: the testing of public web application security. Security professionals test these applications for vulnerabilities and talk about what they found, usually after going through some form of disclosure process. It is clear that the tests are in most cases unauthorized and may even be illegal in some jurisdictions.

There is a long history of testing the security of applications. Nary a day goes by that we do not read about some application security issue. No one wants to be seen as a liability, so when a company is put in the spotlight for security issues, bugs tend to get fixed. Smart companies have embraced this process and even provide security contacts within their company. They then work with the researchers to make the product more robust and to keep their customers safe.

Whereas finding security bugs in an application that you download and install yourself is seen as generally acceptable, testing that same application when installed on a remote system can be seen as offensive. The basic rule of thumb has been that the good guys only test the security of systems they own or manage.

So what is one to do when wanting to perform research against applications which are only remotely-hosted? This results in a natural tension between previously established precedents. With the current trend of moving services online, we find ourselves at a juxtaposition where performing responsible¹ security research on remote systems may lead to an improvement of overall security in an increasingly connected world.

Lofty intentions aside, a security analyst may see no distinction between a security professional performing a SQL injection attempt against a public web server and an attacker doing the same thing. Even if the professional has the intention of following up with an ethical disclosure process, the attempt in and of itself is unauthorized. Even the most innocent of

attempts can have unintended consequences: services can crash, transactions can be corrupted, and sensitive data can be exposed.

“But wait!” say proponents of testing public web applications. If the bad guys are going to be attacking the site, how can a professional’s testing with the intention of responsible disclosure be a bad thing? If it leads to improved security, does it ultimately benefit everyone? Furthermore, if an application is offered to the public, has the company abandoned an expectation of total control? In other words, should they not expect attacks and have secured the application appropriately?

Is it ethical to test the security of public web applications even if it is unauthorized? Does the intent to follow a disclosure process make it ethically palatable? Is it ethical not to test the security of an application accessible to the world, so as to keep raising the bar of protection from which we all benefit? How else can we hold those who are custodians of our information accountable? Should we take their word at face value while the bad guys attack?

As more services move online, the issue of testing public web applications will likely become more contentious. As ISSA members, we have agreed to abide by a standard of conduct, which is embodied in a code of ethics. If there is broad consensus that this is a practice not becoming of our profession, we should stand up and say so now. However, if there is a broader discussion to be had, the time to have this discussion is also now.

Regardless of the decision, one thing is clear: actions have consequences. Those involved in the practice of unauthorized web application testing may want to take a moment for reflection and consider the potential consequences, both professionally and legally.

What do you think? We want to hear from you. Please email ethics@issa.org with your thoughts.

About the Author

Michael Starks, CISSP, CISA, GSNA, is a security analyst working in Arlington, Texas. He is a founding member of the Rochester, NY chapter of ISSA and has served both ISSA and OWASP chapters in various capacities. His personal blog is at <http://www.immutablesecurity.com>, and he can be reached at issa-article@michaelstarks.com.



¹ Responsible research usually implies that vulnerabilities are disclosed first to the software creator and only disclosed publicly after a patch has been issued or if the party declines to address them.

The ISSA International Ethics Committee is an active group of ISSA members missioned to maintain a framework for ethics relating to practices that support the ISSA Code of Ethics, provide guidance on ethical behavior for Information Systems Security professionals, and provide education and outreach that increase awareness and promote positive actions.