Oakland University is a highly respected public university in Oakland County, Michigan. It has nearly 20,000 students and runs an extensive range of bachelors and undergraduate programs, offering professional, masters and doctoral degrees. It is the only major research university in Oakland County, supporting major institutions including the Center for Biomedical Research, the Center for Robotics and the renowned Eye Research Institution.

The Oakland University William Beaumont School of Medicine is a collaborative, diverse, inclusive, and technologically advanced learning community, dedicated to enabling students to become skillful, ethical, and compassionate physicians, inquisitive scientists who are invested in the scholarship of discovery, and dynamic and effective medical educators.

Safeguarding the University’s Web Applications from a Possible Attack

Oakland University needed to protect its web applications from security flaws, web application vulnerabilities, programming errors and other threats.

"Netsparker helped our team increase the visibility into the security of our web applications."
It required a solution that was compatible with its existing repertoire of security audit tools and a variety of web development frameworks.

The university has a number of websites and web applications used daily by university staff and students. This includes student portals, faculty web applications and the Oakland University’s official websites. These provide core services vital to the university’s daily running. If they were hacked or went down due to a programming error or malicious attack, confidential information could be at risk of being lost or stolen. A system’s failure would also impact staff and students who rely on the university’s online services to manage their daily lives.

Dan Fryer, a Senior Windows System Engineer, and Dennis Bolton, a Network Security Analyst, are responsible for managing the security of Oakland University’s web servers. These servers host websites and web applications built on multiple web development frameworks, including Java, PHP, .NET, Ruby, Perl and Python, which run on both IIS and Apache Tomcat web server technology.

Fryer and Bolton needed a web application security solution that could be setup and left to automatically scan for web application vulnerabilities. With an already heavy workload, the solution would need to be quick and easy to manage. It also needed to be compatible with the university’s multiple web development frameworks and its existing security audit tools.

Netsparker Web Application Security Scanner, a market leading vulnerability scanner that can continuously scan and identify web application vulnerabilities, ticked all the boxes.

Looking for the Right Automated Web Application Security Solution

Dan Fryer, a Senior Windows System Engineer, and Dennis Bolton, a Network Security Analyst, are responsible for managing the security of Oakland University’s web servers. These servers host websites and web applications built on multiple web development frameworks, including Java, PHP, .NET, Ruby, Perl and Python, which run on both IIS and Apache Tomcat web server technology.

Fryer and Bolton needed a web application security solution that could be setup and left to automatically scan for web application vulnerabilities. With an already heavy workload, the solution would need to be quick and easy to manage. It also needed to be compatible with the university’s multiple web development frameworks and its existing security audit tools.

Netsparker Web Application Security Scanner, a market leading vulnerability scanner that can continuously scan and identify web application vulnerabilities, ticked all the boxes.

Why Netsparker?

After assessing the available options, Fryer and Bolton decided to use Netsparker; the only false positive free web application security scanner on the market, for the following reasons:

• It has a built in exploitation engine that confirms vulnerabilities that can be setup to automatically test all the university’s web applications for flaws that leave them exposed to hackers.
Checking for and eliminating web application security threats can be a very time-consuming and repetitive task. Netsparker, however, provides the Oakland University’s IT team with a host of user-friendly features that make the process quick and easy to manage.

Scans are scheduled and left to run automatically, while its at-a-glance reporting and actionable insights ensure the university’s IT team knows exactly what to do. There is no time wasted checking for web application vulnerabilities manually or having to figure out a solution. All the information is provided for them. This has enabled the university’s IT team to gain more time to focus on other tasks, while knowing that the university’s web applications are secure and free from vulnerabilities at all times.

"Netsparker provides the Oakland University’s IT team with a host of user-friendly features that make the process quick and easy to manage.

"Since the university’s web applications are frequently changing to adapt to the students’ and university’s needs - and because malicious attacks are becoming more sophisticated - it is important that we keep on scanning all of them frequently for the latest type of security threats to ensure that no vulnerabilities are left undetected," said Fryer.

“We chose Netsparker because it is more tailored to web application security and has features that allow the university to reinforce its web application security needs,” he added.

Fryer now uses Netsparker Web Application Security Scanner to run monthly scans and also do web application security checks on demand.

Once a scan is complete, reports on confirmed flaws and vulnerabilities are generated in PDF or xml format. These are handed to the university’s IT security team (on which Bolton serves) for analysis and to advise on fixes. The IT team then rescans all of the university’s web applications to confirm that reported vulnerabilities are fixed and that web applications are secure.

A 'hands-off' solution that saves time and offers reassurance that web applications are secure

Checking for and eliminating web application security threats can be a very time-consuming and repetitive task. Netsparker, however, provides the Oakland University’s IT team with a host of user-friendly features that make the process quick and easy to manage.

Scans are scheduled and left to run automatically, while its at-a-glance reporting and actionable insights ensure the university’s IT team knows exactly what to do. There is no time wasted checking for web application vulnerabilities manually or having to figure out a solution. All the information is provided for them. This has enabled the university’s IT team to gain more time to focus on other tasks, while knowing that the university’s web applications are secure and free from vulnerabilities at all times.
About Oakland University

Oakland University is a top-rated academic institution in southeast Michigan offering 132 bachelor's degree programs and 124 graduate degree and certificate programs.

“Netsparker has enabled the university's IT team to gain more time to focus on other tasks, while knowing that the university's web applications are free from vulnerabilities.”

As a state-supported institution of higher education, Oakland University has a three-fold mission: It offers instructional programs of high quality that lead to degrees at the baccalaureate, master's and doctoral levels, as well as programs in continuing education; it advances knowledge and promotes the arts through research, scholarship, and creative activity; and it renders significant public service. In all its activities, the university strives to exemplify educational leadership in a diverse and inclusive environment.