PREVOTY

Bleacher Report boosts its security game plan with self-protecting applications

Enterprise Application Security Case Study

April 2015

Bleacher Report's Challenges

1. Foster a safe, trusted community for secure information sharing, quality sports news delivery, and fan engagement

2. Produce around-the-clock, breaking content that informs and entertains without any application performance, availability or functionality setbacks

3. Reduce risk and impact of high attack volume and relieve burden of reactive application security strategies on in-house engineering resources

The Solution

Sports media leader Bleacher Report deployed Prevoty's Runtime Application Self-Protection (RASP) product to prevent application layer threats such as cross-site scripting (XSS) and SQL injections (SQLi) and fight high volumes of spam, profanity and other flagged content. Leveraging Prevoty helped Bleacher Report redouble its efforts on growing a successful digital publishing business and engineer product innovations without fear of data exfiltration, brand defacement, user identity theft and fraud.

Bleacher Report joins the sports media major league

Bleacher Report (B/R), a Turner Broadcasting System company, is a leading sports media publisher of real-time programming content covering hundreds of U.S. and international sports teams. Since launching in 2007, Bleacher Report quickly rose to become a top-ranking sports entertainment destination, nurturing and engaging an audience of over 80 million monthly unique visitors and over 1 billion monthly pageviews.

Sports media technology driven by data and community

A fast-growing digital media innovator, Bleacher Report presents comprehensive sports commentary through a network of paid freelance contributors all accessing shared publishing software. In addition to maintaining a high-traffic web application, Bleacher Report brings real-time sports entertainment to a vast user base through multiple outlets and platforms -- from syndication partners such as USA Today, Los Angeles Times, Philly.com, and the San Francisco Chronicle, to native mobile applications for Android and iOS.

The company initially built its platform on Amazon Web Services (AWS) and the Ruby on Rails framework for their scalability and speed-to-market capabilities. For a while, the company successfully leveraged out-of-the-box security services already available on these platforms. Data informs all of Bleacher Report's engineering decisions, product development and content strategies. This approach has helped fulfill consumer demand and fuel serious growth. As the publication's readership and popularity grew, however, so did its backlog of flagged content and its trove of exploitable personal data.

Content: friend or foe?

Great content and a reliable news experience are the lifeblood of a company like Bleacher Report. In an industry where falling behind is unacceptable, the Bleacher Report team suddenly found itself tackling not just a few spikes of questionable content but hundreds of pages littered with spam and code injection attacks. Heavy onslaughts of excessive content, cross-site scripting (XSS) and SQL injections (SQLi) taint the browsing experience, threaten the security of its users, and ties up the company's technical resources in a neverending chase.

At first, Bleacher Report tapped into its in-house talent to develop a homegrown anti-spam mitigation solution for high-volume, basic "spam" attacks. It handled user-generated flags as well as the results from expression-matching algorithms. This solution worked effectively up to a certain point, but required significant upkeep. The company was constantly dedicating over a quarter of its technical team's time to manually analyze their administrative tool in order to identify new or unusual patterns, monitor and fix logged issues.

The business burden of security expertise

“Less sophisticated attacks will try a technique and with that information, it’s easy to identify and eliminate future attempts. The more sophisticated attackers continue to find new ways to work around simple matching algorithms.” - Chris Nguyen, Senior Director of Product Management

The team set aggressive rules to overcompensate for the increase in sophisticated, unknown attacks, but this introduced a new problem: a constant stream of false positives. The added strain was not only detrimental to the user experience, but it also diverted resources away from critical business projects and into deciphering false alarms.

It soon became clear that a spam detection system -- albeit successful in its original intent -- was not enough for a company with such a large market footprint. A reactive security strategy meant that pattern definitions would often go stale and sophisticated unknown (a.k.a. zero-day) attacks would fly right through their perimeter stopgaps.

Bleacher Report needed a contextual, signatureless application security solution that would help its development team capitalize on its strongest business suit: producing superior applications -- not being security experts.

Bleacher Report and Prevoty: a partnership for self-protecting apps

Bleacher Report teamed up with Prevoty to make its applications smarter and more secure with Prevoty’s runtime self-protection capability. Using Prevoty’s pre-built API libraries, Bleacher Report seamlessly integrated proactive security directly into their applications.

“We wanted a true partnership and not just another vendor,” said Chris Nguyen, Senior Director of Product Management, Bleacher Report. “Prevoty’s attention to detail, follow-up and consultative approach gave us a confidence and transparency that we rarely see.

With applications that could now self-protect against targeted attacks automatically upon deployment, Bleacher Report's team was able to redouble its core product development efforts and reaped many benefits:

Performance

Bleacher Report realized operational performance improvements as a result of using the Prevoty service. With its submillisecond speeds, the Prevoty engine had no impact whatsoever on Bleacher Report's performance. To the contrary, the team actually experienced workflow improvements. For instance, Bleacher Report suspected hardware issues were causing performance degradation, but after deploying Prevoty, they quickly realized that improvements in memory caching improvements would solve the problem.

Threat Prevention

Prevoty's contextual security engine analyzes and sanitizes content, queries and state changing activities. Any attempts at cross-site scripting (XSS) and SQL injection (SQL injection) are prevented in real-time, without relying on past definitions or signatures. By including Prevoty, secure coding best practices are followed and vulnerabilities aren't just identified -- they are mitigated instantaneously. Bleacher Report then used Prevoty's detailed console to interpret attack behavior and gain threat intelligence.

"Prevoty makes sense. It's far more cost-effective to use a tool that can grow with you as your user base continues to grow and as the attacks grow more sophisticated than to bring in full-time staff to take on the role." - Chris Nguyen, Senior Director of Product Management, Bleacher Report.

Bleacher Report moved beyond detection and into active prevention. Security was automatic, requiring far less maintenance.

Bottom Line

"Prevoty was a game changer for our development team -- elevating our internal discussions to build better, faster product and servicing our end users versus focusing on how to secure it." - John Degner, Lead Engineer, Bleacher Report

Partnering with Prevoty gave Bleacher Report the room to dive into its core competencies and focus on the tasks at large: implementing a secure software development life cycle (SSDLC) and defining -- on a holistic level -- the internal processes and workflows that would lead to smarter, attack-resistant applications that sports fans everywhere can trust.

About Prevoty

Prevoty was founded in 2013 with a vision to revolutionize application security: why not enable applications to protect themselves?

Prevoty delivers breakthrough RASP (Runtime Application Self Protection), making it easy for security professionals and application developers to block top application layer attacks automatically, eliminate vulnerabilities, and secure both legacy and new software. In-app calls to Prevoty's contextual security engine validate inputs, queries and user tokens before they hit your application and database.

To find out more about how Prevoty can protect your enterprise from next generation threats in your web application, contact us today:

info.prevoty.com