VERSPRITE

Application Security

– BlackHat Mindset to Emulate Real World Attacks

A key goal of testing exploits is determining how easy and impactful successful exploits are against target networks, systems, and applications. Whitehats in today's industry can often become more enamored with the hunt versus improving technique and truly understanding impact or attack viability as part of a broader threat context.

VerSprite's Application Security Services (AppSec) group focuses on emulating cybercrime and simulating test scenarios that not only reflect current attack patterns, but also threat motives. Our group also focuses on integrated security testing to help organizations integrate AppSec initiatives sooner within a given SDLC process.

Penetration Testing

The key differentiator of a VerSprite penetration test is in our ability to look at the bigger picture. By not limiting our approach to encompass only one set of controls (network, application, physical, system) to defeat, we are able to simulate a true attack scenario. A true attacker will not stop if the front door of your network is locked, and neither will we.

Red Teaming

Our red team exercises are designed to be a comprehensive test of physical, logical, and process based controls. We use a combination of physical, social engineering, mobile, web, networking, and wireless attacks to bring a full arsenal of security tests aimed at exercising your current defensive security posture.

Mobile Security Testing

Mobile applications are being deployed each and every day with a trove of vulnerabilities that find their roots in the lack of proper security assessments. VerSprite recognizes that mobile technologies are leading the future in enterprises and small businesses alike. We offer exclusive security services for mobile application penetration pesting, source code review, and threat modeling. Secure and protect your application, product, and image.

VERSPRITE

Application Security

Application Threat Modeling

To accurately and thoroughly assess the security of a web application requires not only a combination of automated and manual testing, but also an understanding of the software behind the application. Gathering comprehensive information through reconnaissance and analyzing it effectively does not stop at running tools. Having a background in a wide variety of technologies leads to efficient use of attack vectors and successful security assessments.

– AppSec Approach Based on Threat Modeling

1. **Look Ma No Tools**: Tools are great for breadth, but they dull the senses when getting behind the wheel of exploitation. Our team codes techniques to better enumerate, fuzz, and reverse application components in scope. We emulate cyber-criminal intent far beyond the bounties and traditional pen testing groups.

2. **Application Threat Models**: What are you testing for? Our tests fit into a bigger picture of an application threat model that encompasses not only app components, frameworks, and use cases, but also threat motives, architecture, deployments, actor permission sets, and more.

3. **S-SDLC Integration**: Still pen testing like it is 2005 (post-development, post-implementation)? VerSprite provides cost effective unit security testing to mirror client SDLC methodologies to find issues within the development process and build remediation in sooner.

4. **A Better Consistent Craft**: Our team stays hungry, never resting on a 'standard' set of techniques. Attack patterns change, as does our team's craft. Consistency is also important as we pride ourselves in ensuring that our peer review process in every facet of our approach leverages ideas and skill sets of a collective team.