Orange
Cyberdefense

SensePost assessments
Applications

Key benefits

Best practices
Our testing methodologies follow industry-standard best practices, aimed at looking at the most vulnerable areas of applications. These methodologies include the OWASP Top 10 and the SANS Top 25 Most Dangerous Software Errors.

Know our client
A unique presales engagement allows for a thorough understanding of scope. This enables the assessment to be aligned with client requirements, focussing on what's important without compromising the security value-add.

Short turn around – high value
These types of assessments are generally shorter allowing for a high value response within a short timeframe, ideal for pre-go live or revision assessments.

Service description

One of the many entry points into a network is via an application. Businesses often have some form of outward facing application. Whether a “contact us” webform or fully interactive application connected to a customer management system or ERP backend, applications form a vital component of the information security landscape.

The SensePost team leverages in excess of two decades of assessment experience across multiple industry verticals to provide an attacker-led approach to application assessments.

This includes:

- Internet-facing web applications, whether self-hosted or in the cloud

- Stand-alone applications on an internal host on your network

- Thin applications running on client hosts

- Mobile applications; While they are covered, they have their own methodology - see datasheet for mobile assessments.

Application assessments can be performed from either an authenticated or unauthenticated perspective. These are not simply synonyms for blackbox and whitebox assessments, but in fact serve specific and different needs. Blackbox, whitebox and greybox approaches relate to how much information is known beforehand. Authenticated and unauthenticated is more an approach based on the ability to login to the target application.

An authenticated application assessment provides an enriched security understanding resulting in confidence against all kinds of attackers ranging from an opportunistic to an advanced attacker. To truly get the most from this type of assessment one could also include the applications source code for a highly interactive engagement. This expands the scope and by extension understanding to include business-relevant context.

An unauthenticated assessment in contrast answers the question, “are there vulnerabilities an attacker could exploit if they were not able to bypass authentication”. This assumes authentication is strong and effective.

Many applications have some interface accepting input to process server-side, i.e. an API. These range from small and simple unauthenticated API's to large, complicated API's using strong authentication tokens and/or certificates. Part of the scoping process is to thoroughly understand architecture to help define focus areas in the application for testing. This includes both input processing and authentication as an example.

Following our presales engagement, an appropriate response is crafted for your needs. We have standard responses as well as the flexibility for custom and bespoke assessments.

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As a leading go-to security provider, we strive to protect freedom and build a safer digital society.

We are threat research, intelligence-driven, offering unparalleled access to current and emerging threats. With a 25+ year track record in information security, 250+ researchers & analysts and 16 SOCs distributed across the world and sales and services support in 160 countries, we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

We are proud of our high-end security research unit, thanks to which we publish regularly white papers, articles and tools on cybersecurity which are widely recognised and used throughout the industry and featured at industry conferences including, Infosec, Manchester DTX, RSA, BlackHat and DefCon.

SensePost is an ethical hacking team of Orange Cyberdefense, offering offensive security consulting services and trainings. With a 20-year track record, SensePost is seen as trusted advisors who deliver insight, information and systems to enable our customers to make informed decisions about information security that support their business performance.

With team members that include some of the world’s most preeminent cybersecurity experts, SensePost has helped governments and blue-chip companies both review and protect their information security and stay ahead of evolving threats. They are also a prolific publisher of leading research articles and tools on cybersecurity which are widely recognised and used throughout the industry and feature regularly at industry conferences including Black Hat and DefCon.

Key service components

Our testing methodologies include the OWASP Top 10 and SANS Top 25, but also our custom learnings and research whilst covering key areas such as:

- Authentication and Authorization
- Session Management
- Input Validation
- Business Logic
- Configuration Management
- Data Encryption