arts·sec

Securing your digital transformation

www.artssec.com

arts·sec

About Us

ArtsSEC was founded by a group of professionals dedicated to Information Security focused on providing creative solutions and high added value to its customers. The company arised in 2012 from the join of experts in Information Security with extensive experience in multinational companies for over a decade.

Our Mission

Develop and integrate consulting solutions, analysis and implementation of security in information systems. We ensure to provide our customers with the necessary means to protect their assets and information, because we consider extremely important to develop their business safely and reliably.

Our Vision

Work to create a friendly environment with our customers. We have strength and trust in our brand. Through innovation in services, we can provide solutions that meet the needs of customers. In this way, we not only encourage the growth of our company, but also create new job offers opening the market to new professionals.

Our Values

Our values are firm and absolute. They focus on ethics, respect for people and responsibility for others. These values are the "pillars" of ArtsSEC.

Application Security </>

The objective of this service is to identify and analyze vulnerabilities in a company's web applications. These vulnerabilities are generally associated with security mistakes in the application's design, its development, or its implementation. If unchecked, a seemingly small opening can lead to a wider range of possible gaps that could be exploited by attackers. Our methods are aligned with the process described by the OWASP. Specifically, we identify with the first steps in web application security, that is, manual testing to identify vulnerabilities. We also provide implementation of automatic tools, and the corresponding confirmation of potential vulnerabilities.

Our web application analysis services are provided with three distinct approaches.

- Black box analysis.

  This is a simulation of an attack by an experienced user from the Internet with no previous access to information.

- Grey box analysis.

  The application's vulnerabilities are analyzed with a certain levels of information.

- White box analysis.

  This test focuses on vulnerabilities in the source code of an application.

Penetration Testing

Penetration testing is the service analysis of external system vulnerabilities. This method uses of a set of tests to identify vulnerabilities and their associated risks related to company assets that are exposed to the Internet.

The results are tested manually in both cases. If false positives have appeared as a result of the automated tools, they are identified and removed.

The tests are divided into the following phases:

- Identify unprotected services on the Internet.
- Perform tests on the registered services to identify vulnerabilities.
- Simulated exploitation, a series of carefully controlled tests that attempt to cash in on vulnerabilities like an attacker would.
- A written report about the vulnerabilities and their associated risks is provided with strategic recommendations.
- A re-test is performed after 30 to 45 days to verify the effectiveness of implemented controls.

Threat Modeling

Threat Modeling is a complex and ongoing process, where our security professionals identify threats to the security of your organization, and provide consultation on how to eliminate risks.

ArtsSEC offers on-point threat modeling for companies of all sizes, and websites or databases of all types.

- We take a look at any exchanges which may occur between your front-end - whether it’s an application, a client, or a website, and external sources like servers or the Internet.
- Comprehensive models are formed by the most relevant threats to your business according to their damage potential. The intent and scale of these threats is conveyed to our clients in a way that is digestible by non-IT managers and staff.
- We roll up our sleeves and come up with solutions to harden your defenses against the threats we discovered, implementing our own preventative measures where applicable, providing best practices and references.

Mobile Security

For mobile security, we use automated scanning, manual testing, and design testing to find weaknesses and mend them quickly. This is done by hardening backend servers, which are usually responsible for the data execution for a mobile application.

We also express practices for keeping the applications safe after we've left—protecting sensitive data from exposed misconfigurations, consistent patch management, limiting access to authorized personnel, typical platform vulnerabilities, and the most persistent vectors of attack.

Here is a listing of the Top 10 mobile device risks, according to OWASP:

- Weak Server Side Controls
- Insecure Data Storage
- Insufficient Transport Layer Protection
- Unintended Data Leakage
- Poor Authorization and Authentication
- Broken Cryptography
- Client Side Injection
- Security Decisions Via Untrusted Inputs
- Improper Session Handling
- Lack of Binary Protections

Client-Side Attacks

While building their defenses with software and hardware, many companies will marginalize the possibility of human error to create vulnerabilities. The main target of this service is to simulate an attack against a company's sensitive data using techniques that exploit the latter.

Rather than the straightforward approach of finding code-based vulnerabilities, it is done through social engineering strategies, wherein attackers use direct communication and human nature to find information about companies.

The goal of these tests is to identify the level of information available to each user and find the weakest links. Then, we will assess the potential threats to which they are exposed and determine if they are knowledgeable about how to handle sensitive information.

A typical attack stage involves the creation of a website designed specifically for the company.
The site could provide exclusive offers for employees, and follow up with requests to access corporate accrediting documents. Another attack stage may include a series of emails asking to update access information to the company's intranet through a specially designed gate.

Security Awareness ✓

Our security awareness services are for training and continued learning for companies who want to make sure their employees understand their roles in protecting data.

It is a program that we have developed in-house using relevant curriculum from industry experts, as well as materials we've accumulated through our own experiences in the industry.

The programs will focus on the most important aspects of security awareness:

- The best practices for security awareness according to industry standards, and according to our standards, which are higher in most cases.
- How to respond to direct attacks—those where the offending party attempts to dupe the employee into revealing information by taking advantage of human nature. These are the spam emails, suspicious phone calls, and solicitations by external parties who use various methods to lower an employee's guard.
- Avoiding human mistakes like leaving terminals unlocked or failing to discard written information that compromises the system (like a written-down password).

Hardening

The term "hardening" applies mostly to servers and their attached nodes, but it can also apply to entire systems. Whenever there is a risk of devices and machines leading back to a centralized source of data, the routes into that source need to be well-defended.

Hardening is a process involves altering the configurations of software to make it more resistant external attacks. After identifying weaknesses that can be exploited by outside attackers, we deliver a complete document with findings based on the best practice controls for security.

Our software hardening consists of strategic measures at each level of data transmission through your system. It begins with system-level configuration optimization, where we assess the security level from the ground up. That includes, but is not limited to: strengthen passwords, firewall implementation, limiting access to authorized individuals, and implementing necessary updates.

We then take measures to audit the hardware devices that require checks, like switches and routers. Configurations for these devices are checked at the software level to make sure they meet our lofty standards based on the best industry practices.

Bugs Bounty Program Managment

Bugs bounty programs are incentives offered by different companies that reward individuals or groups for finding critical bugs within their systems.

The programs are a way to expand the company's base of knowledge, while allowing resourceful users the opportunity to actively participate in improving the quality of products they find useful. Skilled programmers and hackers will prevent threats before attackers do.

The incentives the programs offer can be quite lucrative, and often give hackers who want to earn legitimate income for their skills a chance to do using private or public programs and report vulnerabilities.

ArtsSEC will use standard bug bounty programs platforms to foster constant improvement of all your web security systems, to elevate your quality assurance operation beyond outstanding to the upper echelon of industry standards.

Planned incentives will vary based on programs, which we will continue to revamp according to their effectiveness and consumer feedback.

arts·sec

Training

Courses with lab exercises where students have the chance to test the most commonly occurring vulnerabilities taking their skills to next level! Our trainings are for Developers, (Penetration) Testers, Hackers, Security Researchers and Humans!

- Dominating Burp Suite
- Web Hacking
- Ethical Hacking
- AppSec for Developers
- Social Engineering (Hacking HumanOS)

Partners

ArtsSEC not only distributes this products and services, we also know and use them every day to provide creative solutions and delivering high-value services to our costumers.

wallarm
CISOFY
AUDITING-HARDENING-COMPLIANCE
PORTSWIGGER
WEB SECURITY
FraudWatch
International
BURPSUITE
netsparker
vFeed
SOLARED
CYBER SECURITY

Participation
@Security Conferences.

black hat
8.8
H2HC
HACKERS TO HACKERS CONFERENCE
DEF CON

arts·sec

Securing your
digital transformation

www.artssec.com