POSITIVE TECHNOLOGIES

POSITIVE TECHNOLOGIES APPLICATION SECURITY ASSESSMENT AND ASSURANCE SERVICES

Comprehensive Security Assurance

Infrastructure Penetration Testing

Web Application Security Assessment

Mobile Application Security Assessment

Specialized Security Assessment Services for Business Applications

Assuring and enhancing your security

UNTESTED SECURITY IS NO SECURITY AT ALL

The digital transformation of business is a bonanza for hackers—and a headache for IT security teams. Companies must cover every possible security gap to prevent breaches, while hackers only need to be right once to succeed. So to prevent cyberincidents, it's essential to find and fix every vulnerability.

We wish application security was as simple as a one-time "set and forget" task you could easily do yourself, but it isn't. AppSec MUST be an ongoing process. Companies need their whole infrastructure, including web and mobile applications, to operate securely, 24/7. AppSec is mission-critical.

Assurance in action: the importance of getting a second opinion

Positive Technologies recently provided Assurance Services to a large bank. Like any smart company, the bank already invests wisely in security, including a web application firewall. Existing cybersecurity processes also include regular penetration testing. But the bank constantly seeks new ways to improve security of its customers and assets, so it asked expert pentesters from Positive Technologies to perform validation pentesting. They found:

+ Five active attack vectors, any one of which could be used for intrusion.
+ Four out of five of these vectors exploited web vulnerabilities.
+ Two systems with functioning web shells (scripts allowing remote access) that had been left exposed. These triggered a forensics investigation.

The result? The bank now has a clear view of significant security holes that were putting its operations, customers, and reputation at huge risk. It also has visibility of shortcomings in current security arrangements, and recommendations from Positive Technologies to enable prompt remediation.

The Positive Technologies team of security professionals knows exactly how hackers think. This helps us predict how they will act and keep our clients one step ahead, creating security services and solutions that adapt to the changing threatscape. Our clients not only get visibility of vulnerabilities sooner, they have expert help to resolve them quickly.

Don't settle for superficial security

Our mission is not to check your system once, tick a compliance box, and then disappear. We build long-term relationships with clients who view us as trusted advisors, helping to enhance their security, build their confidence, and proactively protect themselves against threats that aren't yet known.

Positive Professionals: Not just another set of pentesters

Your organization's security needs are complex. Flaws won't always be found by standard tests and tools. Our dedicated team of pentest professionals has assessed hundreds of global networks. You can trust them to test your security systems to the limit, reveal the true level of risk, and ensure best return on your AppSec investments.

PENETRATION TESTING: GIVING YOU TOTAL VISIBILITY

Penetration testing (pentesting) means looking at digital infrastructure through a hacker's eyes, to find the vulnerabilities that a real attacker would try to use. We conduct dozens of pentests each year at large international companies, including many that already have web application firewalls and regular testing regimes. Time and again we see that security-conscious companies can still fall victim to hackers. Here's what we've found in our pentests over the last three years:

70% of pentests result in successful intrusion—even though most of the companies already have regular security assessments to eliminate vulnerabilities

By continuing what our testers did, real attackers could have obtained full control over company infrastructure in 80% of tests (in 2016, it was 100% of tests!)

Every system tested was vulnerable. In some cases, as many as 10 separate attack vectors were found which, in combination, led to successful intrusion

Our experts have often caught and stopped targeted attacks (APTs) that were currently in progress

What we do: Expert services from dedicated pentest professionals

+ **Perimeter and internal applications inventory.** Large companies are diverse environments with many constantly-changing parts. You can't provide adequate protection until you know exactly what is there.
+ **Evidence of the weak spots in your infrastructure and a demonstration of potential attacks.** Our auditors will act like external attackers, trying to bypass protection measures and break into your company's network.
+ **Ongoing expert support and advice.** Every pentest report includes expert recommendations for remediation and mitigation of the threats found.
+ **Validation testing.** To ensure maximum security, our testers will return after an agreed period to verify whether your security team have successfully eliminated all the security flaws found.

How we do it: a comprehensive approach

Like real hackers, our testers combine techniques and tools, piecing together weaknesses that could let hackers through your perimeter:

+ **External penetration testing:** discovers vulnerabilities used by attackers without rights or inside knowledge of your system.
+ **Internal penetration testing:** looks for attack vectors accessible to users who are physically inside your perimeter, ensuring privileges cannot be misused.

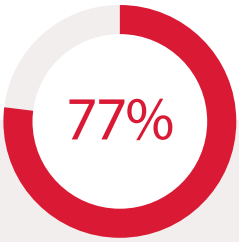
Penetration testing projects can be extended on demand with additional services such as: wireless networks security assessment and sociotechnical penetration testing (using attacks based on social engineering techniques).

WEB APPLICATION SECURITY ASSESSMENT: FINDING THE WEAKEST LINK

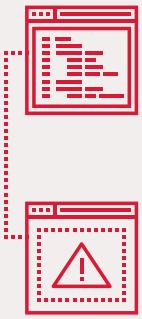
Almost all web applications are vulnerable. Even if your app doesn't contain critical vulnerabilities (and in our experience most of them do) you're still exposed: hackers can combine medium severity vulnerabilities to find a way in.

Web applications with critical vulnerabilities

Web applications with medium severity vulnerabilities



Successful intrusions through web vulnerabilities (pentests)



The combined findings of all penetration testing performed by Positive Research during 2016.

As business-critical applications grow in both number and complexity, IT security must keep pace. Especially as apps make up a growing percentage of perimeter infrastructure.

Even if you think your web apps would offer little value to hackers, remember that a poorly protected app is an open door to your entire infrastructure. As we have seen, 77% of successful intrusions by our pentesters were due to web vulnerabilities.

Diving deeper for full disclosure

So why aren't these flaws being picked up by existing security tools and procedures? It's because they're not looking deep enough. Positive Technologies web application security assessment services analyze both the application and the constantly-shifting environment it operates in. Unlike cursory "set and forget" testing solutions, our team combines 15-years of proven human expertise with cutting-edge in-house smart testing tools to deliver:

Comprehensive assessment of web-based applications. Examines the app thoroughly with both manual approaches and automated tools. Black-box, gray-box and white-box techniques are combined with instrumental security analysis via PT Application Inspector.

Exceptional accuracy and visibility. Probability assessments determine the likelihood that attackers will exploit the identified flaws. Used alongside our practical demonstrations of exploitation techniques, this helps you focus on tackling your greatest risks.

Recommendations for fixes and remediation. Detailed reports include recommendations for eliminating the detected vulnerabilities and boosting security of both applications and your whole perimeter.

Verification of vulnerability elimination. We'll return to validate whether you have successfully eliminated the vulnerabilities found.

MOBILE APPLICATION SECURITY ASSESSMENT: THE CINDERELLA OF SECURITY

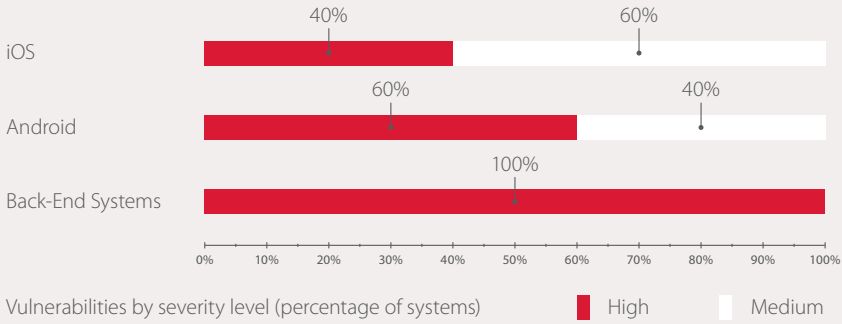
Balancing customer satisfaction with application protection

The public has largely shaken off its distrust for mobile services. Consumption is growing—along with users' appetite for new services and features. But hackers are capitalizing on these new opportunities and generally poor security awareness. As mobile becomes not just the first, but the ONLY platform of choice for banking, e-commerce, and many other industries, safeguarding customers must rank as a priority alongside protecting your own infrastructure.

The Mobile Banking Revolution

The majority (54%) of consumers say they use a mobile banking app—up from 48% in 2015. Millennials are the most likely to use the app (75%), also up from 59% in 2015

(Bank of America, Trends in Consumer Mobility Report, 2016)



Any attack that interrupts services, puts confidential data at risk, or makes customers vulnerable to direct attack via their own mobile device is sure to send existing customers into the arms of your competition. The long-term damage to your brand and reputation could be catastrophic.

Unprotected back-end: The illusion of security?

While the importance of web application security is well understood by most large companies, mobile security is still underserved. This exposes mobile users to more hacks, and leaves server-side infrastructure at risk. Organizations may believe web applications to be an easier target, but on the server-side, mobile apps use the same web technologies and face the same range of risks.

Addressing the whole mobile app environment

Positive Technologies mobile application security assessments uncover vulnerabilities in both the application client and its server-side infrastructure, providing objective and independent assessment of the overall security level. This helps organizations reduce operational, financial, and reputational risk. An assessment typically includes:

+ **Mobile application back-end assessment.** Uses the same combination of black-box, gray-box and white-box testing as our web app assessments, alongside code review using PT Application Inspector.
+ **Deep client-side security assessment.** Reveals client-side-specific vulnerabilities such as sensitive data stored in clear-text and the ability to gain unauthorized access to the application's critical functionality (for example, financial transactions).

SPECIALIZED SECURITY ASSESSMENT SERVICES FOR BUSINESS APPLICATIONS

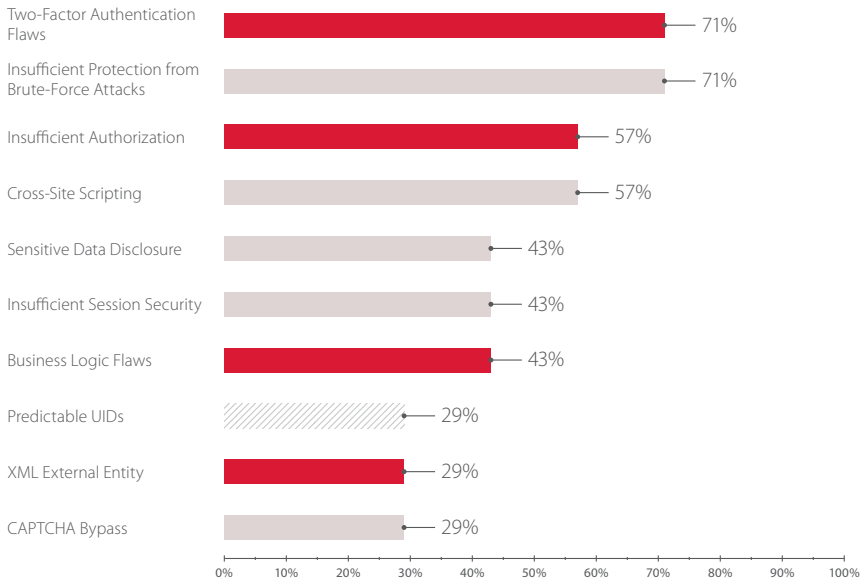
From online and mobile banking to e-commerce, customer-service portals and ERP systems, almost every industry uses business-critical applications to automate daily operations and better serve their customers. While these specialized apps may vary widely in their business logic, complexity and the degree of sensitive data they contain, they are all essential to business continuity. They must be protected from attack. Many of these apps are at least partially web-based, but some operate within a web-browser ("thin clients") which makes them a target for web threats. Others ("rich clients") are resistant to those same web threats but still vulnerable to other attacks.

Securing business application is made harder because many were developed before AppSec risks were fully understood. Organizations rely on such legacy software to maintain critical processes, leaving them reluctant to retro-fit security measures for fear of interrupting normal business operations.

Our tailored services give clients a comprehensive view of their risk from business-critical applications, along with detailed recommendations. Our thorough examine of critical functions includes:

+ Identification, authentication, two-factor authentication (2FA) and authorization
+ Business logic
+ Web security assessment (if applicable)
+ Rich client application reverse engineering (if applicable)

The diagram below illustrates the results of our business application security assessments in exposing the risks faced by the banking sector.



Top 10 online bank vulnerabilities — High — Medium — Low

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com