POSITIVE TECHNOLOGIES

WEB APPLICATION ATTACK STATISTICS

2017 IN REVIEW

CONTENTS

TRENDS AND FORECASTS

Throughout 2017, we published quarterly reports on web application attacks. This review will briefly summarize the outcomes of 2017 and expectations for 2018.

Government

Attacks that use the websites of unwitting third parties as the method for initial infection of user workstations are becoming increasingly common. For such attacks, hackers prefer using official government websites, because they are regarded by users as highly trustworthy.

In addition, since government websites attract the attention of the media, criminals may deface these sites for the sake of publicity.

2017 saw successful attempts to use cyberattacks as a way to affect the political situation. In 2018, a big and tempting target for attackers will be websites connected with presidential and parliamentary elections in a number of countries, including Latvia, Brazil, and Mexico. We also expect a wave of attacks against websites related to this year's major sports event, FIFA World Cup 2018.

Banks and e-procurement platforms

Attacks on financial web applications still tend to target users. Attackers are lured by the funds they can steal from users of online banking or payment systems. What's more, web applications are a weak spot in bank security. Therefore attackers continue to target bank sites in order to penetrate internal infrastructure and steal money via banking systems.

The cryptocurrency boom and plethora of initial coin offerings (ICOs) in 2017 also attracted the attention of hackers, who actively exploited web application vulnerabilities in attacks against ICOs and cryptocurrency exchanges. It seems unlikely that criminals will pass up such a lucrative method this year.

Healthcare

Attacks against healthcare web applications primarily aim to access patient data, which can be used for blackmail or sold on the darknet. Healthcare websites, like government websites, usually have relatively weak protection. Poor defenses make these websites popular among hackers as a way to infect users' computers with malware, such as for mining cryptocurrency.

Education

Information technology in education provides unscrupulous students with new opportunities to "improve" their performance by hacking electronic gradebooks, obtaining exam materials, or adding their names to admission lists. We saw examples of such attacks last year, and expect that their number will increase.

Energy and manufacturing

Although attacks on energy and manufacturing web applications were relatively few, they were particularly dangerous due to the high skill level and meticulous planning demonstrated by the attackers. We expect attackers to redouble their interest in these sectors, but this increase may not be reflected in the number of attacks. Rather, they will focus on using more sophisticated attack techniques that are more difficult to detect.

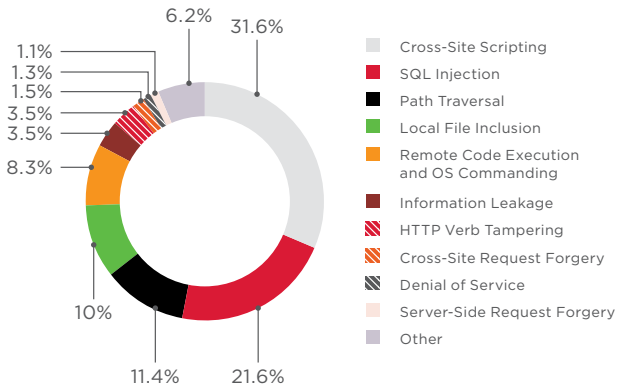
Information technologies

Web applications in the IT sector received the largest number of attacks. Such attacks are becoming more frequent because hackers can use the websites of trusted technology companies to distribute malware or attack website users. We expect this method of spreading malware in both mass and targeted cyberattacks to gain popularity among attackers.

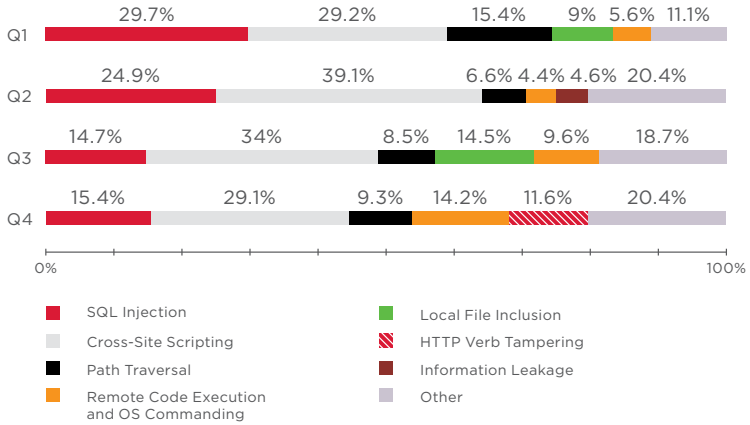
WEB APPLICATION ATTACKS: STATISTICS

Attack types

Throughout 2017, changes in the relative frequency of the five most common attacks were minor. Cross-Site Scripting, which targets users, made up almost one third of the total number of attacks. Other popular attacks involved the ability to access data or execute commands on the server: SQL Injection, Path Traversal, Local File Inclusion, and Remote Code Execution and OS Commanding.



Top 10 web application attacks



Top five attacks in 2017 by quarter

Statistics by sector

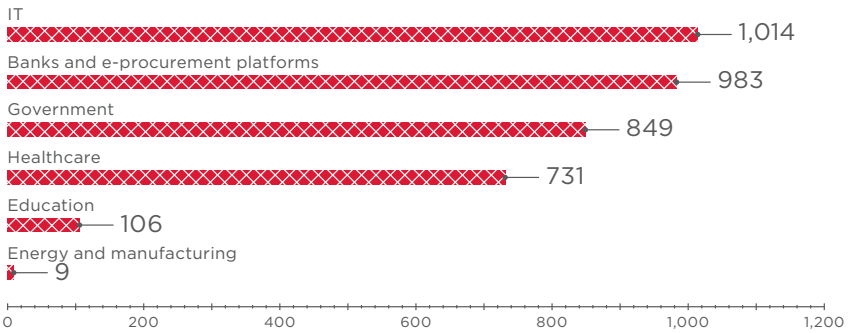
Average number of attacks per sector

In 2017, web applications for IT and finance, particularly banks and e-procurement platforms, suffered the largest number of attacks per day—over 900. Attackers are lured by the possibility of profit from compromising banking applications or attacking users. IT may be attractive for attackers because of its customers, who tend to hire external contractors to support their business processes, internal infrastructure, or web applications. Access to an IT company can open the door for hackers to access the infrastructure of its clients. Last year, a mass cyberattack using NotPetya encryptionware started with the hack of a company that develops accounting software.

Government and healthcare websites also attract attackers. Throughout the year, we saw numerous successful attacks against government websites in pursuit of achieving political aims or infecting ordinary users with malware. High-profile cases in healthcare consisted primarily of information leakage and extortion (demanding money for deletion of stolen data).

Education websites suffered fewer attacks. Educational institutions have little to offer profit-driven criminals, so students themselves are usually the culprits: they try to either alter their grades in electronic gradebooks or obtain access to exam materials.

Manufacturing and energy were the rarest targets for attackers, with a company experiencing a mere nine attacks per day. In these cases, attackers' objective is usually to access the corporate network. These attackers tend to be among the most skilled; they meticulously plan their actions and act as stealthily as possible to avoid detection during the early stages of an attack.



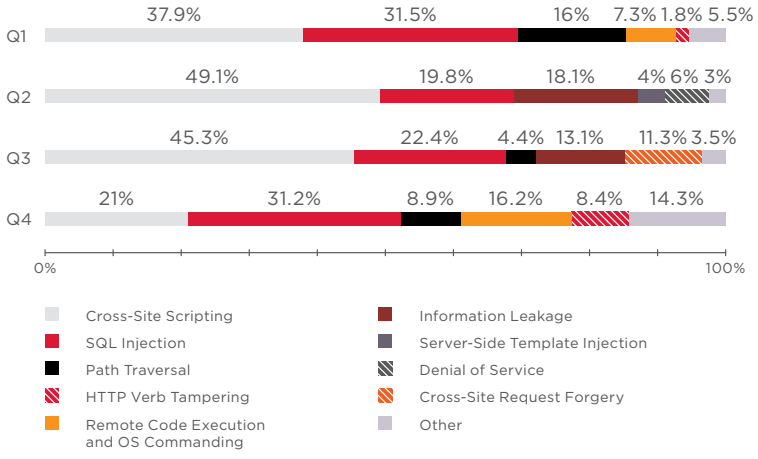
Average number of attacks on a company's web applications per day

Let's review the most common attacks in each sector and trace the changes that occurred in 2017.

Government

In 2017, the most common attacks against government websites were Cross-Site Scripting and SQL Injection, which totaled more than half of all attacks. This high rate of attacks against users is most likely caused by two reasons. Firstly, users of government websites tend to be not security-savvy. As a result, attackers can easily infect their computers with malware. Secondly, government websites may be an intermediate link in a watering-hole attack against another company, if that company's employees regularly visit an official government website as part of their work. The computer of an employee of the target company may then be infected, leading to a breach of the network perimeter and penetration of corporate infrastructure. Early 2017 saw revelation of a large-scale campaign in which code was injected by attackers on the websites of embassies and other authorities, which infected the devices of website visitors with malware. Later on, the U.S. National Foreign Trade Council was hacked with the same aim.

Government websites may also be attacked for political reasons. In 2018, a big and tempting target for attackers will be websites connected with presidential and parliamentary elections in a number of countries, including Latvia and Brazil. Government websites can be hacked in cyberwarfare to give credibility to incendiary materials: fake news planted on the official website of a Ministry of Foreign Affairs can trigger a diplomatic row and put a strain on international relationships. One such attack was performed in Qatar in early 2017: hackers published fake remarks attributed to the emir of Qatar, causing a crisis in diplomatic relationships with other countries.

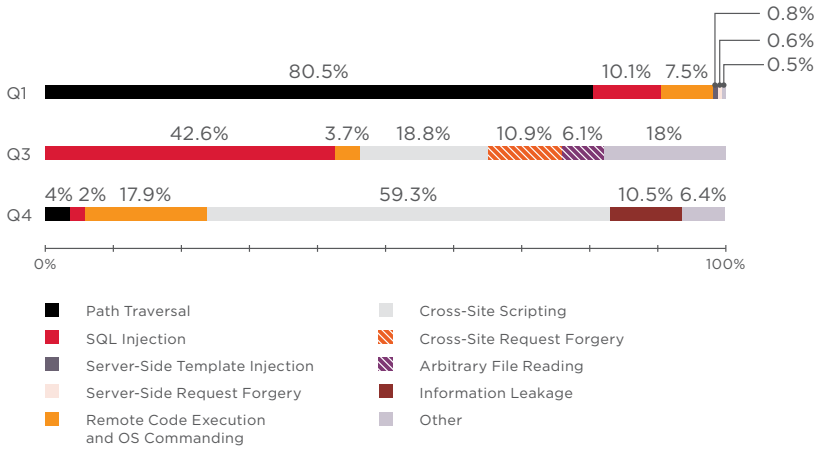


Top five attacks on government web applications

Banks and e-procurement platforms

In 2017, attacks against banking web applications (SQL Injection, Remote Code Execution and OS Commanding) aimed to execute commands on the web application server in order to identify flaws in network perimeter protection. As found during our penetration tests, web application vulnerabilities were the only vector for penetration of bank intranets. The fourth quarter saw a sharp rise in Cross-Site Scripting attacks against bank customers, which can be explained by the increased number of transactions performed by customers during the holiday season.

2017 saw a cryptocurrency boom and plethora of ICOs, which immediately attracted hackers' attention. Most attacks against cryptocurrency exchanges and ICO platforms took advantage of poor web application security. Examples include attacks on CoinDash and Enigma Project, in which hackers changed wallet addresses on ICO websites to dupe investors.

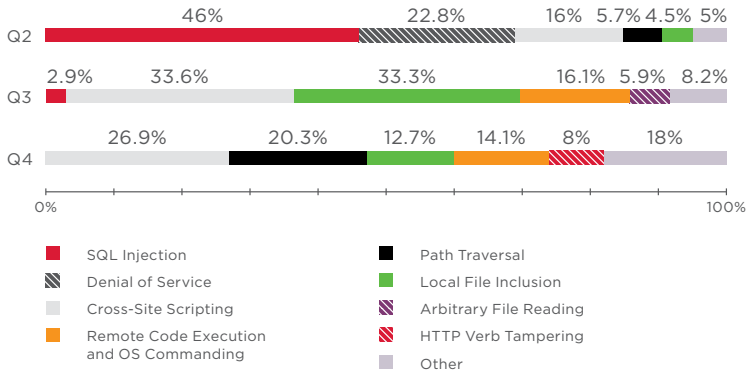


Top five attacks on banking web applications and e-procurement platforms

Healthcare

Attacks on healthcare websites had varying motivations. Throughout 2017, we saw attacks aimed at gaining control of a server or accessing data. On multiple occasions, media reports described leaks of data from medical centers, followed by a ransom demand sent to clinic management and patients. One incident occurred at a Lithuanian plastic surgery clinic, when over 25,000 photos, including unclothed "before" and "after" pictures, were made public. For deleting the data, the hackers are reported to have demanded a ransom from both the clinic (EUR 344,000) and its clients (up to EUR 2,000 each). In October, a plastic surgery clinic in the United Kingdom was attacked, with hackers obtaining photos of patients, including celebrities and high-profile clients.

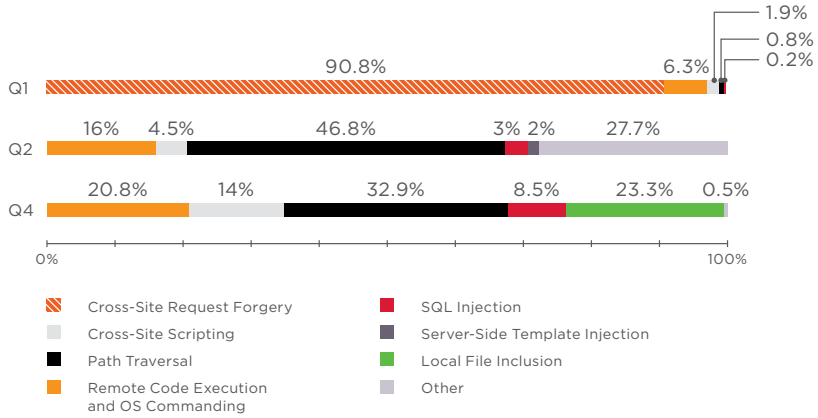
Healthcare websites have the same problem as government ones: although they are regarded by users as highly trustworthy, the users of these websites are unlikely to know the basics of how to stay safe online. Therefore users may fail to pay attention to suspicious activity on their computers while visiting such websites. Throughout the entire period considered, hackers conducted attacks that would facilitate injection of malicious code on websites (including Cross-Site Scripting, Remote Code Execution and OS Commanding, and SQL Injection) in order to infect a user's computer with malware most commonly intended to steal bank accounts or use the victim's CPU to mine cryptocurrency.



Top five attacks on web applications of healthcare institutions

Education

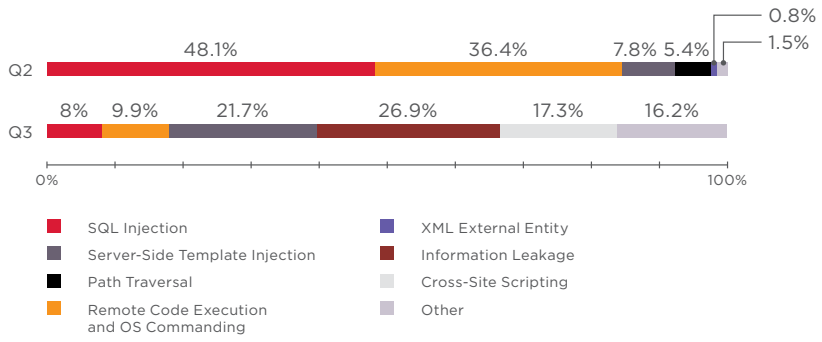
For education, the latter half of 2017 was dominated by attacks aimed at gaining control of a web application or server and at obtaining data: Remote Code Execution and OS Commanding, Path Traversal, and SQL Injection, among others. Attackers were mostly students desperate to improve their grades. The results in the first quarter were likely distorted by the small size of the dataset.



Top five attacks on web applications of educational institutions

Energy and manufacturing

Energy and manufacturing websites were tested during Q2 and Q3. Attacks detected during this period mostly aimed to execute commands on the web application server and, in some cases, to obtain information needed to continue an attack, including SQL Injection, Remote Code Execution and OS Commanding, and Server-Side Template Injection. The goal of these attacks was to obtain access to corporate IT networks and, ultimately, industrial networks containing ICS/SCADA components. Process disruption may lead to accidents and damage to expensive equipment, causing large costs in the form of repairs and lost profits, or even environmental disaster and loss of life.

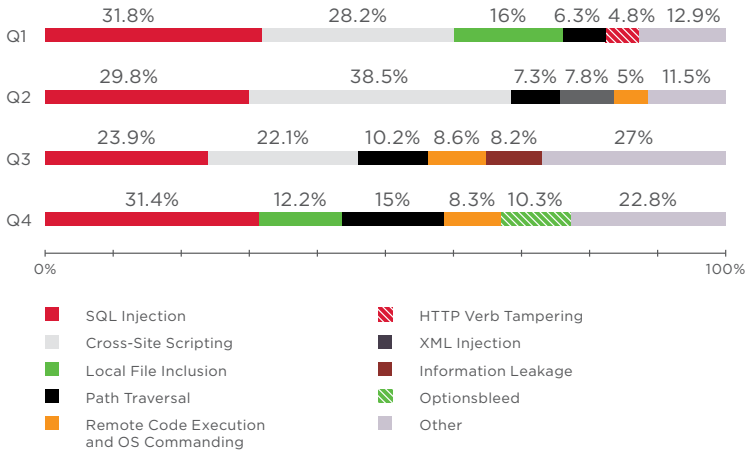


Top five attacks on energy and manufacturing web applications

Information technologies

For IT web applications, SQL Injection attacks dominated in all four quarters of 2017, followed by Cross-Site Scripting, Local File Inclusion, Path Traversal, and Remote Code Execution and OS Commanding. In our assessment, IT web applications are increasingly targeted in attempts to compromise trusted sources as a way to spread malware. For instance, June 2017 saw a cyberattack involving NotPetya encryptionware. The epicenter of the outbreak was a developer of accounting software. In the fall, malicious code was also detected in the installer for CCleaner hosted on the utility's official website. Using the website of a well-known IT company (such as a network equipment, software, or service provider) as a command-and-control server or malware distribution source is advantageous for attackers, because connections to the IP addresses of such companies tend to not raise suspicions among administrators and security. In addition, attackers can obtain information necessary for attacks on the company's customers. Data leakage from Amazon Web Services is one example of such an attack.

In Q4, attacks exploiting the Optionsbleed vulnerability (CVE-2017-9798) took their place among the top five attacks. Notably, the first attempts to exploit the vulnerability (in Q3) were recorded only three hours after detailed information about the vulnerability was published. This short head start gave defenders no opportunity to take countermeasures.



Top five attacks on web applications of IT companies

CONCLUSION

As we saw in 2017, attacks against web applications had diverse motivations: theft of funds, financial gain via ransom, penetration of internal infrastructure, political goals, espionage, and more. Any web application, even if it is not itself a target, may be of interest to attackers. Web applications not properly secured by their owners tend to be easy pickings for hackers and can be used in a mass or targeted cyberattack.

Detecting vulnerabilities as part of comprehensive web application protection requires security assessment, including source code audits, at every stage of development and in production. Software components of web applications should also be updated on a regular basis. But even these protection measures may not be enough: attackers keep a close eye on new vulnerabilities as they are published, rushing to try them out before defenders can react. According to our research, the time between a vulnerability being published and attempts to exploit it in 2017 was as little as three hours. Software developers might have no chance to remediate the vulnerability and release patches before attacks start. Therefore, effective measures against attackers should include additional preventive security tools, such as a web application firewall (WAF), to detect and prevent attacks against web applications without delay. A WAF can do more than protect from known attacks at the level of applications and business logic: it also detects attempts to exploit zero-day vulnerabilities, prevents attacks against users, and analyzes and correlates events in order to build attack chains. Performing these tasks requires advanced implementations of normalization, heuristics, machine learning, and behavioral analysis. Another useful function is interaction with external security information and event management (SIEM) systems and notification to network-level DDoS protection tools. In concert, these steps enable stopping attackers in due time.

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