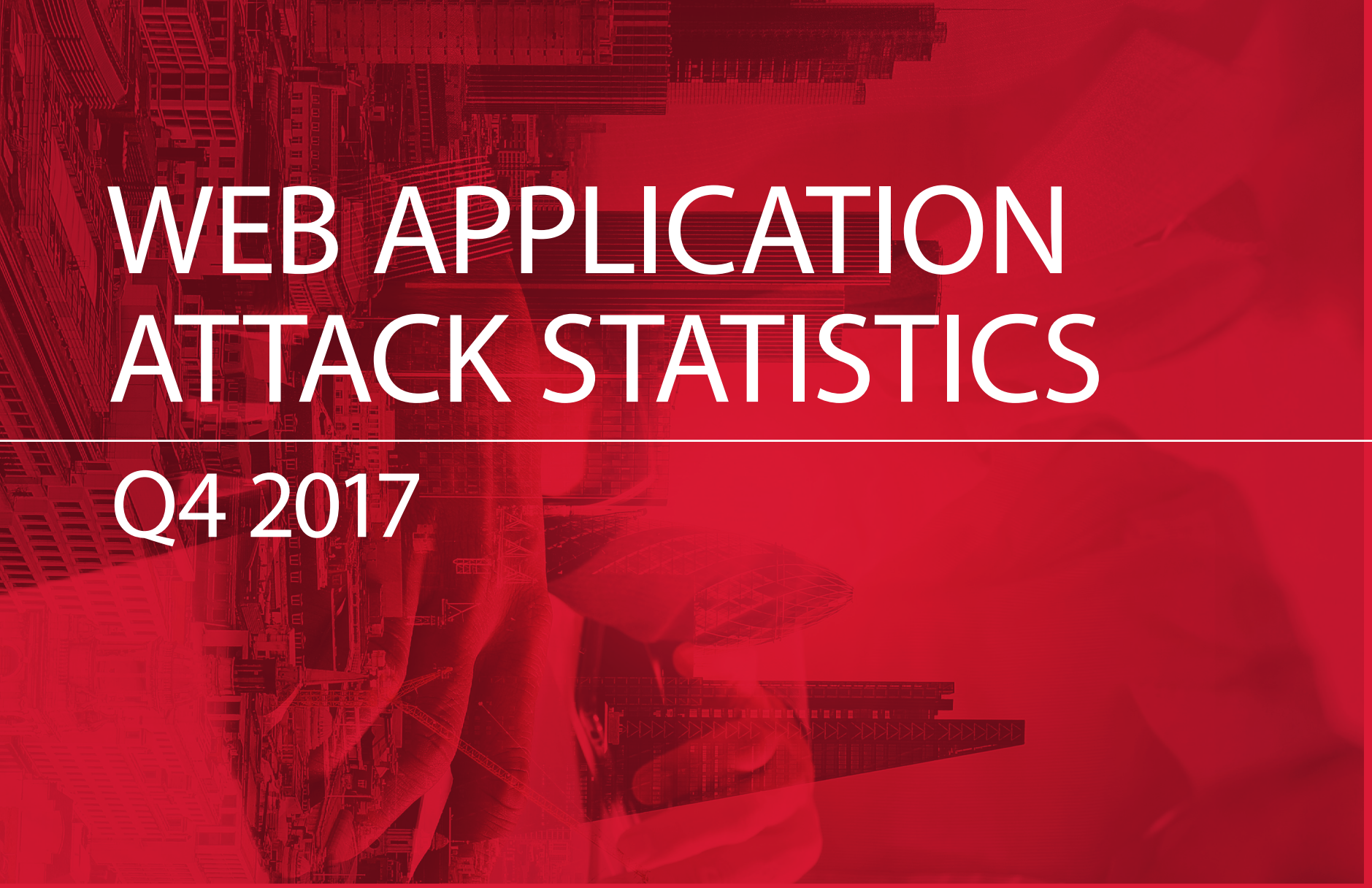


WEB APPLICATION ATTACK STATISTICS

Q4 2017

POSITIVE TECHNOLOGIES

CONTENTS

INTRODUCTION

This report provides statistics on attacks performed against web applications during the fourth quarter of 2017. Sources of data are pilot projects involving deployment of PT Application Firewall, as well as Positive Technologies' own PT AF installations.

The report describes the most common types of attacks, objectives, intensity, and time distribution of attacks. It also contains statistics by industry. With this up-to-date picture of attacks, companies and organizations can monitor trends in web application security, identify the most important threats, and focus their efforts during web application development and subsequent protection.

To obtain more consistent results, automated vulnerability scanners (such as Acunetix) have been excluded from the data used here. The example attacks presented in this report have been manually verified to rule out false positives.

Protection data for Positive Technologies itself has been classified under the IT sector for reporting purposes.

RESULTS AT A GLANCE

Approximately 40% of attacks

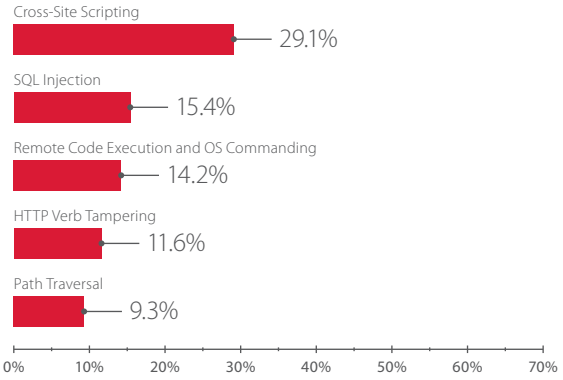
are aimed at accessing data

1 out of 3 attacks

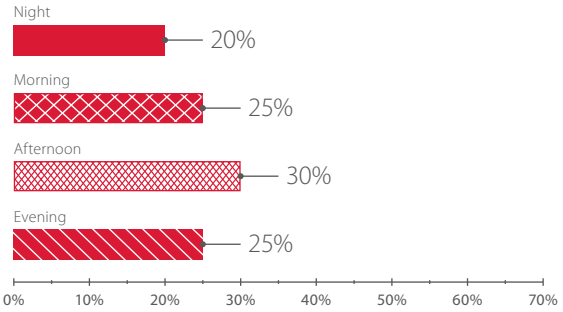
is aimed at web application users

34,629

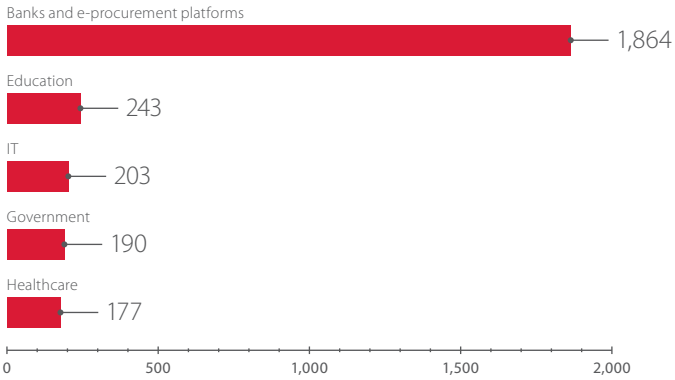
highest number of attacks on a company in a single day (pilot projects)



Most frequent attacks



Distribution of attacks by time of day (local time of target)

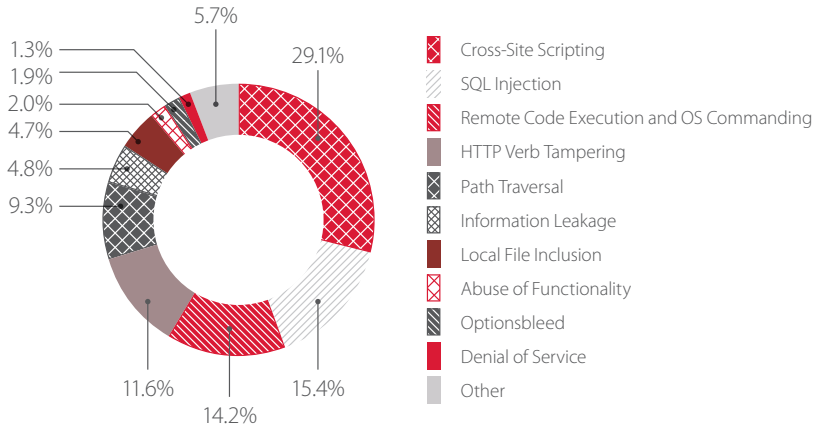


Average number of attacks per day per company

WEB APPLICATION ATTACKS: STATISTICS

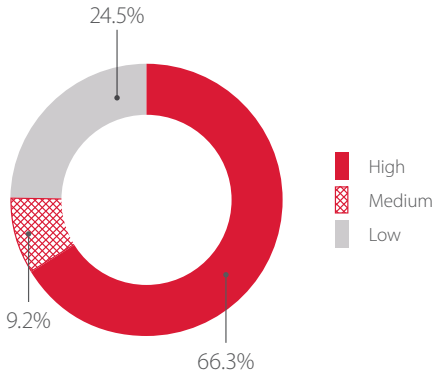
Attack types

In Q4 2017, Cross-Site Scripting and SQL Injection were still the most common web application attacks and made up nearly half of the total. But unlike the previous quarter, Cross-Site Scripting took first place in the list. Successful exploitation of this vulnerability allows attacking web application users and infecting their computers with malware. In addition, Remote Code Execution and OS Commanding almost doubled in frequency. These dangerous attacks have the potential to provide attackers with full control over the server hosting a web application. This type of attack took third place. The relative frequency of other attacks was essentially the same as in previous quarters.



Web application attacks: types

The distribution of attacks by degree of risk (as classified by PT AF) is shown in the following graph.



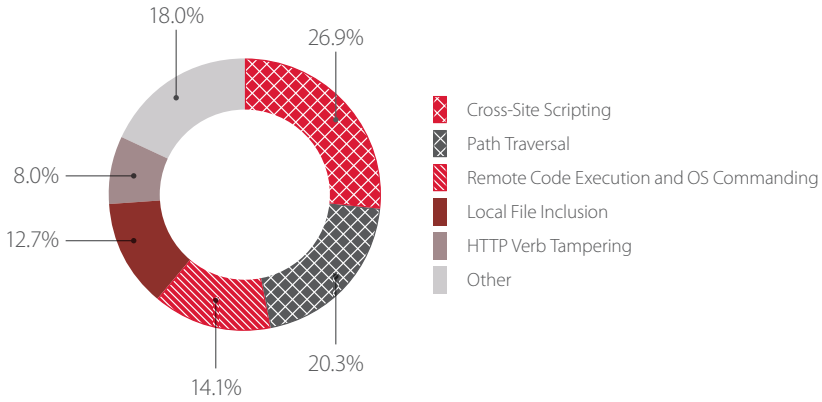
Distribution of web application attacks, by severity level

Statistics for web applications by industry for Q4 cover the following sectors: healthcare, education, banks and e-procurement platforms, IT, and government. Attack data for any given industry may vary across periods, because the particular web applications protected in PT AF pilot projects change from quarter to quarter.

Healthcare

Most healthcare web applications tested in the fourth quarter were online appointment booking systems. Users of such web applications are often not security-savvy, which makes them a prime target for attackers.

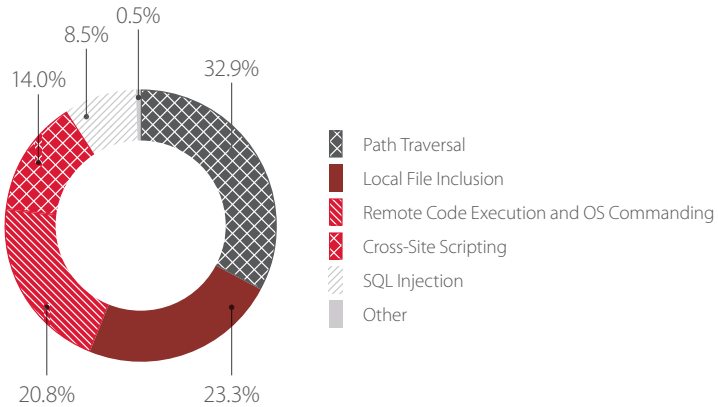
When implementing Remote Code Execution, OS Commanding, and Local File Inclusion attacks, hackers are not necessarily hoping to gain LAN access, bring an application offline, or obtain sensitive data. Sometimes the exploitation scenarios are more original. One recent incident involved malware for mining Monero cryptocurrency, which had been planted on the online appointment booking website of a regional health agency. The undocumented script was intended to earn cryptocurrency by using the CPU capacity of website visitors. The malware performed mining for as long as the website was open in the user's web browser; when the user closed the site, the mining stopped. The script may have been the result of a successful web application attack. However, opportunities to make extra money could also be tempting to an unscrupulous system administrator.



Types of attacks on web applications of healthcare institutions

Education

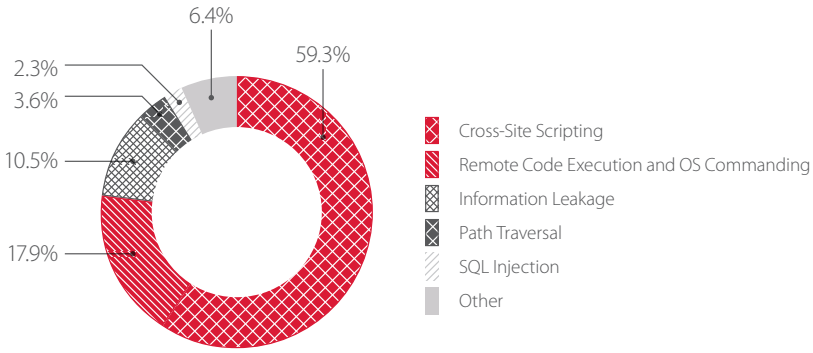
Our monitoring results show that educational websites are mostly attacked by their students. The main target is to access data that they could use to boost grades, such as exam materials, by implementing Path Traversal and Local File Inclusion attacks. Some attackers attempt to use SQL Injection to "improve" their current grades, alter exam results, or add their names to lists of scholarship winners.



Types of attacks on web applications of educational institutions

Banks and e-procurement platforms

In Q4, we assessed not only banking web applications, but also e-procurement platforms for auctions, bidding, and procurement. Considering the large number of visitors typical for such websites, attackers first try to identify whether a website is vulnerable to Cross-Site Scripting and, if so, use it to distribute malware among website visitors and vendors. Moreover, successful Remote Code Execution and OS Commanding can bring an e-procurement platform to a halt and disrupt scheduled auctions. Such malicious actions can result in complaints from users and fines from government regulators. Attackers are especially interested in auction bids and offers on procurement websites, since these business secrets can be used by competing companies to obtain an unfair advantage.

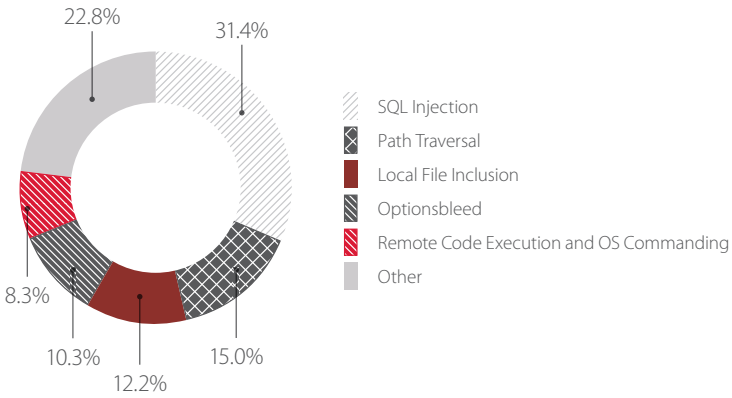


Types of attacks on web applications of banks and e-procurement platforms

IT

Q4 is different from previous quarters for IT web applications mostly because of a significant reduction in Cross-Site Scripting attacks. The reason is that some of the web applications included in this quarter's research do not have the visitor numbers that, for an attacker, would make them attractive for spreading malware to visitors. The most common type of attack on IT web applications is SQL Injection. An example of successful SQL Injection is an attack on Hetzner,[1] an Internet hosting company and data center operator. In November 2017, hackers gained access to client data (including names, addresses, and phone numbers), domain names, FTP passwords, and payment information (except for credit cards).

This quarter was notable for two things: an increase in the number of Optionsbleed attacks and a case of successful prevention of botnet attacks on the news website of an IT company with the help of PT AF. Both Optionsbleed and botnet attacks will be reviewed later in this report in more detail.

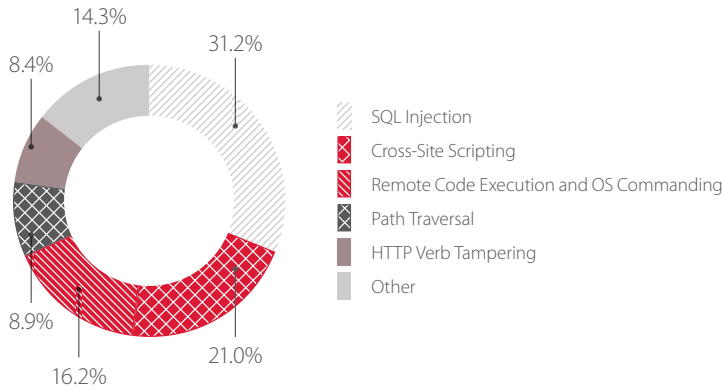


Types of attacks on web applications of IT companies

1 hetzner.co.za/news/konsoleh-database-compromise/

Government

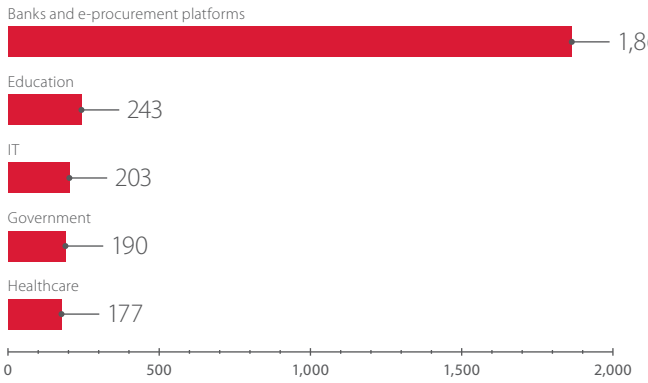
Most government web applications are intended either for handling personal data or for providing information and news to the public. Attackers usually start with SQL Injection and Path Traversal to gain unauthorized access to personal data and other sensitive information. Web application users were the target in every fifth attack. Attackers take advantage of the fact that most users of government web applications are not well-versed in technology and security.



Types of attacks on web applications of government institutions

Average number of attacks per sector

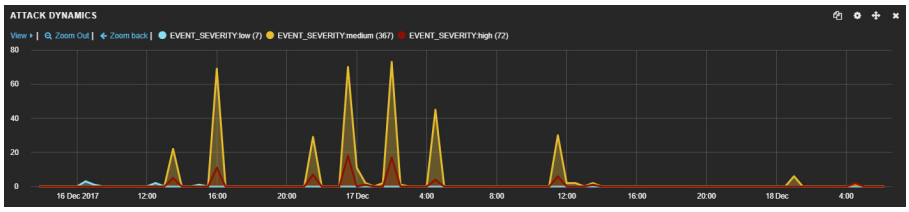
Banks and e-procurement platforms took the brunt of attacks in the outgoing quarter, recording the highest number of events per day of any sector. This large difference from other sectors has two explanations. First, attackers can directly profit from successful attacks on online banking applications and their clients. Second, information obtained by compromising e-procurement platforms can be sold to other bidders and competitors.



Average number of attacks per day, by sector

Attack examples

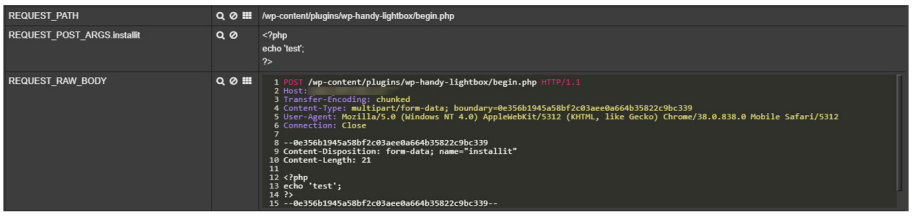
Results of a pilot PT AF deployment in the IT sector showed a number of attempts to exploit recently disclosed vulnerabilities in the WordPress content management system. Subsequent investigation revealed that these attacks were most likely performed using a botnet with more than 300 devices. Over 400 HTTP requests were sent within one day, while the attackers tried to stay unnoticed as much as possible, with each botnet host sending a maximum of two requests.



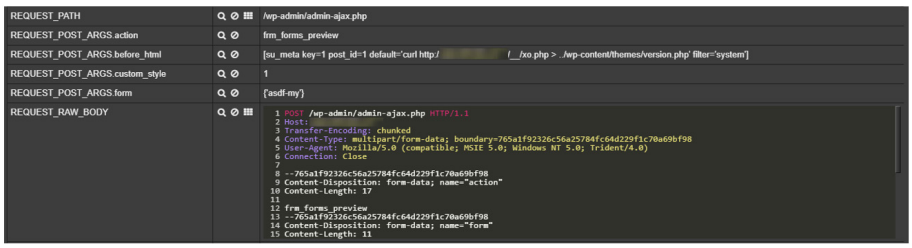
Attacks against a WordPress-based application on December 17—18 (screenshot from PT AF)

high	Local File Inclusion	A Local File Inclusio...	[redacted]	REQUEST_ARGS.book...	162.245.81.239
high	OS Commanding	An OS Command Injecti...	[redacted]	REQUEST_ARGS.regist...	222.255.122.58
high	OS Commanding	An OS Command Injecti...	[redacted]	REQUEST_ARGS.checkpr	45.252.191.22
high	OS Commanding	An OS Command Injecti...	[redacted]	REQUEST_ARGS.regist...	197.232.17.83
high	OS Commanding	An OS Command Injecti...	[redacted]	REQUEST_ARGS.installit	45.115.236.80
high	OS Commanding	An OS Command Injecti...	[redacted]	REQUEST_ARGS.regist...	143.0.191.2
high	OS Commanding	An OS Command Injecti...	[redacted]	REQUEST_ARGS.installit	174.102.89.130
high	Path Traversal	A path traversal atte...	[redacted]	REQUEST_ARGS.befor...	213.233.57.135

IP addresses of botnet hosts (screenshot from PT AF)

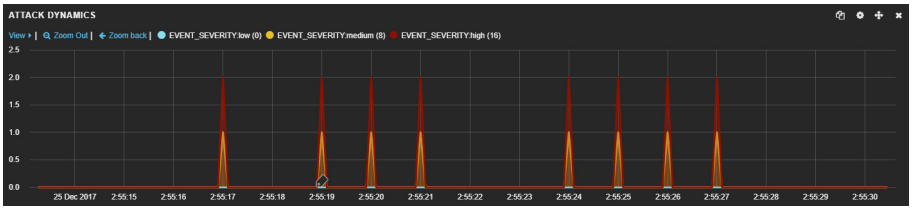


Request intended to exploit a vulnerability in WordPress (screenshot from PT AF)



Request intended to exploit a vulnerability in WordPress (screenshot from PT AF)

Another pilot project revealed a chain of attacks aimed at defacing a web application. In the space of a day, attackers tried to bypass PT AF and use a publicly available exploit in the process.[2]

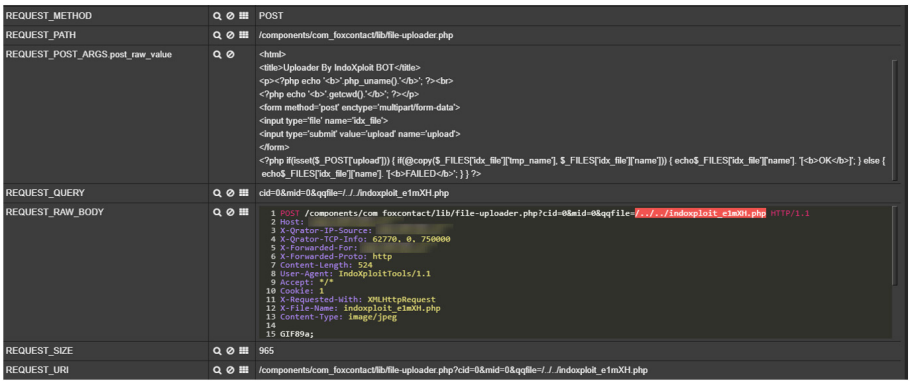


Attacks intended to deface the web application on December 25 (screenshot from PT AF)

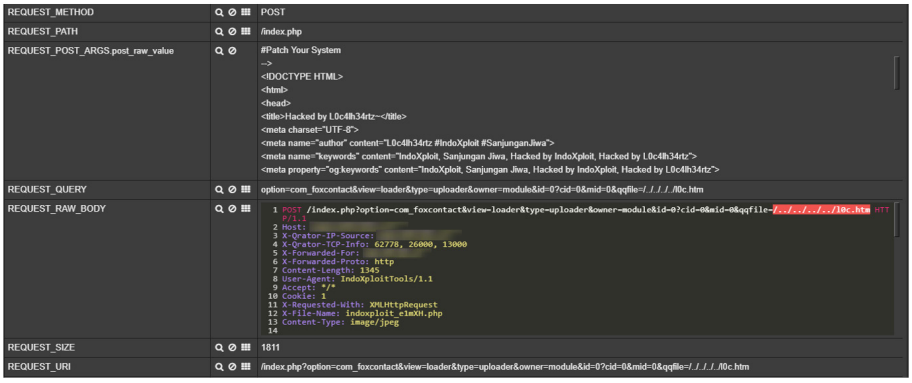
high	Path Traversal	A path traversal atte...	[redacted]	REQUEST_URI, REQU...	198.24.187.37	2017-12-25 02:55:17
high	Local File Inclusion	A Local File Inclusio...	[redacted]	REQUEST_ARGS.qqfile	198.24.187.37	2017-12-25 02:55:17
medium	Evasion	The POST request has ...	[redacted]		198.24.187.37	2017-12-25 02:55:17
high	Path Traversal	A path traversal atte...	[redacted]	REQUEST_URI, REQU...	198.24.187.37	2017-12-25 02:55:19
high	Local File Inclusion	A Local File Inclusio...	[redacted]	REQUEST_ARGS.qqfile	198.24.187.37	2017-12-25 02:55:19
medium	Evasion	The POST request has ...	[redacted]		198.24.187.37	2017-12-25 02:55:19
high	Local File Inclusion	A Local File Inclusio...	[redacted]	REQUEST_ARGS.qqfile	198.24.187.37	2017-12-25 02:55:20
high	Path Traversal	A path traversal atte...	[redacted]	REQUEST_URI, REQU...	198.24.187.37	2017-12-25 02:55:20

List of attacks intended to deface the web application (screenshot from PT AF)

2 indoxploit.or.id/2017/12/joomla-component-comfoxcontact.html

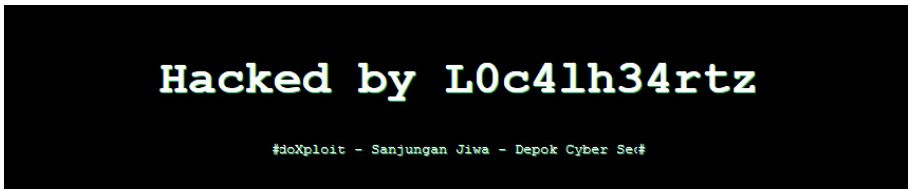


Request intended to exploit a vulnerability for the purpose of web application defacement (screenshot from PT AF)



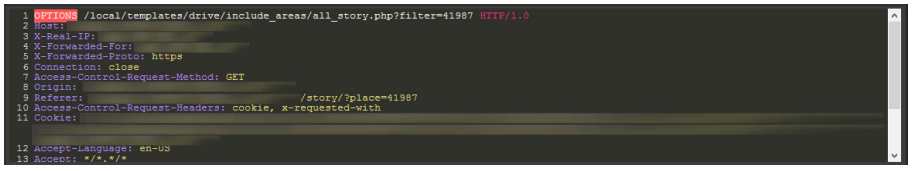
Request intended to exploit a vulnerability for the purpose of web application defacement (screenshot from PT AF)

The attack was unsuccessful, and the hackers were unable to alter the website content. However, not all web applications are properly secured by their owners. Investigation of the incident involving the attack in question revealed that the main page of other websites had been defaced by the same group (by writing the name of the hacker group on a black background). As soon as a defaced page was opened in a browser, music added by the attackers to the page HTML code started to play.

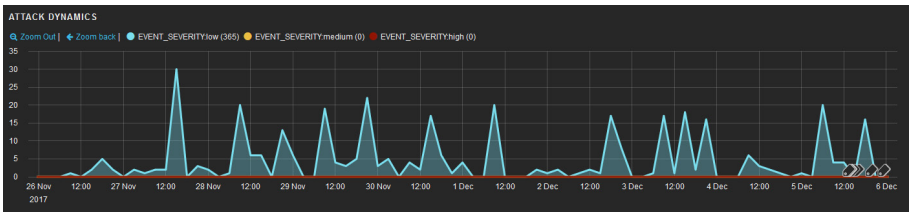


Web application start page after defacement

In our report for Q3, we wrote that PT AF recorded the first attempts to exploit vulnerability CVE-2017-9798, known as Optionsbleed, only three hours after detailed information about it was published. This quarter saw a significant increase in the number of such attacks: Optionsbleed is among the top 10 most common attacks recorded during our pilot projects.



Example of a request used in an Optionsbleed attack (screenshot from PT AF)



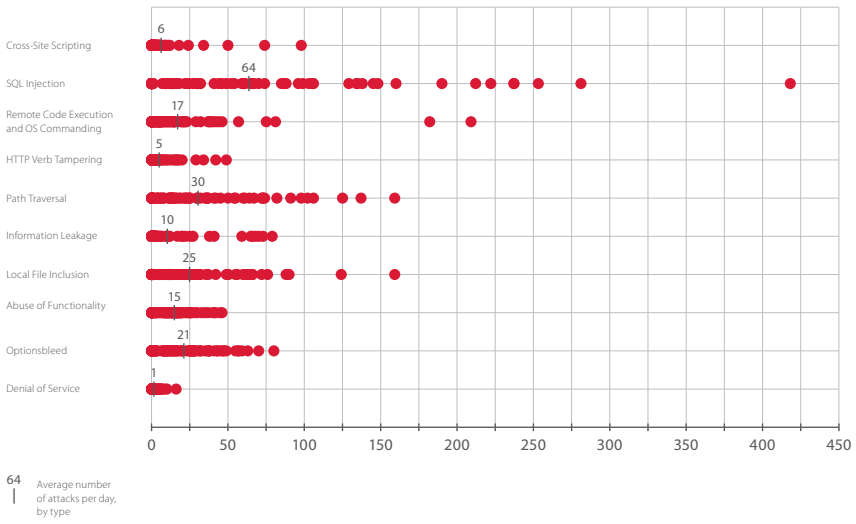
Graph of Optionsbleed attacks during a 10-day period (screenshot from PT AF)

Most Optionsbleed attacks were against websites of IT companies providing shared hosting, because only this type of hosting configuration is vulnerable to such attacks.

Attackers closely monitor publications of new vulnerabilities and create botnets to conceal their attempts to exploit vulnerabilities in websites. The most tempting targets for them are misconfigured systems or web applications with components that have not been updated.

Attack trends

The statistics collected in Q4 allow reconstructing the distribution of attacks over time. Attack trends were evaluated based on results of a PT AF pilot project, which lasted for nearly the entire quarter (80 days) starting on October 2, 2017. The graph displays the 10 most frequent attack types, with the daily number of attacks of each type. The results suggest which attack types stood out in terms of the number of requests sent by attackers.



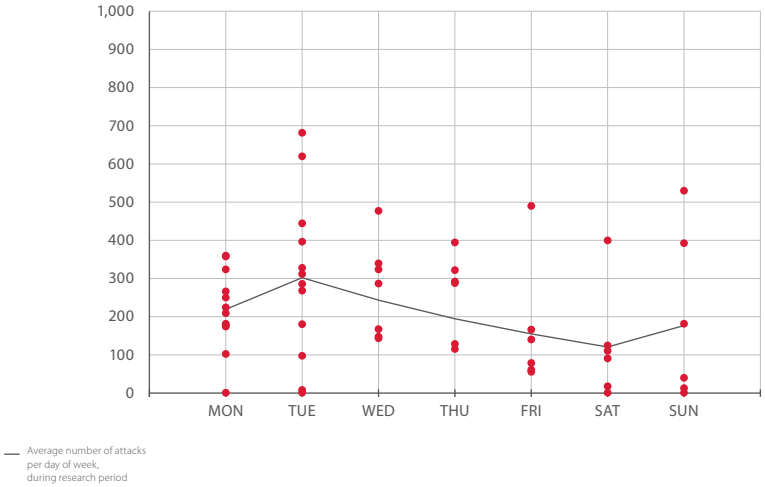
Number of attacks per day, by type

SQL Injection stands head-and-shoulders above the others as the most frequent attack type and is the second most common attack type in Q4. On some days, there were more than 250 SQL Injection attacks. The web application protected by PT AF in the pilot project received a small number of Cross-Site Scripting attacks: the low traffic of the application, among other factors, discouraged hackers from attempting attacks on users.

High-severity SQL Injection and Local File Inclusion attacks remained stable throughout the quarter, generally staying below 100 per day. This observation is explained by the fact that successfully performing such attacks requires bruteforcing improperly filtered characters or names of scripts, directories, and files. Therefore a single attack can last for several days and comprise many such attempts, which are correlated by PT AF into a single attack chain.

Overall, the average number of attacks of other types was less than two dozen per day.

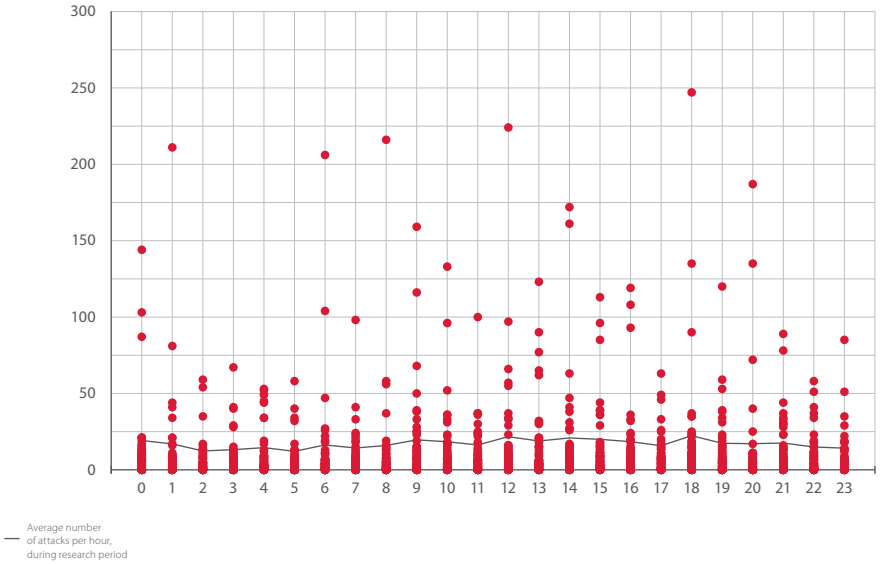
Attacks can be broken down by day of the week as well.



Distribution of attacks by day of week

The web application in question was hit by 200 to 300 attacks on average per day, rarely dipping below 100. Attackers' activity declines later in the week, but in some cases spikes have been seen on weekends as well. The maximum number of attacks recorded in a single day was 683.

Trends can be seen both by day of week and time of day. Time of day is the local time of the target.



Distribution of attacks by time of day: 0 = 12 a.m. (midnight), 12 = 12 p.m. (noon)

Q4 was consistent with the broad trends observed throughout 2017. As in the previous quarters, the number of attacks slightly increases during the afternoon and evening. When designing web application security, it should be taken into account that attackers do not restrict themselves to business hours, as the spikes on the graph prove. Most attacks during the afternoon and evening target web application users, who are particularly active during these hours. By contrast, when active during the night or morning in the target's time zone, attackers are hoping to catch defenders unaware in order to slip by unnoticed. An effective tool for consistent 24-hour threat detection and response is a web application firewall (WAF).

CONCLUSION

The fourth quarter of 2017 confirmed the fundamental trends that have been observed in previous web application reporting:

+ Any web application can be a target, regardless of its functionality.
+ Most attacks aim to obtain sensitive information or target web application users.
+ Hackers do not take holidays, weekends, or vacations. Nor do they keep regular working hours—web applications can be attacked on any day of the week and at any time.
+ As soon as a newly found vulnerability is published on the Internet, hackers race to develop exploits and try them on web applications.
+ In addition to publicly accessible ready-made exploits and tools, attackers can use botnets in automated attacks.

Therefore, effective protection requires a multipronged approach built on timely updates of web application software, periodic white-box security assessment (including source code audit) of web applications with automated scanning, and other assessment methods, complemented by proactive solutions such as a web application firewall to detect and prevent attacks against web applications.

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