WEB APPLICATION ATTACK TRENDS

2017

POSITIVE TECHNOLOGIES

Contents

Introduction

Vulnerabilities in the Internet-connected software run by large organizations create a large security risk. A single successful exploit — which can be as short as a few characters typed in the wrong place — can abuse these flaws and set a breach in motion. Exploits can be leveraged to access corporate databases and other sensitive information, causing financial and reputational damage to the target, system hijacking, theft of intellectual property, and downtime. Visitors to the websites of these companies can also be put in danger, since successful attacks can result in theft of credentials and malware infection of user computers.

The aim of our web application attack research was two-fold: to determine which attacks are most commonly used by hackers in the wild, and to find out which industries are being targeted and how. With this data, organizations can be more aware of digital threats and protect themselves accordingly.

Summary of findings:

- Organizations across the board are being targeted with a high volume of attacks on their web applications.
- Governmental organizations and e-commerce companies showed themselves to be particular targets. These two sectors are also subjected to the highest level of manual (non-automated) compromise attempts.
- Attack types are tailored to specific sectors. For example, e-commerce sees a mix of attempts designed to cause downtime and access internal files. By contrast, 65% of all attacks in the finance sector attempt to steal the login information of website visitors.
- Sectors seeing the lowest attack volumes, conversely, see the highest volume of automated web attacks from hackers, who use specialized software to search for vulnerabilities automatically.
- Easy-to-execute methods such as SQL Injection and OS Commanding are the most commonly used methods across all sectors. Rarer attacks include Arbitrary File Execution and Cross-Site Request Forgery.

Methodology

The source data for our research was collected from a cross-section of deployments of PT Application Firewall (PT AF) throughout 2016. As a web application firewall (WAF), and unlike common firewalls and intrusion prevention systems, PT AF detects and prevents known attacks at the level of application and business logic. PT AF also protects against zero-day exploits and user attacks, and analyzes and correlates events to uncover attack chains using a number of self-learning and behavioral analysis techniques such as machine learning. The specific organizations have been anonymized here, but include governmental, educational, financial, transportation, industrial, and IT organizations in multiple countries. All examples given in this research were manually verified to exclude false positives and proved reliable. An attack is defined as a single malicious request.

Government, e-commerce, and finance in the spotlight

While attackers' motivations are sometimes unclear and attribution is difficult, we see trends in the types of organizations that are targeted.

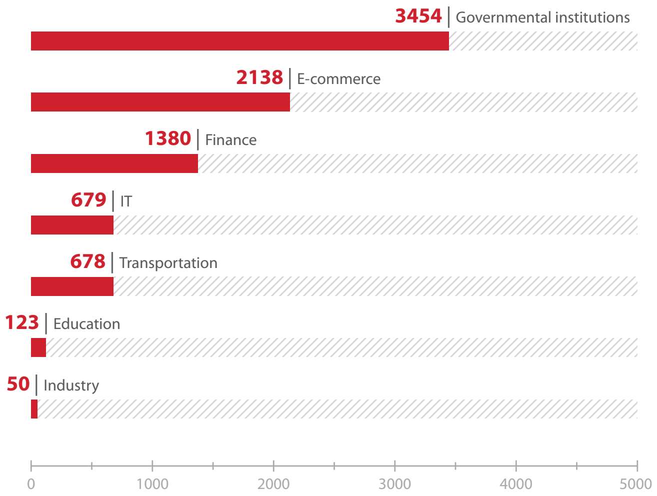
Out of the data analyzed, Government was by far the most under threat, logging nearly 70x more attacks per day than industrial systems, the sector with the least attacks. For governmental institutions, more than 70% of attempts were Path Traversal attacks. This relatively simple attack allows hackers to access vulnerable file system directories to potentially compromise files stored on servers.

E-commerce sites, characterized by an abundance of web applications, saw the second-highest average number of attacks in the sample day analyzed. This sector handles large volumes of sensitive consumer data, such as personal and financial information. The most popular attack vector in this sector, too, is Path Traversal, which potentially gives attackers access to file system directories. Denial of Service (DoS) attacks also constitute a significant portion of attacks (14%), a method that can render web applications inaccessible in a sector in which uptime is critical.

The finance sector rounded off the top three in terms of daily attack volumes, with the sample set registering an average of around 1,400 attacks per day. In this sector, about 65% of attacks consisted of Cross-Site Scripting (XSS) and Cross-Suite Request Forgery (CSRF) directed at system users. The widespread nature of such attacks in the financial industry underlines a special hazard for this sector, since XSS and CSRF can be used to steal cookie values and user credentials. Attacks on the finance sector appeared to be more complex overall than attacks in other sectors, suggesting a higher level of technical competence.

The transportation and IT companies analyzed had to withstand on average about 680 attacks per day.

Number of attacks per day by sector.



Fugure 1. Number of attacks per day by sector.

Automated vs. manual attacks

Interesting trends can be seen in the breakdown of web application attacks as either automated (generated by vulnerability scanning software) or stand-alone manual (human-originated) attacks. The latter indicates one-off attempts to exploit specific vulnerabilities, as opposed to the higher-volume automated approach of scanning for vulnerabilities in bulk.

Interestingly, the most targeted sectors (in terms of attack volume) also saw the highest number of manual attacks. Nearly all (99%) of attacks against e-commerce sites did not use automated software at all, potentially indicating a diverse range of isolated actors undertaking low-level attempts to exploit web application vulnerabilities. A similarly high percentage of compromise attempts on governmental web applications also had manual origins.

By contrast, most attacks across all remaining industries are performed with the help of specialized vulnerability detection software. Automated scanning includes attempts to perform various attacks such as SQL Injection and Path Traversal using security analysis tools. Attackers can use this analysis to exploit vulnerabilities and design an attack vector to gain access to sensitive information, local networks, and critical systems, or attack users.

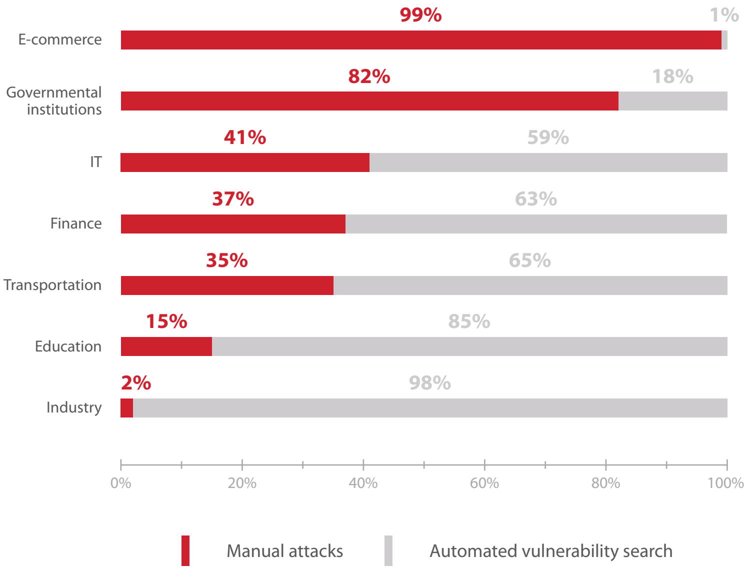
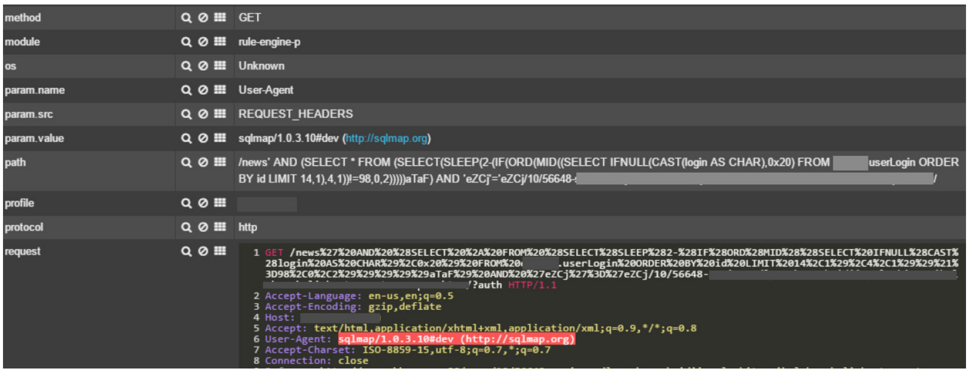


Figure 2. Automated scanning vs. manual attacks

The figure below shows an example of automated scanning that has been detected using sqlmap. PT AF found unwanted content in a User-Agent HTTP header and a request containing an SQL Injection attempt.



method	GET
module	rule-engine-p
os	Unknown
param.name	User-Agent
param.src	REQUEST_HEADERS
param.value	sqlmap/1.0.3.10#dev (http://sqlmap.org)
path	/news' AND (SELECT * FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(login AS CHAR),0x20) FROM [redacted] userLogin ORDER BY id LIMIT 14,1),4,1))!=98,0,2)))))aTaF) AND 'eZCj'='eZCj/10/56648-[redacted]/
profile	[redacted]
protocol	http
request	

```
GET /news%27%20AND%20%28SELECT%20%2A%20FROM%20%28SELECT%28SLEEP%282-%28IF%28ORD%28MID%28%28SELECT%20IFNULL%28CAST%
28login%20AS%20CHAR%29%2C0x20%29%20FROM%20[redacted].userLogin%20ORDER%20BY%20id%20LIMIT%2014%2C1%29%2C4%2C1%29%29%21%
3D98%2C0%2C2%29%29%29%29%29aTaF%29%20AND%20%27eZCj%27%3D%27eZCj/10/56648-[redacted]
[redacted]/?auth HTTP/1.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Host: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: sqlmap/1.0.3.10#dev (http://sqlmap.org)
Accept-Charset: ISO-8859-15,utf-8;q=0.7,*;q=0.7
Connection: close
```

Figure 3. Example of detection of automated scanning

Attack types

The most common attacks detected were SQL Injection and OS Commanding, which allows for a deeper level of compromise. Such attempts were recorded on over 80% of systems. The third-most common attack type was Path Traversal. Taken together, the prevalence of these more "primitive" techniques shows that hackers tend to focus on simple attacks with low barriers to entry.

Typically, the less common an attack is, the more difficult it is to implement, or the more unlikely attackers are to find the other conditions necessary for accomplishing their goal. One example of a less common attack is attempts to compromise the file upload function in a web application. Most Arbitrary File Upload attacks exploit critical vulnerabilities and may completely compromise a web application and server, enabling an attacker to gain access to local network resources.

Our list of most popular attacks does not include the attacks performed by automated web application vulnerability scanners such as Acunetix or sqlmap.

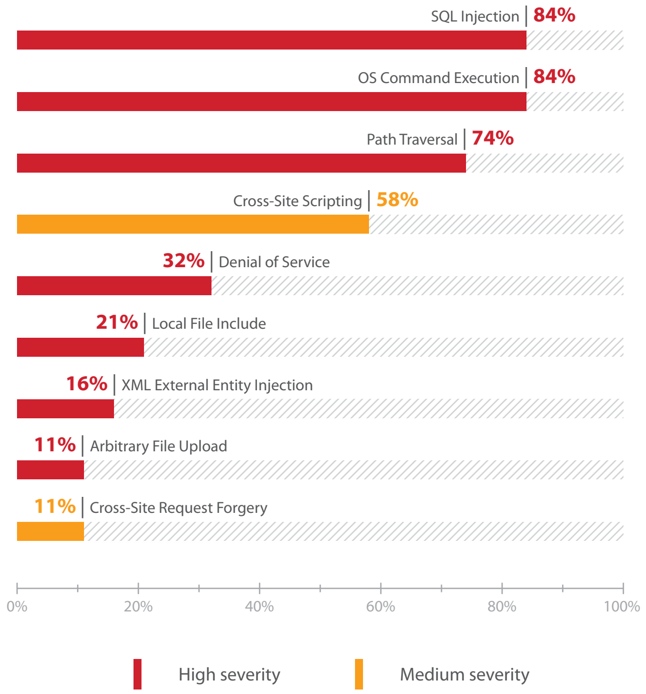


Figure 4. Most popular attacks (% of web applications attacked)

Conclusions

The results make clear that hackers target certain sectors more than others: specifically, those bringing the most return in terms of sensitive information or financial reward. This is not a new trend in the cybersecurity space, but unfortunately one that will continue to drive malicious activity. Attackers are beginning to show a higher level of technical competence and capabilities in their attempts to steal funds and sensitive data in web application attacks. In order to accurately construct attack chains and perform incident forensics in such a fluid environment, including advanced persistent threats, it is important to implement technological solutions able to successfully correlate a vast range of variables and take appropriate countermeasures with minimal human intervention. For more information, visit PT AF page.

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