



WEBTOTEM

CYBER RISK SCORING OF BANKS IN POLAND

WEBTOTEM.AI

© WebTotem 2017-2020, All Rights Reserved

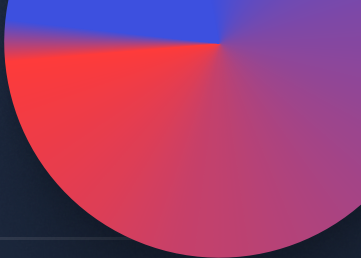
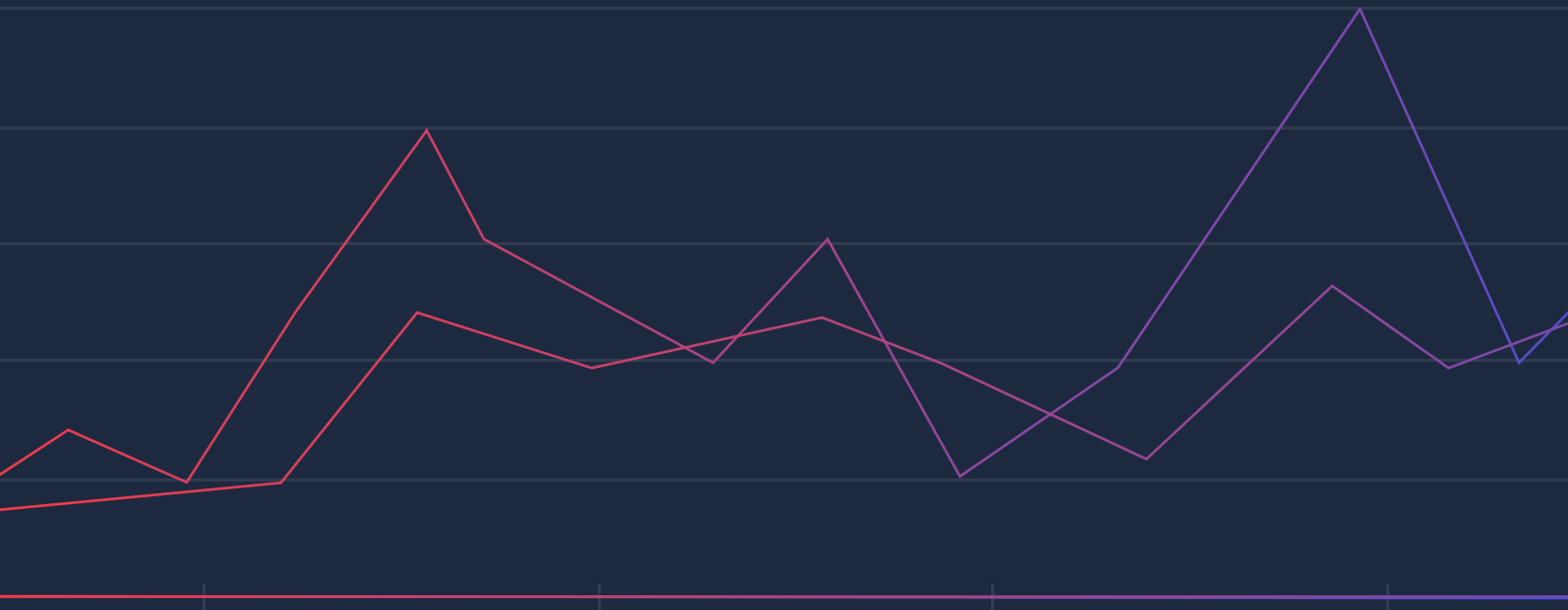


Table of contents

• Glossary	03	• Conclusion	27
• Introduction	04	• Summary	28
• Purpose of the study	05	• Cases	29-30
• Subjects of the study	06	• About the company	31-32
• Brief results	07-09	• Why us?	33
• Scoring Methodology	10	• Contacts	34

• The main results 11-26

a. Software composition	11	g. Network Security (open ports)	20
b. Website performance	12	h. Email security	21-23
c. IP/Domain reputation	13	i. Current state	24
d. HTTP Security Headers and Content Security Policy Scoring	14-15	j. GDPR compliance	25
e. Traffic encryption	16-18	k. Security.txt compliance	26
f. Information leak:	19		



Information security

preservation of confidentiality, integrity and availability of information.

Vulnerability

weakness of an asset or control that can be exploited by one or more threats.

Attack

attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Threat

potential cause of an unwanted incident, which can result in harm to a system or organization.

Risk

effect of uncertainty on objectives.

Today, 3 of 5 modern European banks are located in Poland.

According to Deloitte, the Polish banking market is the leader of digital maturity in Internet and mobile channels. The "CE Banking Outlook Winning in the Digital Arms Race" report distinguishes 3 banks from Poland among the top five most modern banks in Central Europe.

In addition, Poles are currently the European leader in terms of online shopping, contactless payments and distance payments.

The main objective of this study was to find out how Polish banks ensure the security of their web resources. The best international practices and recommendations of recognized software developers and global communities were selected as a reference.

The research was conducted using the WebTotem AI product.

During research, WebTotem AI specialists did not interfere in the operation of the bank's Internet resources: for the checks, it was enough to send "light" HTTP and DNS requests and analyze the responses that came from the server. Thus, all the data was collected in the way a regular user visiting the resource could do it

This work does not pertain to attacks and vulnerabilities, protection against which is based on filtering user input, and therefore does not imply explicit attacks on the resource. It includes an analysis of the use of approaches to make recommended settings for web servers and related components.

We hope that the results of the study will make it easier for information security departments of banks to note the identified vulnerabilities that could potentially become accessible to cybercriminals today.

We also expect that this analysis will contribute to verification of the web resources of these banks by internal services, and in the future, will help to increase the level of protection through the application of best international practices.

**The audit was
conducted in the
first half of June
2020**

The main objective of this study is to assess the security level of publicly available banking resources (we are talking about the official website of the bank) in accordance with best practices (such as PCI DSS, GDPR, OWASP Top-10, OWASP Application Security Verification Standard). We have selected several control points that can be checked without interfering with the work of the bank's web resource, thus eliminating any technical damage.

It is important to note that all the information analyzed by us is publicly available, and working with it does not require special skills or tools that are not available to the ordinary user. In other words, we wanted to show that any interested user with technical skills can come to similar results.



During our research, we tried to find out what potential attack vectors can be accessed by hackers. A security settings checklist like ours can easily be compiled by an attacker to build vectors of further attacks on the bank and its customers.

For research, we have selected the following banks in Poland

- o PKO Bank Polski
- o mBank
- o Alior Bank
- o ING Bank Śląski SA
- o BNP Paribas Bank Polska
- o Bank Millennium SA
- o GETIN Bank SA
- o Bank Gospodarstwa Krajowego
- o Danske Bank Polska
- o Mercedes-Benz Bank Polska SA
- o Toyota Bank Polska
- o Bank Spółdzielczy w Brodnicy
- o Bank Ochrony Środowiska S.A.
- o Credit Agricole (former Lukas Bank)
- o Bank Polskiej Spółdzielczości
- o Santander Consumer Bank SA (former CC-Bank)
- o Bank Poczty
- o Pekao Bank Hipoteczny
- o Haitong Bank, S.A., Warsaw Branch
- o NOBLE Bank SA
- o Volkswagen Bank Polska
- o Societe Generale
- o Inteligo
- o Nordea Bank Polska
- o Skandinaviska Enskilda Banken AB (SA) (SEB)
- o Idea Bank Spółka Akcyjna
- o FCE Bank Polska (former Ford Bank)
- o UBS a.g.
- o HSBC Bank Polska
- o Bank Handlowy w Warszawie SA (part of Citigroup)
- o Bank BPH
- o Bank DnB NORD Polska;
- o Mazowiecki Bank Regionalny

* These banks were selected because their servers are physically located in Poland.

33

Verification was carried out for each official website of the bank. A total of 33 sites were checked.

33

Polish banks were checked

61%

The average banking site security index is 61%

1

1 bank's website has a negative domain reputation

61%

Information leaks were detected in 61% of banks

76%

76% of banks have problems with ensuring the protection of customers' personal data

45%

45% of banks are at risk of exploitation of web vulnerabilities

9%

Only 9% of domains have a high security rating for HTTP and CSP headers

4500

More than 4500 information leaks were found

12%

of banks have open ports

80%

The average Email Security Index of banks is 80%

21%

21% of domains have low site loading speed

18%

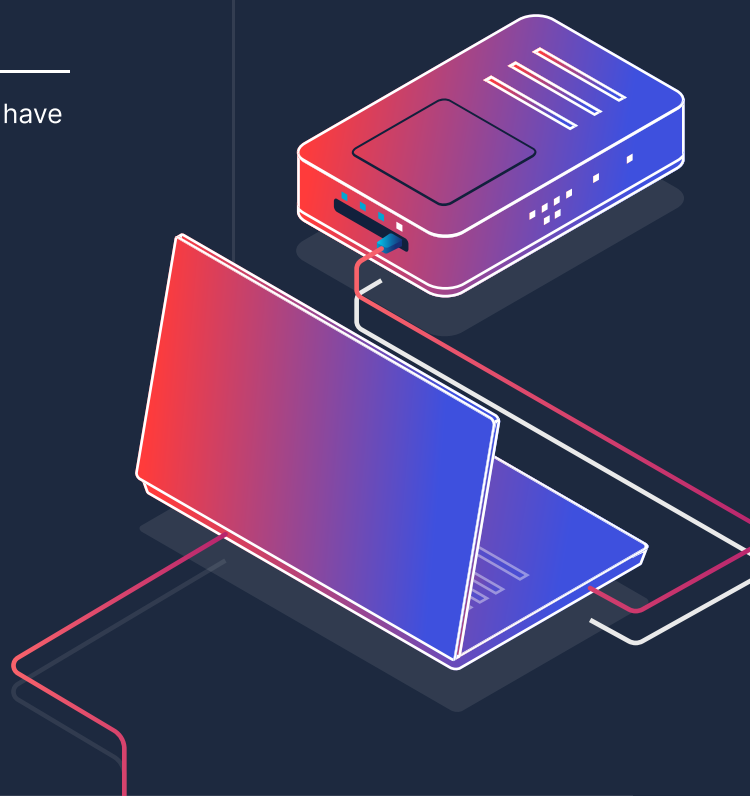
of banks failed SSL / TLS settings verification

2500

More than 2500 information leaks were detected in one of the banks

100%

of banks do not comply with the Security.txt standard



Final security rating of banks in Poland

PLACE	#	SITE	NAME	SECURITY RATE,% *
1	A1	vwbank.pl	Volkswagen Bank Polska	90,8
2	A2	hsbc.pl	HSBC Bank Polska	88,7
3	A3	aliorbank.pl	Alior Bank	83,7
4	A4	-	🔒🔒🔒	83,6
5	B1	-	🔒🔒🔒	78,6
6	B2	-	🔒🔒🔒	78,5
7	B3	-	🔒🔒🔒	76,6
8	B4	-	🔒🔒🔒	73,5
9	B5	-	🔒🔒🔒	71,5
10	B6	-	🔒🔒🔒	68,8
11	B7	-	🔒🔒🔒	68,6
12	B8	-	🔒🔒🔒	68,1
13	B9	-	🔒🔒🔒	66,5
14	B10	-	🔒🔒🔒	66,0
15	B11	-	🔒🔒🔒	64,7
16	B12	-	🔒🔒🔒	64,5
17	B13	-	🔒🔒🔒	61,7
18	B14	-	🔒🔒🔒	58,7

Final security rating of banks in Poland

PLACE	#	SITE	NAME	SECURITY RATE,% *
19	B15	-	🔒🔒🔒	58,5
20	B16	-	🔒🔒🔒	56,5
21	B17	-	🔒🔒🔒	54,5
22	B18	-	🔒🔒🔒	53,5
23	B19	-	🔒🔒🔒	53,3
24	B20	-	🔒🔒🔒	53,0
25	B21	-	🔒🔒🔒	51,5
26	B22	-	🔒🔒🔒	49,5
27	B23	-	🔒🔒🔒	49,2
28	C1	-	🔒🔒🔒	48,6
29	C2	-	🔒🔒🔒	43,8
30	C3	-	🔒🔒🔒	43,5
31	C4	-	🔒🔒🔒	38,6
32	C5	-	🔒🔒🔒	38,5
33	C6	-	🔒🔒🔒	33,7

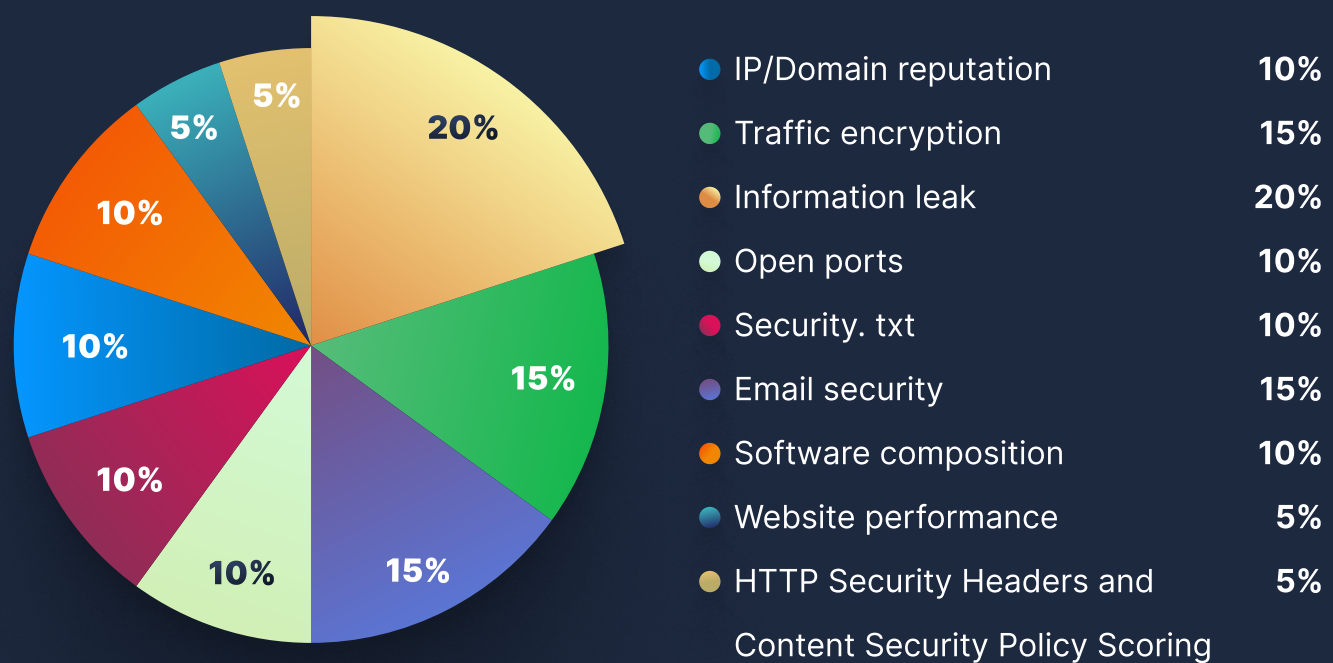
* The lower the indicator, the worse the web security situation of the bank.

In the rating, starting from 4th place, the names of banks are hidden for privacy purposes.

- The percentage score characterizes the number of undetected or discovered security errors.
- The rating for a perfectly securely configured web resource is 100%.
- Points are deducted for every insecure, incomplete, or unreliable configuration of your website or web server.

A+	Score greater than 100	B+	Score between 70 - 79	C+	Score between 35 - 49
A	Score between 90 - 99	B	Score between 60 - 69	C	Score between 20 - 34
A-	Score between 80 - 89	B-	Score between 50 - 59	C-	Score lower than 20

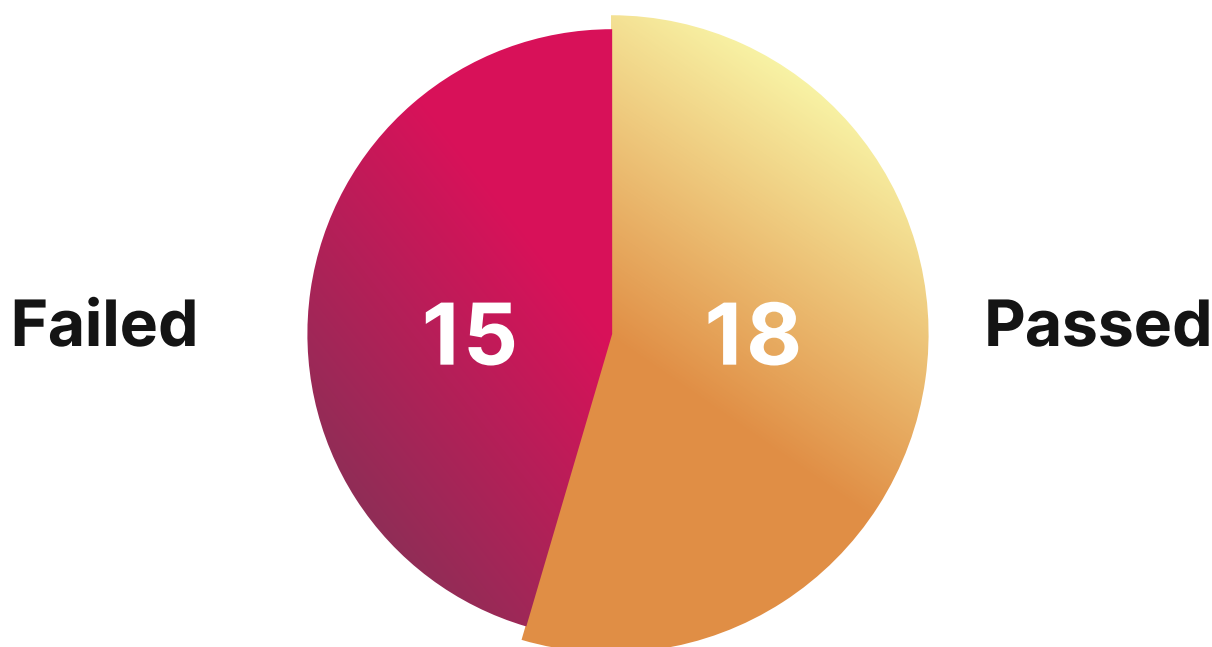
Criticality of criteria for the final result of a web resource security assessment



Software composition

This section describes the results that could describe the risk of exploiting web vulnerabilities such as SQL Injection, Cross Site Scripting, Broken Authentication and Session Management, Insecure Direct Object References, Cross Site Request Forgery, Security Misconfiguration, Insecure Cryptographic Storage, Failure to restrict URL Access, Insufficient Transport Layer Protection, Unvalidated Redirects and Forwards. More information can be found at <https://www.owasp.org/>.

As a result, out of **33 domains**, only **18 domains** pass this item on the cybersecurity checklist



Vulnerability: using an outdated version of the software, which is highly likely no longer supported by the developer. The CMS or its components has not been updated.

Risk: There is a high probability of an exploit that allows attackers to exploit the vulnerabilities of older versions.

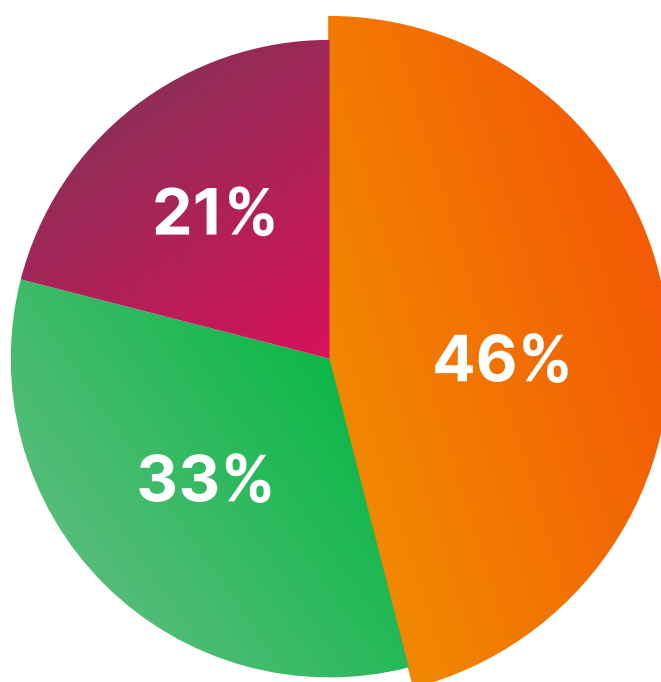
Negative Consequences: Unlawful Access to Data.

Website performance

Estimation of download speed is based on FCP and FID data obtained by simulating site loading.

Testing of best performance practices is performed to analyze the site's resistance to stress.

As a result, **33%** of domains have a high download speed, the next **46%**- average, and the last **21%**- low.



High speed **80-100%** Average speed **50-79%** Low speed **0-49%**

Vulnerability: Slow site loading speed;

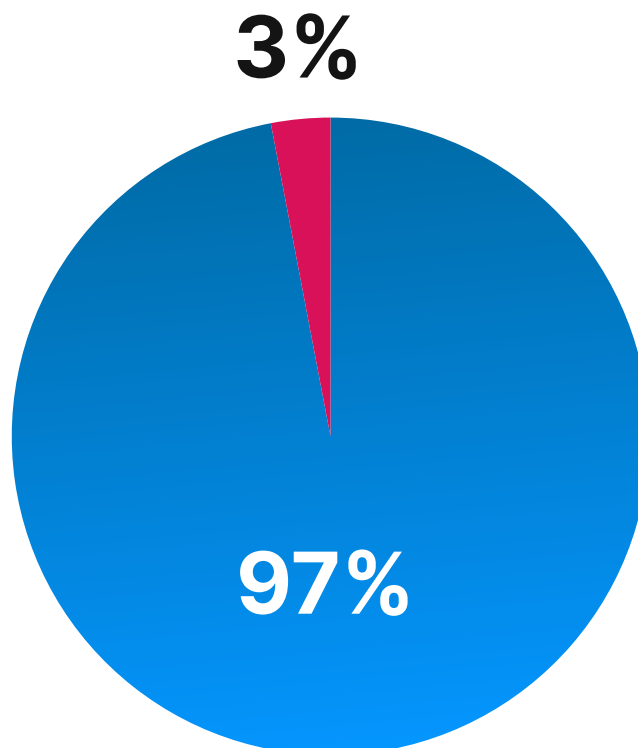
Risk: Poor performance will allow attackers to overload the web resource by means of specially selected requests;

Negative consequences: inaccessibility of a web resource for users.

IP/Domain reputation

A good reputation means that a web resource is secure, while but a domain is given “black list” status, antiviruses warn guests of possible security threats when they attempt to visit the resource.

Generally, **97%** of web-sites are considered “clean”, and only **3%**(1 domain) was seen in suspicious activity **Proxy/windows exploit**



Vulnerability: domain's presence on the “black list”;

Risk: If a web resource is registered in the “black list” of one of the reputation databases, the web resource can be blocked from visiting browsers and can even disappear from search engine results;

Negative consequences: This primarily leads to loss of traffic, customers' trust, and therefore, of money. Check the reputation of the domain in different databases for anti-virus software.

HTTP Security Headers and Content Security Policy Scoring

Whenever a browser requests a page from the web-server, the server answers with content bearing an HTTP response header. Some of these headers include metadata like Content-Encoding, Cache-Control, status codes, and so on. Along with this, there are also HTTP security headers that tell your browser how to behave when working with your site's content. For example, using Strict-Transport-Security, you can force the browser to interact exclusively over HTTPS. Below, we'll look at six different HTTP security headers (in no particular order) that you should be aware of, and we recommend using them if possible.

Content-Security-Policy ("Content Protection Policy", CSP) - the Header provides an additional level of security. This policy helps prevent attacks such as cross-site scripting (XSS) and other code-based attacks by identifying approved content sources and thus allowing the browser to download them.

All major browsers currently offer full or partial support for content security policies. And it won't disrupt content delivery; if it's actually delivered to an older browser, it just won't be executed.

X-XSS-Protection - this Header is designed to enable the cross - site scripting (XSS) filter built into modern web browsers. This is usually enabled by default, but using it will result in execution. It is supported by InternetExplorer 8+ and Safari.

HTTP Strict Transport Security (HSTS) - The Strict-Transport-Security-Header represents a

security improvement that restricts web-browsers to accessing the web-server exclusively via HTTPS. This ensures that no insecure HTTP connection, which may be susceptible to attacks, can be established.

At this moment, all the major modern browsers support strict transport HTTP security, except Opera Mini and the previous version of Internet Explorer.

X-Frame-Options-Header provides protection from Click Jacking attack by not allowing floating frames to load on the web-site. It is supported by IE8+, Chrome 4.1+, Firefox 3.6.9+, Opera 10.5+, Safari 4+.

Expect-CT header prevents the use of incorrectly issued certificates by allowing web-sites to create reports and to additionally ensure compliance with the transparency requirements of certificates. When this header is enabled, the web-site requests the browser to check whether the certificate appears in public CT logs.

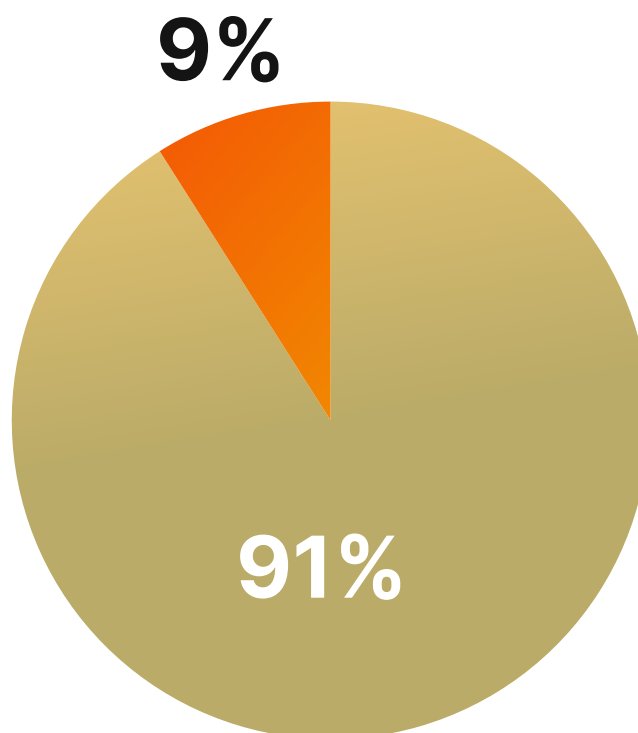
X-Content-Type-Options- the X-Content-Type header offers countermeasures against MIME wiretapping. It instructs the browser to follow the MIME types specified in the header. Used as a function to detect the format of a downloaded file, MIME sniffing can also be used to perform cross-site scripting attacks.

Feature-Policy-Header allows you to permit or disable browser functions, both in its own frame and in the content inside the embedded frame (<iframe>).

HTTP Security Headers and Content Security Policy Scoring

Content-Security-Policy(CSP) - it is one of the main ways of reducing the risks that arise when XSS attacks are performed. Using CSP, the site administrator can define attributes that are allowed to be used on pages – fonts, styles, images, JS scripts, SWF, and so on.

As a result, **9%** of domains score high, and the next **91%** have an average score.



Vulnerability: a flaw in security headers;

Risk: Implementation of attacks that target users, such as inject malicious code, XSS, and modification of a web resource's content to be malicious;

Negative consequences: unauthorized access to data, or an attacker gaining control over a web resource.

Traffic encryption

We have selected the following SSL/TLS checks

NAME OF THE CHECK	BRIEF DESCRIPTION
Rating	Overall rating of SSL settings, according to the SSL Labs resource. It depends on many factors: whether the certificate is correct, the server settings, the algorithms supported by the server, and so on. Gradation from A+ to F.
Support for weak parameters of the Diffie-Hellman algorithm	Weak parameters can be used to exchange keys over the Diffie-Hellman Protocol which reduces the security of the resource.
POODLE Vulnerability	Allows for decryption of users' data.
FREAK vulnerability	Attacker can force the user and server to use "export" keys that have a very limited length, while they establish a connection and exchange data.
Vulnerability to Logjam attack	Like the FREAK vulnerability, Logjam is based on lowering the encryption level to the export level, where the key's length is 512 bits.
ROBOT vulnerability	Completely violates TLS privacy when using RSA to get a session key.
Beast vulnerability	Attacker can decipher data exchanged between two sides using TLS1.0, SSL 3.0 and earlier versions.
CVE-2016-2017 vulnerability	A remote attacker can use this vulnerability to extract text from encrypted packets using the Padding Oracle technique.
Heartbleed vulnerability	Getting access to data stored in the client or server memory.
Ticketbleed vulnerability	A remote attacker can extract fragments of server memory content using the session ID field of the TLS Protocol.
SSL Renegotiation	Secure SSL re-negotiation reduces the risk of DoS or MITM attacks.
RC4 support	Researchers have found that it is possible to decrypt data that was hidden using the RC4 cipher in a short time.

Traffic encryption

We have selected the following SSL/TLS checks:

NAME OF THE CHECK	BRIEF DESCRIPTION
Forward Secrecy support	A property of certain key negotiation protocols that ensures that session keys are not compromised, even if the server's private key is compromised
TLS version	The TLS protocol encrypts all types of Internet traffic, making data exchange on the Internet secure.
SSL 2.0 and SSL 3.0 support	Both protocols are considered outdated and have many vulnerabilities, therefore it is recommended to disable them on the server side.
NPN and ALPN support	Allows you to indicate which protocol to use after establishing a secure SSL/TLS connection between client and server.
DROWN vulnerability	Allows attacker to decrypt customers' TLS-traffic, if SSL 2.0 support is not disabled on the server side for all servers that use the same private key.

One of the most important things to check are the SSL/TLS settings, because today, these cryptographic protocols are the most popular method of ensuring secure data exchange over the Internet. In 2019, the creators of FireFox, Safari, Edge and Chrome browsers reported that in 2020, starting in March, browsers will no longer support TLS 1.0 and 1.1. We Recommend switching to TLS 1.2, or even better TLS 1.3, otherwise browsers will display an error.

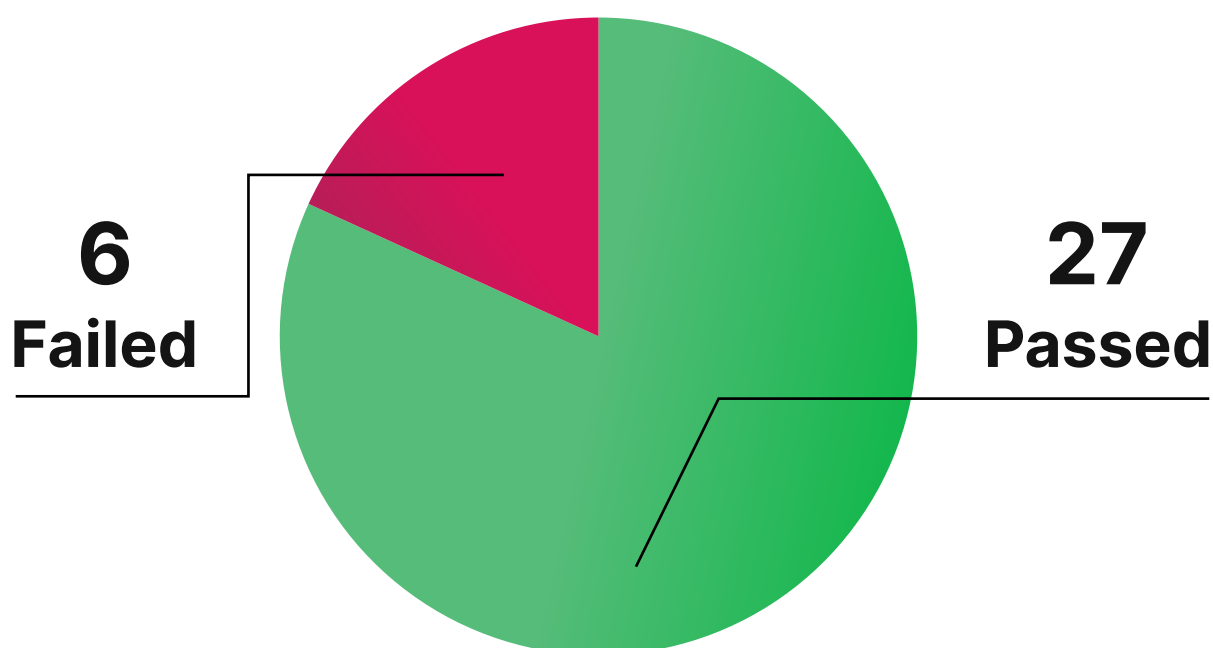
Risk factors: Data interception - this is just one of several different types of attacks combined under a common name: "man in the middle". Every "man in the middle", or MITM, attack implies the presence of an intermediary (a person or device) that has the ability to intercept and modify data sent between two users of a network, who, as a rule, do not even suspect that hackers are interfering in the exchange of information between them.

The essence of the attack is that the attacker routes the victim's web traffic (possible by changing DNS-server parameters or the hosts file on the victim's machine) through itself. While the victim believes that they are accessing their Bank's website directly, the traffic passes through an intermediary node of the attacker, who thus receives all the data sent by the user (username, password, PIN code, etc.).

Traffic encryption

Banks' results with respect to the SSL / TLS settings check:

As a result, out of **33** domains, **27** domains pass this item on the checklist.



Vulnerability: absence or incorrect configuration of SSL/TLS;

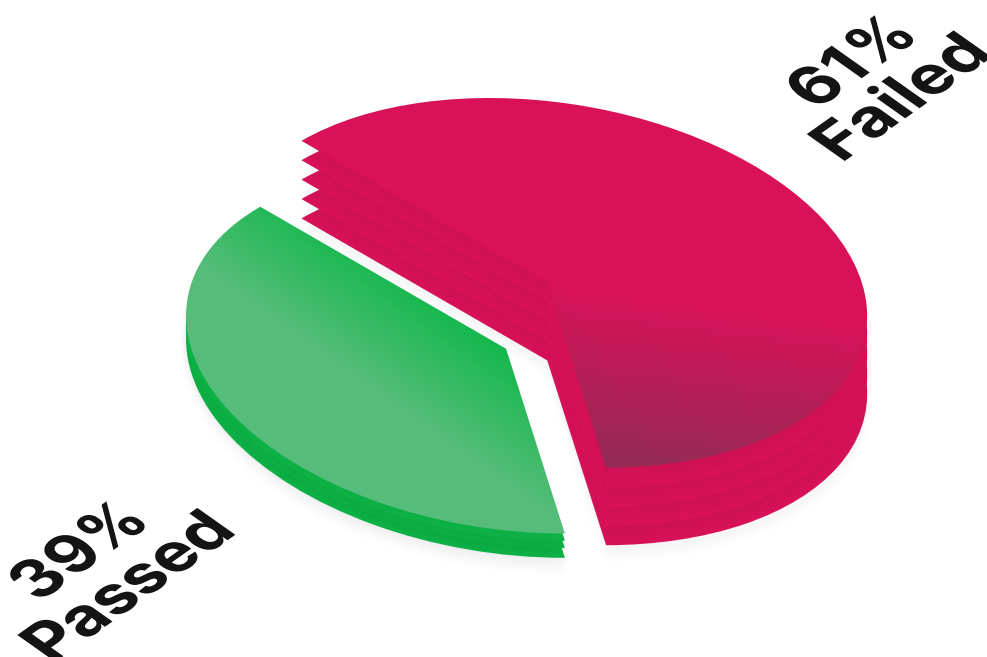
Risk: Interception of data by “man in the middle” attacks. Such attacks imply the existence of an intermediary (human or device) that has the ability to capture and modify data that is sent between two users of a network who usually do not suspect that hackers are interfering in the exchange of information between them.

Negative consequences: Attackers can have access to all of the user's information (login, password, PIN-code, etc.) that could have been sent. Leads to leaking of customers' data, financial losses.

Information leak

Today, information plays a greater role in the life of any company or government organization than it did a couple of decades ago. The one who owns information owns the world, and the one who owns other people's information is much better prepared to compete than his rivals. Any leak of information carries certain negative economic consequences for the company.

As a result, only **13** banks out of **33** pass this item on the cybersecurity checklist.



Vulnerability: employees using the Bank's corporate email when registering on various services. Very often, in 90% of cases, the passwords of user accounts on different services match.

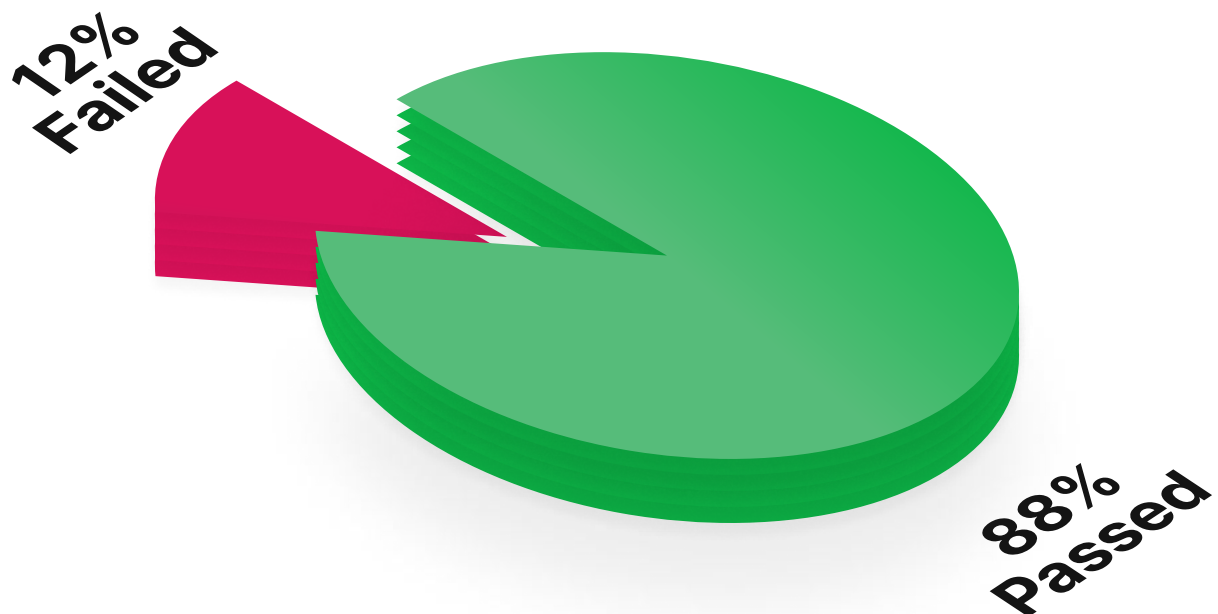
Risk: Hackers can get access to corporate mail, work correspondence, and company documentation. Access to sensitive information obtained by hackers can be used to mount an attack on the information system of the Bank.

Negative consequences: unauthorized access to data, financial and reputational losses.

Network Security (open ports)

We analyzed ports that are not directly used by the web server itself (ports 80 and 443).

As a result, out of **33** banks, this item on the checklist is passed by only **29** banks.



Vulnerability: from the point of view of best security practices, a web server should not have open ports other than those that involve working with web services

Risk: unauthorized access and control over internal information resources by hackers

Negative consequences: unauthorized access to data, financial and reputational losses.

Email security

More than 90% of email traffic contains spam, phishing, malware, and other electronic threats. Email is the main vector of infection for ransomware and malware. This check is to verify whether the web resource's mail server is configured correctly to prevent these common threats.

NAME OF THE CHECK	BRIEF DESCRIPTION
MX ConnectionTest	If port 25 is blocked from external access on the MX server itself, the server will not be able to receive incoming messages (sending servers will never search for an alternative port). The port must at least be accessible via a proxy server or router. If 3 ports are open (25, 465, and 587), your system requires authentication (AUTH) on port 587 before the MAIL FROM command is issued. If the connection to port 25 or 465 fails, the score is reduced.
Reverse DNS Test	Many mail servers perform a reverse search to verify the sender's domain identity. If the test fails, communication with the sending server may be blocked. Various reputation services may also give your system a lower score if there is no feedback. To send and receive email correctly, a valid domain must have a corresponding MX record in the DNS, which contains 3 parts of information: the domain name, the host name (for example, servername.domain.com) and IP. A request for a host name to convert an address to its IP address is called a direct search. Reverse lookup is the reverse process: converting an IP to its hostname. Many mail servers perform a reverse search to verify the sender's domain identity. If the test fails, communication with the sender's server may be blocked. Various reputation services can also give your system a lower score if there is no feedback.
SPF ServerTest	Today, nearly all obnoxious messages in the email are sent from spoofed sender addresses. Victims whose addresses are abused often suffer from the consequences because their reputation is reduced and they have to take responsibility for abuse or spend their time sorting out mistakenly forwarded crash messages (Source: OpenSpf.org). This test checks whether you confirm your local sender addresses. The usual practice of sending spam includes spoofing (faking) the email address used in the FROM field. The Sender Policy Framework (SPF) is a method used to prevent this type of spoofing: you create an SPF record on your DNS server to specify and restrict which host addresses are allowed to send email using your domain name.

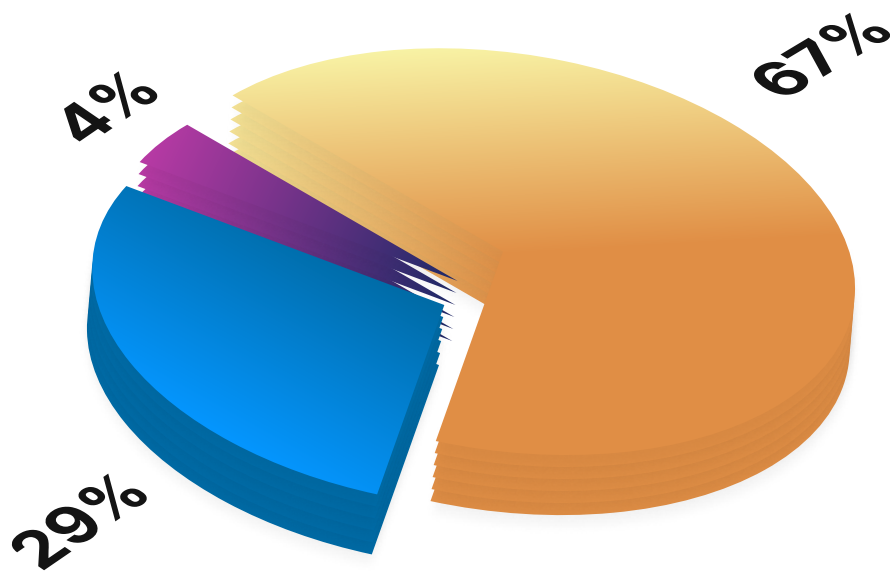
Email security

NAME OF THE CHECK	BRIEF DESCRIPTION
DNSBL VerificationTest	If an IP belonging to your network is blacklisted, mail servers that subscribe to DNSBL block communication with your server. A DNS-based blacklist checks IP addresses associated with spam and other malware.
SPF ClientTest	If your server does not support SPF check, the problems that arise can be twofold: 1) You risk accepting and processing more spam, which increases the load on system resources. 2) You risk handling a larger number of unacceptable failures and delivery failures, known as backscattering.
Open Relay and Email Format Test	If the server allows messages to be sent to non-local addresses (by unauthorized senders or untrusted IP addresses), it is considered an open relay. Thus, the server can be used by spammers and, therefore, blacklisted.
SMTP Plain Text Authentication Test	Spammers can hack into user accounts by collecting passwords that are sent to the server in plain text using the PLAIN or AUTH LOGIN mechanisms. This test tries to connect to the mail server via ports 25 and 465. For each connection, it checks the list of available authentication methods. The server will get the lowest number of points if port 25 supports PLAIN or AUTH LOGIN. The highest score is awarded if SMTP SSL is enabled and the PLAIN and AUTH LOGIN mechanisms are not available on port 25. Please note that if AUTH is not supported, your MX passes the test because plain text passwords cannot be listened to.
POP3 ConnectionTest	If a POP3 connection uses standard port 110, the connection is not secure and can be hacked, which can lead to loss of messages and privacy. Checks which port is used by POP3. If a POP3 connection uses the standard port 110, the connection is not secure and may be disrupted, resulting in potential loss of messages and privacy.
IMAP Connection and Authentication Test	Initially, IMAP support encrypted login mechanisms, but this protection can be circumvented if you use plain text log-in via port 143. Therefore, the content of the message is vulnerable to impact and loss of privacy. Checks the port used for IMAP. The standard, unreliable port for IMAP connections is 143. The secure, encrypted port is 993.

Email security

Banks' results with regard to the web resource mail server check

As a result, **67%** of the studied banks have a high Email security score, **29%** have an average score, and **4%** have a low Email security score.



High rate Average rate Low rate

Vulnerability: incorrect configuration of the browser's post server.

Risk: email is the main vector of infection for ransomware and malware.

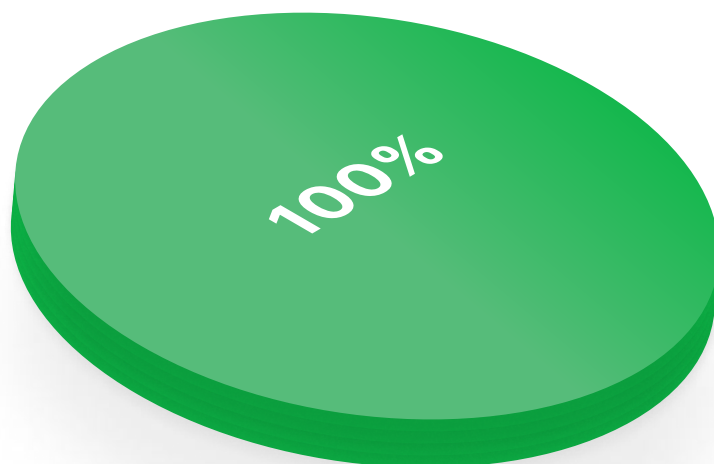
Negative consequences: receiving unwanted mail that carries useless information and contains malicious code (botnets, Trojans, worms), a vector for phishing.

Current state

Checks for hacking of the resource, based on external signs:

- Presence of malicious scripts on the website;
- The presence of a hidden network of cryptocurrency miners;
- Check the speed of the website;
- Complaints from users about the presence of viruses on the site detected by their antivirus software;
- Site's presence on "black list" of search engine reputation databases;

As a result, **100%** of banks passed the check for resource hacking, based on external signs.



Vulnerability: presence of malware, extortionist programs like web crypto-jacking, etc.

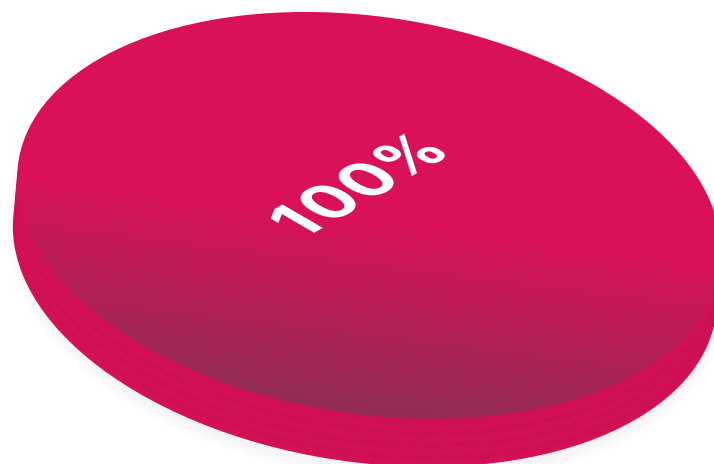
Risk: web crypto-jacking (also known as passing crypto-mining) is the most common form of crypto-mining malware. As a rule, this malware works with scripts, which are launched on a web-site, and this allows the victim's browser to mine the cryptocurrency automatically during a visit. These network miners are implemented covertly on different websites, regardless of their popularity or category.

Negative consequences: unauthorized access to information, bypassing existing access control rules; performance degradation, crashes, and unavailability of services.

Security.txt compliance

When independent security researchers detect a threat in a web service, they often do not have enough communication channels with the owner of the web service to report the vulnerability. As a result, no security issues are reported. Security.txt defines a standard to help organizations determine how security researchers can safely disclose vulnerabilities.

As a result, **100%** of banks failed Security.txt compliance verification.



Vulnerability: identified vulnerabilities may remain unknown to the owners of the web resource.

Risk: the vulnerability can be exploited by attackers.

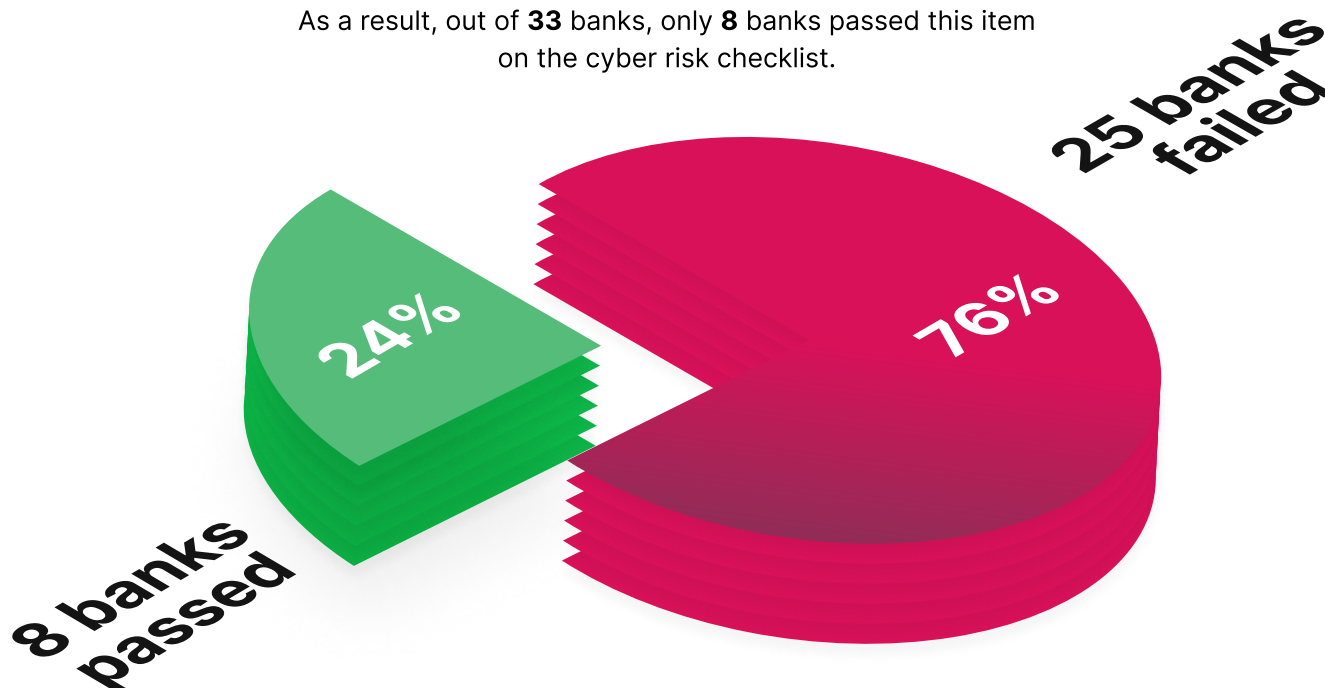
Negative consequences: unauthorized access to information, bypass of the existing rules of access distinction, loss of productivity, failures and unavailability of services.

GDPR compliance

Personal data must be processed in such a way as to ensure proper security, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (" integrity and confidentiality ").

According to the GDPR (General Data Protection Regulation) and the privacy and electronic communications Directive (ePrivacy Directive), websites are required to provide users with information about how their personal data is processed, about cookies, and how user data is transmitted.

As a result, out of **33** banks, only **8** banks passed this item on the cyber risk checklist.



Vulnerability: cookie files can store a lot of data sufficient to identify the user without their permission and consent. In most cases, users of a website must accept all rules for storing and processing their personal information.

Risk: unauthorized or illegal processing of customers' personal information.

Negative consequences: discrepancy with legislative and normative requirements.



As a result of research of the security of web resources of banks in Poland, we found an average rate of implementation of publicly available recommendations for configuring web servers and related components.

After getting a general picture of the security of banks' web resources, we came to the main conclusion that: many banks neglect even the most common and easy-to-implement measures for improving the security of their web resources.

After checking the web resources of banks in accordance with the previously described criteria, we found that fairly well-known vulnerabilities and security problems are still present on the web resources of banks in Poland. The current situation allows attackers to count on successful implementation of their attacks on these financial organizations.



The research conducted by WebTotem pointed out a number of weak and vulnerable points of Polish banks, which, although seemingly insignificant at first glance and difficult to implement by hackers, can subsequently lead to significant financial losses and even irreversible reputational collapse. Currently, in the era of high-speed information exchange and a rapidly changing digital world, the priority for customers is to guarantee the confidentiality and integrity of their data when choosing services.

The good news is that Polish banks today have all the opportunities and ready-made tools to establish an information security management system and to implement timely measures and products to ensure their protection and sustainable development.

- In 2017, the computer systems of several banks in Poland were infected with malware as a result of the largest cyberattack on the financial sector in the history of the country.

This attack on Polish banks is one example of a targeted attack on banking systems. Hackers used a typical vector of penetration into the internal network of banks: they discovered and used a vulnerability in the web portal of the state website of the financial sector and created a channel for delivering malware to the workstations of Bank employees.

As a result of the attack, 20 Polish banks were affected and suffered damage from large data losses.

Source

#	URL
1	CybelAngel. 2020. A Major Cyberattack Targets The Polish Banking Industry. [online] Available at: < https://cybelangel.com/blog/cyberattack-targets-polands-banks/ > [Accessed 16 June 2020].
2	ONeill, P. and O'Neill, P., 2020. Hackers Break Into Polish Banks Through Government Regulator Charged With Bank Security Standards - Cyberscoop. [online] CyberScoop. Available at: < https://www.cyberscoop.com/hackers-break-polish-banks-government-regulator-charged-bank-security-standards/ > [Accessed 16 June 2020].
3	Constantin, L., 2020. Recent Malware Attacks On Polish Banks Tied To Wider Hacking Campaign. [online] PCWorld. Available at: < https://www.pcworld.com/article/3169413/recent-malware-attacks-on-polish-banks-tied-to-wider-hacking-campaign.html > [Accessed 16 June 2020].
4	BadCyber. 2020. Several Polish Banks Hacked, Information Stolen By Unknown Attackers. [online] Available at: < https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ > [Accessed 16 June 2020].
5	Security Affairs. 2020. Crooks Hacked Polish Banks With A Malware Planted On Government Site. [online] Available at: < https://securityaffairs.co/wordpress/56056/cyber-crime/polish-banks-malware.html > [Accessed 16 June 2020].

• The current situation in connection with the COVID -19 virus

During the COVID-19 surge, the financial sector became increasingly vulnerable. Between February and March 2020, analysts observed a 38 percent increase in cyber-attacks against financial institutions. Worldwide and in various sectors, there has been an increase in the transition to remote work. Attackers used COVID-19 to launch phishing attacks, fake apps / maps, Trojans, backdoors, crypto miners, botnets, and ransomware.

It is obvious that while the fight against COVID-19 continues around the world, hackers will continue to attack vulnerable populations and organizations.

Source

#	URL
1	VMware Carbon Black. 2020. Amid COVID-19, Global Orgs See A 148% Spike In Ransomware Attacks; Finance Industry Heavily Targeted VMware Carbon Black. [online] Available at: < https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/ > [Accessed 16 June 2020].
2	Cert.bournemouth.ac.uk. 2020. Amid COVID-19, Global Orgs See A 148% Spike In Ransomware Attacks; Finance Industry Heavily Targeted – BU-CERT. [online] Available at: < https://cert.bournemouth.ac.uk/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/ > [Accessed 16 June 2020].
3	SDxCentral. 2020. Ransomware Attacks Spike 148% Amid COVID-19 Scams - Sdxcentral. [online] Available at: < https://www.sdxcentral.com/articles/news/ransomware-attacks-spike-148-amid-covid-19-scams/2020/04/ > [Accessed 16 June 2020].
4	Cert.bournemouth.ac.uk. 2020. Amid COVID-19, Global Orgs See A 148% Spike In Ransomware Attacks; Finance Industry Heavily Targeted – BU-CERT. [online] Available at: < https://cert.bournemouth.ac.uk/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/ > [Accessed 16 June 2020].



WEBTOTEM

a monitoring system designed to
protect web resources from intrusions
and cyber threats



Application of the world's
best practices for ensuring
information security.



The best SaaS & B2B
solution at the Echelon Asia
Summit in Singapore in 2018



Certified specialists of the
IS: OSCP, OSCE, CEH,
CHFI, CISA, ISO 27001



Top 3 on Latitude



Choosing global innovation through
science and technology with the
support of the US government



Top 3 on Emerge

Monitoring of Polish
companies **1,148,036** sites
in the .pl domain zone

THE WEBTOTEM CLIENT CAN

The mission of WebTotem is to provide a revolutionary product based on artificial intelligence to people from the non-technical sphere, so that they have the opportunity to protect their business with one click



Prevent hacking with step-by-step security recommendations



Receive proactive protection from new cyber threats



Cybersecurity risk assessment and management

We raise the level of information security of business sites around the world.

WHY CONDUCT AN INFORMATION SECURITY AUDIT?

An audit of a company's information resources and infrastructure allows us to identify and prevent potential threats and significantly reduce risks to business processes.

The audit includes a set of activities aimed at assessing the current state of information security processes, including penetration testing (Pentest), namely modeling the actions of attackers, instrumental scanning with manual verification of vulnerabilities and other methods, in accordance with the international practice of large international organizations such as the Web Application Security Consortium (WASC) and the Open Web Application Security Project (OWASP v.4 - currently).

The security assessment process consists of the following steps:

- conducting manual checks and analyzing the results obtained;
- conducting instrumental tests of applications;
- research of detected vulnerabilities in order to determine ways to exploit them;
- analysis of system security from external threats;
- research of wireless networks configuration;
- audit of used IS configurations;
- generation of an analytical report and recommendations for eliminating identified vulnerabilities.

Following our expert recommendations provides a higher level of security and minimizes risks to your business.

By conducting a security audit, you receive the following benefits:

- Our comprehensive independent assessment of the security level of your web resource. The client receives recommendations for its improvement from highly qualified specialists with many years of relevant experience.
- Audit by WebTotem helps improve the confidentiality of commercial and other important information, protect information systems from unauthorized access and virus threats.
- An information security audit avoids unnecessary IT and security costs as it provides only adequate recommendations. In addition, it reduces reputational risks associated with poor information security, which is important for any business, from government authorities to specialized enterprises
- By implementing our recommendations based on the audit, the client optimizes the IT infrastructure and related processes in accordance with current security requirements, improving the quality of internal control.



info@wtotem.com
wtotem.com