Mohsen Abdollahzadeh Aghbolagh[1], Andrey I. Trufanov[2],
School of Information Technology and Data Science,
Irkutsk National Research Technical University,
Lermontova Str., Irkutsk 664074, Russia
[1]*e-mail: mohsen.abdollahzadeh001@gmail.com, https://orcid.org/0000-0002-6414-2847*
[2]*e-mail: troufan@gmail.com, https://orcid.org/0000-0002-6967-3495*

Iran's Cyber Capabilities and Assessing Security Standards for Popular Iranian Websites

DOI: http://dx.doi.org/10.26583/bit.2023.1.04

Abstract. The security of online users depends on various factors. One of the most important factors are to follow security standards and use of reliable and updated technology as well as the standards and technologies that have been created in recent years specifically to increase data and communication security on websites and various internet services. However numerous studies show that the current state of global web security is not desirable yet, and these standards and technologies are not being applied as fast as they are developed. Our research in CERTFA Lab on popular Iranian websites (414 websites) show that the security of Iranian websites is not different from the global level, and very few websites are fully utilizing the security standards and modern technologies. According to our investigation, only 7 websites from our assessed sites have been used CSP2 configuration, which the implementation of Cafebazaar.ir and Virgool.io have more detail and other 5 websites just use the upgrade-insecure-requests option as a default setting for CSP. In other cases, popular websites, not only did not use the CSP header, they have also forgotten to use the basic security header. Also, the results of modern standards analysis in this study (such as DNSSEC, CAA, DMARC, SPF, and Expect-CT), which is mandatory for most Internet businesses, indicate that just Eligasht.com, one of the Iranian popular websites, has properly used these standard configurations. Since these security standards and modern technologies are easy to use and cheap to implement, we could say that the reason for this undesirable situation might be the negligence of admins and service providers.

Keywords: Online Security, Security Standards Requirements, Website Security.
For citation: AGHBOLAGH Mohsen Abdollahzadeh; TRUFANOV Andrey I. Iran's Cyber Capabilities and Assessing Security Standards for Popular Iranian Websites. IT Security (Russia), [S.l.], v. 30, no. 1, p. 58–69, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1471. DOI: http://dx.doi.org/10.26583/bit.2023.1.04.

Introduction

Website security has become a sensitive and important challenge for users and online business owners [1, 2]. The rising trend of cybercriminals has concerned websites owners and users. Finding numerous vulnerabilities in the technologies used in the hosting infrastructures and website designs, the hacking of popular websites and internet services and leaking the information of their users are among the reasons why these concerns have increased.

Although the issue of security in the digital world can never be guaranteed 100 percent, in most cases, implementing standards and security policies, regular updates, and fixing the identified vulnerabilities minimize security threats for websites and their users.

Security experts and web-related technology developers constantly seek measures to fight these conventional problems and to increase security on the internet [3, 4]. As a result, each year we see new security standards and modern technologies being introduced in order to increase user security and patching security vulnerabilities.

In this regard, we could say the Open Web Application Security Project (OWASP) is one of the best sources of material for learning security tips about all websites. In the next steps, following and implementing standards such as HIPAA, PCI DSS, and NIST is considered necessary for businesses and websites that handle sensitive user data.

However, our goal for sharing this analysis is not to explain the function of OWASP and other standards, as other educational sources have spent enough time explaining them fully. Our goal is to raise awareness about who follows these standards in Iran, and to encourage online platforms to implement security standards [5, 6]. We reviewed 414 most popular Iranian websites and assessed their general protocols of security standards in this research.

Iran's Cyber Capabilities

Executive Summary

Iranian cyber capabilities are meager in comparison to many well-developed nations. However, it is rapidly expanding its cyber operations and becoming a more significant advanced persistent threat (APT) actor in the cyberspace environment. Receiving technical support from Russia and China [7], Iran's cyber operations are more robust than a decade ago.

Accustomed to covert operations and strategic planning, Iran appreciates the use "of cyber as an instrument of national power" [8] and "using cyber as a tool for coercion and force" [8]. Furthermore, "Tehran views these operations as a safe, low-cost method to collect information and retaliate against perceived threats" [7].

These threats are initiated by its citizens. Iran fears its population the most and believes that influences from the internet could spark civil unrest within the nation. To minimize these threats, Iran "began to develop their hacking abilities during the 2009 "Green Revolution" to extend domestic surveillance and control" [8]. As a result, it has effectively limited the population's exposure to outside internet sources and conflicting ideologies.

Background

After the infamous Stuxnet cyberattack on Iranian nuclear centrifuges in 2010, Iran realized the importance of cyber defense and operations, prompting the country to invest and develop its cyber capabilities. Shifting from local censorship to utilizing "phishing and defacing campaigns against commercial enterprises, as well as cyberespionage against military and government data" [7].

Some of Iran's favorite targets are "aerospace companies, defense contractors, energy and natural resource companies, and telecommunications firms for cyberespionage operations" [9]. However, Iran is very cautious not to push the boundaries of what could be perceived as an act of war and invoke a violent response. Typically, Iran is retaliatory in nature. For example, "after a 2012 malware attack targeting an Iranian oil facility, Iran responded with a cyberattack on Saudi Aramco and Qatari RasGas, using malware to cause irreparable damage to thousands of computers" [7]. The malware in question was called "Shamoon" [10], which "renders infected systems useless by overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data" [10].

Many of these attacks are executed in part by Iran's Islamic Revolutionary Guard Corps (IRGC) [11] or one of the many state-sponsored APT actors such as Magic Hound [12]. Despite being available for years, the usage rates of modern defensive security technologies was frustratingly low. A lack of tooling combined with poor and scattered documentation had led to minimal awareness around countermeasures such as Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), and Subresource Integrity (SRI), [13].Utilizing state-sponsored APT actors shifts the responsibility from Iran to independent actors within the country. One example of the use of these actors is the September 2020 Pulse Secure virtual private network (VPN) exploit. Conducted by a group named Pioneer Kitten, or UNC757, the cyber actors conducted reconnaissance using mass-scanning tools like "Nmap, to identify open ports" [14]. Once the ports were identified, vulnerabilities within the VPN were exploited, privileges escalated, and

persistence within the systems was maintained. This attack intended to exfiltrate and sell data to "serve the threat actor's own financial interests" [14].

Impact

Targeting infrastructure and SCADA systems, Iranian APT actors could potentially disrupt facilities within the United States and cause irreparable damage like the Shamoon attacks on Saudi Aramco and Qatari RasGas. It also has proved its capability of disrupting financial institutions in the United States with "massive denial of service attacks" [8] in 2011 through 2013. However, modern cyber defense operations and tactics have significantly reduced Iran's capabilities, for now.

Significance

Iran's cyber capabilities may not be the world's greatest threat, but it is a force to watch due to its rapid development. Especially with backing from two of the most significant threats to the United States government and the private sector, Russia and China. Proving that it can conduct advanced offensive attacks and cyber espionage, it would be wise to monitor the region.

Data

For this assessment, we chose the top 500 most popular websites in Iran according to Alexa on 23 August 2021, and in order to achieve more precision, we removed the non-Iranian websites from this list. Only 414 websites that are hosted and owned by Iranians have been examined.

Assessment method

Merely "implementation of general protocols" and "websites configuration for HTTP response" were assessed in the same conditions, using these tools:

- HTTP Observatory, created by Mozilla Foundation [9]
- Hardenize, created by Hardenize team [14]

Assessed Standards and Criteria

While several methods are available for testing the usability of website interfaces, no true consensus exists regarding which method works best in identifying problems in a user's experience that should be corrected. In order to achieve reliable results, the criteria have been divided into two sections based on function and importance, such as: implementing basic security settings and hardening security configuration.

These criteria have been chosen since they are the conventional methods to access website security standards and availability of websites as well as delivering reliable outcome.

1. Basic security settings that all websites are required to implement:

HTTP Redirection

URL Redirection is considered a weakness which enables an attacker or hacker to force users of your application to an untrusted external site. The attack is most often performed by delivering a link to the victim, who then clicks the link and is unknowingly redirected to the malicious website. A redirect test is a sort of A/B test that allows you to test various web pages and compare to each other. A redirect test uses different URLs for each variant. Redirect tests are useful in case you need to test multiple different landing pages, or perform a complete redesign of a page.

Cookies and Sessions Security

Cookie Testing is defined as a Software Testing type that checks Cookie created in your web browser. A cookie is a small piece of information that is stored in a text file on user's (client) hard drive by the web server. This piece of information is then sent back to the server each time the browser requests a page from the server. Cookie often contains personalized user data and information which is applied to communicate between various web pages.

Cross-origin Resource Sharing

Cross-Origin Resource Sharing (CORS) is an HTTP-header based mechanism and allows a server to mention any different origins (domain, scheme, or port) different from its own from which a browser should permit loading resources.

X-Content-Type-Options

The X-Content-Type-Options HTTP Response header tells the web browser whether the Content-Type headers are deliberately set and must be followed. In the absence of this, browsers may use MIME type sniffing to guess at the Content-Type. MIME (Multipurpose Internet Mail Extensions) is an extension of the original Simple Mail Transport Protocol (SMTP) email protocol. It lets users exchange different kinds of data files, including audio, video, images and application programs, over email. They may do this when the Content-Type header is missing or when it is thought to be incorrect. Since types of content are executable, this can have some security consequences. This test looks for the presence of this header with a value of nosniff. In case the header is missing or if it has any other value, a warning will be issued. Nosniff blocks all request if there "style" MIME-type is not text/css and JavaScript MIME-type. Plus it enables the cross origin if there MIME-Type text/html, text/plain, text/jason, application/jason and any type of xml extension.

X-Frame-Options

It prevents sites from being displayed inside an iframe. This HTTP response header is applied to allow or block the page from being loaded inside of an iframe. A server can use this to avoid certain attacks in a website in order to prevent their content from being embedded in other websites. Deleting the header allows the page to be embedded in iframes. When you want to limit this, include this header. There are only two valid values for this header:

- SAMEORIGIN: A page can be loaded inside an iframe, but only inside a page on the same origin.
- DENY: Prevent the page from being loaded inside iframes.

X-XSS-Protection

The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they find reflected cross-site scripting (XSS) attacks. (XSS) attacks occur when data enters a web application via an untrusted source, most frequently a web request.

Content Security Policy

Content Security Policy (CSP) is an added layer of security and would help to scan and mitigate certain sorts of attacks, including Cross-Site Scripting (XSS) and data injection threats. These attacks are done for everything ranging from data theft, to site defacement, to malware distribution.

Subresource Integrity

(SRI) is a security feature that allows various browsers to accept and verify resources they fetch (from a CDN) are delivered without unexpected manipulation. It works by allowing users to provide a cryptographic hash that a fetched resource should match.

Referrer Policy

The Referrer-Policy HTTP header controls the amount of referrer information (sent with the Referer header) should be included while requesting. Aside from the HTTP header, this policy can be set in HTML.

HTTP Strict Transport Security

(HSTS) feature allows a web application inform the browser using a special response header that it should not establish a connection to the specified domain servers using un-encrypted HTTP. Instead, it should automatically establish all connection requests to access the site through HTTPS. It also prevents users from overriding certificate errors.

2. Hardening security configuration that businesses and popular websites are recommended to implement:

DNSSEC (Domain Name System Security Extensions)

DNSSEC protects users from receiving bad data from a signed zone by detecting the attack and preventing the user from receiving the tampered or manipulated data.

CAA (Certification Authority Authorization)

CAA Checking is a control to prevent CAs that can issue certificates for a particular domain name and domain owners can select which Certification Authorities are authorized to issue certificates to that domain name.

EXPECT-CT

Certificate Transparency (CT) is an open framework of logs, monitors as well as auditors created to aid domain owners ignore digital certificates issued for their brands. CT logs help domain owners protect their brands by providing a way to spot misissued certificates conveniently.

SMTP-TLS

By enabling TLS, you are encrypting the SMTP (Simple Mail Transfer Protocol) on the transport layer by wrapping SMTP inside of a TLS connection. This successfully secures SMTP and alters it into SMTPS. Port 587 and 465 are both frequently used for SMTPS traffic.

SPF (Sender Policy Framework)

The Sender Policy Framework (SPF) is an email authentication protocol and part of email cybersecurity used to preventing and minimizing phishing attacks. It makes companies able to decide who is allowed to send email on behalf of your domain.

DMARC (Domain-based Message Authentication, Reporting, and Conformance)

DMARC, is a technical standard that protects email senders and recipients from spam, spoofing, and phishing. DMARC publishes a policy that defines email authentication practices and provides instructions to receiving mail servers for how to enforce them. DMARC establishes a method for a domain owner to:

Publish its email authentication practices, state what actions should be taken on mail that fails authentication checks, and enable reporting of these actions taken on mail claiming to be from its domain.

DANE (DNS-based Authentication of Named Entities)

DANE provides a way to cross-verify the domain-name information and the certificate being used. It can warn you that your connection is insecure.

MTA-STS (MTA Strict Transport Security)

(Mail Transfer Agent Strict Transport Security) MTA-STS is a security standard that ensures the secure transmission of emails via an encrypted SMTP connection. MTA stands for Message Transfer Agent, which is transfers email messages between computers.

TLS-RPT (SMTP TLS Reporting)

SMTP TLS Reporting concerns receiving reports from the internet regarding possible connection security complications that servers might experience while connecting to your email

systems. Due to the open structure nature of the SMTP protocol, the connections between SMTP servers are susceptible to SMTP TLS downgrade attacks.

Due to legal restrictions for advanced security tests, which must be approved by the owners of websites and companies, we only assessed basic standards which all can be categorized as the general features of websites, but according to legal restrictions and our policies, we will not publish all details in this report. Additionally as a reminder, we did not penetration test or test bypass methods of configurations

Results

In this section, Minitab 17 has been utilized to plot the diagrams based on the outcome gained according to the tests done on the mentioned websites. Fig. 1 represents the types of tests done in order to evaluate websites' security including: redirection, x-xss-protection, cookies, cross-origin-resource-sharing, public-key-pinning, contribute, strict-transport-security, subresource-integrity, x-content-type-options, x-frame-options, content-security-policy. [15]

```
> observatory ssllabs.com --format=report --zero

HTTP Observatory Report: ssllabs.com

Score Rule                          Description
   -5 redirection                   Initial redirection from http to https is to a different host, preventing HSTS.
    0 x-xss-protection              X-XSS-Protection header set to "1; mode=block".
    0 cookies                       All cookies use the Secure flag and all session cookies use the HttpOnly flag.
    0 cross-origin-resource-sharing Content is not visible via cross-origin resource sharing (CORS) files or headers.
    0 public-key-pinning            HTTP Public Key Pinning (HPKP) header not implemented.
    0 contribute                    Contribute.json isn't required on websites that don't belong to Mozilla.
    0 strict-transport-security     HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000).
    0 subresource-integrity         Subresource Integrity (SRI) is not needed since site contains no script tags.
    0 x-content-type-options        X-Content-Type-Options header set to "nosniff".
    0 x-frame-options               X-Frame-Options (XFO) header set to SAMEORIGIN or DENY.
    5 content-security-policy       Content Security Policy (CSP) implemented without 'unsafe-inline' or 'unsafe-eval'.

Score: 100
Grade: A+

Full Report Url: https://observatory.mozilla.org/analyze.html?host=ssllabs.com
```

Fig. 1. Types of tests

For a brief definition of standards and types of tests, we have mentioned helpful descriptions from Mozilla Infosec [14] and Hardenize Website [14] at below of each chart (Fig. 2–20).

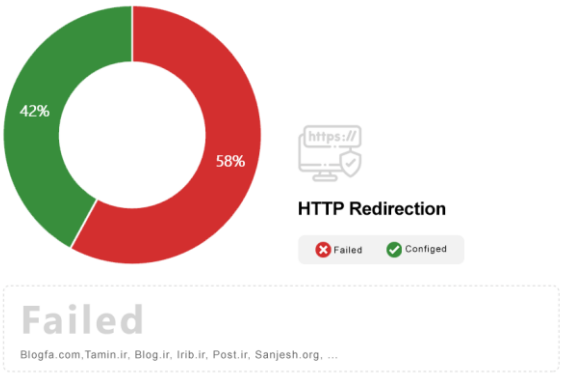

Fig. 2. Websites may continue to listen on port 80 (HTTP) so that users do not get connection errors when typing a URL into their address bar, as browsers currently connect via HTTP for their initial request. Sites that listen on port 80 should only redirect to the same resource on HTTPS

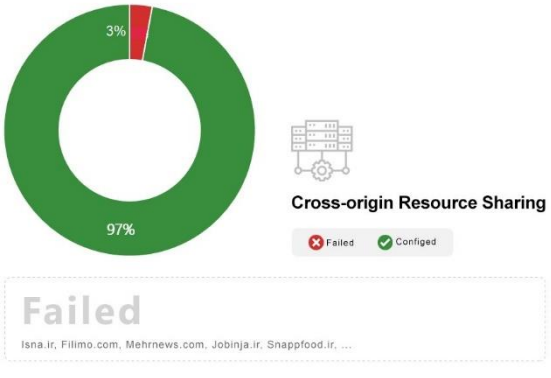

Fig. 3. Access-Control-Allow-Origin is an HTTP header that defines which foreign origins are allowed to access the content of pages on your domain via scripts using methods such as XMLHttpRequest. crossdomain.xml and clientaccesspolicy.xml provide similar functionality, but for Flash and Silverlight-based applications, respectively. These should not be present unless specifically needed

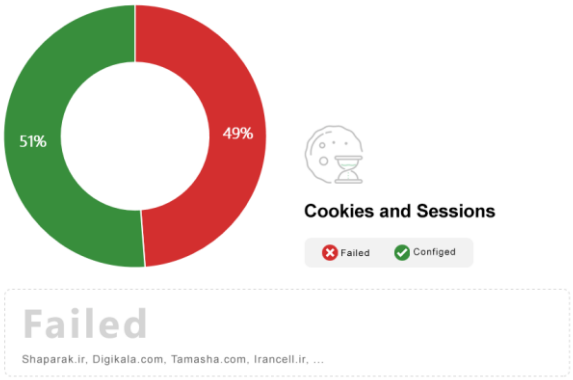

Fig. 4. All cookies should be created such that their access is as limited as possible. This can help minimize damage from cross-site scripting (XSS) vulnerabilities, as these cookies often contain session identifiers or other sensitive information

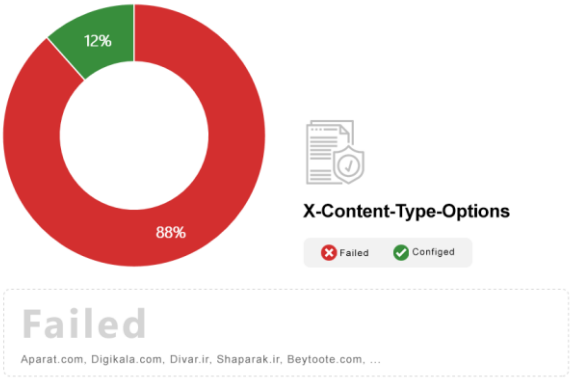

Fig. 5. X-Content-Type-Options is a header supported by Internet Explorer, Chrome and Firefox 50+ that tells it not to load scripts and stylesheets unless the server indicates the correct MIME type. Without this header, these browsers can incorrectly detect files as scripts and stylesheets, leading to XSS attacks. As such, all sites must set the X-Content-Type-Options header and the appropriate MIME types for files that they serve

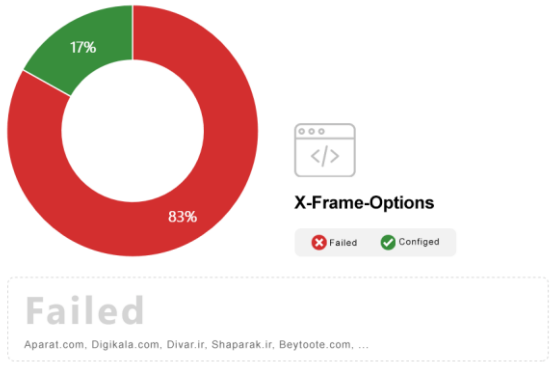

Fig. 6. X-Frame-Options is an HTTP header that allows sites control over how your site may be framed within an iframe. Clickjacking is a practical attack that allows malicious sites to trick users into clicking links on your site even though they may appear to not be on your site at all. As such, the use of the X-Frame-Options header is mandatory for all new websites, and all existing websites are expected to add support for X-Frame-Options as soon as possible

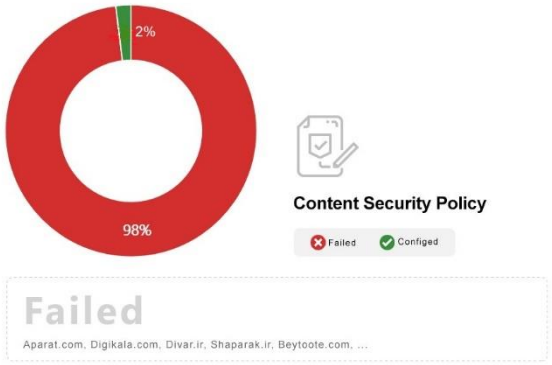

Fig. 7. Content Security Policy (CSP) is an HTTP header that allows site operators fine-grained control over where resources on their site can be loaded from. The use of this header is the best method to prevent cross-site scripting (XSS) vulnerabilities. Due to the difficulty in retrofitting CSP into existing websites, CSP is mandatory for all new websites and is strongly recommended for all existing high-risk sites

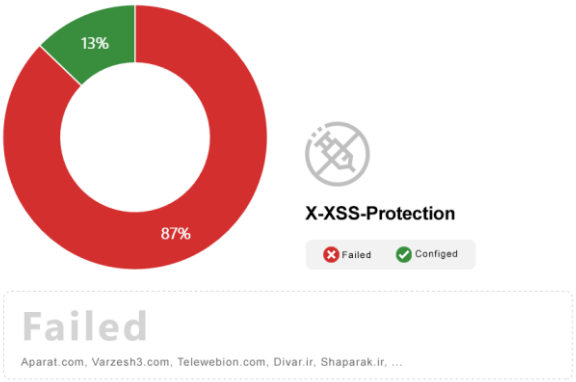

Fig. 8. X-XSS-Protection is a feature of Internet Explorer and Chrome that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. Although these protections are largely unnecessary in modern browsers when sites implement a strong Content Security Policy that disables the use of inline JavaScript ('unsafe-inline'), they can still provide protections for users of older web browsers that don't yet support CSP

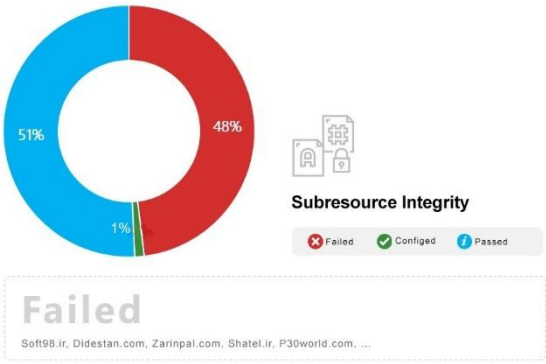

Fig. 9. Subresource integrity is a recent W3C standard that protects against attackers modifying the contents of JavaScript libraries hosted on content delivery networks (CDNs) in order to create vulnerabilities in all websites that make use of that hosted library. For example, JavaScript code on jquery.org that is loaded from mozilla.org has access to the entire contents of everything of mozilla.org. If this resource was successfully attacked, it could modify download links, deface the site, steal credentials, cause denial-of-service attacks, and more

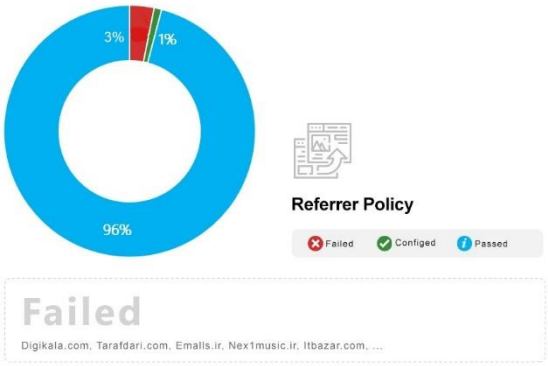

Fig. 10. When a user navigates to a site via a hyperlink or a website loads an external resource, browsers inform the destination site of the origin of the requests through the use of the HTTP Referer (sic) header. Although this can be useful for a variety of purposes, it can also place the privacy of users at risk. HTTP Referrer Policy allows sites to have fine-grained control over how and when browsers transmit the HTTP Referer header

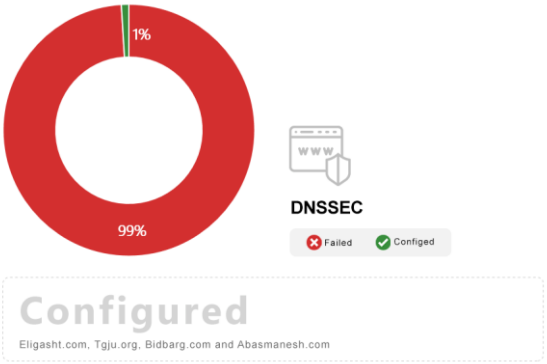

Fig. 11. DNSSEC is an extension of the DNS protocol that provides cryptographic assurance of the authenticity and integrity of responses; it's intended as a defense against network attackers who are able to manipulate DNS to redirect their victims to servers of their choice. DNSSEC is controversial, with the industry split largely between those who think it's essential and those who believe that it's problematic and unnecessary

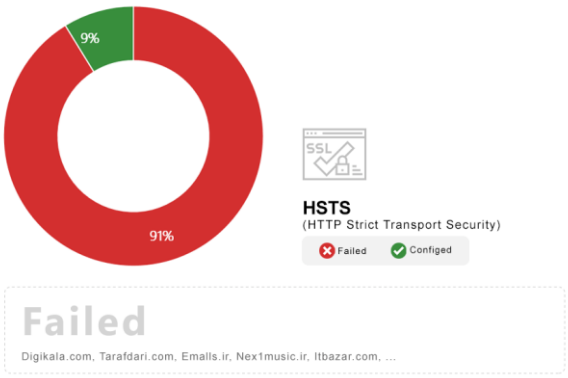

Fig. 12. HTTP Strict Transport Security (HSTS) is an HTTP header that notifies user agents to only connect to a given site over HTTPS, even if the scheme chosen was HTTP. Browsers that have had HSTS set for a given site will transparently upgrade all requests to HTTPS. HSTS also tells the browser to treat TLS and certificate-related errors more strictly by disabling the ability for users to bypass the error page

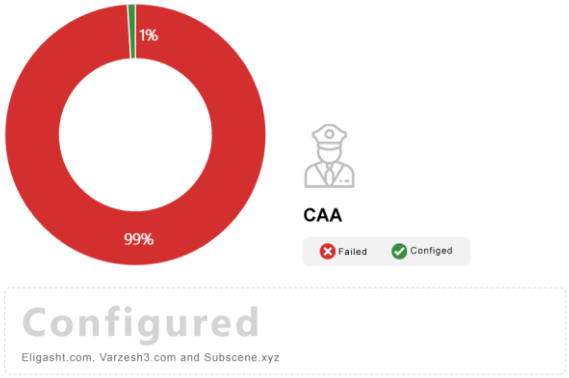

Fig.13. CAA (RFC 6844) is a new standard that allows domain name owners to restrict which CAs are allowed to issue certificates for their domains. This can help to reduce the chance of misissuance, either accidentally or maliciously. In September 2017, CAA became mandatory for CAs to implement

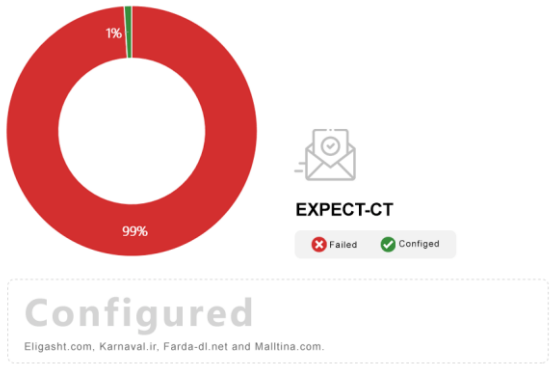

Fig. 14. Expect-CT is a response HTTP header that web sites can use to monitor problems related to their Certificate Transparency (CT) compliance. Additionally, they can also instruct browsers to reject any certificates in their name that are not CT-compliant

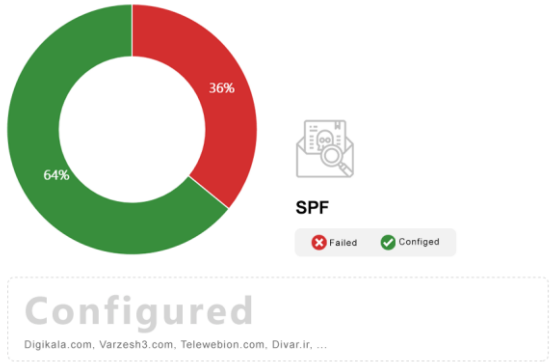

Fig. 15. Sender Policy Framework (SPF) is a protocol that allows domain name owners to control which internet hosts are allowed to send email on their behalf. This simple mechanism can be used to reduce the effect of email spoofing and cut down on spam

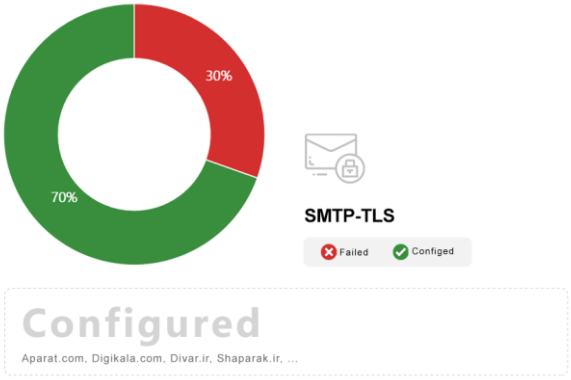

Fig. 16. Transport Layer Security (TLS) is the most widely used encryption protocol on the Internet. In combination with valid certificates, servers can establish trusted communication channels even with users who have never visited them before. Network attackers can't uncover what is being communicated, even when they can see all the traffic

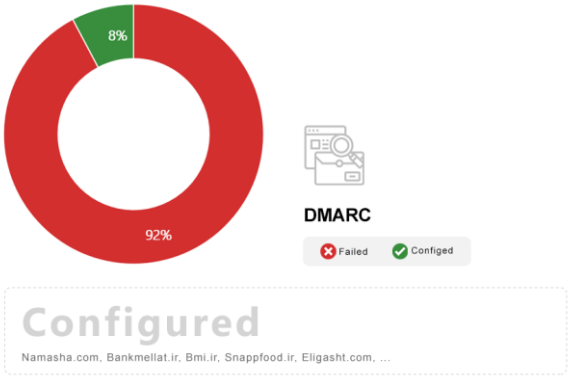

Fig. 17. Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a scalable mechanism by which a mail-originating organization can express domain-level policies and preferences for message validation, disposition, and reporting, that a mail-receiving organization can use to improve mail handling

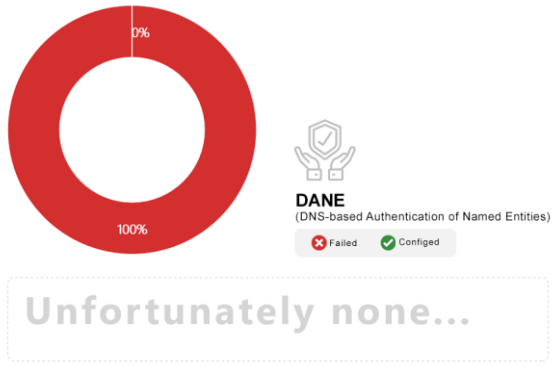

Fig. 18. DNS-based Authentication of Named Entities (DANE) is a bridge between DNSSEC and TLS. In one possible scenario, DANE can be used for public key pinning, building on an existing publicly-trusted certificate. In another approach, it can be used to completely bypass the CA ecosystem and establish trust using DNSSEC alone

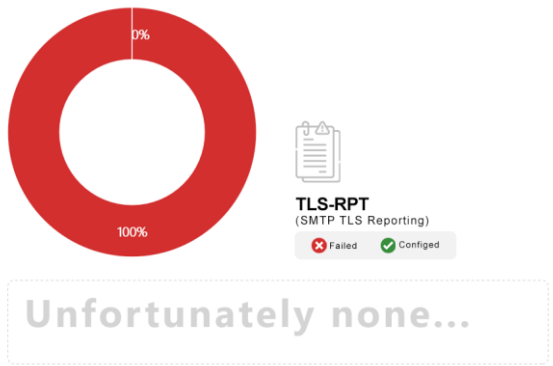

Fig. 19. SMTP TLS Reporting (RFC 8460), or TLS-RPT for short, describes a reporting mechanism and format by which systems sending email can share statistics and specific information about potential failures with recipient domains. Recipient domains can then use this information to both detect potential attacks and diagnose unintentional misconfigurations. TLS-RPT can be used with DANE or MTA-STS

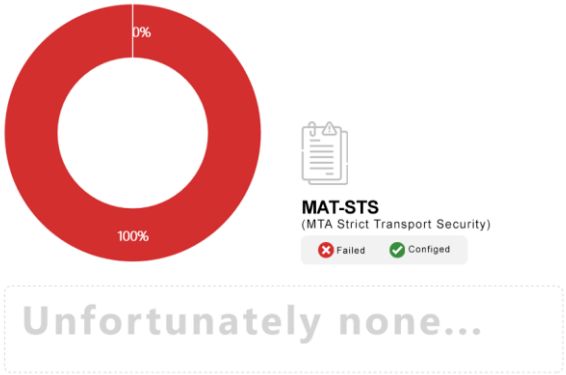

Fig. 20. SMTP Mail Transfer Agent Strict Transport Security (MTA-STS) is a mechanism enabling mail service providers to declare their ability to receive Transport Layer Security (TLS) secure SMTP connections, and to specify whether sending SMTP servers should refuse to deliver to MX hosts that do not offer TLS with a trusted server certificate

Conclusion

Unfortunately, the results of our assessing at CERTFA Lab show that the current state of implementation for security standards on popular Iranian websites is not satisfactory. In most cases, basic HTTP security settings and headers are not used properly, and even on some websites, the configurations are implemented in such a way that their visitor's security may be compromised.

In this regard, we recommend to all developers, managers, and owners of Iranian online businesses to pay close attention to security tips and official standards by reviewing their website status. Since applying security configuration and adhering to standard guidelines, given the abundance of resources available, is completely free and without additional costs, this can easily have a huge impact on improving their own security as well as users and the Internet. In this concern the next Useful Resources and Tools might be mentioned OWASP Top Ten [15], Enterprise Information Security [15], Hardenize, Comprehensive web site configuration test [14], Mozilla Observatory [15], Analyse your HTTP response headers[15], Report URI [15], SRI Hash Generator[15], and DNSSEC Analyzer [15].

REFERENCES:

[1] Yan Chen, Fatemeh Mariam Zahedi, Ahmed Abbasi, David Doboly, Trust calibration of automated security IT artifacts: A multi-domain study of phishing-website detection tools, Information & Management. January 2021, vol. 58, Issue 1, 103394. DOI: http://dx.doi.org/10.1016/j.im.2020.103394.

[2] Nur Azimahbt Mohd, Zarul Fitri Zaaba. A Review of Usability and Security Evaluation Model of Ecommerce Website, Procedia Computer Science. 2019, vol. 161, p. 1199–1205. DOI: http://dx.doi.org/10.1016/j.procs.2019.11.233.

[3] William Derrickson, Kartikeya Tripathi, Difference in risk perception of onboard security threats by aircrew and aviation security experts, Transportation Research Interdisciplinary Perspectives. December 2022, vol. 16, 100666. DOI: http://dx.doi.org/10.1016/j.trip.2022.100666.

[4] Nandita Pattnaik, Shujun Li, Jason R.C.Nurse. Perspectives of Non-Expert Users on Cyber Security and Privacy: An Analysis of Online Discussions on Twitter, Computers & Security,Available online 9. November 2022, 103008, In Press. DOI: http://dx.doi.org/10.1016/j.cose.2022.103008.

[5] Ferda ÖzdemirSönmez. Security Qualitative Metrics for Open Web Application Security Project Compliance, Procedia Computer Science. 2019, vol. 151, p. 998–1003. DOI: http://dx.doi.org/10.1016/j.procs.2019.04.140.

[6] Navdeep S. Chahal, Preeti Bali, Praveen KumarKhosla. A Proactive Approach to assess web application security through the integration of security tools in a Security Orchestration Platform, Computers & Security. November 2022, vol. 122, 102886. DOI: http://dx.doi.org/10.1016/j.cose.2022.102886.

[7] Defense Intelligence Agency (August 2019). Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance. dia.mil. Accessed November 2, 2021. URL: https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/Iran_Military_Power_LR.pdf (accessed: 29.11.2022).

[8] Lewis James A. (June 25, 2019). Iran and Cyber Power. csis.org. Accessed November 2, 2021. URL: https://www.csis.org/analysis/iran-and-cyber-power (accessed: 29.11.2022).

[9] CISA. (September 15, 2020). Alert (AA20-259A): Iran-Based Threat Actor Exploits VPN Vulnerabilities. us-cert.cisa.gov. Accessed November 2, 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa20-259a (accessed: 29.11.2022).

[10] CISA. (July 20, 2021). ICS Joint Security Awareness Report (JSAR-12-241-01B): Shamoon/DistTrack Malware (Update B). us-cert.cisa.gov. Accessed November 2, 2021. URL: https://us-cert.cisa.gov/ics/jsar/JSAR-12-241-01B (accessed: 29.11.2022).

[11] CISA. (n.d.). Iran Cyber Threat Overview and Advisories. us-cert.cisa.gov. Accessed November 2, 2021. URL: https://us-cert.cisa.gov/iran (accessed: 29.11.2022).

[12] ThaiCert. (n.d.). Threat Group Cards: A Threat Actor Encyclopedia: APT group: Magic Hound, APT 35, Cobalt Gypsy, Charming Kitten. thaicert.or.th. Accessed November 2, 2021. URL: https://apt.thaicert.or.th/cgibin/showcard.cgi?g=Magic%20Hound%2C%20APT%2035%2C%20Cobalt%20Gypsy%2C%20Charming%20Kitten (accessed: 29.11.2022).

[13] Analysis of the Alexa Top 1M sites by Mozilla Observatory – April 2019. URL: https://s.certfa.com/RZVBwA (accessed: 29.11.2022).

[14] Content Security Policy. URL: https://s.certfa.com/cRh8um (accessed: 29.11.2022).

[15] Alexa Top 1 Million Analysis by Scott Helme - February 2019. URL: https://s.certfa.com/j2cRsk (accessed: 29.11.2022).

Received – November 29, 2022. The final version – February 01, 2023.