Cryptography and Network Security

Internal Evaluation 1

SECURITY ANALYSIS REPORT FOR THE HINDUSTAN TIMES

Group members:-

120B1F110	Amit Pawar
120B1F142	Atharva Upasani
120B1F153	Gaurav Kasliwal

Under the guidance:
Dr. Jayashree Katti

Department of Information Technology
Pimpri Chinchwad Education Trust's
Pimpri Chinchwad College of Engineering 2023-2024

INDEX

I. INTRODUCTION

The Hindustan Times is a highly regarded English-language daily newspaper in India, distinguished by its rich history and substantial influence within the nation. Established in 1924 by Sunder Singh Lyallpuri and Mahatma Gandhi, it has remained a prominent source of news and information. The newspaper's headquarters are situated in New Delhi, where it has garnered a broad readership and substantial impact, not solely in the national capital but also across India and globally.

Over its many years of operation, the Hindustan Times has earned a reputation as a trustworthy news outlet. It diligently covers an extensive array of topics, including politics, business, entertainment, sports, culture, and more. This comprehensive coverage, coupled with its unwavering commitment to editorial integrity and journalistic standards, has solidified its position as a reliable source of accurate and impartial reporting for its readers.

In response to the changing landscape of media, the Hindustan Times has proactively embraced digital platforms and cutting-edge technologies to engage a wider audience. In addition to its traditional print edition, the newspaper has established a robust online presence through its website and various social media channels, ensuring that its content reaches readers not only across India but also around the world.

Supported by a dedicated team of journalists, correspondents, and editors, the Hindustan Times continues to fulfill its crucial role in informing and influencing public opinion in India. Its commitment to excellence in journalism has earned it numerous awards and accolades, solidifying its status as an indispensable institution within the Indian media landscape.

WEBSITE OVERVIEW

Hindustan Times, headquartered in New Delhi, is one of India's leading English-language newspapers, founded in 1924 by Sunder Singh Lyallpuri and Mahatma Gandhi. Known for its extensive national and international news coverage, it reaches a broad readership both in India and globally. The newspaper has adapted to the digital age with a strong online presence, offering comprehensive reporting on politics, business, entertainment, sports, culture, and more, maintaining its reputation for accuracy and integrity in journalism.

The website is divided into several sections, including:

- Homepage: Homepage consists of all new and trending news.
- Latest news : This section provides us with the latest news.
- Sports : This section provides us with all sports news information
- Education : This section highlights the key features about what is happening in the education world.
- INDIA: This section elaborates the happenings in INDIA
- World : This section gives us the latest news of happenings in the world
- Astrology : All the astrological prediction given by the experts were shown in this section
- Shop now : All the sponsors of Hindustan times and their respective e-commerce sites were put in this section.

Hindustan Times is invaluable, delivering trusted news, comprehensive coverage, and diverse insights, benefitting people with accurate information, fostering awareness, and shaping informed opinions on a global scale.

Here are some of the key features of the Hindustan Times website:

1.Trusted Source: Hindustan Times is a reputable and trusted news source in India, known for its accuracy and objectivity.

2.Comprehensive Coverage: The newspaper provides in-depth coverage of politics, business, entertainment, sports, and culture.

3.Strong Digital Presence: With a robust online presence, Hindustan Times reaches a global audience through its website and social media.

4.Editorial Integrity: The newspaper upholds high editorial standards, ensuring reliable reporting.

5.Influential Impact: Hindustan Times holds substantial influence, shaping public opinion both nationally and internationally.

II. VULNERABILITIES

Vulnerabilities are weaknesses in a system that can be exploited by a threat actor to gain unauthorized access, steal data, or disrupt operations. Vulnerabilities can exist in any type of system, including software, hardware, and networks.

The Hindustan Times website is an online news portal that offers a wide range of news and information services covering national and international news, business, sports, entertainment, lifestyle, and more. It serves as a prominent source of news and updates for readers interested in current events and stories. It is likely that the Hindustan Times website has vulnerabilities, just like any other software system. Some of the most common vulnerabilities that can be found in websites include:

Top 10 Vulnerabilities Found (Threat level High to Low)

1. **SSL/TLS:Report Vulnerable Cipher Suites for HTTPS:** This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exist only on HTTPS services. These rules are applied for the evaluation of the vulnerable cipher suites: - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

2. **SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection:** Deprecated TLSv1.0 and TLSv1.1 protocols with known flaws like BEAST and FREAK pose a security risk. Attackers could exploit these flaws to eavesdrop on secure connections, potentially compromising sensitive data. These protocols no longer receive security updates, making them even riskier. Upgrade to a more secure TLS version immediately.

3. **Absence of Anti-CSRF Tokens :** No Anti-CSRF tokens found in HTML form, making it vulnerable to Cross-Site Request Forgery (CSRF). CSRF can exploit user trust, perform actions, or disclose information on the victim's behalf, especially when combined with XSS. Ensure CSRF protection mechanisms are in place to prevent these attacks.

4. **Cross-Domain Misconfiguration:** Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server

5. **Multiple X-Frame-Options Header Entries:** X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

6. **Missing Anti-clickjacking Header:** The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks

7. **Content Security Policy (CSP) Header Not Set:** Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files

8. **X-Content-Type-Options Header Missing:** The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

9. **Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s):** The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

10. **Cookie with SameSite Attribute None:** A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'crosssite' request. The SameSite attribute is an effective countermeasure to cross-site request forgery, cross-site script inclusion, and timing attacks

III. POSSIBLE ATTACKS

An attack on a website such as Hindustan Times is an attempt to gain unauthorized access to a website, steal data, or disrupt operations. Website attacks can have a significant impact on an organization, especially a news sharing website. They can lead to data breaches, financial losses, and reputational damage. It is important for organizations to take steps to protect their websites from attack. There are many different types of attacks that can be launched against websites.

- **Types of Attacks**

  Here are some of the common types of attacks that can be launched against a website like Hindustan Times:

1. **Denial-of-service (DoS) attacks:** A DoS (Denial-of-Service) attack on Hindustan Times website floods the site's servers with excessive traffic, rendering it slow or inaccessible to users. This overload consumes server resources, leading to extended loading times and potential errors for users. The consequences include lost revenue, a damaged reputation, and the need for mitigation and recovery measures.
2. **Data breaches:** A data breach on Hindustan Times news website is an unauthorized intrusion where cybercriminals access and potentially steal sensitive user data, such as personal and financial information. This breach can result in legal penalties, reputational damage, and the need to notify affected users. Long-term consequences include financial losses and efforts to rebuild trust through improved security measures.
3. **Malware attacks:** A malware attack on Hindustan Times website entails the insertion of harmful software (malware) into the website's servers or content. The attackers aim to compromise the website's security, potentially leading to various harmful outcomes.
4. **Phishing attacks:** A phishing attack Hindustan Times news website involves cybercriminals creating fake web content or emails that mimic the news site's appearance. They trick users into clicking on links or providing sensitive information, aiming to steal data or install malware. User education is key to prevention.
5. **Zero-day attacks:** A zero-day attack on this news website involves hackers exploiting a previously unknown software vulnerability. It's a stealthy threat, as there's no prior defense. The attack can lead to data breaches or website disruptions, requiring an immediate response.

IV. PASSIVE ATTACKS

The OWASP ZAP passive web application scan crawls the pages of a web application. It inspects the web pages as well as the requests and responses sent between the server. The passive scan checks for vulnerabilities such as cross-domain misconfigurations, insecure cookies, vulnerable js dependencies, and more.

Total number of risks found by severity - **18**

Summary list of all detected risks -

Top 10 vulnerabilities are mentioned below

1. Absence of Anti-CSRF Tokens
2. Cross-Domain Misconfiguration
3. Multiple X-Frame-Options Header Entries
4. Missing Anti-clickjacking Header
5. Content Security Policy (CSP) Header Not Set
6. X-Content-Type-Options Header Missing
7. Cross-Domain JavaScript Source File Inclusion
8. SSL/TLS:Report Vulnerable Cipher Suites for HTTPS
9. SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
10. Cookie Without Secure Flag

V. ACTIVE ATTACKS

The OWASP ZAP active web application scan crawls the pages of a web application. It scans for all of the passive scan checks and additionally makes requests and submits forms to actively test an application for even more vulnerabilities. The active scan checks for vulnerabilities such as SQL injection, remote command execution, XSS, and more. Hindustan Times news website doesn't have a single active attack according to our Vulnerability Testing Tool.

Total number of risks found by severity - **0**

VI. SECURITY MECHANISMS

The scope of testing included in Hindustan Times depends on the specific needs of the organization. However, some common areas of testing include:

1. **Web Software Security test** : Web software security testing is the process of evaluating and identifying vulnerabilities in web applications to ensure they are protected against cyber threats and breaches.

2. **GDPR compliance test :** GDPR compliance testing verifies that an organization's data processing activities align with the General Data Protection Regulations legal requirements to protect individuals' privacy rights.

3. **PCI DSS compliance test :** PCI DSS compliance testing confirms that an organization's payment card data handling and security practices comply with the Payment Card Industry Data Security Standard to prevent data breaches and safeguard cardholder information.

4. **HTTP header security :** HTTP header security involves setting response headers to protect web applications from various security threats and vulnerabilities, enhancing overall web security.

5. **Content security testing :** Content security testing checks digital content for vulnerabilities and threats to ensure its safe distribution and access

The scope of testing can also be divided into different levels, such as unit testing, integration testing, system testing, and acceptance testing. Unit testing is performed on individual units of code, integration testing is performed on groups of units of code, system testing is performed on the entire system, and acceptance testing is performed by the customer.

The specific tests that are performed will depend on the specific needs of the organization and the software. However, the above are some of the common areas of testing that are performed on Hindustan Times.

Here are some additional considerations for the scope of testing on Hindustan Times:

1. The size and complexity of the software.
2. The target audience for the software.
3. The budget and time constraints.
4. The level of risk associated with the software.
5. The regulatory requirements.

By considering these factors, the organization can develop a scope of testing that is appropriate for Hindustan Times

VII. SECURITY RECOMMENDATIONS

1. **SSL/TLS Report Vulnerable Cipher Suites for HTTPS** :-

   The service configuration should be modified to discontinue the acceptance of presently allowed cipher suites. This adjustment is likely prompted by security considerations or the necessity for more robust encryption mechanisms to enhance data protection and safeguard against potential vulnerabilities or threats.

2. **SSL/TLS Deprecated TLSv1.0 and TLSv1.1 Protocol Detection :-**

   For improved cybersecurity, it's recommended to disable obsolete TLSv1.0 and TLSv1.1 security protocols and migrate to the more secure TLSv1.2. This transition bolsters data protection by addressing vulnerabilities tied to outdated encryption standards, ensuring a safer and more resilient security posture.

3. **X-Content-Type-Options Header Missing :-**

   Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-TypeOptions header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIMEsniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

4. **Cross-Domain Misconfiguration :-**

   Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

5. **Missing Anti-clickjacking Header :-**

   Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

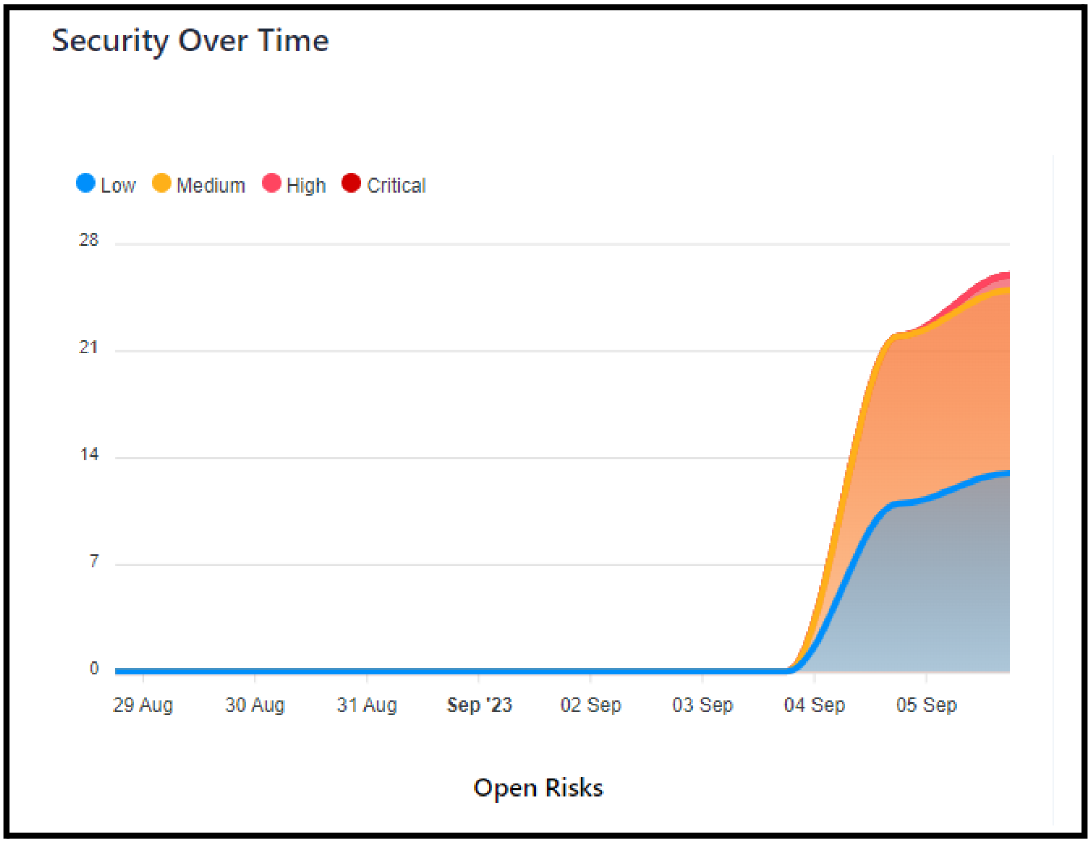
VIII. CONCLUSION

News websites like Hindustan Times face diverse vulnerabilities, from code flaws to outdated software, risking data security and site integrity. Such issues, including SQL injection and XSS, can harm users and erode trust.

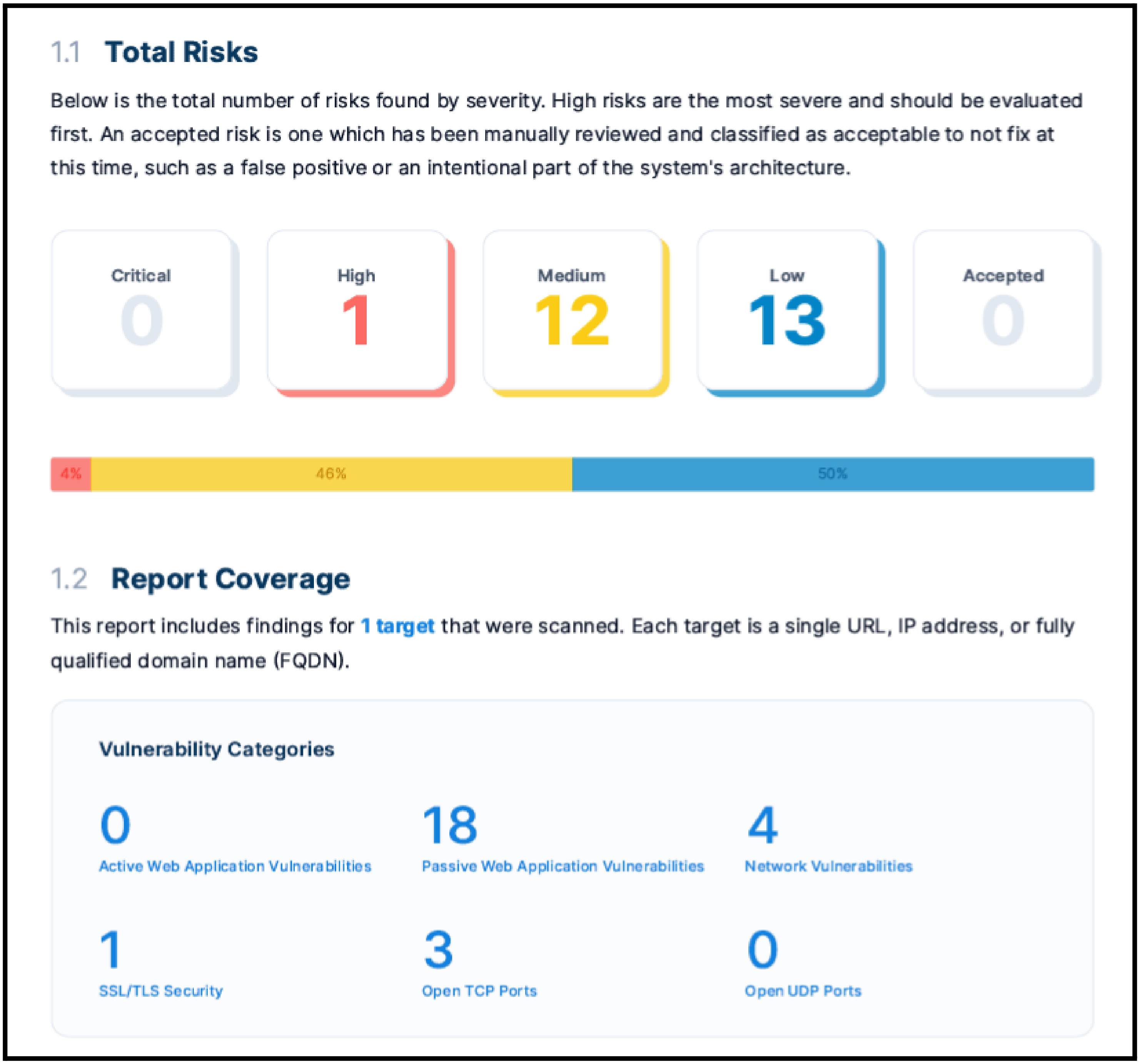
Mitigation requires proactive cybersecurity. Regular assessments, prompt patching, strong access controls, and employee training are essential. These measures protect users' sensitive data and uphold the website's credibility.

As vital sources of information, news websites must prioritize cybersecurity to ensure long-term trust and reliability. By investing in security practices, they not only safeguard their users but also maintain their pivotal role in society's information dissemination.

In an era where the credibility of news sources is of paramount importance, maintaining the security of news websites goes beyond mere technical considerations. It is a fundamental aspect of preserving user trust and the credibility of journalism in the digital age.



IX. VULNERABILITY REPORT USING ONLINE TOOLS



1.1 Total Risks

Below is the total number of risks found by severity. High risks are the most severe and should be evaluated first. An accepted risk is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive or an intentional part of the system's architecture.

Critical	High	Medium	Low	Accepted
0	1	12	13	0

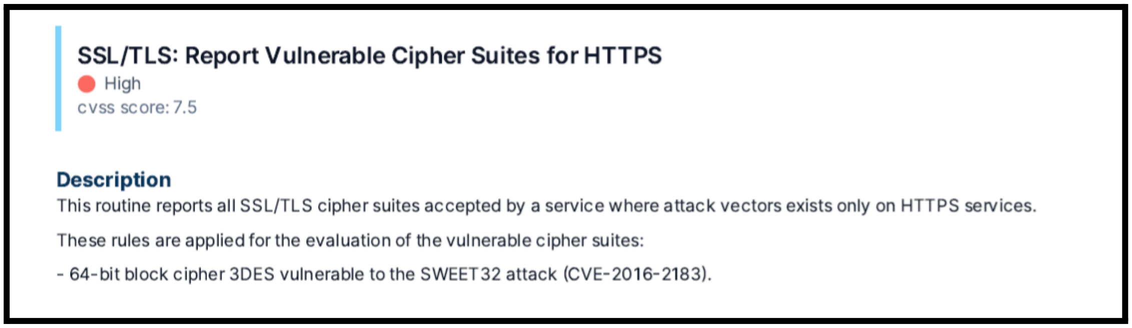
1.2 Report Coverage

This report includes findings for 1 target that were scanned. Each target is a single URL, IP address, or fully qualified domain name (FQDN).

Vulnerability Categories

0 Active Web Application Vulnerabilities	18 Passive Web Application Vulnerabilities	4 Network Vulnerabilities
1 SSL/TLS Security	3 Open TCP Ports	0 Open UDP Ports

Key Vulnerabilities found are:



SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

● High

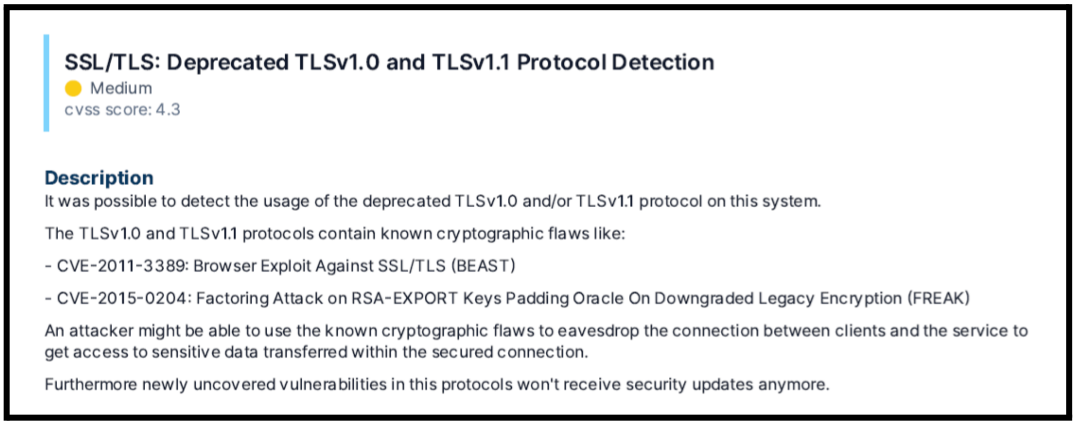
cvss score: 7.5

Description

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).



SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

● Medium

cvss score: 4.3

Description

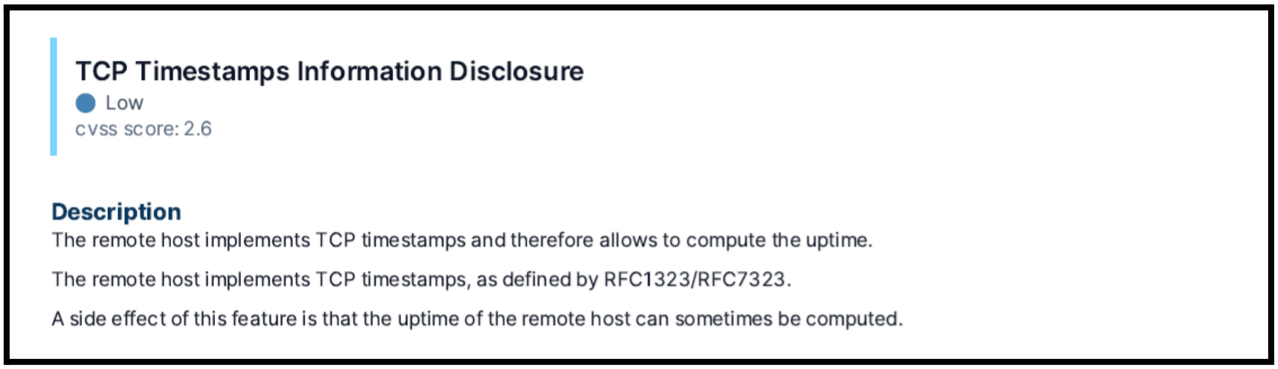
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.



TCP Timestamps Information Disclosure

● Low

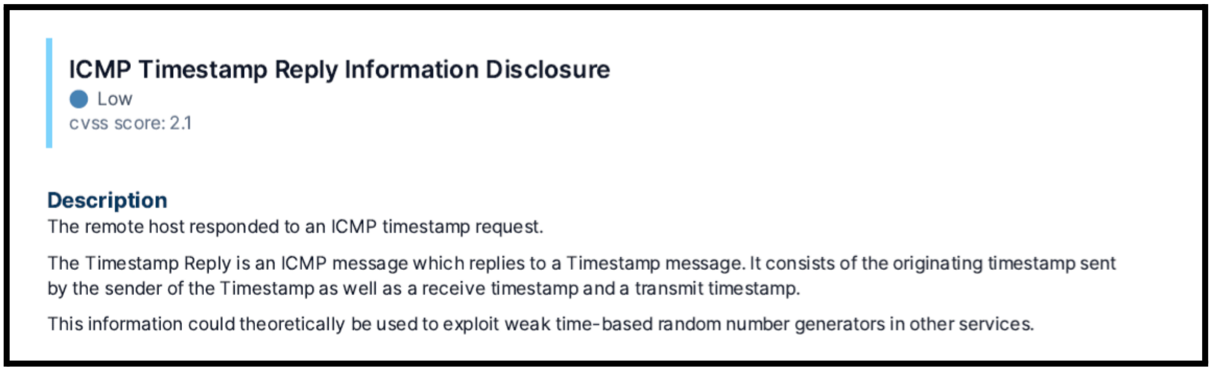
cvss score: 2.6

Description

The remote host implements TCP timestamps and therefore allows to compute the uptime.

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

A side effect of this feature is that the uptime of the remote host can sometimes be computed.



ICMP Timestamp Reply Information Disclosure

● Low

cvss score: 2.1

Description

The remote host responded to an ICMP timestamp request.

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

This information could theoretically be used to exploit weak time-based random number generators in other services.