Port scan on Chameleon Website

CHAMELEON

FOR OUR SMARTER WORLD

Table of Contents

Executive summary:

This executive summary presents the key findings and recommendations resulting from a recent port scan conducted on the Chameleon website. Port scanning is a crucial technique in cybersecurity used to identify open ports on a computer or network device. In this case, it was employed for security assessment purposes to pinpoint potential vulnerabilities in the Chameleon website. This report primarily focuses on the discovered open ports and offers actionable recommendations to address associated risks.

Introduction

What is Port Scan)?

Port scanning is a technique used in computer networking and cybersecurity to discover open ports on a computer or network device. Ports are virtual endpoints for communication in a network, and they are associated with specific services or protocols. Port scanning is typically performed for various reasons, including network administration, security assessments, and troubleshooting. Here's an overview of port scanning:

Usages and Purpose:

Port scanning is a versatile tool with both legitimate and malicious applications. In this case, it was used for security assessment to identify potential vulnerabilities in the Chameleon website. This report focuses on the open ports discovered during the scan and provides recommendations to mitigate associated risks.

Tools used

- Kali Linux
- Nmap (VM and local computer)
- Wireshark

Steps:

Tutorials of these types of attacks are available on website and YouTube videos.

Nmap (In VM and Local Environment):

nmap: This pivotal command is the core directive to initiate the Nmap utility, signifying the commencement of the scanning process.

- -sS: Employed as a strategic choice, this option signifies a TCP SYN scan, a sophisticated port scanning method meticulously designed to ascertain the accessibility of TCP ports on the target system. This technique dispatches SYN packets to each port and meticulously analyzes the responses, discerning whether a port is open or closed.
- -T4: To optimize efficiency and expedite the scan, this setting configures the timing template to "Aggressive" (T4). This selection ensures a relatively swift pace of scanning while maintaining precision.

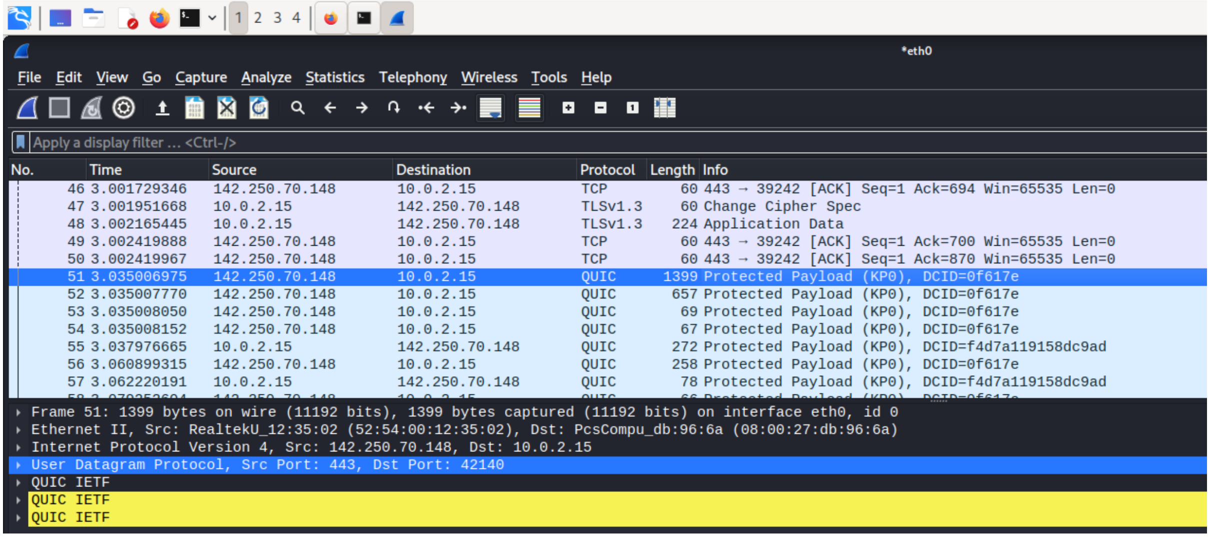
- -v: A crucial element for enhanced insight, the verbose (-v) option is activated, furnishing a comprehensive, real-time data stream regarding the scan's progression.
- -n: By choosing this option, Nmap is instructed to abstain from engaging in DNS resolution for IP addresses and hostnames. This streamlined approach accelerates the scanning process, particularly when the sole focus is on IP addresses.
- --max-parallelism 10: This strategic specification dictates the maximum quantity of simultaneous probes dispatched during the scan, a count capped at 10. This feature optimizes scan speed and resource utilization.
- -Pn: By opting for this configuration, host discovery is intentionally disabled. It operates under the assumption that the host is operational even if it refrains from responding to conventional host discovery probes. This capacity proves invaluable when assessing unresponsive hosts.
- --top-ports 100: This parameter carefully directs the scan's focus towards the top 100 most frequently utilized ports. Nmap maintains a curated inventory of these ports, thus refining the scan by homing in on the primary network ingress points.

These meticulously chosen tools and configurations ensure a comprehensive and efficient examination of the Chameleon website's port configuration, facilitating the detection of potential vulnerabilities with precision and thoroughness.

IP addresses:

To find the IP address for VM and website, we used Wireshark.

The IP address for the Chameleon website (142.250.70.148) and the Kali Linux virtual machine (10.0.2.15) were identified using Wireshark.


1 2 3 4
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time         Source          Destination     Protocol Length Info
  46 3.001729346  142.250.70.148  10.0.2.15       TCP        60 443 → 39242 [ACK] Seq=1 Ack=694 Win=65535 Len=0
  47 3.001951668  10.0.2.15       142.250.70.148  TLSv1.3    60 Change Cipher Spec
  48 3.002165445  10.0.2.15       142.250.70.148  TLSv1.3   224 Application Data
  49 3.002419888  142.250.70.148  10.0.2.15       TCP        60 443 → 39242 [ACK] Seq=1 Ack=700 Win=65535 Len=0
  50 3.002419967  142.250.70.148  10.0.2.15       TCP        60 443 → 39242 [ACK] Seq=1 Ack=870 Win=65535 Len=0
  51 3.035006975  142.250.70.148  10.0.2.15       QUIC     1399 Protected Payload (KP0), DCID=0f617e
  52 3.035007770  142.250.70.148  10.0.2.15       QUIC      657 Protected Payload (KP0), DCID=0f617e
  53 3.035008050  142.250.70.148  10.0.2.15       QUIC       69 Protected Payload (KP0), DCID=0f617e
  54 3.035008152  142.250.70.148  10.0.2.15       QUIC       67 Protected Payload (KP0), DCID=0f617e
  55 3.037976665  10.0.2.15       142.250.70.148  QUIC      272 Protected Payload (KP0), DCID=f4d7a119158dc9ad
  56 3.060899315  142.250.70.148  10.0.2.15       QUIC      258 Protected Payload (KP0), DCID=0f617e
  57 3.062220191  10.0.2.15       142.250.70.148  QUIC       78 Protected Payload (KP0), DCID=f4d7a119158dc9ad
```

```
Frame 51: 1399 bytes on wire (11192 bits), 1399 bytes captured (11192 bits) on interface eth0, id 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_db:96:6a (08:00:27:db:96:6a)
Internet Protocol Version 4, Src: 142.250.70.148, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 443, Dst Port: 42140
QUIC IETF
QUIC IETF
QUIC IETF
```

- **Virtual Machine IP:** The IP address 10.0.2.15 corresponds to a private IP address allocated for the Kali Linux virtual machine. This address serves as the gateway for conducting network operations from within the virtual environment.
- **Chameleon Website IP:** The IP address 142.250.7.148 is associated with the legacy Chameleon website. This address is a critical reference point for identifying the target of the port scan.

Command: The executed command line for the port scan is as follows:

```
nmap -sS -T4 -v -n --max-parallelism 10 -Pn --top-ports 100 142.250.70.148
```

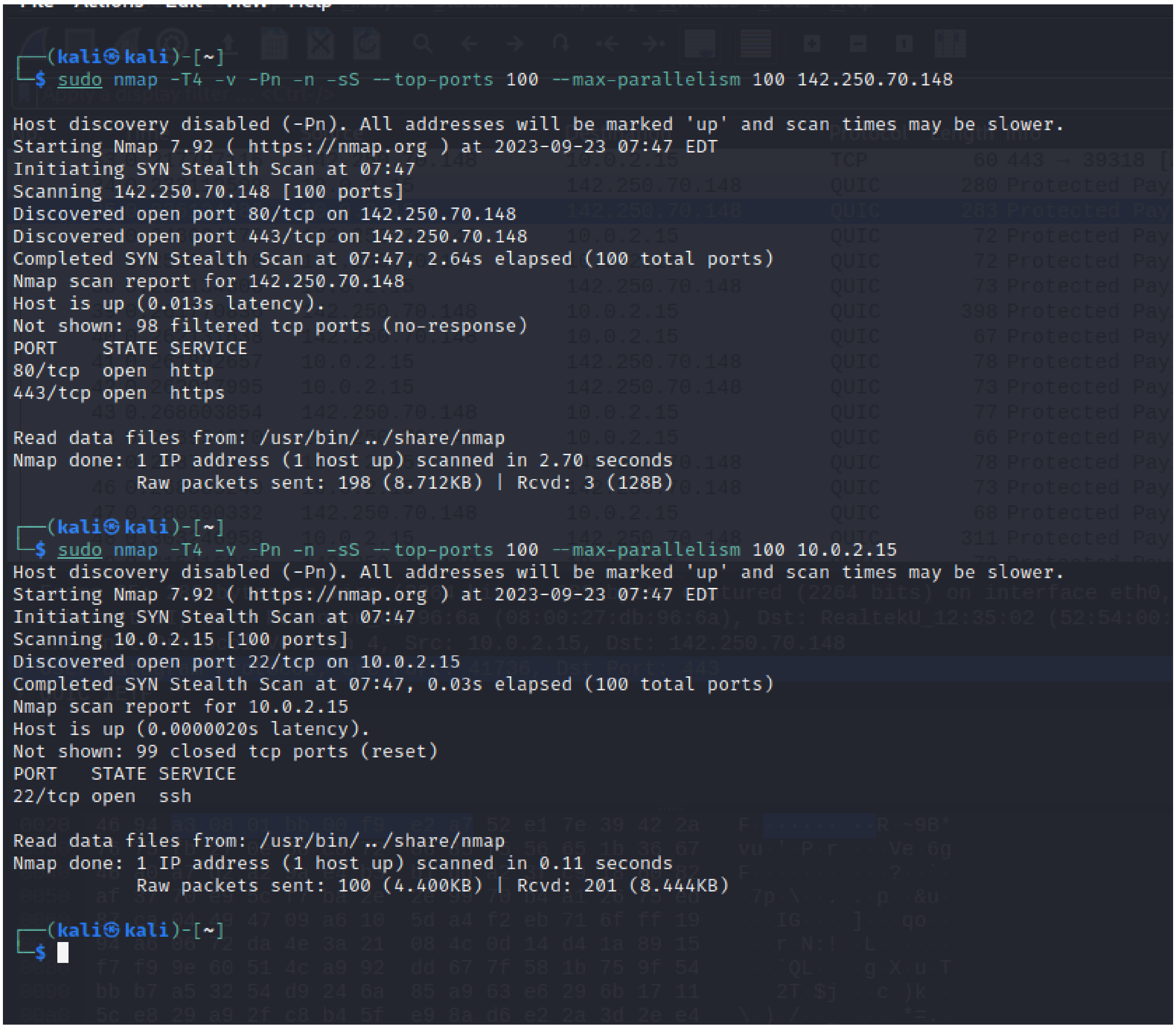
Explanation of Options:

- -sS: This option initiates a TCP SYN scan, a technique designed to identify open TCP ports by sending SYN packets to each port and analyzing responses.
- -T4: The timing template "Aggressive" (T4) is chosen for faster scan execution, optimizing efficiency.
- -v: The "verbose" option is enabled, offering comprehensive scan progress details.
- -n: DNS resolution is bypassed for IP addresses and hostnames, expediting the scan while focusing solely on IP addresses.
- --max-parallelism 10: This parameter controls the maximum number of concurrent probes sent during the scan, with a limit set at 10, enhancing scan speed.
- -Pn: Host discovery is disabled, assuming the host is operational even if it doesn't respond to standard host discovery probes. This is useful for scanning unresponsive hosts.
- --top-ports 100: The scan is concentrated on the top 100 most frequently used ports, streamlining the analysis by focusing on common network entry points.

This meticulously crafted command line maximizes the effectiveness of the port scan, ensuring that the Chameleon website's port configuration is thoroughly examined for potential vulnerabilities.

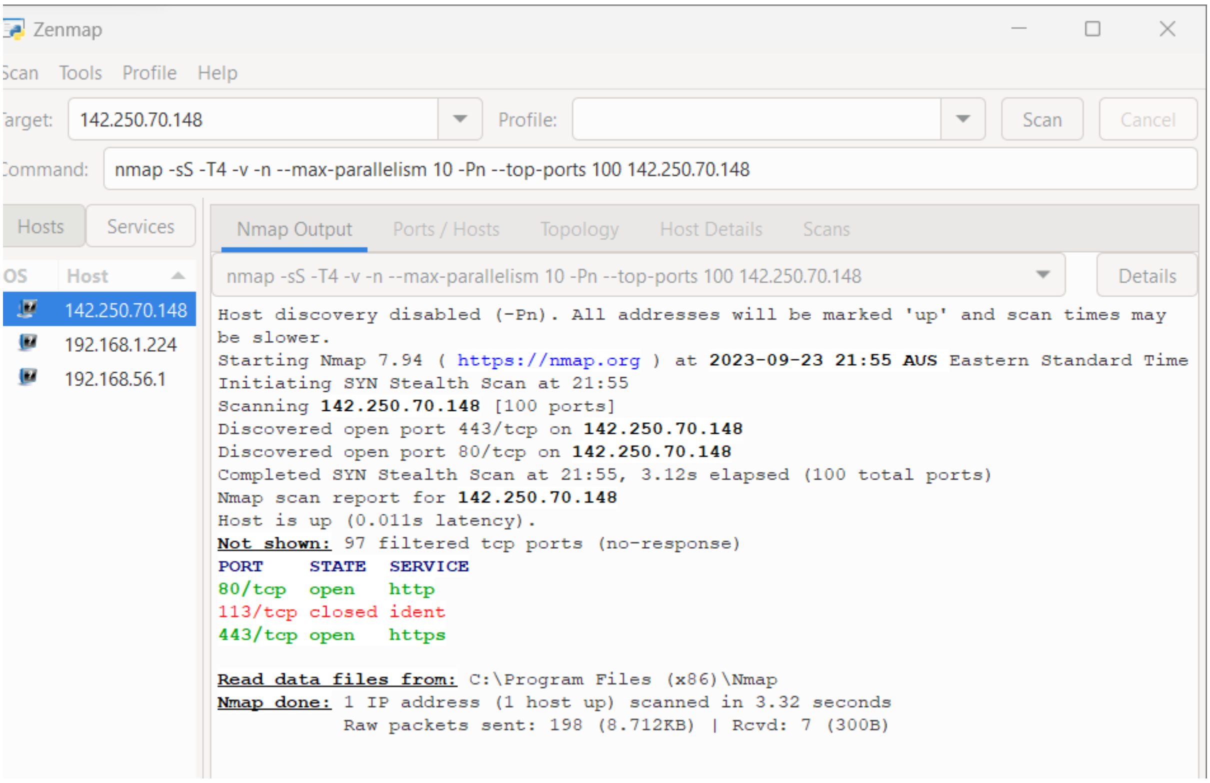
Port being scanned:

Screenshot of Port being scanned on Virtual Machine:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -T4 -v -Pn -n -sS --top-ports 100 --max-parallelism 100 142.250.70.148

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-23 07:47 EDT
Initiating SYN Stealth Scan at 07:47
Scanning 142.250.70.148 [100 ports]
Discovered open port 80/tcp on 142.250.70.148
Discovered open port 443/tcp on 142.250.70.148
Completed SYN Stealth Scan at 07:47, 2.64s elapsed (100 total ports)
Nmap scan report for 142.250.70.148
Host is up (0.013s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.70 seconds
           Raw packets sent: 198 (8.712KB) | Rcvd: 3 (128B)

┌──(kali㉿kali)-[~]
└─$ sudo nmap -T4 -v -Pn -n -sS --top-ports 100 --max-parallelism 100 10.0.2.15
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-23 07:47 EDT
Initiating SYN Stealth Scan at 07:47
Scanning 10.0.2.15 [100 ports]
Discovered open port 22/tcp on 10.0.2.15
Completed SYN Stealth Scan at 07:47, 0.03s elapsed (100 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.0000020s latency).
Not shown: 99 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
           Raw packets sent: 100 (4.400KB) | Rcvd: 201 (8.444KB)

┌──(kali㉿kali)-[~]
└─$ 
```

Screenshot of port of website scan at local computer:



Target: 142.250.70.148

Profile:

Command: nmap -sS -T4 -v -n --max-parallelism 10 -Pn --top-ports 100 142.250.70.148

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may
be slower.
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-23 21:55 AUS Eastern Standard Time
Initiating SYN Stealth Scan at 21:55
Scanning 142.250.70.148 [100 ports]
Discovered open port 443/tcp on 142.250.70.148
Discovered open port 80/tcp on 142.250.70.148
Completed SYN Stealth Scan at 21:55, 3.12s elapsed (100 total ports)
Nmap scan report for 142.250.70.148
Host is up (0.011s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed ident
443/tcp open   https

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 3.32 seconds
           Raw packets sent: 198 (8.712KB) | Rcvd: 7 (300B)
```

Interpretation of port scan results:

The ensuing section elucidates the outcomes derived from the exhaustive port scan, shedding light on the specific open ports unearthed during the assessment. This comprehensive analysis serves to underscore potential vulnerabilities intrinsically linked to these ports, which encompass various facets such as outdated software, configuration anomalies, and the potential presence of web applications susceptible to exploitation.

Within this context, it is imperative to delineate the plausible security risks associated with both open and closed ports, namely:

Port 80/tcp (HTTP):

- Service: HTTP (Hypertext Transfer Protocol)
- Vulnerability Risk: Port 80 is ubiquitously employed for the dissemination of web content through HTTP. Notably, the mere presence of an open Port 80 does not inherently signify a vulnerability. Rather, the risk is contingent upon the web server's intricate configuration and the software operating therein. Potential risks encompass:
- Vulnerabilities stemming from outdated or unpatched web server software, which can potentially culminate in security breaches. Emphasis should be placed on maintaining the web server software's currency through the timely application of security patches.
- Exposure to risk due to server misconfiguration, which may inadvertently divulge sensitive data, directories, or yield to compromised security settings.

- The latent danger posed by vulnerable web applications hosted on the server. It is imperative to diligently assess and fortify these applications to preempt potential exploitation by malicious actors.

Port 443/tcp (HTTPS):

Service: HTTPS (HTTP Secure)

Vulnerability Risk: Port 443 is dedicated to secure web traffic conducted over HTTPS, and akin to Port 80, the vulnerability quotient hinges upon the web server's intricate setup and the underlying software. Key considerations encompass:

Vulnerabilities stemming from SSL/TLS configuration anomalies that might render the server susceptible to security lapses. The safeguarding of the server entails the utilization of up-to-date and secure SSL/TLS protocols and ciphers.

Risks associated with certificate issues, including the potential pitfalls associated with improperly configured SSL/TLS certificates or the utilization of self-signed certificates, which could introduce security vulnerabilities.

The lurking threat of vulnerabilities resident within web applications operating over HTTPS. Prudent measures should be adopted to proactively address and mitigate these vulnerabilities.

Port 113 (Ident):

- Vulnerability Risk: Port 113 is conventionally associated with the Ident protocol, an instrument employed for the identification of users engaged in specific TCP connections. Notably, the port's closure, as indicated in the scan results (not open), generally implies a minimal risk threshold. In essence, as long as this port remains closed, no substantial vulnerabilities are anticipated to be associated with it.

Furthermore, in the context of developing the new website, the following mitigation strategies warrant diligent consideration:

- **Web Application Security:** Should the website incorporate web applications, the adoption of secure coding practices becomes imperative to preclude common web vulnerabilities, such as SQL injection, cross-site scripting (XSS), and Cross-Site Request Forgery (CSRF). Additionally, the integration of web application firewalls (WAFs) serves as a formidable barrier against potential attacks.
- **Error Handling:** The implementation of customized error handling mechanisms assumes paramount importance as they serve the dual purpose of averting the inadvertent disclosure of sensitive information in error messages while simultaneously providing users with generic error messages. Moreover, robust error logging practices ensure the secure storage of detailed error information.

These meticulous considerations underscore the multifaceted nature of cybersecurity assessments and delineate a strategic roadmap for fortifying the security posture of the examined systems.

Recommendations:

Several actionable recommendations are proposed to mitigate the identified risks. These recommendations encompass tasks such as updating software, enhancing SSL/TLS configurations, and implementing robust error handling mechanisms for web applications.

- **Regular Software Updates:**
  Ensure that all software components, including the web server software, operating system, and any third-party applications, are regularly updated with the latest security patches and updates. Timely updates help mitigate known vulnerabilities.
- **SSL/TLS Configuration Review:**
  Conduct a thorough review of the SSL/TLS configuration on the web server to ensure it adheres to best practices. This includes using up-to-date and secure SSL/TLS protocols and ciphers.
- **Certificate Management:**
  Implement robust certificate management practices to ensure SSL/TLS certificates are properly configured, valid, and issued by trusted certificate authorities. Avoid the use of self-signed certificates in production environments.
- **Web Application Security:**
  If the website hosts web applications, follow secure coding practices to prevent common web vulnerabilities such as SQL injection, cross-site scripting (XSS), and Cross-Site Request Forgery (CSRF).
  Utilize web application firewalls (WAFs) to provide an additional layer of protection against web-based attacks.
- **Server Configuration Review:**
  Conduct a comprehensive review of the web server's configuration to ensure it follows security best practices. Pay special attention to access controls, directory permissions, and security settings.
- **Error Handling Improvement:**
  Implement custom error handling to avoid the exposure of sensitive information in error messages. Provide users with generic error messages while securely logging detailed error information for analysis.
- **Ongoing Vulnerability Scanning:**
  Establish a routine schedule for conducting vulnerability scans and security assessments on the Chameleon website. Regular scans can help identify and address emerging threats and vulnerabilities.
- **Security Awareness Training:**
  Train staff members and developers involved in website maintenance about security best practices, including secure coding, password management, and incident response procedures.

Implementing these recommendations will help enhance the security posture of the Chameleon website and reduce the risk of security incidents. Regular monitoring and proactive measures are essential to safeguard against evolving threats in the cybersecurity landscape.

Conclusion:

In conclusion, the port scan conducted on the Chameleon website has shed light on potential security vulnerabilities that require attention. While open ports such as Port 80 (HTTP) and Port 443 (HTTPS) are essential for web services, the risks associated with outdated software, misconfigurations, and possible vulnerabilities in web applications should not be underestimated.

The provided recommendations offer a clear path to strengthen the security posture of the Chameleon website. These include staying vigilant with software updates, ensuring secure SSL/TLS configurations, and implementing sound web application security practices, such as protection against common threats like SQL injection, cross-site scripting (XSS), and Cross-Site Request Forgery (CSRF).

It's crucial for the Chameleon website to proactively address these issues, considering the ever-evolving threat landscape. Regular security assessments, continuous monitoring, and a commitment to best practices will contribute to maintaining a secure and resilient online presence. By heeding these recommendations, the Chameleon website can enhance its security and protect both its assets and its users from potential cyber threats.

References:

[1] “Pentest-Tools.com,” Pentest-Tools.com, 2013. https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap (accessed Sep. 23, 2023).

[2] “What is a Port Scan?,” Palo Alto Networks, 2016. https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan (accessed Sep. 23, 2023).

[3] I. Hacker, “How to Port scanning with Kali Linux,” YouTube. May 12, 2021. Accessed: Sep. 23, 2023. [YouTube Video]. Available: https://www.youtube.com/watch?v=6915d2IZUv4&t=82s

[4] I. Hacker, “How to Port scanning with Kali Linux,” YouTube. May 12, 2021. Accessed: Sep. 23, 2023. [YouTube Video]. Available: https://www.youtube.com/watch?v=6915d2IZUv4&t=82s

[5] NetworkChuck, “Nmap Tutorial to find Network Vulnerabilities,” YouTube. Jul. 09, 2020. Accessed: Sep. 23, 2023. [YouTube Video]. Available: https://www.youtube.com/watch?v=4t4kBkMsDbQ