Executive Summary - Penetration Test Report for artstailor.com

Saijayanth Chidirala

2024-01-21

Contents

1 Project Overview **2**

2 Goals **2**

3 Risk Ranking/Profile **3**

4 Summary of Findings **4**
4.1 Finding: *Accessible Hosts* 4
4.2 Finding: *Outdated vsftpd* 5
4.3 Finding: *Buffer Overflow in Brian's Service* 6
4.4 Finding: *Default Password in OPNSense and RDP Vulnerability* . . 6
4.5 Finding: *Privilege Escalation* 7
4.6 Finding: *Password Cracking* 8
4.7 Finding: *Service Discovery* 9
4.8 Finding: *Ease of Access Vulnerability* 9
4.9 Finding: *Secret Page* 10
4.10 Finding: *Vulnerable Version of Sudo* 11
4.11 Finding: *Spoofing wpad* 11
4.12 Vulnerability: *Social Engineering* 12
4.13 Brian's Project: *Missing Input Validation* 12
4.14 Brian's Project: *File Inclusion Vulnerability* 13
4.15 Reverse Engineering: *APK* 13

5 Recommendation Summary **14**

6 Strategic Roadmap **14**

1 Project Overview

The penetration test conducted on Artstailor.com aimed to provide a comprehensive evaluation of the organization's cybersecurity resilience. Beginning with a meticulous project overview, the testing methodology encompassed a systematic examination of the network infrastructure, web applications, and potential points of vulnerability. This involved simulating various cyber threats to assess the effectiveness of existing security measures, identify weaknesses, and gauge the overall readiness of Artstailor.com to withstand potential attacks. The overarching objective was to offer a holistic view of the organization's security posture, emphasizing proactive measures to fortify defenses against emerging threats.

Throughout the project, the testing team adhered to industry standard methodologies, leveraging a combination of automated tools and manual techniques to ensure a thorough examination of the digital landscape. The collaborative effort involved comprehensive vulnerability assessments, risk profiling, and in-depth analysis of specific findings. The resulting report encapsulates a detailed account of the identified vulnerabilities, their potential impact, and prioritized recommendations for mitigation. By providing a clear and actionable roadmap, the project overview serves as a foundational document guiding Artstailor.com in the pursuit of a resilient and robust cybersecurity framework. The insights gleaned from this penetration test offer invaluable strategic guidance to fortify the organization's defenses, enabling it to navigate the ever-evolving landscape of cyber threats with heightened resilience and confidence.

2 Goals

The primary objectives of the penetration test conducted on Artstailor.com were centered around assessing the overall security posture of the organization's digital infrastructure. The foremost goal was to identify and evaluate potential vulnerabilities within the network, systems, and applications. By simulating real-world cyberattacks, the aim was to uncover any weaknesses that malicious actors could exploit to gain unauthorized access, compromise sensitive data, or disrupt normal operations. This proactive approach enabled the organization to gain a comprehensive understanding of its security landscape and prioritize remediation efforts effectively.

Another key goal of the penetration test was to assess the effectiveness of existing security controls and protocols in place. This involved evaluating the resilience of firewalls, intrusion detection systems, and other defensive mechanisms against various attack vectors. By examining the responsiveness of security measures, the objective was to identify potential gaps or areas where improvements could be made to enhance the overall defense against cyber

threats. This comprehensive assessment contributed to refining and strengthening the organization's security posture, ensuring a robust and proactive defense against evolving cyber risks.

Additionally, the penetration test aimed to provide actionable insights and recommendations for mitigating identified vulnerabilities. Beyond merely highlighting weaknesses, the goal was to equip the organization with a roadmap for enhancing its security measures. This included practical and prioritized recommendations for implementing security best practices, fortifying network configurations, updating software, and improving user awareness. The overarching objective was to empower Artstailor.com to take informed and strategic steps toward bolstering its cybersecurity defenses, thereby reducing the risk of potential breaches and safeguarding the integrity of its digital assets.

3 Risk Ranking/Profile

The risk ranking/profile serves as a pivotal component within the report, offering a concise summary of the threat and vulnerability levels associated with each finding. This profile is instrumental in providing a quick and comprehensive understanding of the severity of each identified issue, aiding in the formulation of a prioritized resolution schedule. The assigned rankings not only facilitate the targeted addressing of the most vulnerable findings but also present an opportunity to compute an aggregate metric. This aggregate metric can be instrumental in discerning which domains contribute most significantly to the overall vulnerabilities, guiding a strategic approach to remediation.

In this report, the Common Vulnerability Scoring System (CVSS) is employed as the framework for risk assessment. CVSS, developed by the National Institute of Standards and Technology, forms the basis for our ratings, specifically utilizing version 3.0. This version incorporates distinct parameters to calculate the severity rating of a vulnerability, offering a standardized and objective approach to risk evaluation. The parameters encompass aspects such as the Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), User Interaction (UI), Scope (S), Confidentiality (C), Integrity (I), and Availability (A). Leveraging CVSS 3.0 enhances the precision and consistency of our risk assessments, ensuring a robust foundation for effective cybersecurity decision-making.

Throughout the duration of this penetration test, we successfully achieved administrator/root level access in numerous instances of vulnerability discovery. It is noteworthy that several of these vulnerable services are openly exposed to the internet, making them potentially accessible to any individual worldwide at minimal cost. Furthermore, the system exhibits a susceptibility for a malicious actor to attain domain administrator rights. The elevated prob-

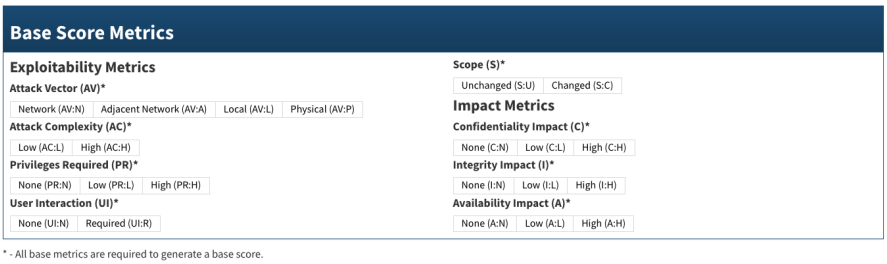

Figure 1: CVSS 3.0

ability of exploitation is heightened by the system's high visibility and the relatively straightforward scanning apparatus employed. Additionally, it is imperative to underscore that many of the identified vulnerabilities are well-known, with established pathways and thoroughly tested tools readily available on the internet for potential malicious exploitation. This collective assessment underscores the urgency for robust security measures to fortify the system against imminent threats and mitigate the potential repercussions of these identified vulnerabilities.

4 Summary of Findings

4.1 Finding: *Accessible Hosts*

The following hosts were discover-able on the network. While this not be entirely detrimental, it is wise to make sure that important hosts are not discoverable. It is also important to make sure that the hosts that are exposed are secure.

ns.artstailor.com	172.70.184.133
costumes.artstailor.com	10.70.184.39
KEY005-hKku4 –SLASH–qTxNsmJIG0iT8pSQ.artstailor.com	10.70.184.40
mail.artstailor.com	172.70.184.3
innerouter.artstailor.com	172.70.184.3
pdc.artstailor.com	10.70.184.90
books.artstailor.com	10.70.184.91
pop.artstailor.com	172.70.184.3
devbox.artstailor.com	10.70.184.100
ceo.artstailor.com	10.70.184.101
linuxserver.artstailor.com	10.70.184.133

Internal IP Address block : 10.70.184.0/24

Severity Rating - Common Vulnerability Scoring System

CVSS Base Severity Rating: 6.5 AV:N AC:L PR:N UI:N S:U C:L I:N A:L

Vulnerability Description

The nature of vulnerability for the system in question is network based. Several external and internal routers are directly exposed to the internet. This opens up your system to attacks that might overwhelm your system. These open systems might also allow an attacker to use a different class of vulnerability against you. Some host names give off information on the software being used on the hosts.

Confirmation method

The following command can verify the existence of these open nodes: fierce –domain artstailor.com –traverse 255

Mitigation or Resolution Strategy

artstailor.com can use a content delivery network(CND) to mask the actual server IP addresses by flowing traffic though CDN. Proxy servers can be implemented between the external network and the shop system to better hide the server. Rename servers to obscure names(almost like passwords) so that discovery via lookup is extremely difficult.

4.2 Finding: *Outdated vsftpd*

Severity Rating - Common Vulnerability Scoring System

CVSS Base Severity Rating: 8.8 AV:N AC:L PR:N UI:R S:U C:H I:H A:H

Vulnerability Description

The nature of vulnerability for the system in question is internal software based. Said software is also exposed to the internet. This opens up your system to attacks that might give malicious users access to your system files. This file access might also allow an attacker to use a different class of vulnerability against you.

Confirmation method

1. Open a Linux shell instance on the server machine for ns.artstailor.com (172.70.184.133).
2. Type in the command 'vsftpd -version' without the quotes; note the output.
3. If the output says : 'vsftpd : version 2.3.4', the current version of this software on your system is vulnerable.
4. Refer https://www.tenable.com/plugins/nessus/55523 for more details.

Mitigation or Resolution Strategy

Vulnerability is of critical nature. Suggested immediate update for vsftpd 2.3.4 on all systems existing under artstailor.com.

4.3 Finding: *Buffer Overflow in Brian's Service*

Vulnerability Description

The nature of vulnerability for the system in question is internal software based. Said software is also exposed to the internet. This opens up your system to attacks that might give malicious users access to your system files. This file access might also allow an attacker to use a different class of vulnerability against you.

Confirmation method

1. Open a Linux shell on a machine different from the one that www.artstailor.com is running on.
2. Use command 'nc 172.70.184.133 1337'. When asked for a username, use 'brian' and not down the list of valid commands. Disconnect using 'Ctrl + Z'.
3. Repeat step 2, only this time, instead of username 'brian' use username 'aaaaaaaaaaaaaaasl'. Upon repetition of the username prompt, use 'brian'.
4. If the list of commands has changed with the command 'ls' being present in the list of commands, vulnerability exists.
5. Replace 'sl' at the end of the username string 'aaaaaaaaaaaaaaasl' with the reverse of any Linux command to add it to the list of valid commands.

Mitigation or Resolution Strategy

1. Immediately block port 1337 until the service is redeveloped to be rid of any vulnerabilities.
2. Use 'strncmp' and 'strncpy' instead of 'strcmp' and 'strcpy' which have been deprecated for a long time.
3. keep list of valid commands strictly static and create a subroutine to kill the process if any change is detected in the list of valid commands.

4.4 Finding: *Default Password in OPNSense and RDP Vulnerability*

Vulnerability Description

The nature of vulnerability for the system in question is internal software based. Said software can also exposed to the internet using port forwarding. This opens up your system to attacks that might give malicious users access to your system files. This file access might also allow an attacker to use a different

class of vulnerability against you. Existing password policy allows users to set passwords that are easily discover-able.

Confirmation method

1. Open the browser and go to the website https//:172.70.184.3:8443 . The password is set to the default root::opnsense
2. An open RDP session exists on costumes.artstailor.com. Use port forwarding in OPNsense to forward the port 3389 on IP 10.70.184.39. Then use the command **rdesktop -g95% 172.70.184.3** to gain access to the remote desktop connection. 3. Verify discovered credentials s.XXXXXXs::SprXXXXXX3. (obscured to preserve confidentiality)

Mitigation or Resolution Strategy

1. Immediately change the password to the OPNsense dashboard.
2. Implement a strong password policy that requires users to use alphanumeric, uppercase and lowercase characters with a minimum password length greater than 10 characters.
3. Close RDP session on costumes.artstailor.com (10.70.184.39)

4.5 Finding: *Privilege Escalation*

Vulnerability Description

The existing vulnerability allows a malicious party to connect to the RDP session through an exposed standard user. This access allows the actor to use a malicious scanning service to discover know vulnerabilities and create a local administrator account leading to a classic case of privilege escalation. A malicious party can use this escalated privilege to ex-filtrate password hashes stored on the system.

CVSS Base Severity Rating

CVSS Base Severity Rating: 7.8 AV:L AC:L PR:L UI:N S:U C:H I:H A:H

Confirmation method

Verify the passwords discovered through the password spraying attack.

Mitigation or Resolution Strategy

use LAPS (Local Administrator Password Solution) to randomize the local Administrator account password and place a secured backup of it into the computers' active directory account properties. This will prevent users from being able to create local administrator accounts.

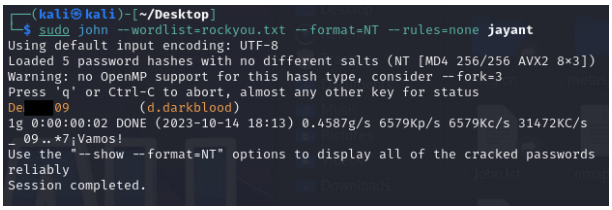

Figure 2: Password Spraying

4.6 Finding: *Password Cracking*

Vulnerability Description

This is a policy based vulnerability where a weak password policy allows users to set common and easy to crack passwords. If the hashes of these passwords can be obtained, they can be used in combination with a password spraying tool to discover weak passwords.

CVSS Base Severity Rating

CVSS Base Severity Rating: 7.7 AV:L AC:H PR:L UI:N S:C C:H I:H A:L

Confirmation method

Verify the redacted user accounts and hashes provided against existing users on the *costumes* computer.

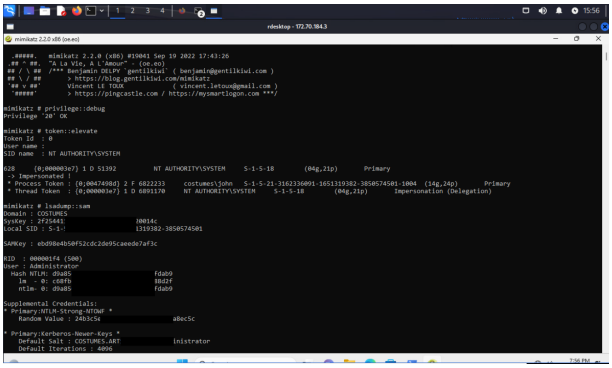

Figure 3: Exfiltrated Hashes (redacted)

Mitigation or Resolution Strategy

The passwords discovered in this and previous instances indicate that art-stailor.com is not enforcing NIST-recommended password security practices.

Specifically, they lack complexity requirements, password aging, and restrictions on common words. Additionally, artstailor.com is not following good Windows-specific practices, such as account lockout policies, a minimum password length, password history, password expiry notifications, and two-factor authentication. To enhance security, artstailor.com should implement NIST-recommended password complexity and aging rules, restrict common words, and adopt Windows-specific practices for account lockouts, longer passwords, password history, password expiry notifications, and consider implementing two-factor authentication.

4.7 Finding: *Service Discovery*

Vulnerability Description

This vulnerability is related to a faulty network configuration allowing a malicious actor access to sensitive and important hosts like devbox.artstailor.com. Via this access, a malicious actor is able to find out information about the technology stack being use by a server. This information can be used to arm future malicious actions.

CVSS Base Severity Rating

CVSS Base Severity Rating: 5.0 AV:N AC:H PR:H UI:N S:U C:L I:H A:N

Confirmation method

This attack vector can be confirmed from us having knowledge of the fact that the server devbox.artstailor.com is running Apache2.4.57 on a Debian OS.

Mitigation or Resolution Strategy

1] Modify server response messages in a way that does not divulge sensitive information like technology stack.
2] Obscure development servers behind a strong firewall to prevent un-authorized external access.

4.8 Finding: *Ease of Access Vulnerability*

Vulnerability Description

This is a known vulnerability where a Windows 10/11 OS fails to handle the ease of access menu on the lock screen. A malicious actor who successfully exploits this vulnerability becomes capable of running commands with a high privilege. This in combination with Brian's modifications make the system vulnerable.

CVSS Base Severity Rating

CVSS Base Severity Rating: 6.8 AV:P AC:L PR:N UI:N S:U C:H I:H A:H

Confirmation method

This attack vector can be confirmed from us having access to the file: C:/Users/l.strauss/Documents/creds from host books.artstailor.com with the following content:

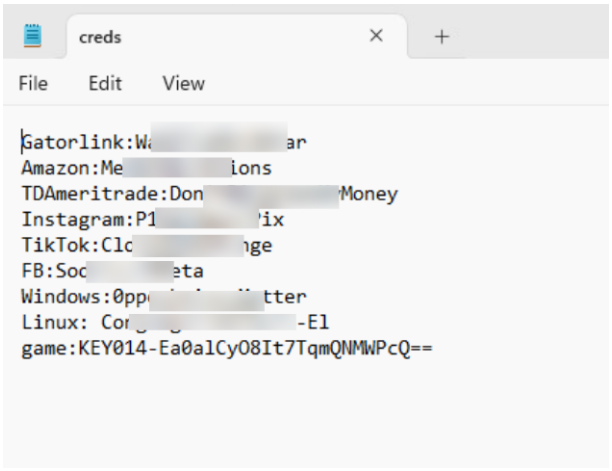

Figure 4: creds

Mitigation or Resolution Strategy

Update the Windows 11 operating system to the latest version including all security updates.

4.9 Finding: *Secret Page*

Vulnerability Description

1. Root level user passwords on a certain development server are exposed and can be used to gain root access to devbox.artstailor.com.
2. An exploitable internet protocol is being used exposing passwords to man in the middle attack.

Confirmation method

1. Capture traffic between devbox.artstailor.com and ceo.artstailor.com to detect encrypted credentials that can be decrypted using base64 decryption.

Severity Rating

CVSS Base Severity Rating: 5.4 AV:A AC:H PR:L UI:N S:U C:H I:L A:N

Mitigation or Resolution Strategy

1. Apply strict password policy and implement a need based authorization policy on devbox.artstailor.com.
2. Discontinue the use of HTTP and replace it with HTTPS across the board. A reasonable way to implement this is to use HSTS (HTTP Strict Transport Security)

4.10 Finding: *Vulnerable Version of Sudo*

Vulnerability Description

This vulnerability exploits a discontinued version of sudo(vulnerable to buffer overflow attack) program to allow a malicious actor to gain root access through a user that does not have root access.

CVSS Base Severity Rating

CVSS Base Severity Rating: 7.8 AV:L AC:L PR:L UI:N S:U C:H I:H A:H

Confirmation method

This vulnerability can be confirmed by running command *sudo -V* in a terminal, if the return output indicates a version number 1.8.27, the vulnerability exists.

Mitigation or Resolution Strategy

Update sudo to the latest version

4.11 Finding: *Spoofing wpad*

Vulnerability Description

This vulnerability allows a malicious actor to manipulate network traffic and trick victims into entering their credentials into an insecure window created by the malicious actions of the actor.

CVSS Base Severity Rating

CVSS Base Severity Rating: 5.4 AV:P AC:L PR:H UI:R S:U C:H I:H A:N

Mitigation or Resolution Strategy

1) Create DNS entry with WPAD that points to the proxy server.
2) Disable "Autocorrect Proxy Settings" on all browsers.

4.12 Vulnerability: *Social Engineering*

Vulnerability Description

This is a user based vulnerability. A user might be enticed into opening web pages that might contain malicious scripts. In this case, we were able to extract an important database admin token that might be used to gain advance database access in the future. This is done using a browser exploitation framework.

CVSS Base Severity Rating

CVSS Base Severity Rating: 8.1 AV:N AC:L PR:N UI:R S:U C:H I:H A:N

Mitigation or Resolution Strategy

1) Implement a server level whitelist that restricts employees from visiting web-pages that are not relevant to the business.
2) Engage employees in training that might better equip them against social engineering attacks.

4.13 Brian's Project: *Missing Input Validation*

Vulnerability Description

Missing server side input validation on uploads made to the website allowing a malicious actor to upload a file of their choice. This is possible because tools like burpsuite can be used to bypass client side input validation and upload non-sanitized data/files. Input validation is, in general, a very important aspect of website design. Input validation must be done on all inputs coming from a client's side and the validation operation must be done on the server side.

Severity Rating

CVSS Base Severity Rating: 9.8 AV:N AC:L PR:N UI:N S:U C:H I:H A:H

Confirmation Method

Use browser debugger to bypass the code block that does the validation. The fact that this can be done is in itself an argument against front end validation.

Mitigation or Resolution Strategy

1) Implement server level input validation.

4.14 Brian's Project: *File Inclusion Vulnerability*

Vulnerability Description

Faulty image display method allows using *raw* parameter with *file* parameter to access any file present in the image directory. This is a vulnerability that can present itself if insecure website development frameworks are used.

Severity Rating

CVSS Base Severity Rating: 8.6 AV:N AC:L PR:N UI:N S:U C:H I:L A:L

Confirmation Method

Visit URL : *http://www.artstailor.com/brian/getimage.php?file=htpasswd&raw=true*. If the file htpasswd is displayed, the vulnerability exists.

Mitigation or Resolution Strategy

Implement website frameworks that are know to be secure.

4.15 Reverse Engineering: *APK*

Vulnerability Description

A simple search in the source code can give a malicious actor information that could threaten the integrity of the application. This is a case of missing code obfuscation and readily available credentials, both of which do not follow good programming practices.

Severity Rating

CVSS Base Severity Rating: 8.2 AV:N AC:L PR:N UI:N S:U C:H I:L A:N

Confirmation Method

Search for the string *username* in the source code file *com/example.artstailornews/ItemListActivity*.

Mitigation or Resolution Strategy

1) Remove the hosted .apk file from the website and route user installs through the app store(host your app on the app store).
2) Implement code obfuscation to prevent string searches.
3) Stop hard-coding credentials and start storing credentials in encrypted format in a configuration file. Maintain end to end encryption of a high encryption standard.

5 Recommendation Summary

The penetration test on Artstailor.com has unveiled critical vulnerabilities across various facets of the infrastructure. To address the risk posed by accessible hosts, Artstailor.com should promptly deploy a content delivery network (CDN) for masking server IP addresses, implement proxy servers to fortify security, and obscure server names to impede unauthorized discovery. Simultaneously, the outdated vsftpd software needs immediate attention, mandating an urgent update to mitigate the potential exploitation of file access vulnerabilities. These proactive measures will significantly enhance the security posture of Artstailor.com against external threats.

In tandem with securing network exposure, the report underscores the pivotal role of robust password policies in safeguarding against password-related vulnerabilities. Artstailor.com must enforce stringent password requirements, including alphanumeric characters, uppercase and lowercase letters, and a minimum length. This comprehensive strategy aims to counteract vulnerabilities such as password cracking, privilege escalation, and RDP exploits. By implementing two-factor authentication and regularly updating critical software components like sudo, the organization can build a robust defense against evolving security threats.

Moreover, the mitigation and resolution strategies extend to user education and secure coding practices. Artstailor.com should prioritize user training programs to mitigate social engineering risks, fostering awareness and resilience among employees. Simultaneously, secure coding practices, encompassing server-side input validation, prevention of file inclusion vulnerabilities, and code obfuscation, are imperative to fortify the website against potential exploitation. By adopting these multifaceted strategies, Artstailor.com can establish a resilient security framework, minimizing vulnerabilities and ensuring a more secure digital environment.

6 Strategic Roadmap

Crafting a strategic road-map to address the fifteen identified findings requires a systematic and prioritized approach. Commencing with vulnerabilities as-

signed the highest Common Vulnerability Scoring System (CVSS) ratings, the resolution plan should focus on accessible hosts, necessitating the implementation of a content delivery network (CDN) and proxy servers, along with renaming servers for enhanced security. Concurrently, addressing the outdated vsftpd software involves an immediate update to eliminate potential file access vulnerabilities. The ”Brian’s Service” vulnerability requires the immediate blocking of port 1337 and the adoption of more secure string comparison methods, while resolving the RDP vulnerability entails changing the OPNsense dashboard password and implementing a robust password policy.

Simultaneously, attention must be directed towards mitigating privilege escalation vulnerabilities by implementing Local Administrator Password Solution (LAPS) and monitoring changes in valid commands. Resolving the password cracking issue involves enforcing NIST-recommended password security practices, while the ”Service Discovery” vulnerability necessitates modifying server response messages and securing development servers behind a robust firewall. Addressing the ”Ease of Access Vulnerability” involves updating the Windows 11 operating system, and the ”Secret Page” vulnerability requires the implementation of strict password policies and transitioning from HTTP to HTTPS. A targeted approach to the ”Vulnerable Version of Sudo” involves updating the sudo software to the latest version, while the ”Spoofing wpad” vulnerability requires creating a DNS entry pointing to the proxy server and disabling ”Auto-correct Proxy Settings” on all browsers. The strategic roadmap, tailored to each vulnerability’s unique mitigation strategy, ensures a methodical resolution plan for bolstering Artstailor.com’s cybersecurity resilience.