Spicy IT

We Take The Heat

Security Assessment Report

ABCSoft Internal Network Security Assessment

Title	ABCSoft Internal Network Security Assessment Rep
Version	1.0
Reporting Date	October 27, 2022
Prepared by	Spicy IT
Prepared for	ABC Soft
Contact	Razvan Furdui, Cyber Operations Manager
Classification	Restricted

Spicy IT
We Take The Heat

Table of Contents

1. Document Control

Revision History

Version	Date	Author	Change Description
0.1	October 11, 2022	Cyber Security Team	Initial Draft
0.2	October 26, 2022	Cyber Security Team	Findings Added
0.3	October 27, 2022	Cyber Security Team	Technical Review & Quality Control
0.4	October 27, 2022	Content Writer	Content review and Corporate styling
1.0	October 27, 2022	Quality Control Manager	Final review & Deliver to the client

Confidentiality

All information contained in this document is provided in confidence for the sole purpose of adjudication of the document and shall not be published or disclosed wholly or in part to any other party without **Spicy IT Pty Ltd** or **ABC Soft** prior permission and shall be held in safe custody. These obligations shall not apply to information that is published or becomes known legitimately from some source other than Spicy IT Pty Ltd.

All transactions are subject to the appropriate Spicy IT Pty Ltd Standard Terms and Conditions.

Legal name: SPICY IT PTY LTD	
ABN: 72 657 952 219	
Email: info@spicyit.net	**Website**: spicyit.net

Independent Security Assessment Report

Spicy IT Pty Ltd LTD ("Spicy IT Pty Ltd") has performed the Internal Network Security Assessment for ABC Soft, ("Client") while acting as an independent security assessor. This assessment was performed with the intent of evaluating security, and resiliency of Client's ABCSoft IT systems.

The methodology utilized during this assessment is detailed in Methodology. Spicy IT Pty Ltd developed this methodology based on extensive professional experience and information system security assessment best practices gathered from the NIST Risk Management Framework, Open Source Security Testing Methodology Manual ("OSSTMM"), the National Institute of Standards and Technology ("NIST") Special Publication 800-115: Technical Guide to Information Security Testing and Assessment, the Penetration Testing Execution Standard ("PTES"), NIST Guide Details Forensic Practices, various CIS Benchmarks, and the Open Web Application Security Project ("OWASP") Testing Guide.

While this type of assessment is intended to mimic a real-world attack scenario or identify the capacity of the existing controls, Spicy IT Pty Ltd is bound by rules-of-engagement, defined scope, allocated time, and additional related constraints. Spicy IT Pty Ltd has made every effort to perform a thorough and comprehensive analysis and to provide appropriate remedial advice. However, inherit limitations, errors, misrepresentations, and changes to the Client environment may have prevented Spicy IT Pty Ltd from identifying every security issue that was present in the Client environment at the time of testing. Therefore, the findings included in this report should be considered to be representative of what a similarly skilled attacker could achieve with comparable resources, constraints, and time frame.

Additionally, it is worth emphasizing that the findings and remediation recommendations are the result of a point-in-time assessment based on the state of the Client environment as of October 26, 2022. Spicy IT Pty Ltd therefore does not provide any assurance related to configuration or control modifications in the Client environment, changes in regulatory or compliance requirements, discoveries of new vulnerabilities and attack techniques, or any other future event that may impact the Client's security posture.

The information contained in this report represents a fair and unbiased assessment of the Client's environment based on the agreed upon criteria as defined in the Statement of Work. This report is provided to the Client as notification of outstanding security risks that threaten the confidentiality, integrity, and availability of sensitive information, as well as to provide assistance and direction with remediation. The evidence and references provided for each finding serve as the basis for our qualified opinions in this report.

Spicy IT Pty Ltd has provided this report solely for private and internal use by the Client, and it may not be shared or redistributed without Spicy IT Pty Ltd's express written consent. Spicy IT Pty Ltd's assessments focus exclusively on information security and the conclusions arrived at in this report should not be considered to be a representation or endorsement of the Client's products or services.

Razvan Furdui

Cyber Operations Manager

Spicy IT Pty Ltd, LTD

2. Management Summary

This report details the findings of the ABCSoft Internal Network Security Assessment carried out between October 11, 2022 and October 26, 2022.

The most important objective of the assessment was to determine whether and how a malicious user can gain unauthorized access to assets that affect the fundamental security of the system, files and data, and confirm that the applicable controls required by ABC Soft are in place.

The security team has conducted the assessment based on the Internal Network Security Assessment methodology.

The following issues are evaluated as Critical or High risks and require immediate attention and remediation:

- Active Directory: ADCS misconfiguration leads to domain compromise
- Application is vulnerable to SQL Injection
- Active Directory multiple domain misconfigurations
- MSSQL Server misconfiguration can lead to Remote Code Execution

Spicy IT Pty Ltd identified numerous Low-to-Medium risk issues that address failures to adhere to established security best practices. In some cases, these vulnerabilities increase the attack surface of the assets and may make the exploitation of other weaknesses easier. These findings should be addressed in turn and as time permits.

The security team recommends that the client should conduct a session for planning the remediation of the identified risks, starting with the most important findings.

As a result of conducting this engagement, Spicy IT Pty Ltd has determined that cumulatively the issues identified pose a High risk to ABC Soft. This evaluation was determined by assessing the severity and number of issues identified throughout the environment as well as Spicy IT Pty Ltd's experience in assessing similar systems.

The overall risk can be lowered by remediating the vulnerabilities detailed in the following chapters.

3. Scope of Work

Background Information

Spicy IT performed Internal Network Security Assessment to assess the risk that a real life, targeted attacker poses to the security and integrity of the ABC Soft ABCSoft. Understanding the current vulnerabilities is the first step in remediating and ultimately enhancing ABC Soft's overall security maturity.

The purpose of the assignment was to identify and evaluate any risks or potential issues that could impact Confidentiality, Integrity or Availability of the systems in scope. In this assessment, both automated and manual security testing techniques were used in order to identify weakness in the systems in scope from an attacker's perspective.

Scope Overview

The scope of the assessment included the following assets as authorized by the ABC Soft:

```
https://sample.report
192.168.0.0/24
```

Assessment type: Internal Network Security Assessment

Assessment method: Gray Box

Environment: Staging

Timeframe

The Internal Network Security Assessment was performed in the dates between **October 11, 2022** and **October 26, 2022.**

Objectives

The objective of this assignment is to help ABC Soft strengthen the security posture against cyber threats.

Securing vulnerabilities and reducing risks within the systems will lead to a drastic reduction in the likelihood of:

- Exploitation of publicly available exploits through lack of patching;
- Financial loss through regulatory penalties;
- Disruption of availability through a lack of rate-limiting techniques;
- Breach of integrity through weak authorization checks;
- Systems compromise, data alteration or data destruction attacks;
- Information theft through poor or non-existent cryptographic controls;
- Reputational loss through exploitation of any of the above vulnerabilities.

Limitations

Denial-of-Service (DoS) testing was not performed during this engagement.

This was a time-boxed security assessment. During a time-boxed engagement, the Cyber Security Team prioritizes assessment of the most sensitive portions and functions of the systems in scope.

No other specific limitations were defined in the scoping phase by the client.

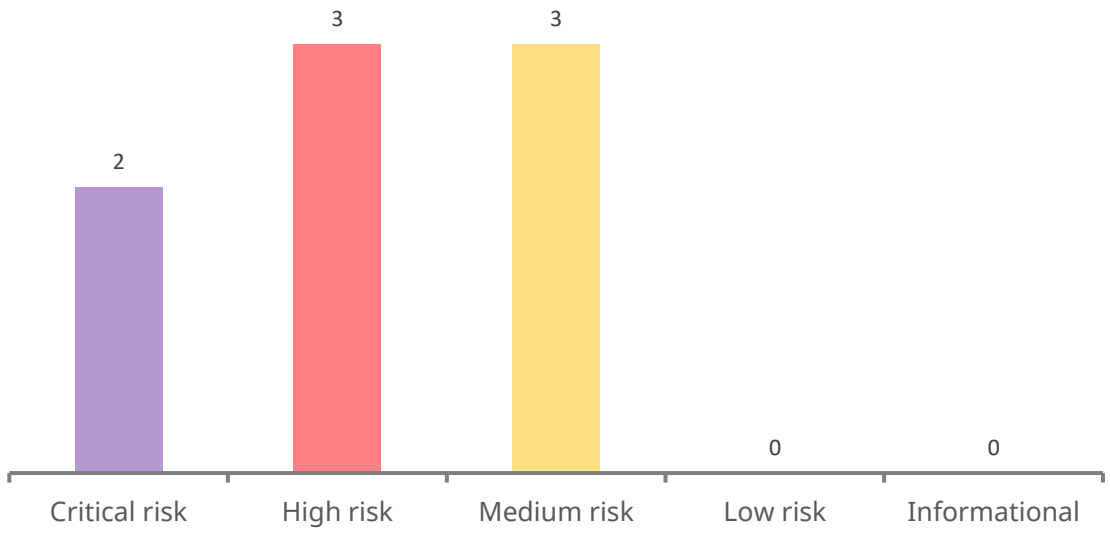
4. Summary of Findings

Using automated and manual techniques, Spicy IT identified a total of **6** findings within **ABCSoft** environment. These weaknesses threaten the confidentiality, integrity, and availability of the application, the environment, and the data contained within it.

Risk Breakdown

The following table summarizes the quantity and severity of the findings identified during this assessment:

Residual Risk Severity	Total
Critical	1
High	3
Medium	2
Low	0
Informational	0
Total	**6**



Category Breakdown

The table below contains a list of areas where vulnerabilities have been identified. The vulnerability categories are defined following the **Common Weakness and Enumeration (CWE)** database.

Vulnerability Categories	Total
Injection	**1**
Security Misconfiguration	**3**
Missing Authorization	**1**
Denial of Service	**1**

Component Breakdown

The table below contains a list of affected components where vulnerabilities have been identified.

Vulnerability Categories	Total
Application	**3**
Server	**1**
Network	**2**

Table of Vulnerabilities

For each finding, Spicy IT uses a composite risk score that takes into account the severity of the risk, application's exposure, technical difficulty of exploitation, and other factors. For an explanation of Spicy IT's risk rating and vulnerability categorization, see the Methodology section.

The table below lists the vulnerabilities identified during the assessment:

Residual Risk	CIA Impact	Title	Identifier
Critical	C I A	Active Directory: ADCS misconfiguration leads to domain compromise	ABC-1
High	C I A	Application is vulnerable to SQL Injection	ABC-0
High	C I A	Active Directory multiple domain misconfigurations	ABC-2
High	C I A	MSSQL Server misconfiguration can lead to Remote Code Execution	ABC-3
Medium	C I A	Chargen UDP Service Remote DoS	ABC-4
Medium	C I A	LDAP anonymous binds are enabled	ABC-5

5. Vulnerability Details

V1. Active Directory: ADCS misconfiguration leads to domain compromise

Affected Entity	**ABCSoft**	**Identifier**	ABC-1
Risk Statement	An attacker could impersonate a high privileged user and compromise the entire active directory domain.		
Affected Component	Application	**Identified Controls**	None Identified
Residual Risk	**Critical**	**CVSS Score**	**9.9**
Classification	Security Misconfiguration	**Likelihood**	High
CVSSv3 code	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H		
Location	• local.domain.controller		

Description

Active Directory Certificate Service is a Server Role that enables a company to construct public key infrastructure (PKI) and use open key cryptography and computerized authentication in their infrastructure. AD CS is an identity technology in Windows Server that allows you to implement PKI for your organization.

PKI is the combination of software, encryption technologies, processes, and services that enables an organization to secure its data, communications, and business transactions. PKI relies on the exchange of digital certificates between authenticated users and trusted resources.

Reproduction Steps

The following steps can be used for validation and remediation verification:

- On a domain-joined machine, download and compile the Certify binary (resource found in references)
- Issue the following command to check whether there are vulnerable templates

```
.\Certify.exe find /vulnerable
```

- If there is a certificate template, issue the following command to request a certificate, supplying an alternative name (user to impersonate)

```
.\Certify.exe request /ca:[CA-NAME] /template:[TEMPLATE] /altname:Administrator
```

- Copy the output into a file, transfer it to a Linux machine and issue the following command (to convert it to a .pfx format)

```
openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic
Provider v1.0" -export -out cert.pfx
```

- Using Rubeus, ask for a **tgt** (ticket-granting ticket) and then inject the ticket into memory

```
.\Rubeus.exe asktgt /user:Administrator /certificate:C:\Temp\cert.pfx
```

Impact	An internal attacker enumerating and finding a vulnerable ADCS certificate template, could request a certificate used for client authentication and impersonate a sensitive user (Administrator). Afterward, they could impersonate that user when interacting with the active directory resources, hence they could install several persistence mechanisms and compromise all AD Users and resources.

The following evidence has been gathered to illustrate this vulnerability.

AD misconfiguration

Request

```
N/A
```

Response

```
N/A
```

Recommendations	**Remediation Difficulty**	**Moderate**

Review the Active Directory Certificate Service Certificate Templates for the permissions set (Enrollment, AutoEnrollment, Owner, WriteOwner, WriteDACL, WriteProperty). For templates that require the **ENROLLEE_SUPPLIES_SUBJECT** flag to be allowed, configure the **Authorized Signatures Required** to at least 1.

A combination of ENROLLEE_SUPPLIES_SUBJECT, PKIExtendedUsage = Client Authentication, and Authorized Signatures Required = 0 could allow a user to compromise the Active Directory Domain. Review the Certificate templates for these specific dangerous combinations.

Recommended Reading:

https://github.com/GhostPack/PSPKIAudit

https://github.com/GhostPack/Certify

https://posts.specterops.io/certified-pre-owned-d95910965cd2

https://specterops.io/assets/resources/Certified_Pre-Owned.pdf

V2. Application is vulnerable to SQL Injection

Affected Entity	**ABCSoft**	**Identifier**	ABC-0
Risk Statement	A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information.		
Affected Component	Application	**Identified Controls**	None Identified
Residual Risk	**High**	**CVSS Score**	**7.2**
Classification	Injection	**Likelihood**	High
CVSSv3 code	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N		
Location	local.sqldatabase/?id=12312		
Description	The application constructs an SQL command using externally-influenced input from the application, but it does not neutralize special elements that could modify the intended SQL command when it is sent to the database component. SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior. Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including the execution of system commands. There are a wide variety of SQL injection vulnerabilities, attacks, and techniques, which arise in different situations. Some common SQL injection attacks include Classic SQLI, Blind or Inference SQL injection, Database management system-specific SQLI. **Reproduction Steps** The following steps can be used for validation and remediation verification: • Submit the single quote character (') and look for errors or other anomalies. • Submit some SQL-specific syntax • Submit Boolean conditions such as OR 1=1 and OR 1=2 and look for differences in the application's responses.		
Impact	An attacker can escalate the attack to compromise the underlying server or other back-end infrastructure or perform a denial-of-service attack. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.		

The following evidence has been gathered to illustrate this vulnerability.

SQL Injection vulnerability

Database exfiltration

Request

```
N/A
```

Response

```
N/A
```

Recommendations	**Remediation Difficulty**	**Moderate**
	Most instances of SQL injection can be prevented by using parameterized queries (also known as prepared statements) instead of string concatenation within the query. With most development platforms, parameterized statements that work with parameters can be used (sometimes called placeholders or bind variables) instead of embedding user input in the statement. A placeholder can only store a value of the given type and not an arbitrary SQL fragment. Hence the SQL injection would simply be treated as a strange (and probably invalid) parameter value.	

	Parameterized queries can be used for any situation where untrusted input appears as data within the query, including the WHERE clause and values in an INSERT or UPDATE statement. They can't be used to handle untrusted input in other parts of the query, such as table or column names, or the ORDER BY clause. Application functionality that places untrusted data into those parts of the query will need to take a different approach, such as white-listing permitted input values, or using different logic to deliver the required behavior. For a parameterized query to be effective in preventing SQL injection, the string that is used in the query must always be a hard-coded constant, and must never contain any variable data from any origin. Do not be tempted to decide case-by-case whether an item of data is trusted, and continue using string concatenation within the query for cases that are considered safe. It is all too easy to make mistakes about the possible origin of data, or for changes in other code to violate assumptions about what data is tainted. **Recommended Reading:** https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet https://portswigger.net/web-security/sql-injection https://cwe.mitre.org/data/definitions/89.html

V3. Active Directory multiple domain misconfigurations

Affected Entity	**ABCSoft**	**Identifier**	ABC-2
Risk Statement	Combined these misconfigurations may help an internal attacker in the process of taking over the entire network		
Affected Component	Network	**Identified Controls**	None Identified
Residual Risk	**High**	**CVSS Score**	**8.0**
Classification	Security Misconfiguration	**Likelihood**	Low
CVSSv3 code	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H		
Location	• local.dc		
Description	The security team observed that the internal domain has several misconfigurations and is missing certain hardening features Microsoft is providing. **Missing features** • LAPS not configured • SMB v1 enabled on 5 DCs • Multiple systems with outdated/obsolete OS (Windows XP/7) • User accounts with passwords set to never expire • Service accounts in the Domain Admin group • Users with passwords older than 3 years • The spooler service is remotely accessible on the Domain Controllers (misconfiguration which could lead to privilege escalation to Domain Controller) • No GPO has been found which disables LLMNR or at least one GPO does enable it explicitly • Domain Controllers not configured to have SMB signing • GPOs contain passwords that can be decrypted (vulnerable to MS14-025) **Reproduction Steps** The following steps can be used for validation and remediation verification: • Using the ADModule, check if LAPS is installed : Get-ADObject 'CN=ms-mcs-admpwd,CN=Schema,CN=Configuration,DC=[name],DC=[name]' • Using the ADModule, check if there are objects that can have empty passwords: Get-ADUser -Properties Name,distinguishedname,useraccountcontrol,objectClass -LDAPFilter "(&(userAccountControl:1.2.840.113556.1.4.803:=32)(!(IsCriticalSystemObject=TRUE)))" -Server [server] | select SamAccountName • Using nmap, check if SMBv1 is enabled : nmap -p 445 --script smb-security-mode [host] • Check if the spool service is running on the remote host: ls \\dc01\pipe\spoolss • From an authenticated console (cmd), run the following command and see if the access is denied or not: .\NetSess.exe [servername]		

Impact	• The missing LAPS module could mean that Domain Administrators are reusing passwords for the local Administrator on different machines in the domain • An attacker which compromises an account (user or machine account) with Delegation enabled, can elevate privileges to Domain Admin/Enterprise Admin • An attacker could use a network sniffer and get the NetNTLM hashes of users in the domain. Moreover, it could replay them to other servers and gain access if the owner of the hash replayed is a local administrator on the machine. • An attacker could relay the NTLM hashes used in the network and gain remote code execution on sensitive servers, such as Domain Controllers. • In case a Domain Admin user has their password leaked and it was not changed every 90 days, an attacker could have persistence in the domain/network. • In case the service that is run with a service account in the Domain Admins group is compromised, an attacker could elevate their privileges to Domain and Enterprise Admin. • Print Spooler has been known to have several vulnerabilities found. In the recent one (CVE-2021-34527), an attacker could execute remote code on systems (in this case on DCs)

The following evidence has been gathered to illustrate this vulnerability.

Multiple AD misconfigurations

Request

```
N/A
```

Response

```
N/A
```

Recommendations	**Remediation Difficulty**	**Moderate**
	• Domain Controllers and AD admin systems need to have the Print Spooler service disabled. The US DoD STIG security guidance has had this recommendation in place for many years. The best way to do this is via GPO • Remove unconstrained delegation from accounts and replace it with constrained delegation (Domain Controllers have unconstrained delegation enabled by default)	

- For net session enumeration:
  - Run the NetCease PowerShell script on a reference workstation.
  - Open the Group Policy Management Console. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click Edit.
  - In the console tree under Computer Configuration, expand the Preferences folder, and then expand the Windows Settings folder.
  - Right-click the Registry node, point to New, and select Registry Wizard.
  - Select the reference workstation on which the desired registry settings exist, then click Next.
  - Browse to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\and select the check box for "SrvsvcSessionInfo" from which you want to create a Registry preference item. Select the check box for a key only if you want to create a Registry item for the key rather than for a value within the key.
  - Click Finish. The settings that you selected appear as preference items in the Registry Wizard Values collection.

Recommended Reading:

https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/

https://www.veeam.com/blog/microsoft-laps-deployment-configuration-troubleshoot-guide.html

https://support.microsoft.com/en-us/topic/microsoft-security-advisory-local-administrator-password-solution-laps-now-available-may-1-2015-404369c3-ea1e-80ff-1e14-5caafb832f53

https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn408187(v=ws.11)?redirectedfrom=MSDN

https://github.com/p0w3rsh3ll/NetCease

https://adsecurity.org/?p=3299

https://dirteam.com/sander/2014/05/23/security-thoughts-passwords-in-group-policy-preferences-cve-2014-1812/

V4. MSSQL Server misconfiguration can lead to Remote Code Execution

Affected Entity	**ABCSoft**	**Identifier**	ABC-3
Risk Statement	An attacker might be able to compromise the database server		
Affected Component	Server	**Identified Controls**	None Identified
Residual Risk	**High**	**CVSS Score**	**7.5**
Classification	Security Misconfiguration	**Likelihood**	High
CVSSv3 code	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		
Location	• 10.10.10.10 • Port: 5443		

Description	The SQL server has configured one or more database links with other databases.
	
	The security team managed to get a set of credentials for one of the SQL servers in the domain, which had configured a DB link with another SQL server. The low privileged user from the 1st database had System Administrator privileges (sa) on the 2nd database.
	
	Reproduction Steps
	
	The following steps can be used for validation and remediation verification:
	
	• Using a tool such as PowerUpSQL, issue the following command to check if the server has configured links. Check if the current user is a system administrator (**SysAdmin)** on the remote MSSQL server
	
	`Get-SQLServerLinkCrawl -instance [instance]`
	
	• Using a tool such as HeidiSQL, log in to the instance and run the following query:
	
	`SELECT * FROM OPENQUERY("[ip]",'Select @@version')`
	
	• Enable RPC OUT, RPC and XP_CMDSHELL
	• Run the OS commands using the same command as below		

Impact	An attacker could enable all features needed (RPC out, RPC, xp_cmdshell) on the remote MSSQL server and then run OS commands as the service account running the SQL service, through the MSSQL DB link. Compromising the database will provide access to sensitive data within it.		
The following evidence has been gathered to illustrate this vulnerability.			

Remote Code Execution in MSSQL

Request

```
N/A
```

Response

```
N/A
```

Recommendations	**Remediation Difficulty**	**Moderate**
	Database links must be carefully managed to ensure security, especially public database links. If you do not need database links, remove them all. All the database links should be configured with the least privilege; restrict access to those databases/tables that are really needed. **Recommended Reading:** https://docs.microsoft.com/en-us/sql/relational-databases/security/sql-vulnerability-assessment?view=sql-server-ver15 https://www.upguard.com/blog/11-steps-to-secure-sql https://blog.quest.com/13-sql-server-security-best-practices/ https://docs.microsoft.com/en-us/sql/relational-databases/security/securing-sql-server?view=sql-server-ver15	

V5. Chargen UDP Service Remote DoS

Affected Entity	**ABCSoft**	**Identifier**	ABC-4
Risk Statement	An internal attacker could use the service to consume resources from the server and make it unresponsive for other users.		
Affected Component	Application	**Identified Controls**	None Identified
Residual Risk	**Medium**	**CVSS Score**	**5.3**
Classification	Denial of Service	**Likelihood**	Low
CVSSv3 code	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L		
Location	• UDP: 192.169.2.2		
Description	The Character Generator Protocol (CHARGEN) is a service of the Internet Protocol Suite. It is intended for testing, debugging, and measurement purposes. The protocol is rarely used, as its design flaws allow ready misuse. When contacted, chargen responds with some random characters (something like all the characters in the alphabet in a row). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection. The purpose of this service was to mostly test the TCP/IP protocol by itself, to make sure that all the packets were arriving at their destination unaltered. It is unused these days, so it is suggested you disable it, as an attacker may use it to set up an attack against this host, or against a third-party host using this host as a relay. An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network. **Reproduction Steps** The following steps can be used for validation and remediation verification: • Using a tool such as Nmap, issue the following command and check if the service is accessible `nmpa -p 19 -sV -sC [host]`		
Impact	An attacker can use the Chargen server to multiply the size of a DDoS by 358 times. UDP CHARGEN is commonly used in denial-of-service attacks. By using a fake source address the attacker can send bounce traffic off a UDP CHARGEN application to the victim. UDP CHARGEN sends 200 to 1,000 times more data than it receives, depending upon the implementation. This "traffic multiplication" is also attractive to an attacker because it obscures the attacker's IP address from the victim.		
The following evidence has been gathered to illustrate this vulnerability.			

DOS to Chargen

Request

```
N/A
```

Response

```
N/A
```

Recommendations	**Remediation Difficulty**	**Easy**

Block UDP port 19 and/or disable Chargen:

- Under Unix systems, comment out the 'chargen' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

```
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen
```

Then launch cmd.exe and type :

```
net stop simptcp net start simptcp
```

To restart the service.

Recommended Reading:

http://www.nessus.org/u?f0dbdf05

cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0103

V6. LDAP anonymous binds are enabled

Affected Entity	**ABCSoft**	**Identifier**	ABC-5
Risk Statement	An attacker can anonymously access information from the LDAP directory		
Affected Component	Network	**Identified Controls**	None Identified
Residual Risk	**Medium**	**CVSS Score**	**5.5**
Classification	Missing Authorization	**Likelihood**	Medium
CVSSv3 code	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L		
Location	• ldap connection		
Description	The remote LDAP server allows anonymous binds. Bind operations are used to authenticate clients (and the users or applications behind them) to the directory server, establish an authorization identity that will be used for subsequent operations processed on that connection, and specify the LDAP protocol version that the client will use. Anonymous binding allows a client to connect and search the directory (bind and search) without logging in because binddn and bindpasswd are not needed. An anonymous simple bind can be performed by providing empty strings as the bind DN and password. **Reproduction Steps** The following steps can be used for validation and remediation verification: • Verify LDAP configuration and observe if it accepts Anonymous binding		
Impact	Unauthorized Information leak: Anyone that can bind to the server can gain SOME level of information access (depends on permissions) Denial of Service: Such as overloading the server with requests once the anonymous connection is established. One could argue that issuing anonymous requests, even if they failed, could be used to perform the same basic denial of service, so this would not be an increased risk due to allowing anonymous binds The potential exploit of bugs: When/if there is a vulnerability in one of the underlying API calls to the AD server once a user has authenticated. Thus a user that would not have the authorization to make a certain call to the AD server as an unauthenticated user, could make the call, and exploit the vulnerability. For example, let's say the fictitious AD_Run_Object call was vulnerable to a buffer overflow. An unauthenticated user trying to make the call would be denied access to the call since they had not authenticated first. However, an anonymous bind would allow the attacker to make the AD_Run_Object call, and exploit the vulnerability.		
The following evidence has been gathered to illustrate this vulnerability.			

Anonymous binds from LDAP

Request

```
N/A
```

Response

```
N/A
```

Recommendations	**Remediation Difficulty**	**Moderate**

If you are not using this service, it is recommended to disable it.

While it is preferable that applications using LDAP authentication explicitly check for empty passwords, it is possible to disable LDAP unauthenticated binds starting from Windows Server 2019. The following PowerShell code snippet is sufficient to make the necessary modification:

```
$RootDSE = Get-ADRootDSE
$ObjectPath = 'CN=Directory Service,CN=Windows NT,CN=Services,{0}' -f
$RootDSE.ConfigurationNamingContext
Set-ADObject -Identity $ObjectPath -Add @{ 'msDS-Other-Settings' =
'DenyUnauthenticatedBind=1' }
```

Recommended Reading:

http://osvdb.org/9723

https://www.owasp.org/index.php/LDAP_injection

http://tools.ietf.org/html/rfc2251

6. Methodology

Overview

Security assessment involves looking for problems on the information systems being tested that may allow a malicious attacker to perform unwanted or undesirable actions. Information systems are comprised of a number of different software and hardware components. Errors in the configuration or programming of these components may create vulnerabilities, or potential weaknesses, that may allow an opportunity for an attacker to perform a malicious action. Different vulnerabilities require different levels of access or skill to be successfully used in a malicious way.

Spicy IT follows a highly structured methodology to ensure a thorough assessment of the system in scope and its environment is conducted. Our methodology uses a phased approach, consisting of information gathering, investigation, assessment, verification, and notification. Spicy IT employs a comprehensive and careful methodology in order to identify any potentially dangerous functionality. Prior to performing assessment against these functions, Spicy IT shares any potential impacts with the client. These steps ensure the least amount of business impact possible.

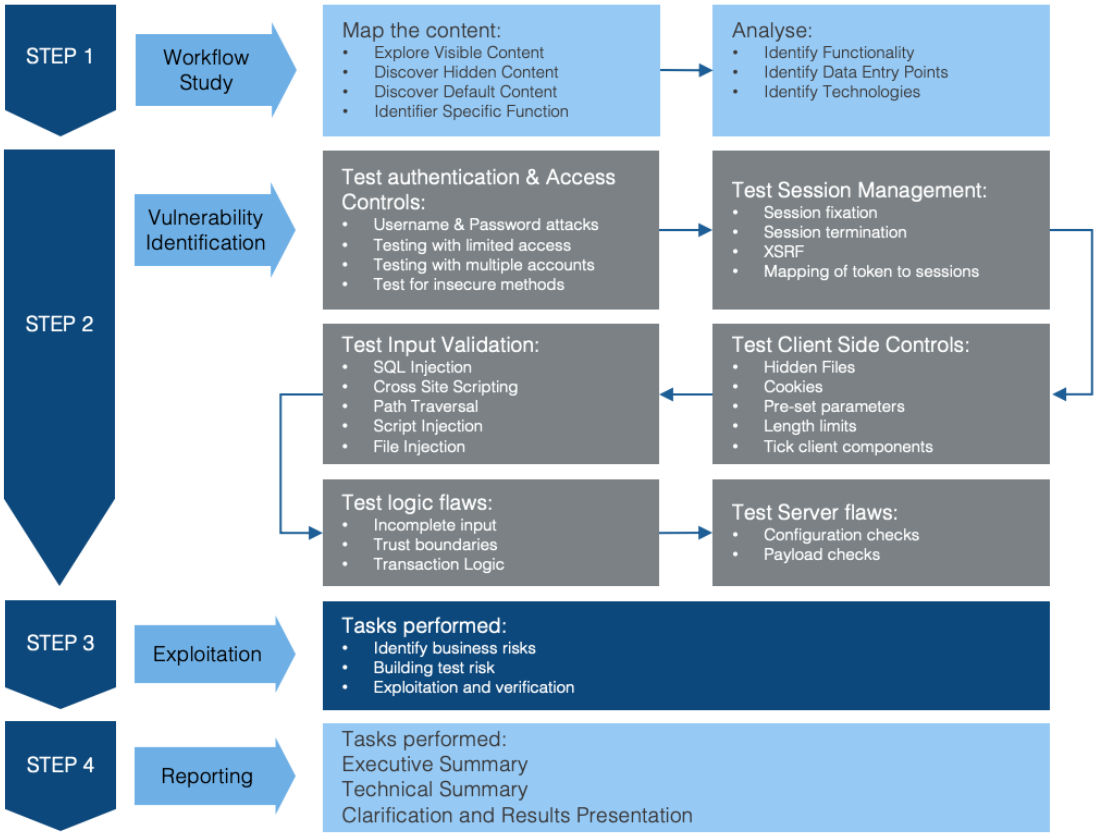
The Spicy IT Team will discuss a plan of attack as well as any potential concerns, and then will seek explicit approval from the client in order to proceed with the exploitation of any vulnerabilities that have the potential to impact production operations. The Spicy IT Team will communicate all verified vulnerabilities identified throughout the engagement that present significant danger to the client's organization. This will allow the client to begin planning remediation activities sooner, potentially closing the window on further exploitation by an attacker prior to the delivery of the final report.

Spicy IT follows industry best practice standards and methodologies when performing security-assessment activities. Such methodologies include:

- Open Source Security Testing Methodology Manual (OSSTMM)
- Penetration Testing Execution Standard (PTES)
- Open Web Application Security Project (OWASP) Testing Guide
- The National Institute of Standards and Technology (NIST)
- PCI Data Security Standard Penetration Testing Guidance (PCI DSS)
- The Intelligence Lifecycle & F3EAD Cycle (Threat Intelligence)
- OWASP Mobile Security Testing Guide (MSTG)
- Penetration Testing Framework for IoT (PTFIoT)
- PCI DSS ATM Security Guidelines
- CIS Cloud Foundations Benchmark Standard
- OWASP Code Review Guide
- Threat Intelligence Based Ethical Red Teaming Framework (TIBER-EU)
- Application Security and Development Security Technical Implementation Guide
- Social Engineering Attack Framework and Toolkit (SET)
- Digital Forensics Framework (DFF)
- Incident Response Framework (NIST)
- Secure Controls Framework (SCF)
- CREST Penetration Testing Guide
- CSA STAR Self-Assessment / CAIQ
- CIS Secure Platforms Benchmarks (CIS Security)
- Application Security Verification Standard (ASVS)

Internal Network Security Assessment Methodology

The methodology employed during an Internal Network Security Assessment involves the following stages:



The steps are aligned to the in-depth security concepts and are focused on process and technical security controls and their implementation in the various phases of the project delivery. The results provided for each activity will include a detailed and comprehensive assessment of client's current security posture, expansive recommendations, and tools and knowledge to facilitate the continuous improvement.

Intelligence Gathering & Workflow Study

Conduct passive and active information gathering to determine the level of information that can be found about the assets in scope. These actions are conducted in order to understand what level of exposure the assets have, and how an attacker can use this information to conduct further attacks.

Vulnerability Assessment & Identification

Security Engineers investigate for vulnerabilities through manual searches complemented by automated tools. The objective is to discover as many vulnerabilities as possible on the target.

Exploitation

The exploitation phase consists in testing possible exploitations of the flaws identified in the previous phase. This step allows using certain flaws as "pivots", in order to discover new vulnerabilities. The exploitation of security vulnerabilities allows evaluating their real impact and thus their criticality level.

Reporting

The Report will communicate to the reader the specific goals of the Penetration Test and technical details of findings of the assessment exercise. The intended audience will be those who are in charge of the oversight and strategic vision of the security program as well as any members of the organization, which may be impacted by the identified/confirmed threats.

Spicy IT security checklist includes, but is not limited to, identification of the following risks:

Application Profiling and Information Disclosure	Platform and Third-Party Misconfiguration	Cookie and Session Handling
▪ Default Banners ▪ Unhandled Error Conditions ▪ HTML/JavaScript Comment Information Leakage ▪ Extraneous Content in Web Root ▪ Source Code Disclosure ▪ Robots.txt Path Disclosure ▪ Content Expiration and Cache Control ▪ Bit Bug/Referrer Header Leakage ▪ Account Enumeration ▪ Backup/Archive Content	▪ Default Administrative Credentials ▪ Default Content and Scripts ▪ Application Script Engine ▪ Web Server ▪ Weak SSL Implementation ▪ Flawed Use of Cryptography	▪ Session Fixation/Hijacking ▪ Set-Cookie Weaknesses ▪ Sensitive Information Disclosure ▪ Cookie Poisoning ▪ Multiple Simultaneous Login Allowed ▪ Session Timeout ▪ Explicit/Implicit Logout Failures ▪ Cookie less Sessions ▪ Custom Session Management

Command Injection Flaws	Logic Flaws	Client-Side Flaws
▪ SQL Injection ▪ XXE, XPath, and XML Injection ▪ SSI/OS Command Injection ▪ Server Script Injection/Upload ▪ Cross-Site Scripting (XSS) ▪ Buffer Overflow	▪ Privilege Escalation ▪ Sensitive Information Disclosure ▪ Data Mining/Inference ▪ Functional Bugs ▪ Application-Specific Control Failures ▪ Cross-Site Tracing (XST) ▪ Weak Data Validation ▪ Race Conditions ▪ CPU-Intensive Functions	▪ Exposure of Sensitive Business ▪ Logic ▪ Reliance on Client-Side Validation ▪ AJAX/Web Service Flaws ▪ Java Applet/ActiveX ▪ Control/Flash Weaknesses

Authentication and Authorization
▪ Unauthenticated Sensitive Content ▪ Poor Separation of Privilege ▪ Brute-Force Login ▪ Weak Password Policy ▪ Account Lockout/Denial of Service ▪ SSO Weaknesses ▪ Security Question Weaknesses ▪ CAPTCHA Flaws

Threat Classification and Reporting

When any exploitable vulnerability is discovered, further research is conducted on that vulnerability to identify its level of severity. The risk is calculated according to the following criteria:

- **Impact**: The security impact on the web application in the event of an exploitation of this vulnerability by an attacker. This criterion indicates the benefit of the attack to the attacker.
- **Ease of Exploitation**: The level of difficulty for an attacker to exploit this problem. Difficulty could increase due to technical complexity, the need for prior knowledge of the network, or other factors. This criterion indicates the cost in time and resources of the attack for the attacker.
- **Popularity and Ease of Identification of the Vulnerability**: This criterion factors in the public availability of information and tools to detect the vulnerability. Problems that have easy to use exploit code available on the Internet, for example, would get a higher rating. This criterion indicates the probability of an attack.

The risk is classified as follows:

Risk Classification	Characteristics
Critical Risk	Vulnerabilities in this category usually have the following characteristics: • Exploitation of the vulnerability results in root/administrator-level access to the system; • The information required in order to exploit the vulnerability, such as example code, is widely available to attackers; • Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victim systems, and does not need to persuade a target user, for example via social engineering, into performing any special functions.
High Risk	Vulnerabilities that score in the high range usually have the following characteristics: • The vulnerability is difficult to exploit; • Exploitation does not result in elevated privileges, but may grant unintended access to data; • Exploitation does not result in a significant data loss.
Medium Risk	Vulnerabilities that score in the medium range usually have the following characteristics: • Denial of service vulnerabilities that are difficult to set up; • Exploits that require an attacker to reside on the same local network as the victim; • Vulnerabilities that affect only nonstandard configurations or obscure applications; • Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics;

	• Vulnerabilities where exploitation provides only very limited access.
Low Risk	Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access.
Informational	These are not vulnerabilities, but additional information gleaned from the target during vulnerability testing.

After identification and classification of the findings is complete, the details of each finding will be documented and detailed recommendations will be given on how to mitigate the discovered threats.

Risk Calculation

Spicy IT utilize the Basic Common Vulnerability Scoring system ("CVSS") version 3 by default for Residual Risk calculation, which takes into consideration the following criteria:

- **Attack Vector**: this metric indicates how 'close' an attacker needs to be to the object. Is physical access needed at one end (AV:P)? Or can the object at the other end be attacked via the network?
- **Attack Complexity**: how easily can the attacker reach their target? Is it within their control?
- **Required Privileges**: does the attacker need privileges (authorization) before they can carry out their attack? If this is the case, the score is lower, otherwise, it is higher.
- **User Interaction**: must a user do anything first before the attacker reaches their target? If the user, for example, has to click on a link first, the value would be 'required' (UI:R).
- **Scope**: the scope describes whether the effects of an attack 'only' affect the vulnerable components or other components. In the last case ('changed' S:C), the scope score increases the base score if the latter has not already reached the maximum value of 10.
- **Confidentiality Impact**: this metric indicates to what extent the attack affects confidentiality. A 'high' (C:H) value means that confidentiality has been totally lost.
- **Integrity Impact**: in the same way, this metric describes the influence on the integrity of the data. If, for example, the attackers were able to modify all files, the impact would be set to 'high' (I:H).
- **Availability Impact**: this measure is also very similar to the other impact metrics. If the attacker succeeds or were able to succeed in denying the availability of the components so that they can no longer be accessed, the maximum value 'high' (A:H) would be reached.

Certifications

Spicy IT's security professionals hold the following certifications:

- CCSP Certified Cloud Security Professional
- Certified Incident Handler (ECIH)
- CompTIA Pentest+
- Certified Penetration Testing Consultant (CPTC)
- Offensive Security Certificated Professional OSCP
- Offensive Security Web Exploitation (OSWE AVAE)
- Certified Ethical Hacker
- CISM Certification Security Manager
- Nexpose NACA Certified Administrator
- Nexpose Certified Administrator
- Fortinet - Network Security Associate
- CCNA CISCO Certified Routing and Switching
- AZ-900|Microsoft Azure Fundamentals
- GCP|Google Associate Cloud Engineer
- Cisco - Certified Network Associate (CCNA)
- CREST CPSA certification
- Splunk - Core Certified User