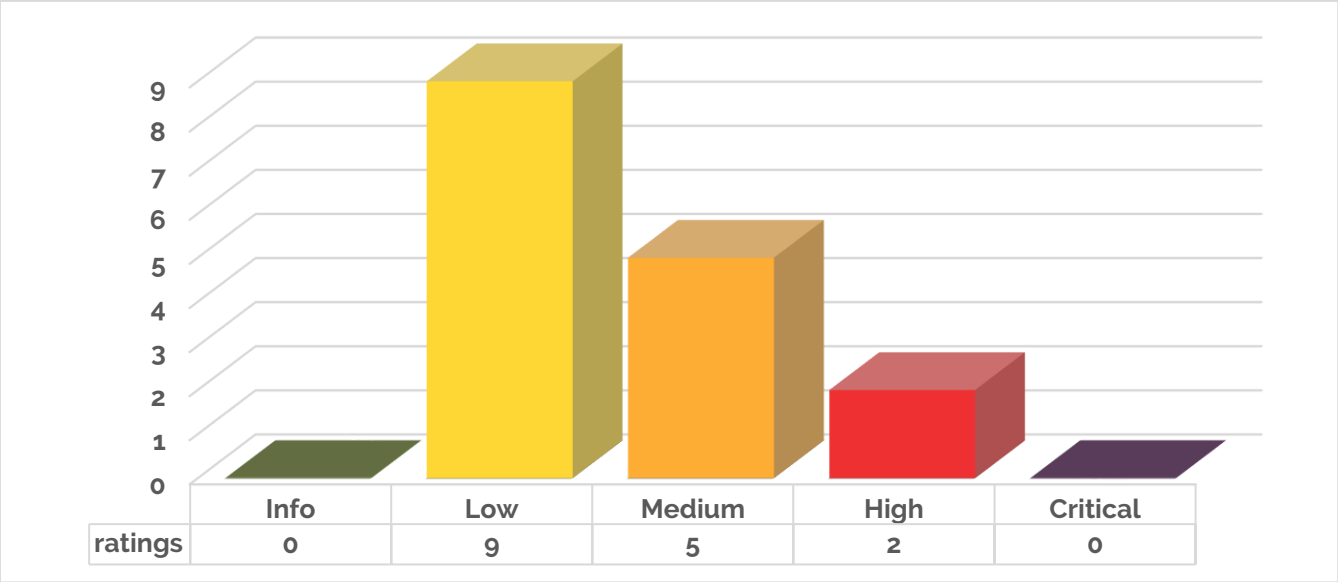
Penetration Test Report

Example Inc

Project	Sample Penetration Test
Date	26/04/2024
Version	1.0
CyberLab Reference	AD12345-RPT-01
Document Classification	CONFIDENTIAL
Report Prepared By	A Tester
Testing Team	A Tester

Executive Summary

CyberLab were engaged by Example Inc to perform penetration testing against the sample network environment and application. Testing was undertaken between the 17th and 19th of April 2024 from the client offices in London.



The above graph illustrates the level of risk that is exposed across the systems tested. It shows the total number of vulnerabilities identified during this assessment along with their severity.

Overview

Overall, Example Inc's security infrastructure demonstrates a commendable security posture, with well-configured security controls prevailing across most of the estate. However, two high-severity concerns were identified. Firstly, missing Windows security updates on two hosts were identified during the server build review phase of testing. Secondly, in the course of web application testing, a stored cross-site scripting vulnerability within the Sample application was identified, attributable to insufficient input validation and output encoding. CyberLab recommends addressing these vulnerabilities promptly to fortifying the overall organisations security stance.

Internal Infrastructure Testing

No high risks issues were identified with the internal testing conducted.

Two medium risk issues were identified that related to clear-text protocols and default management protocol settings. The Telnet protocol was found to be running on the Cisco router, as the Telnet protocol transmits information in clear-text it would be possible to capture and read sensitive information such as usernames and passwords entered from the local network.

The management protocol SNMP was also found to be configured on the Cisco router. This is also a clear-text protocol, but was also configured with default management strings, allowing read only access to information from the router.

Server Build Reviews

Four additional medium risk issues were identified with the security hardening of the servers.

Two of the medium risk issues related to Windows passwords. A weak password policy existed that would allow local user accounts to be created with weak or even blank passwords. Although no evidence was found that weak passwords were in use, this should be configured as per the recommendations within the report.

Common passwords were found between the servers. The local administrator accounts were all found to share the same password. Sharing passwords increases the likelihood of an attack, as if one server was compromised a malicious user would be able to access all the servers using the same account and password.

All other risks were of a low-risk nature and relate to deviations from best security practices.

Web Application Assessment

Expanding on the stored cross-site scripting issue, the assessment also uncovered two medium-risk vulnerabilities within the application. Firstly, the absence of a timeout configuration allows the application to remain active indefinitely, posing a risk if left unattended for over 90 minutes. This could potentially grant unauthorised access to sensitive areas of the system, compromising security.

The application session tokens were also found to be present within the URL of the application. All requests within the URL are entered within web server log files automatically, therefore any compromise of the web server could reveal sensitive session information for users accessing the application.

CyberLab recommends addressing these medium-risk issues alongside the high-severity vulnerabilities to bolstering the application's overall security posture.

All other risks were of a low-risk nature and relate to deviations from best security practices.

Impact

If exploited, the high severity vulnerabilities identified during this assessment could allow an attacker to gain remote code execution on the affected server, enabling a malicious attacker to pivot across the Example Inc infrastructure and potentially expose sensitive information. Additionally, the injection related vulnerabilities could allow an external attacker to compromise user accounts, perform credential phishing attacks and elevate privileges, all leading to sensitive data exposure, reputational and/or financial loss for the organisation.

Key Recommendations

CyberLab recommends that the following remediation actions are conducted:

1 **Apply Missing Security Updates –** Apply missing OS security updates and ensure patching policies and procedures are reviewed to ensure timely application of future security updates.

2 **Remediate Cross-site Scripting –** Review all input validation and output encoding to prevent cross-site scripting vulnerabilities.

3 **Configuration Hardening –** Review the infrastructure and application configuration and harden in line with security best practices and the findings within this report to further reduce risks.

Full details of all recommendations and findings are stated within the technical section of this report.

Table of Contents

Testing Summary

Overview

CyberLab were engaged by Example Inc to perform penetration testing against the sample network environment and application. Testing was undertaken between the 17th and 19th of April 2024 from the client offices in London.

Scope

The scope of the engagement was as follows:

Infrastructure Testing

Unauthenticated vulnerability assessment and manual penetration testing of the following 8 internal IP addresses:

IP Addresses			
192.168.0.100	192.168.0.101	192.168.0.102	192.168.0.103
192.168.0.104	192.168.0.105	192.168.0.106	192.168.0.254

Server Build Reviews

Authenticated build review of the following *3* servers:

Hostname	IP Address	Role
host2.sample	192.168.0.101	Windows 2012 server
host3.sample	192.168.0.103	Windows 2012 server
host4.sample	192.168.0.104	Windows 2012 server

Web Application Testing

Unauthenticated application testing of the following URL:

- https://sampleapp.com

Caveats

The following limitations were identified:

- Where there was a risk of impact to service availability or system performance, active exploitation of identified vulnerabilities was not attempted.

Testing Team

A Tester	Principle Security Consultant Cyber Scheme Team Leader (INF)

Findings Summary

The following sections of the report contain technical information regarding the assessment that was conducted.

Results of Infrastructure Testing

Ref	Risk Rating	CVSS	Issue Title	Status
AD1	MEDIUM	6.0	Clear Text Protocols Identified	**OPEN**
AD2	MEDIUM	6.0	SNMP Agent Default Community Strings	**OPEN**
AD3	LOW	3.0	Banner Information Disclosure	**OPEN**
AD4	LOW	3.0	Weak SSL/TLS Ciphers Supported	**OPEN**

Results of Server Build Reviews

Ref	Risk Rating	CVSS	Issue Title	Status
AD5	HIGH	8.5	Microsoft Windows Patches Missing	**OPEN**
AD6	MEDIUM	6.0	Common Local Administrator Passwords	**OPEN**
AD7	MEDIUM	6.0	Weak Windows Server Password Policy	**OPEN**
AD8	LOW	3.0	Administrator Account Not Renamed	**OPEN**
AD9	LOW	3.0	Cached Domain Credentials	**OPEN**
AD10	LOW	3.0	Unrestricted Internet Access	**OPEN**
AD11	LOW	3.0	Windows Firewall Settings	**OPEN**
AD12	LOW	3.0	Windows Unquoted Service Path	**OPEN**

Results of Web Application Testing

Ref	Risk Rating	CVSS	Issue Title	Status
AD13	HIGH	7.0	Stored Cross-Site Scripting	**OPEN**
AD14	MEDIUM	6.0	Application Session Token In URL	**OPEN**
AD15	LOW	3.0	Cookie Without Secure Flag Set	**OPEN**
AD16	LOW	3.0	Inadequate Application Session Timeouts	**OPEN**

Results of Infrastructure Testing

This section provides the detailed findings and recommendations for the Infrastructure Testing that was performed.

AD1 - Clear Text Protocols Identified

Risk Rating	CVSS	Issue Cause	Status
MEDIUM	6.0	Configuration	**OPEN**

Summary

The Telnet protocol is a legacy service that transmits all information, including credentials in clear-text on the network. As the protocol is not encrypted it would be possible to capture or replay any transmitted information on the local network within Telnet, revealing the information in a clear-text readable format.

Technical Details

The clear-text Telnet services were found to be enabled on the device.

Port scan result:

```
PORT STATE SERVICE REASON
23/tcp open telnet syn-ack ttl 255
```

Connection to device:

```
telnet 192.168.0.254
Trying 192.168.0.254...
Connected to 192.168.0.254.
Escape character is '^]'.

User Access Verification

Password:
```

Recommendation

CyberLab recommends that the clear-text Telnet service is disabled on the device. Secure alternatives such as SSH can be used to manage devices that encrypts all traffic by default.

Systems Affected

TCP Port 23

router1.sample (192.168.0.254)

AD2 - SNMP Agent Default Community Strings

Risk Rating	CVSS	Issue Cause	Status
MEDIUM	3.0	Configuration	**OPEN**

Summary

Simple Network Management Protocol (SNMP) is a management protocol used to communicate with network elements. It is most commonly used to monitor network-attached devices for conditions that warrant administrative attention.

Technical Details

The community string of public was found to be configured on the device. This is a default vendor set community string commonly found on network devices, which allows read-only access to the device.

The following information snippet shows details being extracted from the network device using the read-only default SNMP community string.

```
# snmpwalk -v 2c -c public 192.168.0.254
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK2O3S-M), Version 12.1(22), RELEASE SOFTWARE (fc4)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 30-Dec-03 04:26 by nmasa"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.209
iso.3.6.1.2.1.1.3.0 = Timeticks: (32950) 0:05:29.50
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "Cisco1"
iso.3.6.1.2.1.1.6.0 = ""
```

Recommendation

CyberLab recommends that the SNMP community string value is set to a unique value. In addition, it is recommended that if supported, SNMP version 3 be configured which uses encrypted passwords to protect the community strings.

Systems Affected

UDP Port 161

router1.sample (192.168.0.254)

AD3 - Banner Information Disclosure

Risk Rating	CVSS	Issue Cause	Status
LOW	3.0	Configuration	**OPEN**

Summary

Web server banners can contain version information that can be useful in identifying the software versions installed. Software versions that are disclosed allow the product to be researched for any known vulnerabilities and if found to be vulnerable an attempt to exploit the server could be made.

Technical Details

The following web server banner was identified.

```
HTTP/1.1 200 OK
Cache-Control: public
Content-Type: text/javascript; charset=utf-8
Expires: Wed, 14 Feb 2019 10:01:48 GMT
Last-Modified: Tue, 14 April 2017 10:01:48 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
```

Recommendation

CyberLab recommends that all web server banners should be removed or obfuscated to prevent unnecessary information disclosure.

Systems Affected

TCP Port 443
host5.sample (192.168.0.105)

AD4 - Weak SSL/TLS Ciphers Supported

Risk Rating	CVSS	Issue Cause	Status
LOW	3.0	Configuration	**OPEN**

Summary

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are frameworks which provide encryption and integrity protection for transport layer traffic. The SSL/TLS service can be customised to support specific cryptographic ciphers.

Cipher suites include the following:

- Encryption protocol (e.g. DES, RC4, AES)
- Encryption key length (e.g. 40, 56, or 128 bits)
- Hashing algorithm (e.g. SHA, MD5)

Support for weak cryptographic ciphers suites can increase the risk of compromise of encrypted data.

Technical Details

Weak ciphers of 40bit and 56bit were found to be supported by the web service.

IP Address	Port	Weak Ciphers
192.168.0.254	tcp/443	EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES-CBC(40)
		EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES-CBC(40)
		EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40)
		EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES-CBC(56)

Table 1 – SSL / TLS Weak Cipher Support

Recommendation

CyberLab recommends that support for the weak cipher suites identified are disabled and that only ciphers offering greater than 128-bit encryption are permitted.

Systems Affected

TCP Port 443
router1.sample (192.168.0.254)

Results of Server Build Reviews

This section provides the detailed findings and recommendations for the Server Build Reviews that were performed.

AD5 - Microsoft Windows Patches Missing

Risk Rating	CVSS	Issue Cause	Status
HIGH	8.5	Patching	**OPEN**

Summary

Several Microsoft patches were reported as being missing from internal Windows systems leaving them susceptible to vulnerabilities.

Technical Details

The servers were identified to be missing three Microsoft security updates, dated as far back as 2014. Exploit code for a number of the identified vulnerabilities is known to be publicly available.

Full details of the identified missing patches can be found below.

MS Bulletin	Knowledge Base	Risk	Date	Description
MS14-036	KB2967487	Critical	10/06/2014	Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution
MS16-100	KB3179577	Important	09/08/2016	Security Update for Secure Boot
MS14-040	KB2975684	Important	08/07/2014	Vulnerability in Ancillary Function Driver (AFD) Could Allow Elevation of Privilege

Table 2 – Missing Windows Security Updates & Patches

Note: Some patches may require additional configuration to be applied to the systems such as a registry change for the patch to be fully applied.

Recommendation

CyberLab recommends that the missing Windows OS patches are applied and the root cause for the missing patches is identified.

Systems Affected

```
host2.sample (192.168.0.101)
host4.sample (192.168.0.104)
```

AD6 - Common Local Administrator Passwords

Risk Rating	CVSS	Issue Cause	Status
MEDIUM	6.0	Configuration	**OPEN**

Summary

Local administrator accounts were found to share the same password as each other. If one server was to become compromised, this expands the outbreak of the attack and could allow an attacker to access all other servers on the network that share the same password. If one of these servers has a service or is currently logged-in using Domain Administrator credentials, then this logged-in token can be used to compromise the entire Windows domain.

Technical Details

Several local administrator accounts were identified to use the same passwords across multiple servers.

The following user accounts shared the same password on all servers:

- Administrator
- ROSupport
- ROSupport2
- helpdesk
- Support45

Recommendation

CyberLab recommends that all user accounts have a unique strong password, in accordance with the organisation's password policy. If default passwords are set for new accounts, a policy should enforce the change of those passwords upon first login. Consider the use of Windows Local Administrator Password Solution (LAPS) for the management of local administrative passwords across a domain.

Further information relating to this issue can be found in the following Microsoft document:

Microsoft - LAPS Overview

Systems Affected

```
host2.sample (192.168.0.101)
host3.sample (192.168.0.103)
host4.sample (192.168.0.104)
```

Screenshots

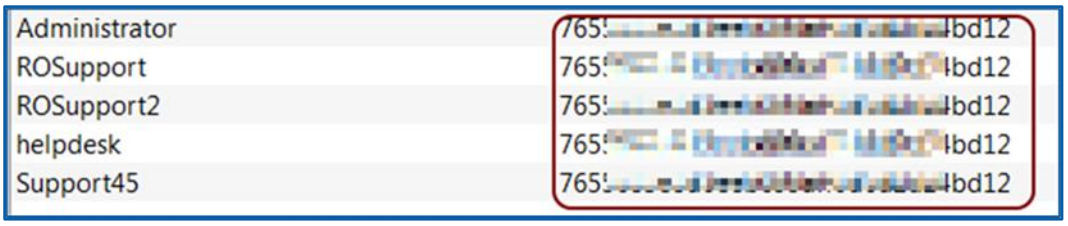


Figure 1 - Common Administrator passwords

AD7 - Weak Windows Server Password Policy

Risk Rating	CVSS	Issue Cause	Status
MEDIUM	6.0	Configuration	**OPEN**

Summary

Passwords are one of the most common methods of authentication to a computer system in order to prove identity. It is important that strong passwords are chosen by users in order to ensure that attackers are not able to gain unauthorised access to these credentials, and the systems that these are used to control access. It is best practice to ensure that strong password policies are technically enforced by the application. If it is left to the user's discretion, then it has been shown that users are more likely to choose a weak password.

Technical Details

A weak local account policy was identified on the servers assessed.

Setting	Configured	Recommended
Enforce password history	24 passwords remembered	24 or more passwords remembered
Maximum password age	60 days	60 or fewer days, but not 0
Minimum password age	1 days	1 or more days
Minimum password length	**0 characters**	At least 14 characters
Minimum password length audit	1 character	n/a
Password must meet complexity requirements	**Disabled**	Enabled
Relax minimum password length limits	Enabled	Disabled
Store passwords using reversible encryption	Disabled	Disabled

Table 3 – Current & Recommended Password Policy Settings

This policy allowed weak or blank passwords to be set for local user accounts, which increases the likelihood of a brute-force attack against the server.

Recommendation

CyberLab recommends that a strong password policy is configured on the servers in line with the organisational password policy.

Systems Affected

```
host2.sample (192.168.0.101)
host3.sample (192.168.0.103)
host4.sample (192.168.0.104)
```

Screenshots

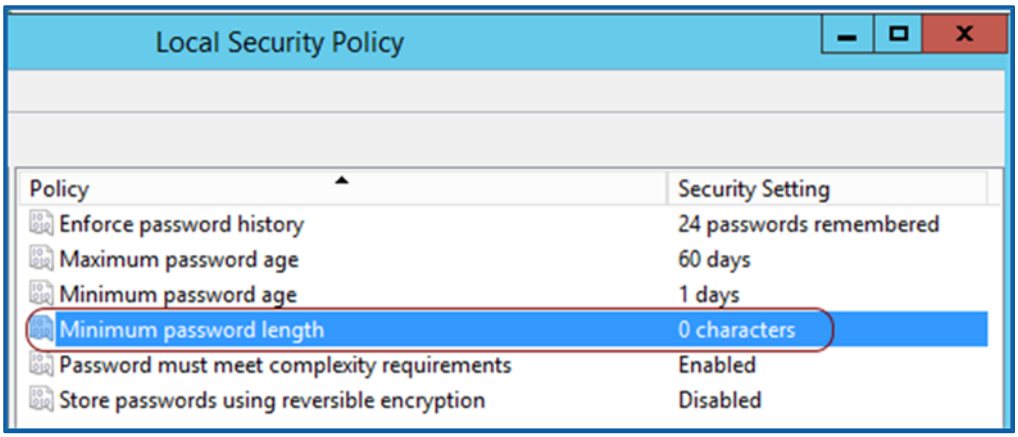


Figure 2 – Weak Password Policy

AD8 - Administrator Account Not Renamed

Risk Rating	CVSS	Issue Cause	Status
LOW	3.0	Configuration	**OPEN**

Summary

Default usernames on systems make it easier for attackers to gain unauthorised access as they need only guess the corresponding password. Windows deployments include two default accounts: Administrator and Guest.

Guest has been disabled by default, however newer versions of Windows also have the administrator user disabled and a new administrator account created in its place.

Technical Details

Analysis identified that the 'Administrator' account had not been renamed from its default value.

Recommendation

CyberLab recommends that the local "Administrator" account should be renamed to something unique. This can be accomplished by modifying the Windows security policy setting below:

Location:

```
Computer Configuration / Windows Settings / Security Settings / Local Policies / Security Options:
```

Title:

```
Accounts: Rename administrator account:
```

Systems Affected

```
host2.sample (192.168.0.101)
```

AD9 - Cached Domain Credentials

Risk Rating	CVSS	Issue Cause	Status
LOW	3.0	Configuration	**OPEN**

Summary

Cached credentials are used to authenticate users when a domain controller is not available. An attacker that is able to access the file system may be able to locate this cached information and launch an offline brute force attack in an attempt to recover user passwords, or use the in a Pass-the-Hash (PtH) attack in an attempt to gain unauthorised access to other systems on the network.

Technical Details

A review of the system configuration identified that domain authentication credentials were cached for the last 10 users to logon interactivity. It was possible to extract the cached password hashes for the following 4 domain administrator accounts.

- jc_adm
- cd_adm
- ga_adm
- tt_adm

Further information relating to this issue can be found in the following URL:

Microsoft - Interactive Logon - Number Of Previous Logons To Cache

Recommendation

CyberLab recommends that only a minimal number of domain credentials are cached on the servers, in line with the recommended values.

This can be accomplished by modifying the following Windows security policy setting below:

```
Location: Computer Configuration / Windows Settings / Security Settings / Local Policies / Security Options
Title: Interactive Logon: Number of Previous Logons to Cache
Value: 0 Logons
```

Alternatively, the number of cached logons can be changed by modifying the registry key at:

```
"HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount"
```

It should be noted that portable devices or those which are located on sites without a permanent network connection to the domain controller should not cache less than 1 domain credential. This ensures that users can still authenticate when not connected to the corporate network.

Systems Affected

```
host2.sample (192.168.0.101)
host3.sample (192.168.0.103)
host4.sample (192.168.0.104)
```

Screenshots

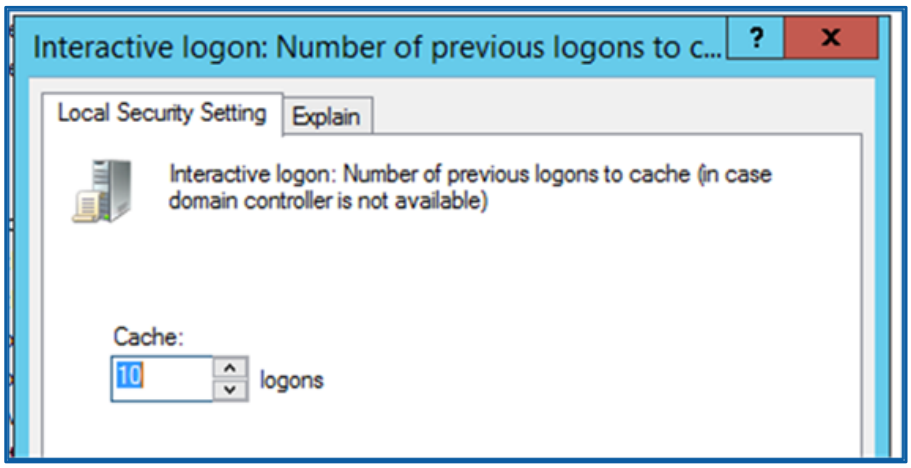


Figure 3 - Cached Domain Logons

Figure 4 - Extracted Domain Admin Cached Password Hashes

AD10 - Unrestricted Internet Access

Risk Rating	CVSS	Issue Cause	Status
LOW	3.0	Configuration	**OPEN**

Summary

With an unfiltered outbound route, there is a risk that servers and workstations can gain direct Internet access and bypass the requirement for content filtering. Direct Internet access introduces a number of threats, including the increased risk of malware being downloaded and executed, Command and Control (C2) channels being established on a compromised server and unauthorised software being installed by sysadmins.

Technical Details

It was possible to obtain unrestricted access to the Internet from the affected servers. It was possible to browse any site located on the Internet, including websites containing exploit code, as shown in Figure 5 below.

Recommendation

CyberLab recommends that server Internet access should be prevented through firewall restrictions if not required. Alternatively, a web filtering or transparent proxy should be implemented to restrict the websites which can be accessed.

Systems Affected

```
host2.sample (192.168.0.101)
host3.sample (192.168.0.103)
host4.sample (192.168.0.104)
```

Screenshots

Figure 5 - Unrestricted Outbound Internet Access

AD11 - Windows Firewall Settings

Risk Rating	CVSS	Issue Cause	Status
LOW	3.0	Configuration	**OPEN**

Summary

Windows Firewall is a built-in, host-based, stateful firewall that is included in Windows XP/2003 onwards.

A host-based firewall on a system allows for sensitive services to be filtered and acts as a means to segregate systems from one another. Effective implementation of host-based firewalls can prevent attackers who compromise a system from gaining lateral access to other systems.

In addition, propagation of malware such as worms or ransomware can be contained where hosts are isolated from one another through use of host-based firewalls.

Technical Details

The Windows Firewall was identified as being disabled, exposing all services and ports on the server internally. This increases the likelihood of a brute-force attack and exposes services that if vulnerable may be subject to remote exploitation.

Recommendation

CyberLab recommends that the Windows host based firewall is enabled.

Systems Affected

```
host2.sample (192.168.0.101)
```

Screenshots

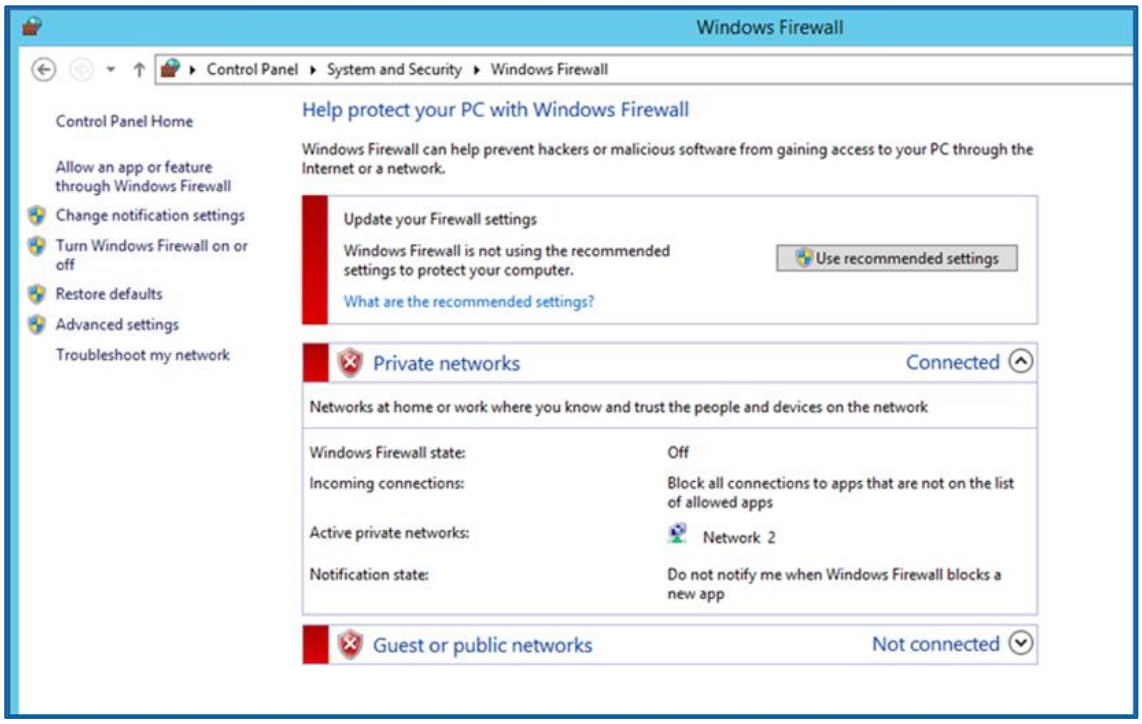


Figure 6 - Windows Firewall Disabled

AD12 - Windows Unquoted Service Path

Risk Rating	CVSS	Issue Cause	Status
LOW	3.0	Configuration	**OPEN**

Summary

Unquoted service paths are a configuration issue within the path of a Windows service, that is normally due to the software vendor not correctly configuring the installer to account for spaces within the service path. A user with local access may be able to gain elevated privilege by inserting an executable file in the path of the affected service.

Technical Details

The following service was found to be affected:

Affected Service	Service Path
Backup Exec System Recovery	C:**Program Files**\Symantec**Backup Exec System Recovery**\Agent\VProSvc.exe

Table 4 – Unquoted Service Paths

This vulnerability takes advantage of the way Windows passes directory paths to execute code. A local attacker could gain elevated privileges by inserting an executable file in the path of the affected service.

Recommendation

CyberLab recommends that the software vendor should be contacted to implement the fix into their installer.

As a workaround, the Windows registry can be manually edited to add quotes to the service path by editing the affected service within the following Registry hive:

```
HKLM\SYSTEM\CurrentControlSet\Services
```

Modify the REG_EXPAND_SZ key corresponding to the affected service and encapsulate the affected path with double quotation marks.

Systems Affected

```
host2.sample (192.168.0.101)
```

Results of Web Application Testing

This section provides the detailed findings and recommendations for the Web Application Testing that was performed.

AD13 - Stored Cross-Site Scripting

Risk Rating	CVSS	Issue Cause	Status
HIGH	7.0	Web Development	**OPEN**

Summary

Stored Cross-Site Scripting vulnerabilities occur when data entered by one user is stored within the application and then later displayed to other users without being sufficiently filtered or validated. A common scenario which may present this vulnerability would be a forum where users can submit their own posts.

This vulnerability would be exploited by an attacker by entering malicious code into a page which is then stored within the web application. A victim would then navigate to the page through normal use of the application and the malicious script would execute in the user's browser within their security context.

An attacker who successfully exploits this issue could hijack application user accounts and run malicious code on the client machines.

Technical Details

Stored Cross-Site Scripting vulnerabilities were identified within one field of the guest book signing application.

The **message** parameter was found to be vulnerable and no input filtering was enforced.

The following code could be inserted to trigger a pop-up window.

```
<script>alert("Cyberlab Stored XSS")</script>
```

Recommendation

CyberLab recommends that all client supplied input is sufficiently escaped before being echoed back to the client's browser. Input validation should be carried out on all input fields to ensure that only input that matched an expected pattern is accepted.

Further information relating to this issue can be found in the following OWASP documents:

OWASP - XSS
OWASP - Cross Site Scripting Prevention Cheat Sheet

Systems Affected

```
sampleapp.com
```

Screenshots

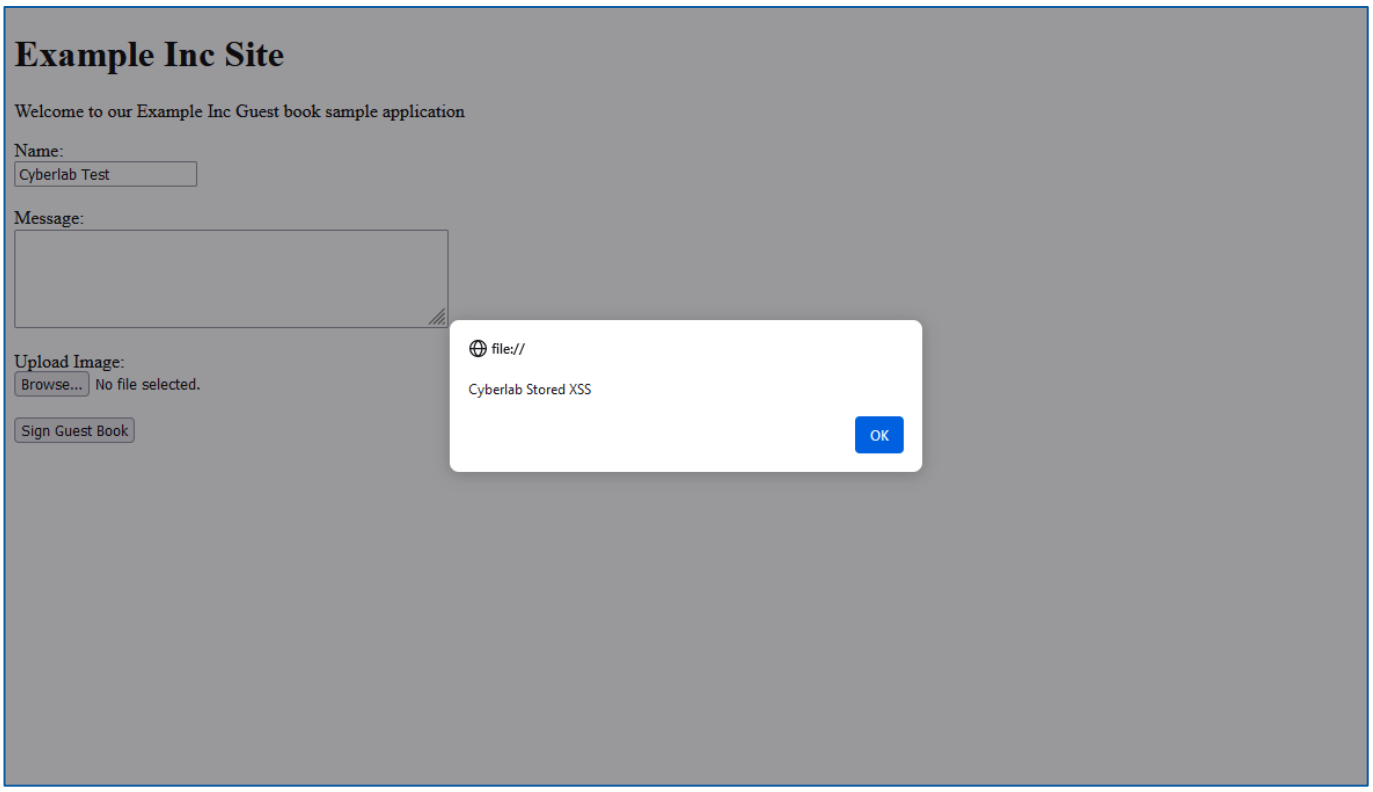


Figure 7 - Stored XSS JavaScript Popup

AD14 - Application Session Token In URL

Risk Rating	CVSS	Issue Cause	Status
MEDIUM	6.0	Web Development	**OPEN**

Summary

Session information from the application was found to be present within the URL visible within the client browser. Any information present within the application URL gets logged in multiple locations that could result in the information being obtained and used to compromise a user's session. Information within the URL normally will be logged within the web server, the client browser or any proxy servers used.

Technical Details

The application session tokens were found to be present within the URL. Token information was being submitted within GET requests, which results in the information being logged within the web server logs and could allow an attacker to replay the token in an attempt to gain unauthorised access to the session.

The following shows the session token RFTOKEN within the URL:

- https://sampleapp/history/routelist.cfm?GFID=2564431&**RFTOKEN=43554**

Further information relating to this issue can be found in the following OWASP documents:

OWASP - Session Fixation
OWASP - Session Management Cheat Sheet

Recommendation

CyberLab recommends that the application is altered so that it does not submit any sensitive information within the URL. Session information or sensitive information should be submitted within the body of the request or within cookies using the POST method.

Systems Affected

```
sampleapp.com
```

AD15 - Cookie Without Secure Flag Set

Risk Rating	CVSS	Issue Cause	Status
LOW	3.0	Web Development	**OPEN**

Summary

Two security related flags can be set within application cookie's to protect the information transmitted and present within the cookie.

- The HTTPOnly cookie flag protects the client from cookie values being read within JavaScript client side attacks, such as Cross-Site Scripting.
- The secure cookie flag protects the cookie being transmitted in clear-text if browsing from HTTP to a HTTPS enabled application.

Technical Details

The secure flag was not set within the application on the below session cookie.

- ASP.NET_SessionId=qymh2ev0zu2hhfjss2wsaa3k1q4; path=/; HttpOnly

Further information relating to this issue can be found in the following OWASP document:

OWASP - Secure Cookie Attribute

Recommendation

CyberLab recommends that all cookies within the application are set to have both the HTTPOnly and the secure flags set.

Systems Affected

```
sampleapp.com
```

AD16 - Inadequate Application Session Timeouts

Risk Rating	CVSS	Issue Cause	Status
LOW	3.0	Configuration	**OPEN**

Summary

The application sessions did not expire after a period of inactivity. Session timeouts help protect applications against session hijacking.

When session tokens do not expire it gives unlimited time to guess or brute-force a valid authenticated session token for a user. If a user's cookie is obtained, it can be used to gain access to that users account within the application.

Technical Details

The application's session token did not expire after a period of inactivity of **90 minutes**.

Further information relating to this issue can be found in the following OWASP document:

OWASP - Session Management Cheat Sheet

Recommendation

CyberLab recommends that all application session tokens be terminated, and users logged out after a set period of inactivity. For applications that handle sensitive information this should be set to from 5 minutes to no more than 20 minutes for low risk applications.

Systems Affected

`sampleapp.com`

Document Management

Document Details

Document Reference	Property
Document Classification	CONFIDENTIAL
Client Name	Example Inc
Document Title	Sample Penetration Test
Author	A Tester
Date	26/04/2024
Document Reference	AD12345-RPT-01
Status	Final

Revision History

Version	Date	Issued By	Summary of Changes
0.1	22/04/2024	A Tester	Initial draft.
0.2	26/04/2024	QA Team	Internal review (QA)
1.0	26/04/2024	A Tester	Final release to client

Document Distribution List

Name	Organisation	Role
Joe Bloggs	Example Inc	Project Manager