ALPHAWEST SECURITY
CYBER THREAT & VULNERABILITY ASSESSMENT SERVICE

Sample report
ACME CORPORATION

Contents

1 About this sample report

This report is an aggregation of findings from a wide range of security assessments conducted over the last three years. This report does not represent the findings of any single test, or any single client, however all issues are actual issues that we have encountered. The ACME CORPORATION Company referenced is a fictional entity devised for the purposes of this sample report. Resemblance to any real-world entity is purely coincidental.

The report provides an indication of our reporting approach, however the content is not intended to be internally consistent between sections. Significant portions of the report – such as code extracts, screenshots, and other proof of concept material – have been removed in the interests of de-identifying prior to release.

2 Executive Summary

2.1 OVERVIEW

ACME CORPORATION has recognised that given expansion into additional market segments and geographies, the organisation is now at an increased risk of cyber-attack and wishes to better understand its current security profile.

As part of this process, **Alphawest** was engaged to conduct a Cyber Threat & Vulnerability Assessment. Testing comprised unauthenticated application security testing, and security testing of the organisation's underlying infrastructure, along with a range of reconnaissance and research tasks using open source intelligence material.

2.2 KEY FINDINGS

Overall, the security posture of the organisation was found to be below industry standard practice. The key findings of each assessment component are listed below:

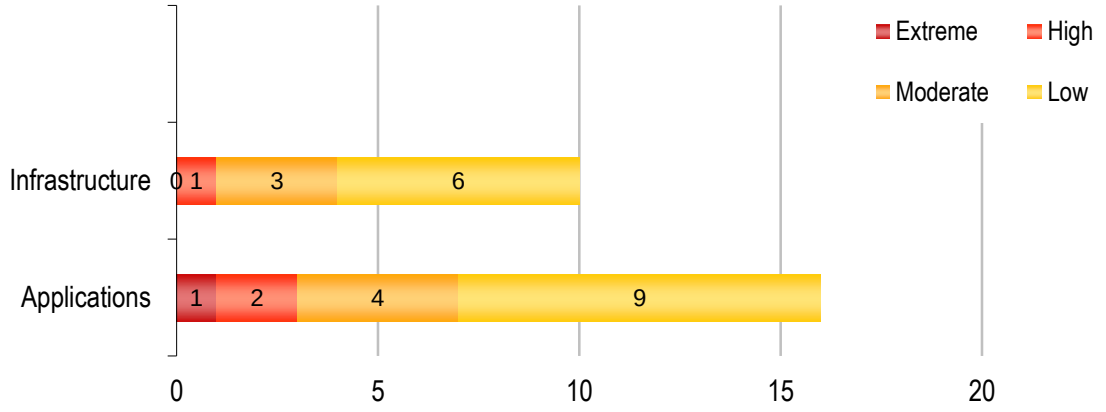
2.2.1 External Security Assessment

- Authentication and authorisation controls were found to be strong, with authorisation checks performed consistently (preventing authorisation bypass).
- Session handling was found to be implemented in line with industry best practice, using unpredictable session tokens which expired in a timely manner.
- In some cases, the trust boundaries in the ACME CORPORATION suite of applications are misplaced, relying on JavaScript and HTML form controls for input validation and restriction. In the most severe cases, this can result in sensitive information disclosure and bypass of business rules.
- The file upload functionality introduced by the social media engagement functionality performs reasonable verification to prevent the upload of malicious code, although this could be made significantly stronger by validating file contents.
- The external-facing servers appear to be well configured and well hardened
- During assessment, it was discovered that direct access to the web servers was achievable as well as access to the to the web servers through virtual services hosted on a load balancer. While there is no direct security risk to the infrastructure, the load balancer aids greatly in providing high availability for the web servers. It is recommended that the load balancer be used where possible to prevent loss of availability to hosted services. ACME CORPORATION have indicated that direct access to the servers is required in the event of the load balancer experiencing issues so that access can be redirected to the real servers.

2.2.2 Personnel Risk Exposure

- A significant number of user names, e-mail addresses, and some personal passwords associated with employees of ACME CORPORATION were able to be obtained from data sources on the Internet. This information could be used in an attack against ACME CORPORATION, and places the organization at an increased risk of compromise.

The following chart and table provide an indication of the risks and vulnerabilities identified:



Review component	Extreme	High	Moderate	Low
Infrastructure	0	1	3	6
Applications	0	2	4	9
Personnel	0	0	2	2
Total	**0**	**3**	**9**	**17**

2.2.3 Risk exposure

Alphawest considers the organisation to be at an HIGH risk of compromise due to the identified presence of multiple cross-site scripting issues and the potential to bypass implemented controls.

3 Schedule of recommendations

The following schedule incorporates all risks and recommendations identified in this deliverable as a result of test cases carried out. Ratings are in line with AS 4360. Further detail on the risk rating can be found in Appendix B - Risk rating scheme. The numbering scheme references the full recommendation, as provided within the report.

Domain references are as follows: Application [**APP**].

Application references are as follows: Web Server 192.168.0.1 [**WEB1**]; Web Server 192.168.0.4 [**WEB4**];

Likelihood ratings are as follows: Rare [**RARE**]; Unlikely [**UNL**]; Moderate [**MOD**]; Likely [**LIK**]; Almost Certain [**AMC**].

Consequence ratings are as follows: Insignificant [**INS**]; Minor [**MIN**]; Moderate [**MOD**]; Major [**MAJ**]; Catastrophic [**CAT**].

Risk Ratings are as follows: Extreme [**EXT**], High [**HIGH**], Moderate [**MOD**]; Low [**LOW**].

Ref.	System	Issue	Like.	Cons.	Risk	Recommendation
HA-02 (p.1)	WEB4	It was identified that a number of security updates on the systems rated as CRITICAL by Microsoft were missing, which would increase the attack surface.	MOD	MAJ	**HIGH**	Test and apply the missing security updates released by Microsoft.
APP-05 (p.2)	Finance System	The application was found to be vulnerable to SQL injection, potentially allowing database values to be retrieved and modified.	UNL	MAJ	**HIGH**	Validate and sanitise all input for SQL special characters and tokens prior to use in database interactions.
HA-08 (p.3)	WEB4	It was identified that a security update on the systems rated as IMPORTANT by Microsoft were missing, which would increase the attack surface	UNL	MAJ	**HIGH**	Test and apply the missing security updates released by Microsoft.
APP-06	Finance System	The application was found to be vulnerable to cross site scripting attacks which can be exploited by a malicious user to execute arbitrary scripts.	UNL	MOD	**MOD**	Apply output sanitisation to all input data before rendering it within an application page.

(p.5)						
APP-03 (p.8)	Finance System	The application was found to use static ID values for some operations for every user and does not enforce proper access control.	UNL	MOD	**MOD**	Modify the application to enforce proper authorisation checks when accessing user specific pages and files.

…large portions of table removed…

Table 1: Schedule of recommendations

4 Review approach

4.1 TESTED ENVIRONMENTS & TIMING

The URLs and usernames provided for the application security assessment are shown below:

- **Corporate Website**
  http://www.clientswebsite.com.au/
- **Corporate Website**
  http://www.otherwebsite.com.au/

Testing was conducted on the following dates:

- Date 1 – System 1
- Date 2 – System 2

4.2 ASSUMPTIONS AND LIMITATIONS

Vulnerability assessments are designed to identify security deficiencies and evaluate the effectiveness of safeguards by mimicking the actions of real-life attackers, using the same processes and tools a genuine attacker would use to infiltrate information systems.

The nature of such testing, and the agreed project scope, presented the following limitations:

- The assessment scope was limited by the available time allocated to the assessment. Vulnerability assessment was 'time boxed' such that testing was completed when the available time (approximately 3 days) was exhausted. **Alphawest** prioritised tests based on our experience, and likely vulnerable areas in the systems. The tests sought to identify systemic issues as opposed to provide a complete list of weaknesses for resolution. Where point-issues are identified, it is possible (and in some cases likely) that additional such issues exist in the application. The proposed 'recommendations' are to be applied throughout the application and other applications similarly developed unless otherwise noted.
- This assessment was a penetration test simulating a malicious attacker; and as such did not include a source code review in parallel with testing. Certain types of vulnerabilities that are more readily identifiable from source code review, may not have been able to be identified through this assessment. If significant vulnerabilities were identified via testing, it is recommended that ACME CORPORATION conduct a thorough code review to ensure these issues are fully understood and mitigated.
- Internet, network and application security are continually growing and evolving fields, and vulnerability assessment by **Alphawest** does not mean that ACME CORPORATION systems are secure from every form of attack. Particularly, the assessment was completed on a specific configuration of the target system, as specified in this report, and at a specific point in time. Future development and system changes may introduce new vulnerabilities not currently identified; and advancement in attack techniques may introduce additional avenues for compromise that are not currently known.

4.3 TEST CASES

Application penetration testing comprised of application familiarisation followed by in-depth assessment using the following test cases as a starting point for response and behaviour analysis:

- **TCA-01 - Information gathering**
  Information gathering is the most fundamental step in application security testing. It allows the tester to become familiar with the application and to identify all the components, entry points and thus potential attack vectors. Subsequently, the tester is able to prioritise testing effort based on the highest risk areas of the system.
- **TCA-02 - Information disclosure**
  A common vulnerability in web applications is the accidental disclosure of sensitive information either directly or implicitly through application behaviour. This includes both confidential information, such as user data or company secrets, and internal application details which may aid an attacker in identifying vulnerabilities including application debug output, source code, application API versions, directory structure and network layout.
- **TCA-03 - Authentication and authorisation**
  If authentication is not conducted robustly, an attacker may be able to access application functionality without identifying themselves to the system or may be able to supply a fraudulent identity when performing application actions. It may also be possible for an attacker to masquerade as a legitimate user – accessing private information or executing actions on behalf of the victim. The failure of authorisation and access controls may allow an attacker to view data or perform actions which they are not entitled to access.
- **TCA-04 - Session management**
  It is common for applications to track an individual's navigation through the use of stored session information, especially when authentication is involved. Session management is closely linked to authentication, as sessions are typically used to prevent the need for a user to provide authentication credentials for every request. This means an attacker who successfully hijacks a valid user session or otherwise subverts session functionality, can access the web application as if they were the session's rightful owner.
- **TCA-05 - Data validation**
  Appropriate data validation within an application allows it to detect and handle incorrect, malformed or unexpected inputs before passing such data to subsystems for processing or execution. Insufficient or inappropriate data validation within an application may allow an attacker to supply unauthorised or malicious commands or parameters to subsystems which may affect the results of processing or cause unauthorised actions to be performed. Data validation issues may occur directly or may arise indirectly through second-order injection attacks where previously stored values are used without validation.
- **TCA-06 - Use of cryptography**
  Failing to secure application data or communications may result in information disclosure or data compromise. Cryptography often provides a means of securing an application and its data however it is notoriously complex to design, implement, and configure securely. Issues with cryptography often result in the compromise of data held within the system as protections are usually applied to important components.
- **TCA-07 - Business logic**
  An individual application contains workflows and implements business rules and policies specific to that application. Business logic can be susceptible to flaws which allow for actions outside these workflows and business rules to be performed. Such issues impact applications in ways specific to their individual context. Certain functionality, by its very nature, may also pose a risk and weak implementations may provide a vector for system or data compromise.

> **TCA-08 - Denial of service**
> Denial of service attacks seek to disrupt the business function being provided an application. There are many forms of denial of service attacks however all target ability of an application to achieve its intended goal are therefore analysed in terms of the applications context.

> **TCA-09 - Auditing and logging**
> Logs are a fundamental component of the intrusion detection process and often form much of the audit trail. In many applications all non-repudiation is provided by logs. Testing of log mechanisms seeks to verify that the data stored can be tampered with, disguised, or otherwise manipulated. Furthermore, it seeks to ensure that logs store a complete and thorough record of events.

The **Alphawest** application security test case to OWASP Top Ten mapping is provided below.

OWASP Vulnerability	TCA-01 Information Gathering	TCA-02 Information Disclosure	TCA-03 Authentication and Authorisation	TCA-04 Session Management	TCA-05 Data Validation	TCA-06 Use of Cryptography	TCA-07 Business Logic	TCA-08 Denial of Service	TCA-09 Auditing and Logging
	Test Case								
A1. Injection					✓				
A2.Cross-Site Scripting (XSS)					✓				
A3. Broken Authentication & Session Management			✓						
A4. Insecure Direct Object Reference		✓	✓						
A5. Cross Site Request Forgery (CSRF)				✓					
A6. Security Misconfiguration		✓							
A7. Insecure Cryptograhic Storage			✓			✓			
A8. Failure to Restrict URL Access			✓						
A9. Insufficient Transport Layer Protection						✓			
A10. Unvalidated Redirects and Forwards			✓						

Table 2: OWASP Top Ten test case mapping

5 Threats and risks to your business

Company Name: ACME CORPORATION **Company Domain:** ACME CORPORATION.com.au

ACME CORPORATION is a leading international financial services business. It is publically listed on the Australian Securities Exchange and is an S&P/ASX Top 200 company. ACME CORPORATION expanded its business in Australia and overseas through amalgamations and joint ventures diversifying to also become a leading manufacturer and distributor of specific products.

[Company background information included here – removed for obfuscation]

An important step when reviewing ACME CORPORATION's internet presence is to identify the brands, subsidiaries and other organisations which are owned or operated by ACME CORPORATION. By reviewing publicly available information the following entities were identified:

[Subsidiary listing removed for obfuscation]

With current high profile operations and weaknesses in ACME CORPORATION's internet facing information systems, there is a **substantial cyber threat with impact on operations, share price and reputation.**

NEWS HEADLINES

ACME CORPORATION CEO resigns

ACME CORPORATION returns lift up to $1.5MN for 2011/2012

ACME CORPORATION invests to reopen closed department in Vic

ACME CORPORATION takes legal action against multi-million dollar supplier

ACME CORPORATION hit by data breach

ACME CORPORATION **is very attractive for targeted cyber attack**

ACME CORPORATION – a leading global business.

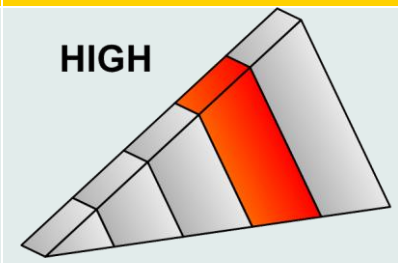
Threat actors' motives:

- impact security & safety
- hinder effectiveness
- steal intellectual property
- steal clients' information
- know proposal positions
- uncover new projects
- harm reputation and
- harm share price

Examples of reputation also damaging business: Sony, RSA, Lockheed Martin & more

6 Exposure of External Perimeter

6.1 APPLICATION SECURITY

Test description	Business risk exposure
ACME CORPORATION application.	

The following table is a summary of the security posture of the application with reference to the **Alphawest** Test Cases. A green tick indicates no issues were found, while a red cross indicates at least one issue was identified.

Ref.	Test case	Result
TCA-01	Information gathering	✓
TCA-02	Information disclosure	✗
TCA-03	Authentication and authorisation	✓
TCA-04	Session management	✗
TCA-05	Data validation	✗
TCA-06	Use of cryptography	✓
TCA-07	Business logic	✓
TCA-08	Denial of service	✓
TCA-09	Auditing and logging	✓

Figure 1: Test case results

6.1.1 TCA-01 Information gathering

Information gathering is the most fundamental step in application security testing. It allows the tester to become familiar with the application and to identify all the components, entry points and thus potential attack vectors. Subsequently, the tester is able to prioritise testing effort based on the highest risk areas of the system.

APP-01	Outdated and Discontinued Version of Apache Tomcat Installed	Moderate Risk

Issue Details

Alphawest identified the Apache Tomcat software on these hosts to be outdated. The detected version is 5.0.28 for which support has been discontinued, and replaced by the 5.5.x branch. From the Apache website it is noted that vulnerabilities fixed in Tomcat 5.5.26 onwards have not been assessed to determine if they are present in the 5.0.x branch.

Classification

- Attack: Abuse of Functionality
- Weakness Information Leakage

Attack Scenario

An attacker may be able to exploit one of a number of issues, such as cross-site scripting, that are have been identified in the 5.5.x branch after the release of 5.5.26.

Risk

The likelihood of the Tomcat installation being exploited is considered UNLIKELY due to the degree of technical knowledge required to exploit these vulnerabilities. The consequences of the vulnerabilities contained in this version of Tomcat being exploited are considered MODERATE due to the type of vulnerabilities seen Tomcat 5.5.x after version 5.5.26. This issue is therefore considered to be a MODERATE risk.

Recommendation

Update to the latest version of Tomcat to ensure that continual updates can be applied to the system. At the time of writing version 5.5.27 is the latest stable version available

6.1.2 TCA-02 Information disclosure

A common vulnerability in web applications is the accidental disclosure of sensitive information either directly or implicitly through application behaviour. This includes both confidential information, such as user data or company secrets, and internal application details which may aid an attacker in identifying vulnerabilities including application debug output, source code, application API versions, directory structure and network layout.

APP-02	Detailed Error Messages	Low Risk

Information disclosure through error messages is one of the most prevalent issues in modern web applications. While in the majority of cases they do not provide a direct means of compromise, they can offer a great source of information to a potential attacker through which further issues can be identified.

Issue details

The application was found to disclose detailed error messages when an error condition was encountered. Multiple types of detailed error message were identified, specifically:

- Error messages generated by the underlying web server, when a file could not be found
- Error messages in page source code comments, when an internal error was encountered by the application
- Error messages in the page text, indicating an error with a back-end web service.

An example of such an error message is as follows:

…

<screenshot deleted>

…

These error messages included stack traces, which contain information about the technologies used in the application's construction, and could be exploited by attackers to assist in identifying vulnerabilities in the application.

Classification

- Attack: Abuse of Functionality
- Weakness Information Leakage

Business impact / attack scenario

An attacker can exploit this issue by triggering an error condition within the application, and using the information disclosed in the resulting error message to determine information about components used in the application's construction.

Risk rating

The likelihood of this issue being identified and exploited is UNLIKELY, as while this issue can be reliably identified using automated tools, no information was disclosed in these error messages which could be used to exploit the application. The consequence of exploitation is INSIGNIFICANT as this is an information disclosure issue only.

As a result, this is considered a **LOW** risk item.

Recommendation

Configure the underlying web server not to generate detailed error messages when an error condition is encountered. Additionally, implement exception handling throughout the application, and cause a generic error message to be displayed if an error condition is encountered in the application.

6.1.3 TCA-03 Authentication and authorisation

If authentication is not conducted robustly, an attacker may be able to access application functionality without identifying themselves to the system or may be able to supply a fraudulent identity when performing application actions. It may also be possible for an attacker to masquerade as a legitimate user – accessing private information or executing actions on behalf of the victim. The failure of authorisation and access controls may allow an attacker to view data or perform actions which they are not entitled to access.

No issues relating to authentication or authorisation were identified during testing.

6.1.4 TCA-04 Session management

It is common for applications to track an individual's navigation through the use of stored session information, especially when authentication is involved. Session management is closely linked to authentication, as sessions are typically used to prevent the need for a user to provide authentication credentials for every request. This means an attacker who successfully hijacks a valid user session or otherwise subverts session functionality, can access the web application as if they were the session's rightful owner.

APP-03	Cross-Site Request Forgery	Moderate Risk

Since HTTP is a stateless protocol and cookies are an implicit form of authentication (the browser appends the appropriate cookies to every HTTP request that a user makes to the domain), web applications have no way to determine where a request originated. Consequently, attackers can force a user to send arbitrary data to a web application with the user's valid authentication. Due to this weakness, web applications need to take specific steps to prevent attackers from being able to force a victim's browser to submit a request that will be processed by the application.

Issue Details

The application was found not to implement appropriate controls against cross-site request forgery. This can be exploited by an attacker to force users to take arbitrary actions within the application, such as changing his/her account details.

For example, an attacker may construct a page which forces a victim's browser to make the following request to the application:

```
POST /test/updatePersonal.do HTTP/1.1
Host: ACME CORPORATION.com.au
```

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3 (.NET CLR 3.5.30729)

Cookie: *Valid cookie, supplied by victim's browser*

Content-Type: application/x-www-form-urlencoded

Content-Length: *Valid Content-Length, supplied by victim's browser*

customerID=one&email=test%40Alphawest.net&phone1=&mobilePhone=

A user viewing such a page while authenticated to the application would have his/her account email changed to "pentest@Alphawest.net".

Classification

- Attack: Cross-Site Request Forgery
- Weakness Insufficient Authentication

Business Impact / Attack Scenario

An attacker could exploit this issue by sending a maliciously crafted link to the victim. When this link is clicked, the victim would be forced to take an arbitrary action within the application.

Risk Rating

The likelihood of this issue being identified and exploited is UNLIKELY, as this issue requires detailed knowledge of the application to exploit. The consequence of exploitation is MODERATE, as exploiting this issue would allow an attacker to force a legitimate user to take arbitrary actions in the application, and possibly compromise the user's account credentials.

As a result, this is considered a **MODERATE** risk item.

Recommendation

Add a randomly generated and unpredictable value (nonce) to each form or link on the site that alters data, and verify that the received value matches the expected value before performing the requested action. Alternatively, force users to re-authenticate with their password before sensitive actions are performed.

6.1.5 TCA-05 Data validation

Appropriate data validation within an application allows it to detect and handle incorrect, malformed or unexpected inputs before passing such data to subsystems for processing or execution. Insufficient or inappropriate data validation within an application may allow an attacker to supply unauthorised or malicious commands or parameters to subsystems which may affect the results of processing or cause unauthorised actions to be performed. Data validation issues may occur directly or may arise indirectly through second-order injection attacks where previously stored values are used without validation.

<content removed>

6.1.6 TCA-06 Use of cryptography

Failing to secure application data or communications may result in information disclosure or data compromise. Cryptography often provides a means of securing an application and its data however it is notoriously complex to design, implement, and configure securely. Issues with cryptography often result in the compromise of data held within the system as protections are usually applied to important components.

<content removed>

6.1.7 TCA-07 Business logic

An individual application contains workflows and implements business rules and policies specific to that application. Business logic can be susceptible to flaws which allow for actions

outside these workflows and business rules to be performed. Such issues impact applications in ways specific to their individual context. Certain functionality, by its very nature, may also pose a risk and weak implementations may provide a vector for system or data compromise.

<content removed>

6.1.8 TCA-08 Denial of service

Denial of service attacks seek to disrupt the business function being provided an application. There are many forms of denial of service attacks however all target ability of an application to achieve its intended goal are therefore analysed in terms of the applications context.

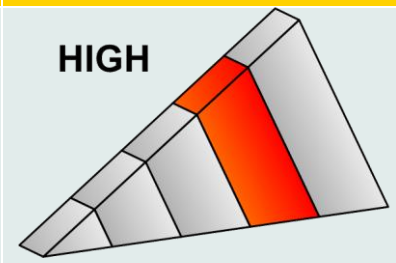
<content removed>

6.1.9 TCA-09 Auditing and logging

Logs are a fundamental component of the intrusion detection process and often form much of the audit trail. In many applications all non-repudiation is provided by logs. Testing of log mechanisms seeks to verify that the data stored can be tampered with, disguised, or otherwise manipulated. Furthermore, it seeks to ensure that logs store a complete and thorough record of events.

<content removed>

6.2 INFRASTRUCTURE SECURITY ASSESSMENT

Test Description	Business Risk Exposure
External penetration testing of the ACME CORPORATION environment	

The following table is a summary of the security posture of the ACME CORPORATION external facing infrastructure with reference to the following commonly identified security domains:

- VA-TC01 Information Gathering
- VA-TC02 Insecure / Inappropriate Services Exposed
- VA-TC03 Missing Patches and Outdated Software
- VA-TC04 Information Disclosure
- VA-TC05 Misconfigured Security Settings

Where a square is marked with a cross (✗) at least one security vulnerability of that type was identified for the system.

System	Hostname	VA-TC01	VA-TC02	VA-TC03	VA-TC04	VA-TC05

192.160.0.1	ACME CORPORATIONwebserver.com	✗	✓	✓	✓	✗
192.160.0.2	ACME CORPORATIONmailserver.com	✗	✗	✗	✗	✓
192.160.0.3	ACME CORPORATIONwebserver2.com	✗	✓	✓	✗	✗

Table 3: External Penetration Test Issues Summary

This section details vulnerabilities identified in the ACME CORPORATION environment infrastructure through the execution of the agreed infrastructure security test cases. Vulnerability assessment was conducted from an anonymous perspective.

6.2.1 Information Gathering

Information gathering is a fundamental step in infrastructure security testing. It allows the tester to identify which are 'live' of the tested IP addresses and ranges, which ports are responsive, and become familiar with type and function of the identified servers.

Server Operating System Identification	Informational

The first step in infrastructure testing is determining the type and function of identified systems. The scanned infrastructure was found to comprise the following systems:

- 1 (one) Windows Server 2003 system
- 2 (two) Windows Server 2008 systems

This information was ascertained from the version of IIS being used by all systems. This is an informational item only and no risk is associated with this finding.

Network Port Identification	Informational

A critical step in Infrastructure testing is identifying responsive ports on the scanned systems.

The following ports were identified to be open on the tested infrastructure:

- TCP port 443 (HTTPS)

This is an informational item only and no risk is associated with this finding.

6.2.2 Insecure / Inappropriate Services Exposed

Servers typically provide access to TCP/IP ports in order to expose underlying services and/or functionality. From a functionality perspective, providing a large number of available ports and services means that the end user may communicate with the server in a variety of ways. However, from a security perspective having a large number of ports available to external users provides an increased surface area for a malicious intruder to attempt to attack and therefore increases the likelihood of an attack.

Security best practice dictates that only the minimum number of services required in order for the system to perform its immediate business function should be made available. In addition, a number of services utilise protocols or provide access to underlying functionality that is considered to be insecure. Typically this occurs in services using protocols that transmit information (including authentication information) 'in the clear' or services providing access to outdated or legacy functionality.

At the time of testing all services appear to be appropriately configured. Only the minimum set of ports were open on the reviewed hosts to allow them to perform their role as secure web servers in line with security best practice.

6.2.3 Missing Patches and Outdated Software

Software vendors frequently issue updates in the form of patches and hotfixes to operating systems to address identified security vulnerabilities. The failure to apply these patches unnecessarily exposes a server system to potential compromise and patching is therefore a critical part of the security process.

Vulnerabilities in the server operating system may allow risks such as the disclosure of sensitive data, denial of service or system compromise to eventuate. Security best practice suggests that all vendor-issued patches that address known vulnerabilities be tested and applied promptly to server systems to address operating system security holes and minimise the possibility of a successful attack being performed on the server.

At the time of testing all software and associated patches reviewed by Alphawest appear to be up-to-date. Interactions with the externally exposed services did not suggest the presence of any outdated software on the server.

6.2.4 Information Disclosure

Server software installed on a system typically provides some information to a computer attempting to connect to the server, often including the name of the software and its version. This is standard behaviour for many servers, such as web and email servers. However, providing this sort of information to an attacker can enable them to identify a vulnerable piece of software and what exploits can potentially be used to compromise the server.

To address this issue, security best practice requires that where possible, server software should be configured to reveal as little information as possible without affecting the functionality of the program.

<information deleted>

6.2.5 Misconfigured Security Settings

Security settings include items such as configuration of audit logs, error handling behaviour, password management controls and default user accounts and associated access permissions. The impact of misconfigured security settings ranges from unauthorised information disclosure, non-compliance with regulatory requirements through to system compromise depending on the particular setting which has been misconfigured.

Hardening guides and security standards are available for the majority of operating systems, both from vendors and from independent organisations such as the Centre for Internet Security (CIS). It is recommended that systems be built in accordance with standards such as these, or internally developed standards (if they exist), as the impact of individual settings can often be subtle but lead to security issues when combined with other issues.

EXT-02	Insecure DNS Recursion Configuration	Low Risk

Issue Details

Alphawest identified two DNS servers to be insecurely configured, enabling external attackers to resolve third party hostnames or to determine which domain names had been resolved recently from these servers. This may allow cache snooping or poisoning attacks against these servers.

Attack Scenario

An attacker may exploit recursive resolution to launch cache poisoning attacks against the host and users of this server or to perform “bounce” denial of service attacks against other systems. Cache snooping may be exploited to gather information about internet connections and usage that can be subsequently used to craft a targeted attack against users.

Risk

The likelihood of this issue being exploited is considered UNLIKELY, as this information cannot be gathered without a specialised information-gathering exercise which requires a significant degree of technical skill to accomplish. The impact of this issue being exploited is considered MINOR, as it does not directly lead to a system compromise. Therefore, this issue is considered **LOW** risk.

Recommendation

Configure the DNS server software to restrict recursive queries to internal hosts and to only process queries for third party domains with the recursion bit set.

Affected Systems:

- One
- Two

EXT-03	Insecure cookie configuration	Low Risk

Since HTTP is a stateless protocol, cookies are used as inherent forms of authentication. If an attacker is able to gain access to a user's browsing cookie, then the attacker is able to effectively log in as that user.

Issue details

One or more cookies used by the application are not marked with the 'HttpOnly' or the 'Secure' attribute. The 'HttpOnly' attribute is used to prevent access to the cookie from the client browser JavaScript engine and provides some mitigation against cross-site scripting attacks. The 'Secure' attribute is used to indicate to the client browser that the cookie is only to be sent using secure (i.e. SSL/TLS) channels and is used to prevent disclosure of the cookie via eavesdropping.

Business Impact / attack scenario

The absence of the 'HttpOnly' attribute may be exploited if a cross-site scripting vulnerability is identified in the application and may allow session credential theft via a cross-site scripting payload.

Without the 'Secure' attribute, an attacker, having acquired access to a node on the network route between client and server, could intercept the cookies reducing the effectiveness of SSL encryption.

Risk rating

The likelihood of this issue being identified and exploited is RARE as successful attacks require either a man-in-the-middle attack, or the presence of a cross-site scripting vulnerability. The consequence of exploitation is considered INSIGNIFICANT as from an unauthenticated perspective; it is unclear if the cookies are used to store sensitive information.

As a result, this is considered a **LOW** risk item.

Recommendation

Set the 'HttpOnly' and 'Secure' attribute on all sensitive cookies.

Affected systems

- One
- Two
- Three

7 Exposure of Employees

7.1 USER NAMES AND DOCUMENT METADATA

The following user names and other information were identified from document metadata available from ACME CORPORATION's website. This along with other information within the metadata can be used by hackers to gain access to ACME CORPORATION's systems.

From a single unsanitised document, an attacker may be able to obtain the following information, and more:

- User name of the user who created the document
- Software and version used to create the document
- Internal path where the document is saved, or has been stored
- Computer operating system version and patch level at the time of document creation
- Document reviewers
- Comments made by reviewers of a document
- Email addresses
- Printers used
- Internal internet protocol addresses

All valuable pieces of information for a successful hack

Table 4 – Metadata obtained from documents on ACME CORPORATION's website.

User Names and other information		
Glen	Mike	violetnine33
w1nne	spinke09	Sunni
Rixi	dcg200	Antwuan
UnitedScape	rdd200	Nazurasu
Malik	jas700	dharmvir123
rbr600		gordondr

7.2 EMAIL ADDRESSES

The following email addresses were identified via search engine references. The ability to obtain valid email addresses provides a vector for targeted attacks using email.

Table 5 – Email addresses found from search engine references.

Email Addresses

<removed1>@<sample>.com.au	<removed7>@<sample>.com.au
<removed2>@<sample>.com.au	<removed8>@<sample>.com.au
<removed3>@<sample>.com.au	<removed9>@<sample>.com.au
<removed4>@<sample>.com.au	<removed10>@<sample>.com.au
<removed5>@<sample>.com.au	<removed11>@<sample>.com.au
<removed6>@<sample>.com.au	<removed12>@<sample>.com.au
	<removed13>@<sample>.com.au

7.3 INTERNAL APPLICATIONS / DEVICES

This software and device information is present in document metadata available on ACME CORPORATION's website. This is useful for determining potentially vulnerable software a threat actor can leverage to gain a foothold into the organisation.

Moreover it can provide an attacker with insight into the system security patching – for example, correlating software versions with their creation date gives a potential attacker advance knowledge of which exploits can be used against a target with a high likelihood of success.

Table 6 – Internal applications and devices found from metadata on ACME CORPORATION's website.

Internal Applications / Devices	
Microsoft Office	Adobe InDesign CS5 (7.0.4)
Microsoft Office 2007	Adobe InDesign CS5 (7.0)
Acrobat Distillier 6.0.1	GNU Ghostscript 7.05
PScript5.dll Version 5.2.2	Adobe Photoshop 5.5
Adobe PDF Library 9.90	Acrobat Distillier 4.05
Adobe Illustrator CS5	Adobe InDesign CS5 (7.0.3)
Acrobat 3.0 Scan Plug-in	Adobe PDF Library 9.0
Adobe PDF Library 8.00	PDFlib 4.0.1
Adobe Illustrator CS3	PDFCreator 0.9.0Windows
Adobe Acrobat 8.0	Ghostscript 8.53
GPL Ghostscript 8.64	Adobe Acrobat 9.3.0
PScript5.dll Version 5.2	GPL Ghostscript 8.70
Adobe PDF Library 8.0	Acrobat Distillier 8.0.0
Adobe InDesign CS3 (5.0.4)	Microsoft Office 2000
Acrobat Distillier 5.00	Acrobat Distillier 8.1.0
InDesign: pictwpstops filter 1.0	Adobe InDesign CS3 (5.0.1)
Microsoft Office 2003	GPL Ghostscript 8.15
Adobe InDesign CS2 (4.0.3)	

7.4 INFORMATION LEAKAGE

Significant information leakage can occur through employees of the organisation posting material to web forums, or through breaches of third parties holding data belonging to ACME CORPORATION.

One common location to find such information is Pastebin. Pastebin is a tool which allows users to quickly share snippets of information anonymously with other users. Often used as a tool by programmers to share code, it is also used by spammers, hackers and other malicious actors to share or obtain information about an organisation in order to plan for an attack. A number of issue motivated groups, including the hacking group Anonymous, regularly uses

Pastebin to plan attacks and post damaging information derived from organisations they have hacked.

There were a number of references to ACME CORPORATION found in searches spanning the past 12 months, however, these were not of direct cyber attack risk to the organisation. They were mainly references to ACME CORPORATION's contact details and information about the company's activities including ASX references. One post for example, mentions potentially sensitive operational information from a shipping contractor regarding difficulties in delivering ACME CORPORATION product. This information would probably be unnecessary to post on such a public site with potentially hostile users. The link to this post is provided below:

> http://pastebin.com/<obfuscated>

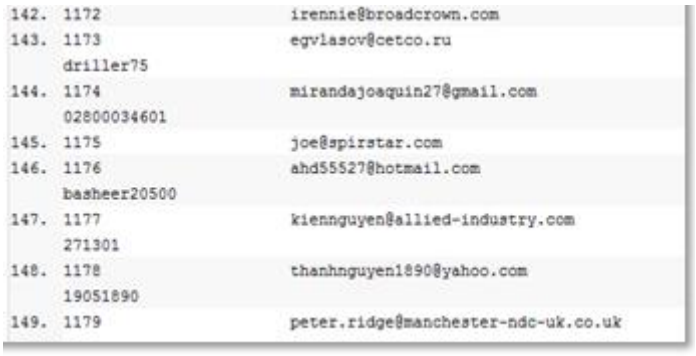
Additional Pastebin references were also identified which identify **users with ACME CORPORATION email addresses who have had credentials compromised on other systems.** This is primarily a risk if these passwords are reused internally within ACME CORPORATION, as has been seen with personnel in other companies. There are approximately 17 references and are available at these links:

> http://pastebin.com/AuWiPDHS

> http://pastebin.com/B0zcfVct

7.5 EMPLOYEE ACCOUNTS ON SOCIAL NETWORKING SITES – LINKEDIN & FACEBOOK

Employee accounts on LinkedIn and Facebook are an excellent source of information for attackers. They can obtain profiles of employees in the company, full names, interests and history to create targeted emails to compromise their work system accounts. For a quick snapshot of which employees have LinkedIn accounts and what information they share about themselves, LinkedIn has several default graphs such as the graph included below. This information can be retrieved and then used to increase the likelihood of a successful social engineering campaign.



ACME CORPORATION has 124 employees on LinkedIn including senior executives and personnel in key positions within the organisation.

Appendix A - Document management

Version	Date	Description
0.1	14-Aug-12	Internal review release of sanitised cyber threat report
0.2	14-Aug-12	ACME CORPORATION release approved

Table 7 – Document history

Appendix B - Risk rating scheme

B.1 LIKELIHOOD

The likelihood rating of an issue encompasses both the likelihood of the issue being identified and attacked as well as the likelihood of an attack being successful. This is evaluated by taking into consideration the following aspects:

- Exploitability
- Reproducibility
- Discoverability
- Frequency

These factors will be employed to formulate a final likelihood rating for a given issue and a table of examples is provided below.

Likelihood rating	Example frequency	Example scenario
Rare	1 incident every 5+ years	Highly skilled and determined attacker with substantial resources
Unlikely	1 incident every 2 years	A skilled attacker with some degree of insider knowledge
Moderate	1 incident every year	An attacker with technical knowledge
Likely	1 incident every 6 months	Published and widely available exploit code exists
Almost Certain	1+ incidents every month	Worm propagating in the wild or widespread availability of an automated attack tool

Table 8: Likelihood Rating Scheme

B.2 CONSEQUENCE

The consequence rating assesses the significance of exposure to a particular risk. This is evaluated by considering the impacts to the affected system and the underlying business. The factors under consideration are outlined in the following table.

Impact	Insignificant	Minor	Moderate	Major	Catastrophic
System – Confidentiality	Disclosure of public information	Minor disclosure of commercial-in-confidence information	Major disclosure of commercial-in-confidence information	Minor disclosure of highly-confidential information	Major disclosure of highly confidential information
System – Integrity	Unauthorised modification of public data	Small-scale unauthorised modification of private data	Large-scale unauthorised modification of private data	Small-scale unauthorised modification of trusted data	Large-scale unauthorised modification of trusted data
System – Availability	Minor increase in processing load	Minor outage in a business system	Outage or unavailability of a business system	Extended unavailability or outage of a business system	Unavailability or outage of a business-critical system

Brand or Reputation	Complaints from small number of customers	Complaints from small number of customers across a broader customer base	Complaints from a large number of customers and localised media coverage	Short term adverse large scale media coverage	Extended adverse large scale media coverage
Regulatory and Legal	Warnings for minor breaches	Formal caution for regulatory breaches or threat of legal proceedings	Targeted audit / investigation by regulator or minor legal proceedings brought against the organisation	Fines imposed and negative media coverage or major legal proceedings brought against the organisation	Service line closed down
Management Impact	A minor event or issue which causes minimal disruption	Minor disruption absorbed through normal management activities and no compromise of technology direction or policy	Disruption absorbed via additional effort to ensure technology direction or policy is not compromised	Considerable deviation and significant compromise of technology direction or policy	Cancellation of the service line and significant recovery and remediation costs incurred

Table 9: Consequence Rating Scheme|

B.3 RISK

A risk measure or rating is determined by the likelihood and adjusted consequence ratings. Use the matrix below to determine each risk.

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Almost Certain	HIGH	HIGH	EXTREME	EXTREME	EXTREME
	Likely	MODERATE	HIGH	HIGH	EXTREME	EXTREME
	Moderate	LOW	MODERATE	HIGH	EXTREME	EXTREME
	Unlikely	LOW	LOW	MODERATE	HIGH	EXTREME
	Rare	LOW	LOW	MODERATE	HIGH	HIGH