

Penetration Testing Report



For
<>
From

DRAFT



NII
Consulting

www.niiconsulting.com

ATTENTION: This document contains information from NII that is confidential and privileged. The information is intended for the private use of <>. By accepting this document you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from NII. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.

Document Details

Company	<>
Document Title	Penetration Testing Report
Date	
Ref	<>/NII/06122005
Classification	<input type="checkbox"/> Public <input type="checkbox"/> Internal <input checked="" type="checkbox"/> Confidential <input type="checkbox"/> Highly Confidential
Document Type	Report

Recipient

Name	Title	Company
		<>

Document History

Date	Version	Author	Comments
	1.0		Initial draft
	1.1		Review and formatting

Contents

1	EXECUTIVE SUMMARY	4
1.1	SUMMARY	4
1.1.1	<i>Approach</i>	4
1.2	SCOPE	5
1.3	KEY FINDINGS	6
1.3.1	<i>Insufficient Authentication</i>	6
1.3.2	<i>Improper Input Filtration</i>	6
1.3.3	<i>Administrator login and Username Enumeration</i>	7
1.4	RECOMMENDATIONS	8
1.4.1	<i>Tactical Recommendations</i>	8
1.4.2	<i>Strategic Recommendations</i>	9
1.5	TABULAR SUMMARY	10
1.6	GRAPHICAL SUMMARY	11
1.6.1	<i>Overall Risk Chart</i>	11
2	TECHNICAL REPORT	12
2.1	NETWORK SECURITY	12
2.1.1	<i>Port Scan Status</i>	12
2.1.2	<i>Service Banner Disclosure</i>	14
2.2	WEB APPLICATION VULNERABILITIES	16
3	CONCLUSION	21
4	APPENDIX	22
4.1	SQL INJECTION	22

1 Executive Summary

1.1 Summary

<> has assigned the task of carrying out Quarterly Penetration Testing of <domain>, to Network Intelligence (I) Pvt. Ltd.

This is the second quarter Penetration Testing report. This Penetration Test was performed during <Date>. The detailed report about each task and our findings are described below.

The purpose of the test is to determine security vulnerabilities in the server configurations and web applications running on the servers specified as part of the scope. The tests are carried out assuming the identity of an attacker or a user with malicious intent. At the same time due care is taken not to harm the server.

1.1.1 Approach

- Perform broad scans to identify potential areas of exposure and services that may act as entry points
- Perform targeted scans and manual investigation to validate vulnerabilities
- Test identified components to gain access to:
 - <10 IP addressed devices>
- Identify and validate vulnerabilities
- Rank vulnerabilities based on threat level, loss potential, and likelihood of exploitation
- Perform supplemental research and development activities to support analysis
- Identify issues of immediate consequence and recommend solutions
- Develop long-term recommendations to enhance security
- Transfer knowledge

During the network level security checks we tried to probe the ports present on the various servers and detect the services running on them with the existing security holes, if any. At the web application level we checked the web servers' configuration issues, and more importantly the logical errors in the web application itself.

1.2 Scope

The scope of this penetration test was limited to the below mentioned IP addresses.

<IP address list>

DRAFT

1.3 Key Findings

In this section we would like to highlight summary of the critical issues that we discovered during our Penetration Testing exercise.

1.3.1 Insufficient Authentication

On pages [...], the user can login and get the access with any username and password.

Recommendation

Proper authentication mechanism should be implemented along with a good password policy.

1.3.2 Improper Input Filtration

The input values are not parsed properly. By exploiting this vulnerability, an attacker can insert a single URL, and send it to another user or steal session IDs. Improper filtration has revealed the following vulnerabilities.

- Database manipulation is possible through an attack technique - SQL injection¹. The vulnerability can be exploited through the username and password fields. Successful exploitation may also allow an attacker to run arbitrary SQL Query on the server.
- The xyz.com servers were found vulnerable to Cross-site scripting (XSS) attack². Absence or lack of Input filtration in the scripts allows an attacker to insert a single URL³, or a malicious Java Script in the link, and send it to another user. As the malicious script is run in the context of <website_name> web site, the victim will consider the malicious URL as a valid URL. This happens when the parameter values are used from the URL to create the web page.
- In another instance, input is not properly sanitized allowing any malicious URL to be sent to the victim with a fake summary. The situation is then very similar to the Cross-site scripting attack.

¹ SQL Injection: http://en.wikipedia.org/wiki/SQL_injection

² http://en.wikipedia.org/wiki/Cross-site_scripting

³ URL: Universal Resource Locator

Penetration Testing Report

Recommendation

All data on all the pages should have input as well as output filtering. If possible, meta-characters like <>,.?^&/\~`'"()- should be completely removed from a user's input. SQL injection should be mitigated by using stored procedures, and reducing the privilege levels with which the database executes.

1.3.3 Administrator login and Username Enumeration

The Administrator login validation script returns different errors when

1. An invalid username is supplied
2. A valid username and invalid password is supplied.

This can assist an attacker to get hold of a valid username and then carry out a brute force attack⁴. Similarly, username enumeration is also possible in case of the vendor login validation script.

A Test account exists on the server. It is recommended to disable/delete such accounts.

Recommendation

Remove any unnecessary accounts and make the error messages across pages consistent so as not to disclose any unsolicited information.

⁴ Phrase reference: http://en.wikipedia.org/wiki/Brute_force_attack

1.4 Recommendations

NII recommends that attention is given to the issues discovered during this assessment and that an action plan is generated to remediate these items.

The recommendations are classified as tactical or strategic. Tactical recommendations are short term fixes to help elevate the **immediate** security concerns. Strategic recommendations focus on the entire environment, future directions and introduction of security best practices. A highlight of the recommendations follows:

1.4.1 Tactical Recommendations

- **Filter User Input** - Users input can have malicious characters which may result in attacks like SQL injection, XSS etc.
- **Use stored procedures**- To mitigate the risk from SQL injection, in addition to user input validation, stored procedures should also be used.
- **Avoid username enumeration** - Display consistent error messages for any combination of username and password.
- **Implement access control on SQL server** - Give appropriate privileges to authorized users only.
- **Change Firewall ACL configuration**: If port 110 is not required to be open on the Internet, modify the ACL to block all incoming traffic.
- **Upgrade phpBB**: Upgrade phpBB to prevent critical attacks exploiting known vulnerabilities in phpBB.
- **Block ICMP incoming traffic** - ICMP can be used to launch denial of service attacks against targeted equipment. Disable ICMP at the router and firewall to ensure this type of action is protected against.
- **Disable HTTP Trace method** - The trace method can be used to leverage cross-site scripting attacks against <>. This method should be disabled from the web service.
- **Disable unnecessary IIS extensions** - Extraneous IIS extensions (.printer & .IDA) can be used to launch attacks against the web service. These extensions should be disabled if not required by <>.
- **Information Disclosure** - MS SQL stored procedure names and its parameters' information is accessible via the error pages on the website. This information should be blocked from web surfers.
- **Block extraneous services** - Access to various services is available via the Internet. These services should be either turned off or blocked so an attacker cannot take advantage of these extra attack vectors.
- **Disable FrontPages** - Microsoft FrontPages was found on a few servers in the environment. This service should be disabled so it cannot be exploited via the Internet.

1.4.2 Strategic Recommendations

- **Conduct proactive security assessments** - As part of security best practices; <client> should ensure that any major changes to their Internet facing infrastructure should require another external security assessment. This should be done to ensure that these changes do not increase the risk to environment.
- **Intrusion Detection (IDS)** - Networks exposed to potentially hostile traffic should implement some capability to detect intrusions. Investigate an IDS solution for the network.

DRAFT

1.5 Tabular Summary

The following table summarizes the System’s Vulnerability Assessment:

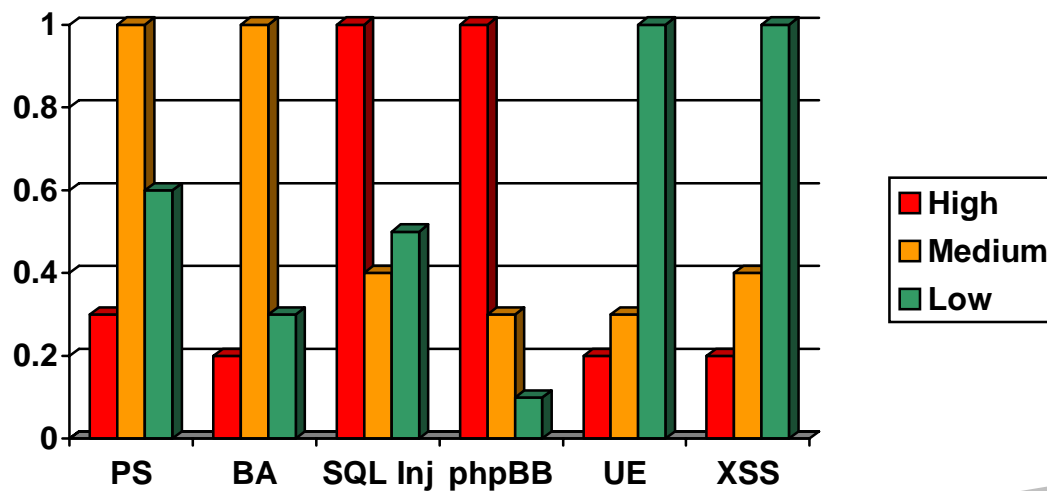
Category	Description		
Systems Vulnerability Assessment Summary			
Number of Live Hosts	50		
Number of Vulnerabilities	29		
High, Medium and info Severity Vulnerabilities	14	6	9

Vulnerability Summary

DRAFT

1.6 Graphical Summary

1.6.1 Overall Risk Chart



PS: Port Scan
BA: Broken Authentication
SQL Inj: SQL Injection
phpBB: phpBB Known Vulnerabilities
UE: User Enumeration
XSS: Cross-site Scripting

2 Technical Report

2.1 Network Security

2.1.1 Port Scan Status

For the domain, 'xyz.com' the below listed IPs were scanned. The listed ports appear to be open on the server. Alongside the port number, we also show the service that usually runs on those ports as well as the banner displayed by the service.

Domain: <hyperlinked domain name>

IP Address: 10.0.180.218

Port No	Service Running	Service Version Details
25	SMTP	
80	HTTP	Apache
110	POP3	
443	HTTPS	OpenSSL

Domain: <hyperlinked domain name>

IP Address: 10.0.137.219

Port No.	Service Running	Service Version Details
25	SMTP	Sendmail
80	HTTP	Apache
110	POP3	UW Imap pop3 server 2003.83rh
443	SSL	Open SSL

Penetration Testing Report

Domain: <hyperlinked domain name>

IP Address: 10.0.167.150

Port No	Service Running	Service Details	Version
22	SSH Remote Login Protocol		--
25	Simple Mail Transfer	Sendmail	
80	World Wide Web HTTP	Apache	
3306	MySQL	MySQL server	

Analysis

We have observed that only the required and genuine ports are open on the server. However, it is recommended that the firewall should block the ping request. As a result of this the number of port scans coming on the network via the internet will decrease (thereby decreasing the reconnaissance attempts).

The SSL certificate of IP 10.0.167.152 has expired.

Penetration Testing Report

2.1.2 Service Banner Disclosure

Severity Level

Medium

Summary

Banner grabbing is a technique of connecting to remote applications and observing the output. It can be very useful to remote attackers. With this an attacker can get the software name and version running on the server, which then allows him/her to concentrate on platform cum version-specific techniques to compromise the server.

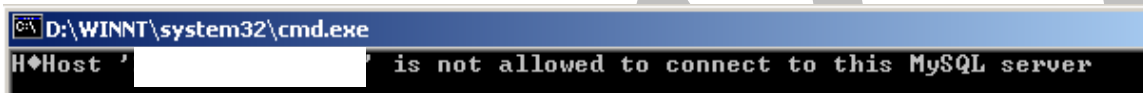
Analysis

1. Banner grabbed for the service running on the port 110



```
C:\> D:\WINNT\system32\cmd.exe - telnet [redacted] 110
+OK POP3 [redacted] v2001.78rh server ready
```

2. Banner grabbed for the service running on port 3306



```
C:\> D:\WINNT\system32\cmd.exe
H◆Host '[redacted]' is not allowed to connect to this MySQL server
```

Penetration Testing Report

3. Banner grabbed for the service on port number 10000 running at IP Address 10.0.167.152

```
Server: Apache/1.3.29 (Unix) mod_ssl/2.8.16 OpenSSL/0.9.7d
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1

127
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>400 Bad Request</TITLE>
</HEAD><BODY>
<H1>Bad Request</H1>
Your browser sent a request that th
is server could not understand.<P>
client sent HTTP/1.1 request without hostname
(see RFC2616 section 14.23): </P>
</BODY></HTML>
```

Recommendation

It is advisable to change the banners of the services running on the server to something generic that does not identify the exact service (and version) running on the server. Also, restrict access to ports that need not to be used by normal users, especially the 'webmin' port 10000, which is used only for server administration.

References

http://www.educause.edu/content.asp?page_id=1298&bhcp=1

2.2 Web Application Vulnerabilities

Risk Description	Threat Level	Potential Corporate Loss	Likelihood of Exploitation	Affected IP's/URI	Recommendation
<p>Broken Authentication The user can login and get the access with any username and password.</p>	Severe	A significant amount of privileged information was found.	Because there was no authentication it is trivial to break in to the system and get sensitive information		Proper authentication mechanism should be implemented along with a good password policy.
<p>SQL Injection SQL injection exists in the username and password fields. This may also allow an attacker to run arbitrary SQL Query on the server.</p>	Severe	An attacker can gain access to personal employee information. The version of SQL server, database, and server name was also revealed. It was possible to enumerate the entire database table and also quite likely to run malicious commands like "drop table",	SQL injection is an old technique and it does not require much technical skills to exploit the database and run malicious queries.		<p>It is advisable to filter all the input data before running the SQL query and allow only valid characters. For e.g.:- disallow single quotes('), comments(--), etc.</p> <p>Use least privilege principle and allow only the necessary privileges.</p>

Penetration Testing Report

		etc.			
Vulnerable PHPbb version	Severe	Possible system compromise as most of the exploits are available.	It is simple to exploit as all exploits are published on vulnerability reporting sites.		Upgrade the version of PHPbb and visit the website for regular updates.
Username Enumeration Error pages returned by the Authentication script disclose valid username details to the attacker.	Moderate	On obtaining valid usernames an attacker could brute force to look for a weak password	Such exploitation is less likely to occur if the password is strong.		The validation script should not reveal the presence of valid username by displaying different error pages as shown in the screen shots. This information is critical in carrying out social engineering attacks.
Cross site scripting It allows an attacker to run arbitrary script in the victim's browser.	Moderate	An attacker may use this flaw to trick your web users to give him/her their credentials (cookie)	This attack is dependant on the victim to execute a crafted link.		All data on all the pages should have input as well as output filtering. If possible, meta-characters like <>,.?^&/\~`' "-()

Penetration Testing Report

		which can be used for session hijacking.			from a user's input should be completely removed. Input: '<' character Modified during output: '<'
FrontPage extensions enabled FrontPage has a long history of remote vulnerabilities as well as mis-configurations which make unauthorized remote publishing possible.	Moderate	An attacker equipped with a FrontPage exploit could remotely compromise the web server.	Hackers actively target and compromise servers with FrontPage extensions enabled.		To prevent having these extensions from being Internet facing, set up a staging server for publishing.
Web server supports TRACE methods TRACE HTTP method is used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks.	Moderate	An attacker may use this flaw to trick your web users to give him/her their credentials.	This attack is dependant on the victim to execute a provided link. Since user interaction is required, this attack is less likely than automated attacks.		Deny HTTP TRACE requests or permit only the methods needed to meet site requirements and policy. More information can be found at: www.kb.cert.org/vuls/id/867593
URL Redirection A known vulnerability exists in Outlook Web Access which allows the attacker to redirect the victim to some malicious web site, this will lead to phishing attack.	Low	No direct loss is attributable. The victim will associate same trust to the crafted URL as he will associate with <client_ur	Such redirection is less likely to occur		URL should be parsed appropriately.

Penetration Testing Report

		>			
Resource exhaustion It is possible to retrieve the entire record by using a wild card ("%"). This results in a resource consuming SQL query.	Low	The attacker can waste the system resources and cause possible denial of service to legitimate user(s).			Implement input filtering
Information Disclosure Error pages disclose stored procedure and the parameters expected in the database. It also reveals the ASP.net version.	Low	An attacker would search for known vulnerabilities for the version disclosed.	Such exploitation is less likely to occur.		Customize the error pages to provide only required information.
Outdated Web Servers Older version of IIS [5.0] is used. This version is highly vulnerable.	Low	An attacker would search for known vulnerabilities for the version disclosed.	Such exploitation is less likely to occur.		Upgrade to IIS 6.0
Outdated SSL Certificate	Low	An attacker can sniff sensitive data	Such exploitation is less likely to occur.		Renew SSL certificate.

Penetration Testing Report

Improper ACL Configuration	Low	Firewall allows incoming and outgoing traffic at Port 110	Such exploitation is less likely to occur	Refer to port scanning result for all IP's showing port 110 closed.	Modify ACL Configuration
----------------------------	-----	---	---	---	--------------------------

DRAFT

3 Conclusion

Experience has shown that a focused effort to address the problems outlined in this report can result in dramatic security improvements. Most of the identified problems do not require high-tech solutions, just knowledge of and commitment to good practices.

For systems to remain secure, however, security posture must be evaluated and improved continuously. Establishing the organizational structure that will support these ongoing improvements is essential in order to maintain control of corporate information systems.

We conclude that the overall security needs to improve. We hope that the issues cited in this report will be addressed.

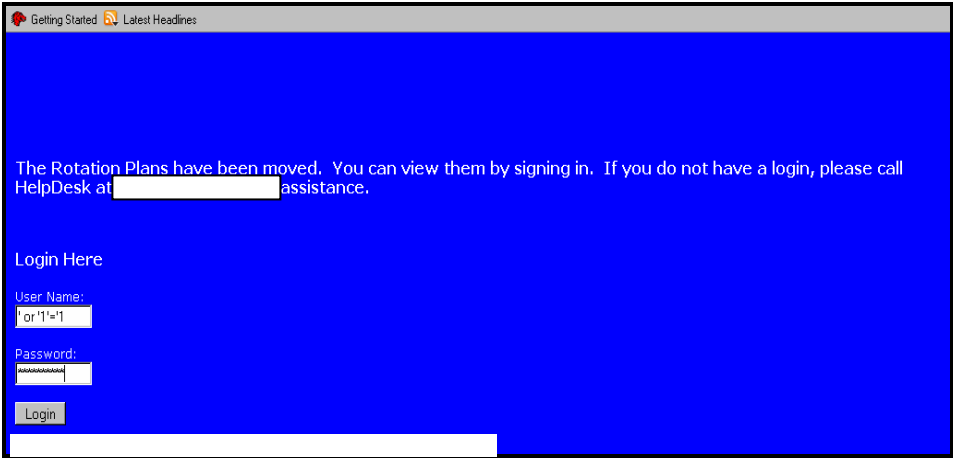
DRAFT

4 Appendix

This section provides the screen shots of the known vulnerabilities presented in the observations and findings table.

4.1 SQL Injection

IP: X.X.X.X



Penetration Testing Report

First record retrieved:

Getting Started Latest Headlines

Country: USA

Citizenship: UNITED STATES

Country Of Residence: UNITED STATES

Passport Info: †

Passport	
Date of Issue:	
Exp. Date:	
Issuing Country:	

* Please fill out this form with information exactly as it appears on your passport.
† Passport required for International travel, including all flights in/out of AK and HI

Contact Information

Permanent Address

Number and Street	
City	
State / Province	
Country	
Postal Code	

Done