Penetration Test Report

ON

Prepared By

Name : Md. Razlin Razwan.
Address : Dhaka, Bangladesh.
Phone Number : +8801711142130 (Whatsapp)
E-mail : razlin2013@gmail.com

Target Website: https://softopos.softologics.com

Build With:

Web Framework:	Laravel
Programming Language:	PHP
Version:	7.4.33
Web Server:	LiteSpeed
IP Address:	109.70.148.51

Dear Sir,

I am writing to submit the Penetration Testing Report for your Web_App, softopos.softologics.com. As a professional penetration tester, I have thoroughly assessed the security infrastructure of your Website and identified critical vulnerabilities that require immediate attention.

In summary, the penetration testing revealed several areas of concern, including potential weaknesses in network security, inadequate access controls, and vulnerabilities in web applications. These findings emphasize the importance of enhancing your organization's security posture to mitigate the risk of unauthorized access, data breaches, and potential financial loss.

In addition to the penetration testing report, I have included executive summaries and technical findings to provide you with a comprehensive understanding of the assessment.

I am available to answer any questions or provide further clarification regarding the findings and recommendations outlined in the report. Please do not hesitate to contact me at your convenience.

Thank you for your time and consideration. I look forward to the opportunity to contribute to the security and resilience of softopos.softologics.com.

Sincerely,
Razlin Razwan
+8801711142130
razlin2013@gmail.com

Attachments
Executive Summaries.
Penetration Testing Report.
Technical Findings.

Table of Contents

1. Executive Summary

This executive summary provides a concise overview of the findings and recommendations from the recent penetration testing conducted for softopos.softologics.com. This summary highlights the key vulnerabilities and risks discovered during the assessment, as well as the recommended actions to improve the organization's security posture.

The assessment was performed using a variety of penetration testing tools and techniques, including:

Network scanning,
Port scanning,
Vulnerability scanning,
Web application testing,
Social engineering testing,
Physical security assessment.

2. Open Web Application Security Project (OWASP) vulnerabilities

1. Injection

Injection flaws occur when untrusted data is sent to an interpreter as part of a command or query. This can lead to malicious code execution, unauthorized data access, and other harmful activities.

2. Broken Authentication and Session Management

Weaknesses in authentication and session management mechanisms can enable attackers to bypass authentication, hijack sessions, or impersonate users, resulting in unauthorized access to sensitive data or functionality.

3. Cross-Site Scripting (XSS)

XSS vulnerabilities occur when an application allows untrusted data to be included in a web page without proper validation or sanitization. This can allow attackers to inject malicious scripts into web pages viewed by other users, leading to session hijacking, defacement, or the theft of sensitive information.

4. Broken Access Control

Inadequate access controls can allow unauthorized users to access restricted functionality or data. This vulnerability can be exploited to perform actions reserved for privileged users or access sensitive information.

5. Security Misconfiguration

Security misconfigurations can occur at any level of an application's architecture, including the web server, application server, database, or framework. These misconfigurations can provide attackers with valuable information or access to sensitive resources.

6. Cross-Site Request Forgery (CSRF)

CSRF vulnerabilities enable attackers to trick authenticated users into performing unintended actions on a website without their knowledge or consent. This can lead to actions performed on behalf of the victim, potentially resulting in account compromise or data manipulation.

7. Using Components with Known Vulnerabilities

Using outdated or vulnerable components, such as libraries, frameworks, or plugins, can expose applications to known security flaws. Attackers often target these components to exploit their weaknesses and gain unauthorized access to the application or its data.

8. Insecure Deserialization

Insecure deserialization vulnerabilities occur when untrusted data is used to exploit flaws in an application's deserialization process. This can lead to remote code execution, injection attacks, or other malicious activities.

9. XML External Entity (XXE) Attacks

XXE vulnerabilities arise when an application parses XML input insecurely, allowing an attacker to read local files, perform remote code execution, or conduct denial-of-service attacks.

10. Insufficient Logging and Monitoring

Insufficient logging and monitoring can make it difficult to detect and respond to security incidents effectively. Without proper logs and monitoring mechanisms, malicious activities can go unnoticed, delaying incident response and recovery.

3. Analysis by Risk Factor

Total alerts found 8

High 0
Medium 3
Low 4
Informational 1

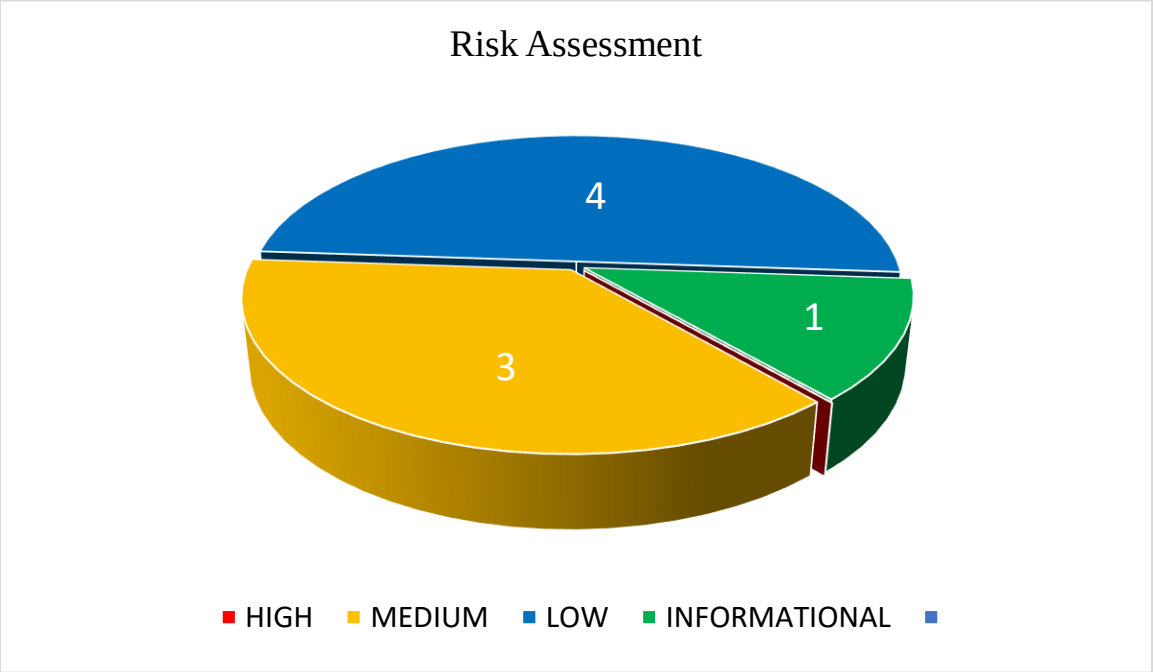
4. Criteria for Risk Assessments

Please find below a summary of the guidelines for assigning risk ratings to identified vulnerabilities:

Risk Assessments	Description
HIGH	Vulnerabilities classified as "Red Alert High Severity" typically have the potential to be exploited by attackers to gain unauthorized access, compromise sensitive data, or disrupt critical services. These vulnerabilities often have a high likelihood of exploitation and can result in severe consequences such as financial loss, reputational damage, or legal implications. The severity rating of "Red Alert High Severity" serves as a clear indicator that urgent action is required to safeguard the systems and protect against potential cyber threats.
MEDIUM	Vulnerabilities classified as "Orange Alert Moderate Severity" have the potential to be exploited by attackers to gain unauthorized access, compromise data, or disrupt services to some extent. While the consequences may not be as immediate or severe as with high-severity vulnerabilities, they still require attention and action to mitigate the risks.
	During a penetration test, when a vulnerability is assigned a "Blue Alert Low Severity," it means that it may not require immediate prioritization or significant resources for remediation. These

LOW	vulnerabilities are often minor security concerns that can be addressed as part of routine maintenance or during the next regular update cycle.
INFORMATIONAL	During a penetration test, "Green Alert Informational" findings can serve as educational opportunities for organizations to better understand security best practices, stay updated with current threats, and address potential weaknesses before they become significant vulnerabilities.

5. Website Risk Assessments by Chart



6. Medium-Risk Findings

6.1 Clickjacking: X-Frame-Options header

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The server did not

return an X-Frame-Options header with the value “DENIES” or “SAMEORIGIN”, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

Impact: The "Referer" header can be modified or removed by the browser or by browser plugins, making it unreliable for security purposes.

Proof of Reference (Code Snippet):

```
GET /login HTTP/1.1 Referer:
https://softopos.softologics.com/
Cookie: XSRF-
TOKEN=eyJpdiI6ImpxaWdDbmhHcEFIejVKTW8wcUVERWc9PSIsInZhbHVlI
joiQlRneWEzaFpRaEtNVTd2Tm9GVVVkd0ZqUWNNV0cwWU52bzhmMHRXQ0ZD
YmNobkc3UzRTaHZzeTVvaWdYWHJCa1FzVnY2aXZQYkVLZktpT3BrR1wveVd
iQjFMXC9PejZcLzdVZ2hGaElyOHFQbFdiaUF4aCtaU0ZudGpSaW1ONFRnaT
IiLCJtYWMiOiIwZDhiMjg5MTA0YjBmMjY5ODVmMDY0NGU4NmMxYmQyZjg1M
mUxYWZkNmE5ZGVlMTA0YjM3YmFjNWE0NmNmNjU1In0%3D;
salepropos_session=eyJpdiI6IlRwQ1lLbW5wR2xrK2xkVDBSUFNaZ2c9
PSIsInZhbHVlIjoiaURiUGFQMmZObmREbUgyWFVacUxBdms2V21KSFNOWUp
IZEdvQk5LU0RHc1dYYU1xYWp2Z25jRmRsVUwwODVJWG1VaXNWNFdzc3A4eH
BwSWtUc0NqQVoxbWxyNUQ4dExicDFaWUtLb3RST2I5TnJzVjk4SzRUbmFOY
jcxSmV5XC8xIiwibWFjIjoiZGJkYTMxYjg3YTdkNGU3Yjg1MGYyMWMwOTdk
ODkwNjJkNGMxMmQwNzE5YTM3ODcwOGY1NzE0OWI3N2VlNzRkMyJ9
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q
=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0
Safari/537.36
Host: softopos.softologics.com
Connection: Keep-alive
```

Recommended Solution:

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References:

OWASP Clickjacking
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

6.2 Content Security Policy (CSP) not implemented

Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. Content Security Policy (CSP) can be implemented by adding a Content-Security-Policy header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

Impact: The "Referer" header can be modified or removed by the browser or by browser plugins, making it unreliable for security purposes.

Proof of Reference (Code Snippet):
```
GET /login HTTP/1.1 Referer:
https://softopos.softologics.com/
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q
=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0
Safari/537.36
Host: softopos.softologics.com
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the Content Security-Policy HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

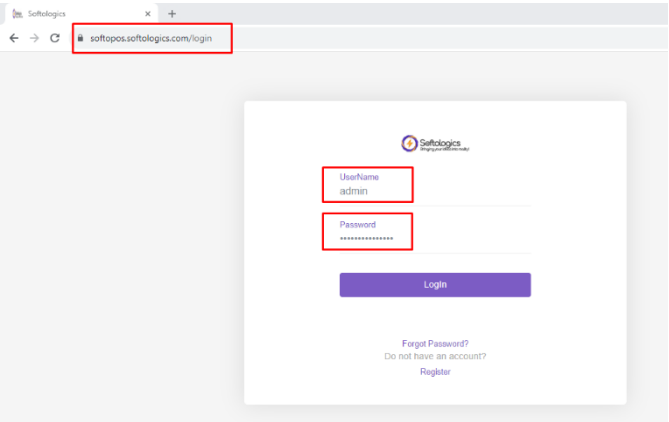
References
Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

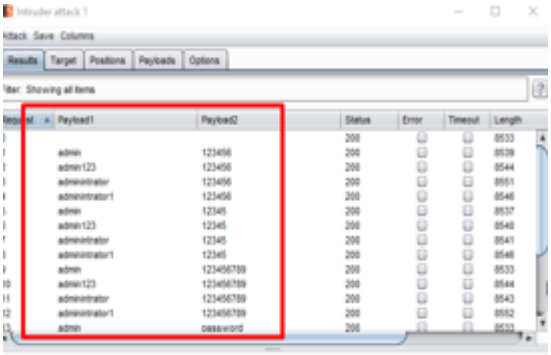
6.3 Brute Force Attack and No Limited Login Setup

Description:

This website do not have login limit for that reason Hackers can easily try to find the username and password for admin panel.

Proof of Reference:





Solution:

To secure the login page and brute force attack from attackers/hackers there are both free and paid tools. Using this types of tools this attack can be stopped.

7 Low-Risk Findings

7.1 Vulnerable JavaScript libraries

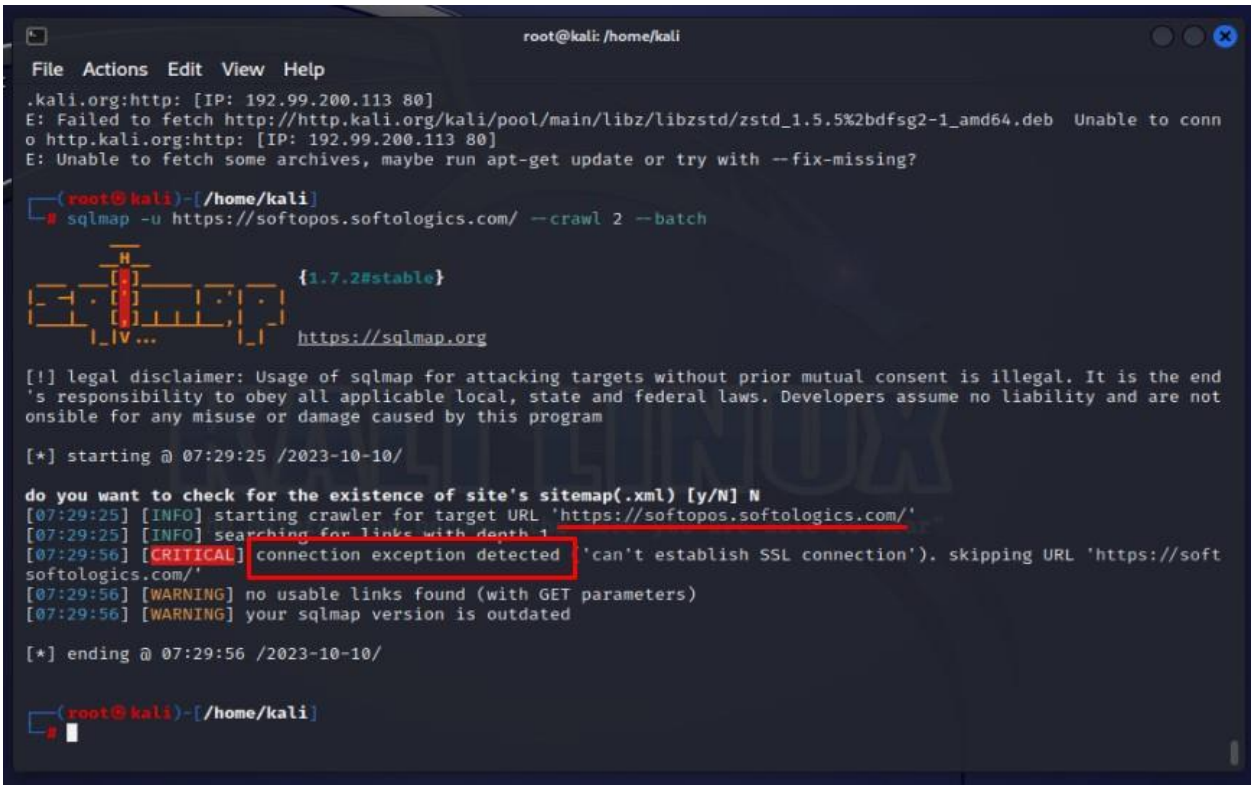
```
GET /public/js/app.js HTTP/1.1 Referer:
https://softopos.softologics.com/password/reset

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0
Safari/537.36
Host: softopos.softologics.com
Connection: Keep-alive
```

7.2 TLS/SSL certificate about to expire

Description:
One of the TLS/SSL certificates used by your server is about to expire. Once the certificate has expired, most web browsers will present end-users with a security warning, asking them to manually confirm the authenticity of your certificate chain. Software or automated systems may silently refuse to connect to the server. This alert is not necessarily caused by the server (leaf) certificate, but may have been triggered by an intermediate certificate. Please refer to the certificate serial number in the alert details to identify the affected certificate.

Prof of Reference:



Impact:
If an application server detects an expired certificate with a system it is communicating with, the application server may continue processing data as if nothing happened, or the connection may be abruptly terminated.

Solution:
Contact your Certificate Authority to renew the SSL certificate.

7.3 Permissions-Policy header not implemented

```
GET /login HTTP/1.1
Referer: https://softopos.softologics.com/
Cookie: XSRF-
TOKEN=eyJpdiI6ImpxaWdDbmhHcEFIejVKTW8wcUVERWc9PSIsInZhbHVlIjoiQl
RneWEzaFpRaEtNVTd2Tm9GVVVkd0ZqUWNNV0cwWU52bzhmMHRXQ0ZDYmNobkc3Uz
RTaHZzeTVvaWdYWHJCa1FzVnY2aXZQYkVLZktpT3BrR1wveVdiQjFMXC9PejZcLz
dVZ2hGaElyOHFQbFdiaUF4aCtaU0ZudGpSaW1ONFRnaTIiLCJtYWMiOiIwZDhiMj
g5MTA0YjBmMjY5ODVmMDY0NGU4NmMxYmQyZjg1MmUxYWZkNmE5ZGVlMTA0YjM3Ym
FjNWE0NmNmNjU1In0%3D;
salepropos_session=eyJpdiI6IlRwQ1lLbW5wR2xrK2xkVDBSUFNaZ2c9PSIsI
nZhbHVlIjoiaURiUGFQMmZObmREbUgyWFVacUxBdms2V21KSFNOWUpIZEdvQk5LU
0RHc1dYYU1xYWp2Z25jRmRsVUwwODVJWG1VaXNWNFdzc3A4eHBwSWtUc0NqQVoxb
WxyNUQ4dExicDFaWUtLb3RST2I5TnJzVjk4SzRUbmFOYjcxSmV5XC8xIiwibWFjI
joiZGJkYTMxYjg3YTdkNGU3Yjg1MGYyMWMwOTdkODkwNjJkNGMxMmQwNzE5YTM3O
DcwOGY1NzE0OWI3N2VlNzRkMyJ9
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0
Safari/537.36
Host: softopos.softologics.com
Connection: Keep-alive
```

7.4 Open Ports:

Impacts:

Hackers/Attackers can use these services in conjunction with open ports to gain unauthorized access to sensitive data.

Prof of Reference:

https://softopos.softologics.com/login

Open Ports

21
22
80
53
143
993
443
587
3306
995
110

Unable to establish connections to:
20, 23, 25, 67, 68, 69, 119, 123, 156, 161, 162, 179, 194, 389, 3000, 3389, 5060, 5900, 8000, 8080, 8888

```
File  Actions  Edit  View  Help
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

┌──(kali㉿kali)-[~]
└─$ nmap softopos.softologics.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-10 09:00 GMT
Nmap scan report for softopos.softologics.com (109.70.148.51)
Host is up (0.97s latency).
rDNS record for 109.70.148.51: snakebite.hostns.io
Not shown: 962 filtered tcp ports (no-response), 25 filtered tcp ports (host-unreach)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql
5960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 198.31 seconds

┌──(kali㉿kali)-[~]
└─$
```

OPEN PORTS

8 Informational -Risk Detection

8.1 HTTP Strict Transport Security (HSTS) not following best practices

Description:

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict Transport Security (HSTS) implementation is not as strict as is typically advisable.

Impact:

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle attacks.

Solution:

It is recommended to implement best practices of HTTP Strict Transport Security (HSTS) in your web application.

9 Conclusion

Finally, I have completed the penetration & vulnerability test of the web application. These tests have been based on technology and known threats to date in this document. All safety issues discovered during this exercise have been analyzed and described in this report. Please note that as technology and risks change over time, so will the vulnerabilities associated with the operation of the systems described in this report, as well as the steps required to reduce the exposure to such vulnerabilities testing, organizations can fortify their websites and demonstrate their commitment to maintaining a secure online environment.