Penetration Testing Report

Client: Nicalc: Software Provider for Bookstores

Conducted By: Group 4 (Evgeni Kurtev, Renis Hila, Stefan-Nikola Stanev, Naadir Twahir, Nikolay Gruychev, Thomas Vasanth, Vlad Bucur)

Date: 11-06-2024

Table of contents

Executive Summary

Objective

The objective of this penetration test was to identify vulnerabilities in the client's website and provide recommendations to enhance its security. The client, a small company providing software for bookstores called Nicalc, requested this assessment to be conducted without DDOS testing to ensure uninterrupted service.

Scope

The scope of this test included all types of attacks, excluding DDOS or other actions that could shut down the website. The focus was on identifying security holes that the client can address to improve their security posture.

Key Findings

1. Open ports on the server, including SMTP (port 25) and IMAP (port 143), without mandatory SSL.

2. Potential directory listing vulnerabilities indicated by Dirbuster results.

3. XSS attempts blocked by site owner validation in the comments section.

4. Site was protected against brute force login attempts.

5. SQL Injection attempts on the SMTP server were secured.

6. XSS attempts did not manage to breach the security and were blocked.

7. Command Injection attempts did not find any vulnerabilities.

Recommendations

- Configure your email servers to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols to encrypt the communication between email clients and servers. This ensures that the data transmitted is secure and cannot be easily intercepted or read by unauthorized parties.

- Evaluate and adjust the settings and configurations of directories (folders) on a web server to ensure that only authorized users can access or modify the files and directories. This is crucial for preventing unauthorized users, including attackers, from accessing sensitive information or exploiting vulnerabilities.

Methodology

Tools Used

- **Dirbuster**: For directory and file brute-forcing.

- **Burp Suite**: For intercepting and analyzing web traffic.

- **Hydra**: For brute-force attacks on login credentials.

- **NsLookup.io**: For hosting + extra information.

Steps Taken

1. **Reconnaissance**: Identified the target IP address and collected basic information about the server and services running.

2. **Scanning**: Used tools like Dirbuster to identify hidden directories and files.

3. **Exploitation**: Attempted various attacks including XSS, SQL Injection, and brute-force login. Tested for XSS and Command Injection: Checked different input fields to find possible vulnerabilities.

4. **Post-Exploitation**: Analyzed the results to determine potential impacts and recommend mitigations.

Findings

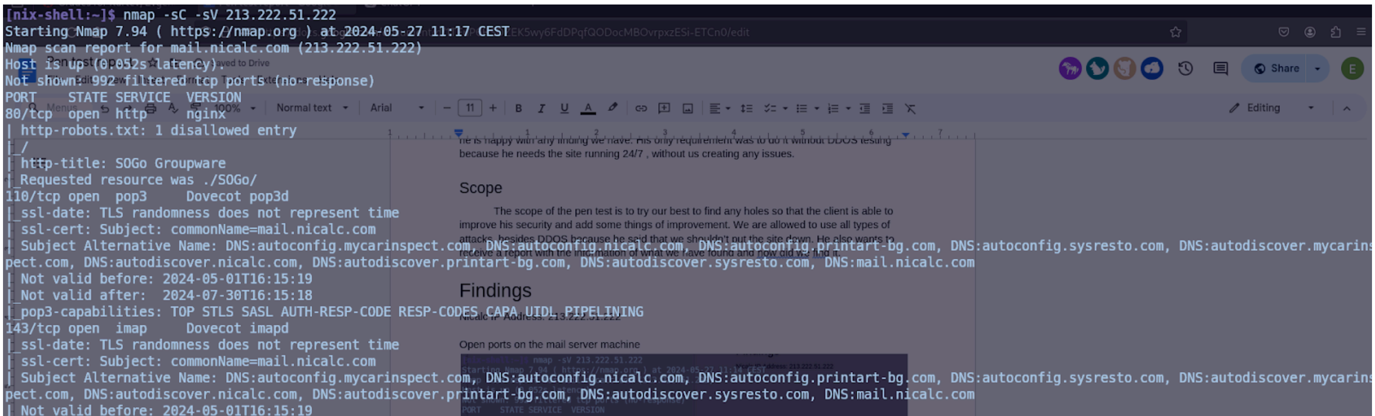
Open Ports

- **SMTP (Port 25)**: We examined the open ports and found that the SMTP port was not using SSL/TLS. This means the communication between the email client and server is not encrypted, which could expose sensitive information.

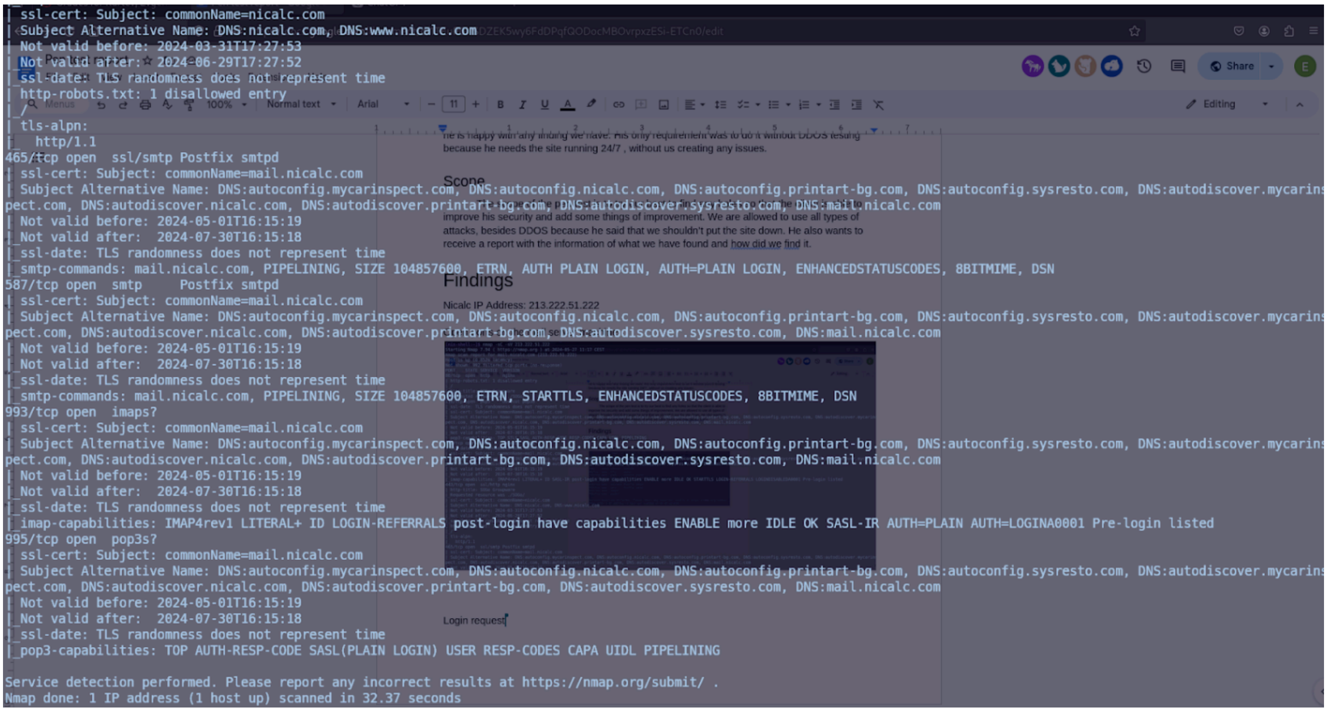
- **MAP (Port 143)**: No mandatory SSL/TLS. Similar to the SMTP port, the IMAP port was also not using SSL/TLS, which poses a security risk.

- **Port 4190 (Sieve)**: We found this port open and noted that it could be targeted to change mail filtering rules maliciously.

Below screenshots of nmap scan:



```
[nix-shell:~]$ nmap -sC -sV 213.222.51.222
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-27 11:17 CEST
Nmap scan report for mail.nicalc.com (213.222.51.222)
Host is up (0.052s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
| http-robots.txt: 1 disallowed entry
|_/
| http-title: SOGo Groupware
|_Requested resource was ./SOGo/
110/tcp open  pop3     Dovecot pop3d
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mail.nicalc.com
| Subject Alternative Name: DNS:autoconfig.mycarinspect.com, DNS:autoconfig.nicalc.com, DNS:autoconfig.printart-bg.com, DNS:autoconfig.sysresto.com, DNS:autodiscover.mycarins
pect.com, DNS:autodiscover.nicalc.com, DNS:autodiscover.printart-bg.com, DNS:autodiscover.sysresto.com, DNS:mail.nicalc.com
| Not valid before: 2024-05-01T16:15:19
|_Not valid after:  2024-07-30T16:15:18
|_pop3-capabilities: TOP STLS SASL AUTH-RESP-CODE RESP-CODES CAPA UIDL PIPELINING
143/tcp open  imap     Dovecot imapd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mail.nicalc.com
| Subject Alternative Name: DNS:autoconfig.mycarinspect.com, DNS:autoconfig.nicalc.com, DNS:autoconfig.printart-bg.com, DNS:autoconfig.sysresto.com, DNS:autodiscover.mycarins
pect.com, DNS:autodiscover.nicalc.com, DNS:autodiscover.printart-bg.com, DNS:autodiscover.sysresto.com, DNS:mail.nicalc.com
| Not valid before: 2024-05-01T16:15:19
```

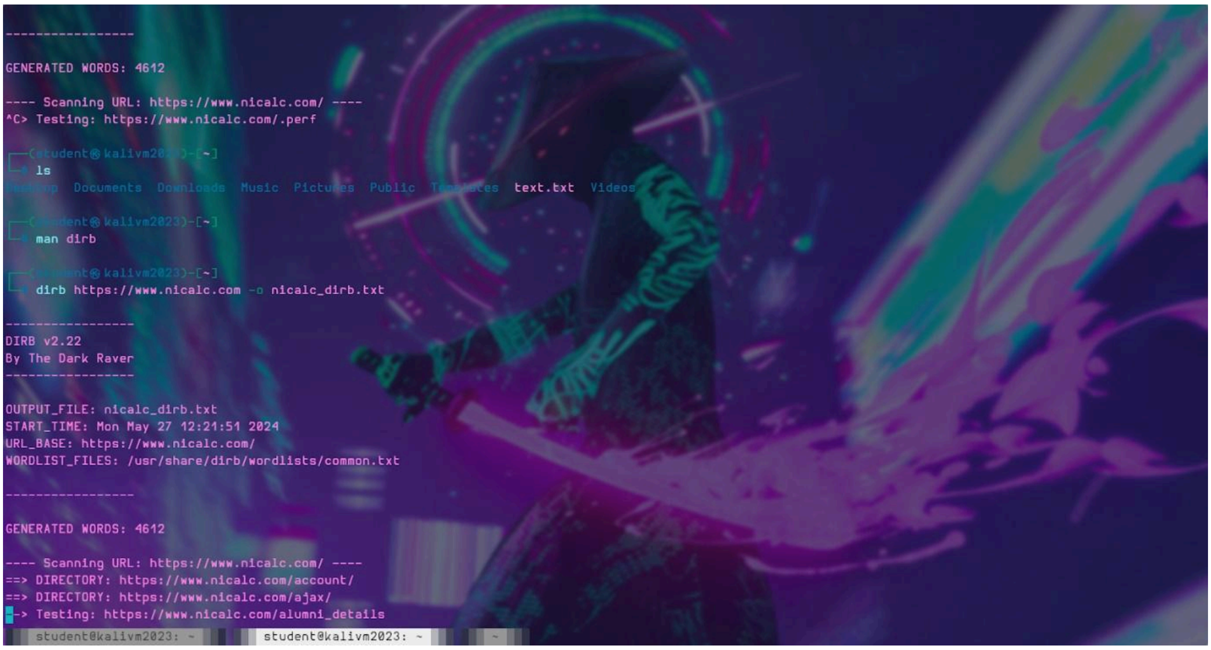


```
| ssl-cert: Subject: commonName=nicalc.com
| Subject Alternative Name: DNS:nicalc.com, DNS:www.nicalc.com
| Not valid before: 2024-03-31T17:27:53
|_Not valid after:  2024-06-29T17:27:52
|_ssl-date: TLS randomness does not represent time
| http-robots.txt: 1 disallowed entry
|_/
| tls-alpn:
|_  http/1.1
465/tcp open  ssl/smtp Postfix smtpd
| ssl-cert: Subject: commonName=mail.nicalc.com
| Subject Alternative Name: DNS:autoconfig.mycarinspect.com, DNS:autoconfig.nicalc.com, DNS:autoconfig.printart-bg.com, DNS:autoconfig.sysresto.com, DNS:autodiscover.mycarins
pect.com, DNS:autodiscover.nicalc.com, DNS:autodiscover.printart-bg.com, DNS:autodiscover.sysresto.com, DNS:mail.nicalc.com
| Not valid before: 2024-05-01T16:15:19
|_Not valid after:  2024-07-30T16:15:18
|_ssl-date: TLS randomness does not represent time
|_smtp-commands: mail.nicalc.com, PIPELINING, SIZE 104857600, ETRN, AUTH PLAIN LOGIN, AUTH=PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN
587/tcp open  smtp     Postfix smtpd
| ssl-cert: Subject: commonName=mail.nicalc.com
| Subject Alternative Name: DNS:autoconfig.mycarinspect.com, DNS:autoconfig.nicalc.com, DNS:autoconfig.printart-bg.com, DNS:autoconfig.sysresto.com, DNS:autodiscover.mycarins
pect.com, DNS:autodiscover.nicalc.com, DNS:autodiscover.printart-bg.com, DNS:autodiscover.sysresto.com, DNS:mail.nicalc.com
| Not valid before: 2024-05-01T16:15:19
|_Not valid after:  2024-07-30T16:15:18
|_ssl-date: TLS randomness does not represent time
|_smtp-commands: mail.nicalc.com, PIPELINING, SIZE 104857600, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
993/tcp open  imaps?
| ssl-cert: Subject: commonName=mail.nicalc.com
| Subject Alternative Name: DNS:autoconfig.mycarinspect.com, DNS:autoconfig.nicalc.com, DNS:autoconfig.printart-bg.com, DNS:autoconfig.sysresto.com, DNS:autodiscover.mycarins
pect.com, DNS:autodiscover.nicalc.com, DNS:autodiscover.printart-bg.com, DNS:autodiscover.sysresto.com, DNS:mail.nicalc.com
| Not valid before: 2024-05-01T16:15:19
|_Not valid after:  2024-07-30T16:15:18
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: IMAP4rev1 LITERAL+ ID LOGIN-REFERRALS post-login have capabilities ENABLE more IDLE OK SASL-IR AUTH=PLAIN AUTH=LOGINA0001 Pre-login listed
995/tcp open  pop3s?
| ssl-cert: Subject: commonName=mail.nicalc.com
| Subject Alternative Name: DNS:autoconfig.mycarinspect.com, DNS:autoconfig.nicalc.com, DNS:autoconfig.printart-bg.com, DNS:autoconfig.sysresto.com, DNS:autodiscover.mycarins
pect.com, DNS:autodiscover.nicalc.com, DNS:autodiscover.printart-bg.com, DNS:autodiscover.sysresto.com, DNS:mail.nicalc.com
| Not valid before: 2024-05-01T16:15:19
|_Not valid after:  2024-07-30T16:15:18
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: TOP AUTH-RESP-CODE SASL(PLAIN LOGIN) USER RESP-CODES CAPA UIDL PIPELINING

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.37 seconds
```

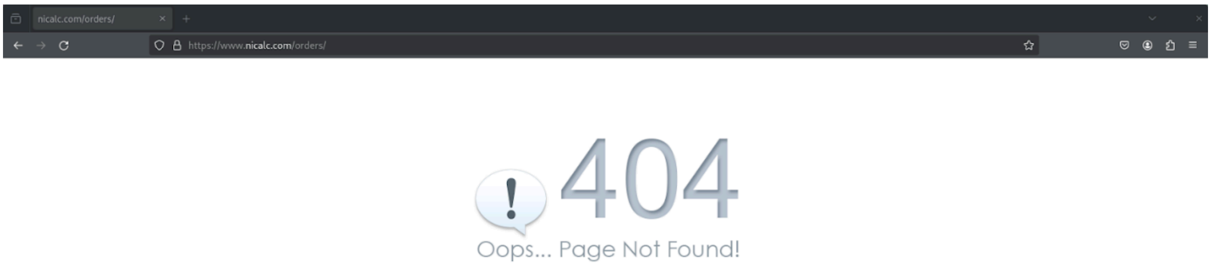
Directory Listing Vulnerability

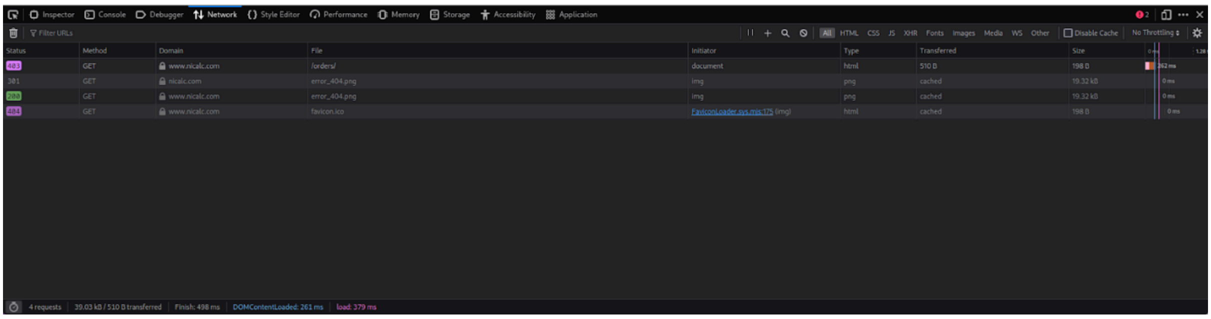
- **Dirbuster Results**: Pages that return 403 errors instead of 404, indicating possible hidden directories without proper index files.

Using Dirbuster, we discovered that several directories returned a 403 Forbidden error instead of a 404 Not Found error. This suggests that these directories exist but lack the appropriate index files, which could expose sensitive information.



```
-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://www.nicalc.com/ ----
^C> Testing: https://www.nicalc.com/.perf

┌──(student㉿kalivm2023)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  text.txt  Videos

┌──(student㉿kalivm2023)-[~]
└─$ man dirb

┌──(student㉿kalivm2023)-[~]
└─$ dirb https://www.nicalc.com -o nicalc_dirb.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: nicalc_dirb.txt
START_TIME: Mon May 27 12:21:51 2024
URL_BASE: https://www.nicalc.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://www.nicalc.com/ ----
==> DIRECTORY: https://www.nicalc.com/account/
==> DIRECTORY: https://www.nicalc.com/ajax/
--> Testing: https://www.nicalc.com/alumni_details
```





Status	Method	Domain	File	Initiator	Type	Transferred	Size
403	GET	www.nicalc.com	/orders/	document	html	510 B	198 B
301	GET	nicalc.com	error_404.png	img	png	cached	19.32 kB
200	GET	www.nicalc.com	error_404.png	img	png	cached	19.32 kB
404	GET	www.nicalc.com	favicon.ico	FaviconLoader.sys.mjs:175 (img)	html	cached	198 B

4 requests | 20.03 kB / 510 B transferred | Finish: 498 ms | DOMContentLoaded: 261 ms | load: 379 ms

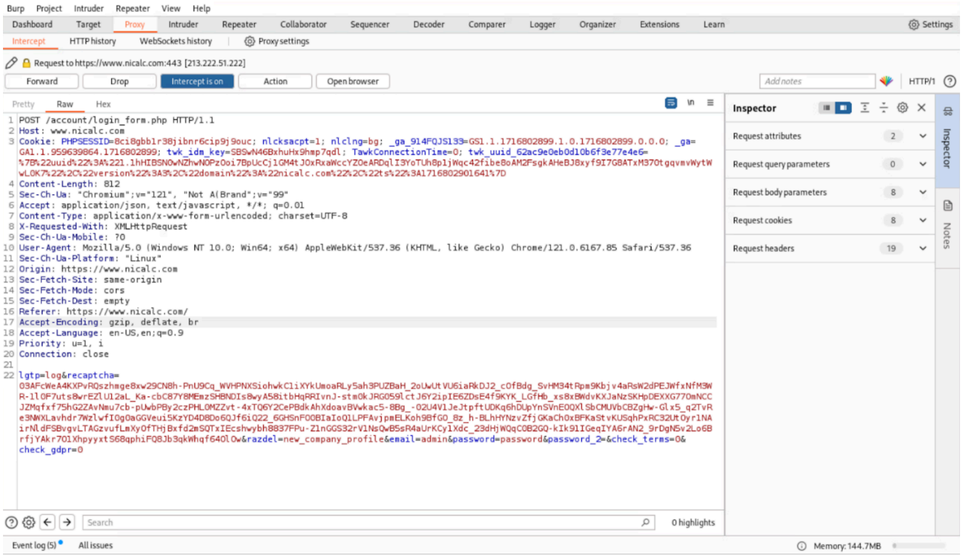
XSS Protection

- **Comments Section**: Attempts to inject XSS were blocked as comments required site owner validation.

We tried to inject XSS payloads in the comments section to see if we could execute malicious scripts. However, our attempts were unsuccessful because the comments required validation by the site owner, effectively blocking our attempts.

Brute-Force Attack

- **Login Interception**: We used Burp Suite to intercept login attempts and then employed Hydra to perform a brute-force attack on the login credentials. However, the site implemented a timeout mechanism and required strong passwords, which made our brute-force attempts unsuccessful.



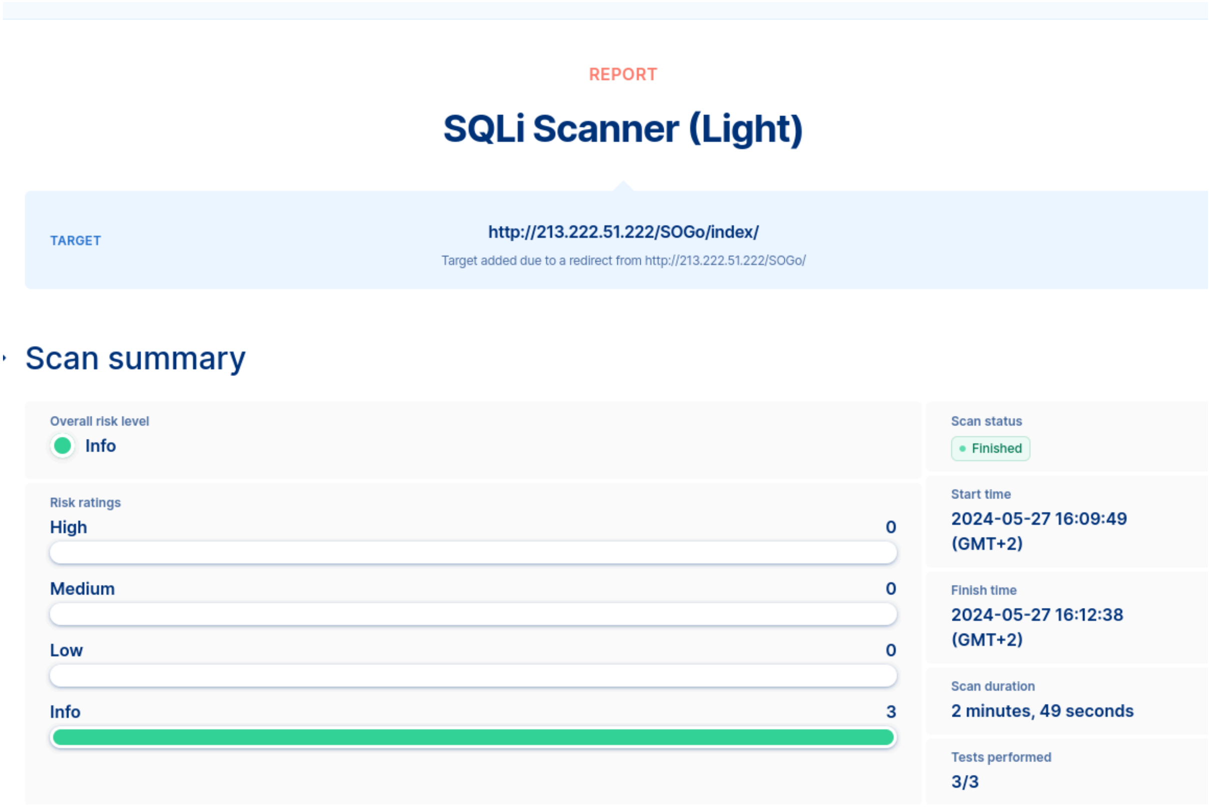
Request to https://www.nicalc.com:443 [213.222.51.222]

```
POST /account/login_form.php HTTP/1.1
Host: www.nicalc.com
Cookie: PHPSESSID=8ci8gbb1r38jibnr6cip9j9ouc; nlcksacpt=1; nlclng=bg; _ga_914FQJS133=GS1.1.1716802899.1.0.1716802899.0.0.0; _ga=
GA1.1.959639864.1716802899; twk_idm_key=SBSwN46BxhuHx9hmp7qdl; TawkConnectionTime=0; twk_uuid_62ac9e0eb0d10b6f3e77e4e6=
%7B%22uuid%22%3A%221.1hHIBSNOwNZhwNOPzOoi7BpUcCj1GM4tJOxRxaWccYZOeARDqlI3YoTUh8p1jWqc42fibe8oAM2FsgkAHeBJ8xyf9I7G8ATxM370tgqvmvWytW
wL0K7%22%2C%22version%22%3A3%2C%22domain%22%3A%22nicalc.com%22%2C%22ts%22%3A1716802901641%7D
Content-Length: 812
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Origin: https://www.nicalc.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.nicalc.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: close

lgtp=log&recaptcha=
03AFcWeA4KXPvRQszhmge8xw29CN8h-PnU9Cq_WVHPNXSiohwkC1iXYkUmoaRLy5ah3PUZBaH_2oUwUtVU6iaRkDJ2_cOfBdg_SvHM34tRpm9Kbjv4aRsW2dPEJWfxNfM3W
R-1l0F7uts8wrEZlU12aL_Ka-cbC87Y8MEmzSHBNDIs8wyA58itbHqRRIvnJ-stm0kJRG059lctJ6Y2ipIE6ZDsE4f9KYK_LGfHb_xs8xBWdvKXJaNzSKHpDEXXG770mNCC
JZMqfxf75hG2ZAvNmu7cb-pUwbPBy2czPHL0MZZvt-4xTQ6Y2CePBdkAhXdoavBVwkac5-8Bg_-02U4V1JeJtpftUDKq6hDUpYnSVnE0QXlSbCMUVbCBZgHw-Glx5_q2TvR
e3NWXLavhdr7WzlwfI0g0aGGVeui5KzYD4D8Do6QJf6iQ22_6GHSnFO0BIaIoQ1LPFAvjpmELKoh9BfG0_8z_h-BLhHYNzvZfjGKaCh0xBFKaStvKUSqhPxRC32Ut0yr1NA
irNldFSBvgvLTAGzvufLmXyOfTHjBxfd2mSQTxIEcshwybh8837FPu-Z1nGGS32rV1NsQwB5sR4aUrKCy1Xdc_23dHjWQqC0B2GQ-kIk91IGeqIYA6rAN2_9rDgN5v2Lo6B
rfjYAkr701XhpyyxtS68qphiFQ8Jb3qkWhqf640l0w&razdel=new_company_profile&email=admin&password=password&password_2=&check_terms=0&
check_gdpr=0
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	8
Request cookies	8
Request headers	19

SQL Injection

- We tested for SQL Injection by entering various SQL commands into input fields related to the SMTP server. For example, we used ' OR '1'='1 and other common SQL injection strings. The server effectively sanitized the inputs and prevented any SQL commands from executing, indicating robust protection against SQL injection.



REPORT

SQLi Scanner (Light)

TARGET http://213.222.51.222/SOGo/index/
Target added due to a redirect from http://213.222.51.222/SOGo/

Scan summary

Overall risk level
● Info

Risk ratings

High	0
Medium	0
Low	0
Info	3

Scan status
Finished

Start time
2024-05-27 16:09:49 (GMT+2)

Finish time
2024-05-27 16:12:38 (GMT+2)

Scan duration
2 minutes, 49 seconds

Tests performed
3/3

Cross-Site Scripting (XSS)

- Many areas were tested, including search fields and user input forms. All XSS attempts were blocked, and no vulnerabilities were found. We manually entered various JavaScript payloads into search fields, comment sections, and other user input areas. Examples of payloads included <script>alert('XSS')</script> and other common XSS attack vectors. Each attempt was blocked by the website's input validation and output encoding mechanisms, demonstrating strong defenses against XSS attacks.

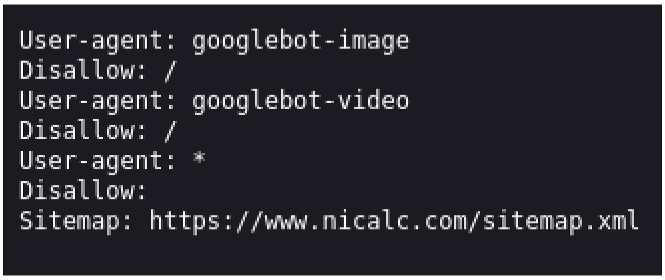
Attacks like this could lead to potential risk for the client,but since they have multiple filtering options it is very hard for us to manage to do something without having access to the filtering software.

Command Injection

- Various input fields and backend scripts were tested for command injection vulnerabilities. We manually tested by entering specially crafted strings into form fields to see if they would execute system commands. For instance, we tried inputs like ` ; ls, | whoami `, and & `cat /etc/passwd` in different fields and URLs. The server consistently sanitized these inputs, preventing any command execution and indicating robust defenses against command injection.

Robots.txt

- We examined the robots.txt file and found no significant vulnerabilities. This file contained standard directives to web crawlers, and there were no exposed sensitive directories or files.



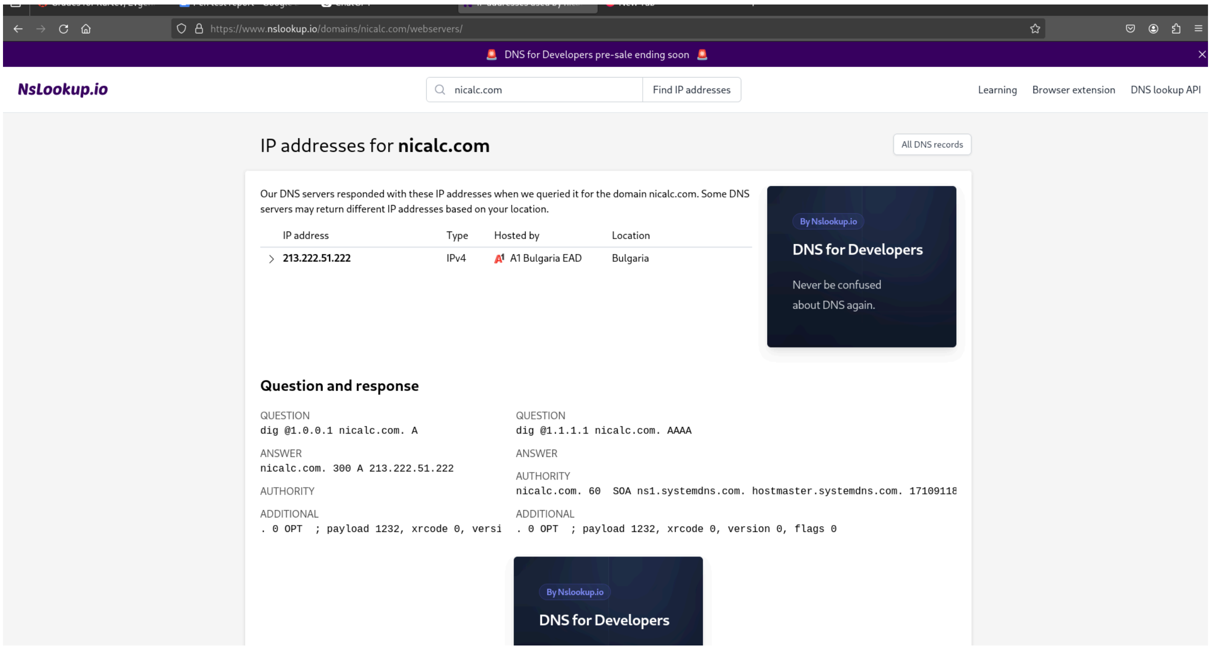
```
User-agent: googlebot-image
Disallow: /
User-agent: googlebot-video
Disallow: /
User-agent: *
Disallow:
Sitemap: https://www.nicalc.com/sitemap.xml
```

Hydra attack

We tried to attack the SoGo login page using hydra but it didn’t work. SoGo has very nice protection against different attacks like brute force,XSS and much more. For more information check SoGo’s CVE page.

DNS lookup

We also tried DNS lookup but unfortunately we couldn't find anything that we can use.



IP addresses for **nicalc.com**

Our DNS servers responded with these IP addresses when we queried it for the domain nicalc.com. Some DNS servers may return different IP addresses based on your location.

IP address	Type	Hosted by	Location
213.222.51.222	IPv4	A1 Bulgaria EAD	Bulgaria

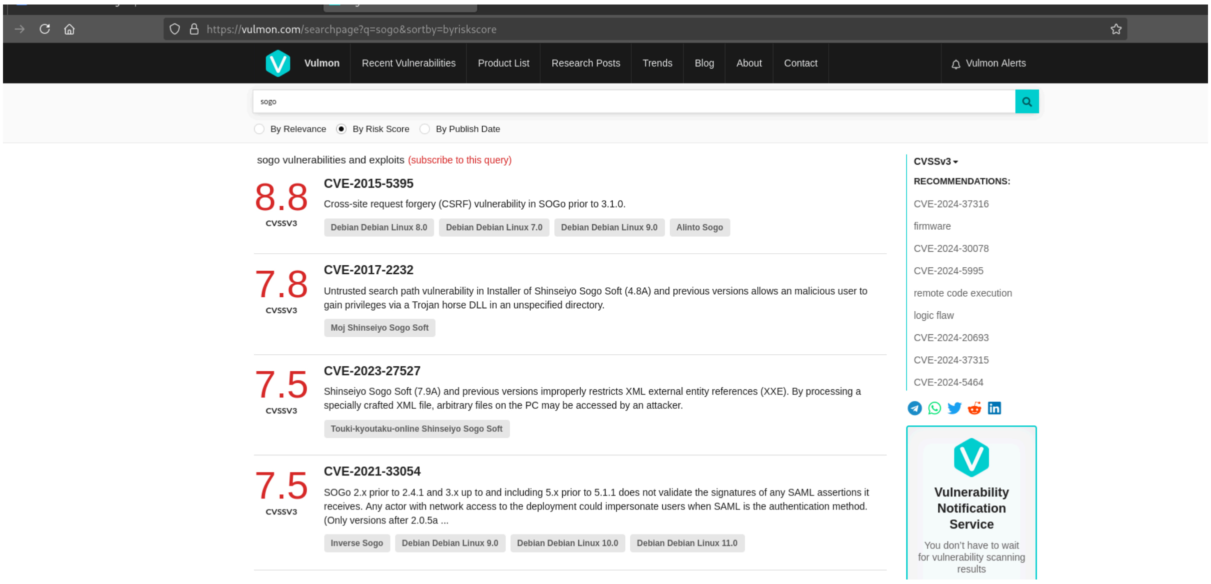
Question and response

```
QUESTION
dig @1.0.0.1 nicalc.com. A
ANSWER
nicalc.com. 300 A 213.222.51.222
AUTHORITY
ADDITIONAL
. 0 OPT  ; payload 1232, xrcode 0, versi
```

```
QUESTION
dig @1.1.1.1 nicalc.com. AAAA
ANSWER
AUTHORITY
nicalc.com. 60  SOA ns1.systemdns.com. hostmaster.systemdns.com. 17109118
ADDITIONAL
. 0 OPT  ; payload 1232, xrcode 0, version 0, flags 0
```

SoGo CVEs

This is the list with CVEs related to SoGo. As you can see the most crucial ones are solved and also there aren’t any new ones.



https://vulmon.com/searchpage?q=sogo&sortby=byriskscore
Vulmon
Recent Vulnerabilities
Product List
Research Posts
Trends
Blog
About
Contact
Vulmon Alerts
sogo
○ By Relevance ● By Risk Score ○ By Publish Date

sogo vulnerabilities and exploits (subscribe to this query)

8.8 CVSSV3 **CVE-2015-5395**

Cross-site request forgery (CSRF) vulnerability in SOGo prior to 3.1.0.

Debian Debian Linux 8.0 | Debian Debian Linux 7.0 | Debian Debian Linux 9.0 | Alinto Sogo

7.8 CVSSV3 **CVE-2017-2232**

Untrusted search path vulnerability in Installer of Shinseiyo Sogo Soft (4.8A) and previous versions allows an malicious user to gain privileges via a Trojan horse DLL in an unspecified directory.

Moj Shinseiyo Sogo Soft

7.5 CVSSV3 **CVE-2023-27527**

Shinseiyo Sogo Soft (7.9A) and previous versions improperly restricts XML external entity references (XXE). By processing a specially crafted XML file, arbitrary files on the PC may be accessed by an attacker.

Touki-kyoutaku-online Shinseiyo Sogo Soft

7.5 CVSSV3 **CVE-2021-33054**

SOGo 2.x prior to 2.4.1 and 3.x up to and including 5.x prior to 5.1.1 does not validate the signatures of any SAML assertions it receives. Any actor with network access to the deployment could impersonate users when SAML is the authentication method. (Only versions after 2.0.5a ...

Inverse Sogo | Debian Debian Linux 9.0 | Debian Debian Linux 10.0 | Debian Debian Linux 11.0

CVSSv3

RECOMMENDATIONS:

CVE-2024-37316
firmware
CVE-2024-30078
CVE-2024-5995
remote code execution
logic flaw
CVE-2024-20693
CVE-2024-37315
CVE-2024-5464

Vulnerability Notification Service

You don't have to wait for vulnerability scanning results

Sieve

One of the best ways to get access to the system would be through manipulating Sieve and maliciously flooding SoGo. We tried to get access to the sieve service running on port 4190,but we couldn't reach it and gain control over the mail filtering.

Recommendations

1. **Implement SSL/TLS for SMTP and IMAP**: Encrypt communication channels to protect sensitive information and prevent eavesdropping.

2. **Review Directory Permissions**: Ensure proper permissions and configuration to prevent unauthorized access to directories and files.

3. **Enhance Input Validation**: Continue to use site owner validation for comments and apply similar measures across the site to prevent XSS.

4. **Rate Limiting and Account Lockout**: Implement these mechanisms to mitigate the risk of brute-force attacks on login forms.

5. **Regular Updates and Patching**: Keep all systems and software up-to-date to protect against known vulnerabilities.

6.**Close ports:** close the open port for the Sieve service