Sri Lanka Institute of Information Technology

Assignment report 07

IT22357762

Web Security -IE2062

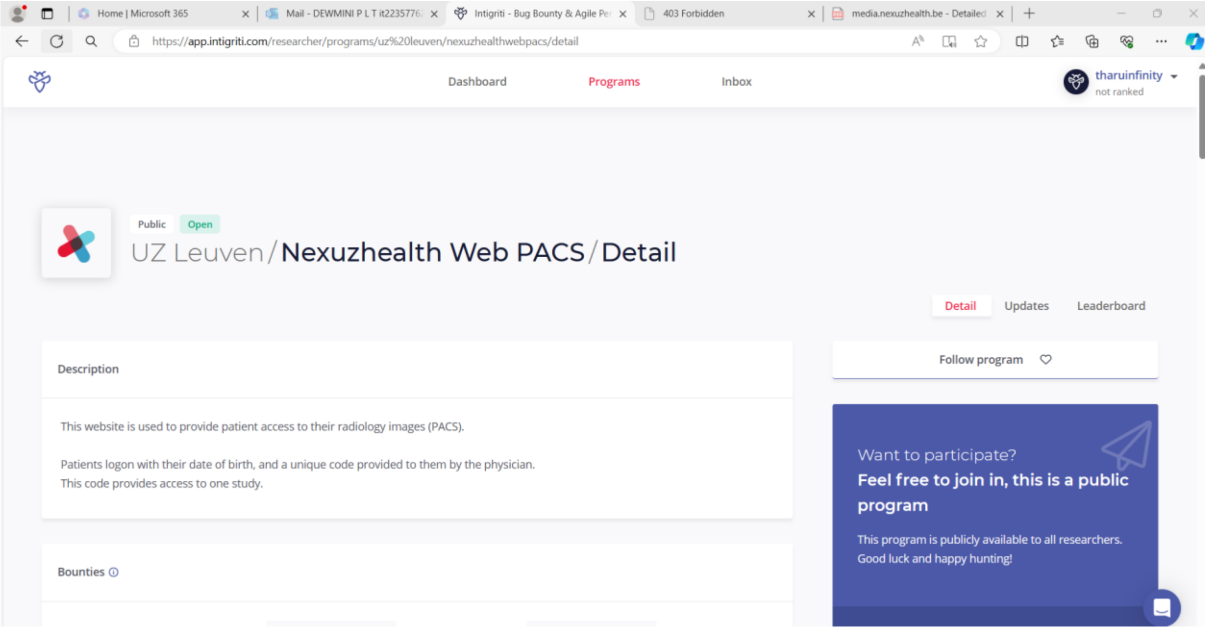
Web Security – IE2062

B.Sc. (Hons) in Information

Contents

1 https://media.nexuzhealth.be

This website serves as a platform for patients to access their radiological images (PACS).Patients authenticate themselves by entering their date of birth and a unique code issued by their physician.


Home | Microsoft 365
Mail - DEWMINI P L T it2235776
Intigriti - Bug Bounty & Agile Pe
403 Forbidden
media.nexuzhealth.be - Detailed
https://app.intigriti.com/researcher/programs/uz%20leuven/nexuzhealthwebpacs/detail
Dashboard
Programs
Inbox
tharuinfinity
not ranked
Public
Open
Detail
Updates
Leaderboard
Follow program
Bounties

UZ Leuven / Nexuzhealth Web PACS / Detail

Description

This website is used to provide patient access to their radiology images (PACS).

Patients logon with their date of birth, and a unique code provided to them by the physician.
This code provides access to one study.

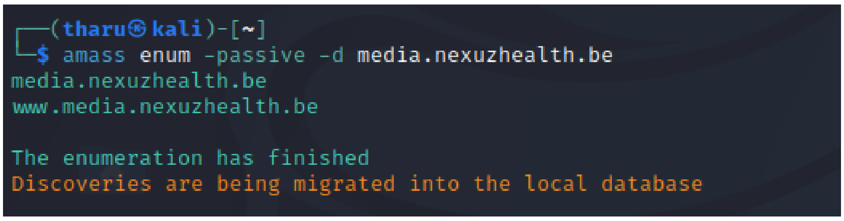
Want to participate?
Feel free to join in, this is a public program

This program is publicly available to all researchers.
Good luck and happy hunting!

1.1 Sub- domain list

Tool – amass

Command – amass enum -passive -d media.nexuzhealth.be



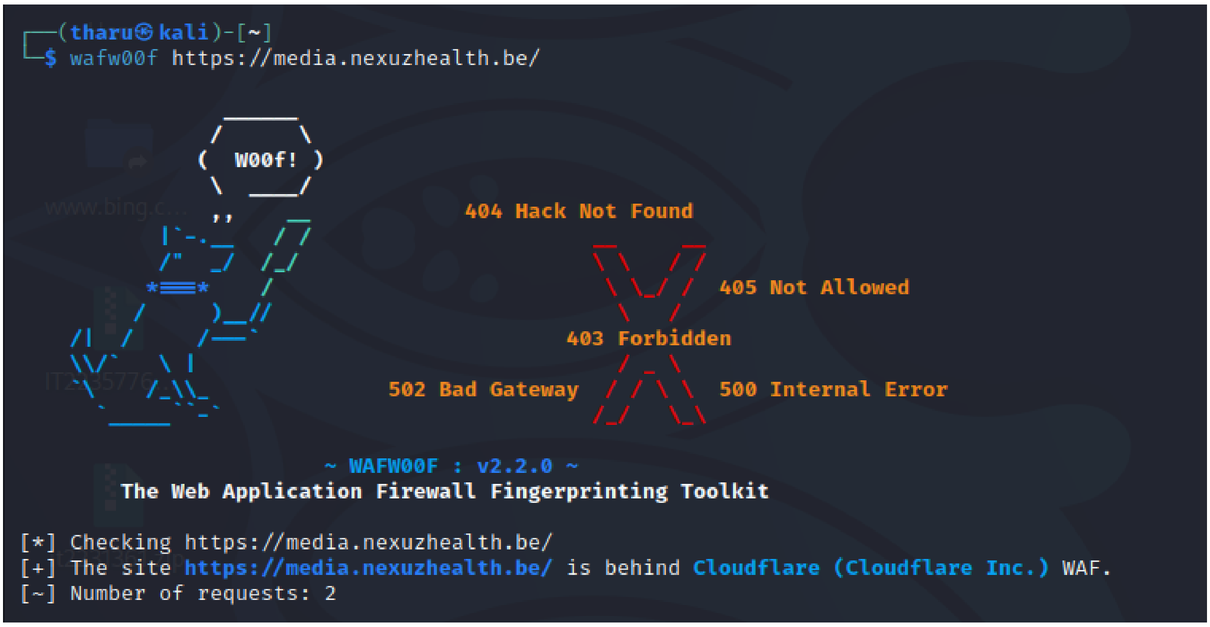
```
┌──(tharu㉿kali)-[~]
└─$ amass enum -passive -d media.nexuzhealth.be
media.nexuzhealth.be
www.media.nexuzhealth.be

The enumeration has finished
Discoveries are being migrated into the local database
```

Sub domain list –

- media.nexuzhealth.be
- www.media.nexuzhealth.be

1.2 Firewall detection

Command – wafw00f https:// media.nexuzhealth.be /

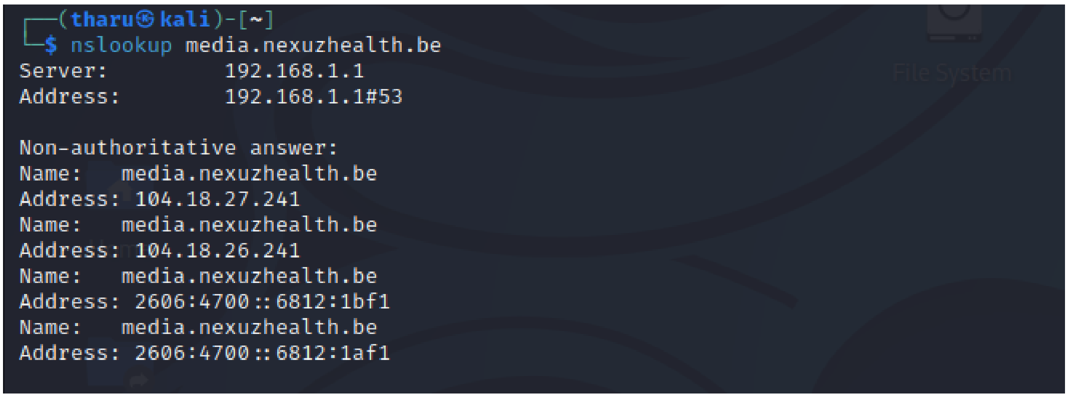


```
┌──(tharu㉿kali)-[~]
└─$ wafw00f https://media.nexuzhealth.be/

                ( W00f! )

                              404 Hack Not Found

                                             405 Not Allowed

                                  403 Forbidden

                         502 Bad Gateway          500 Internal Error

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://media.nexuzhealth.be/
[+] The site https://media.nexuzhealth.be/ is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

1.3 IP scanning

Tool – nslookup

Command – nslookup media.nexuzhealth.be

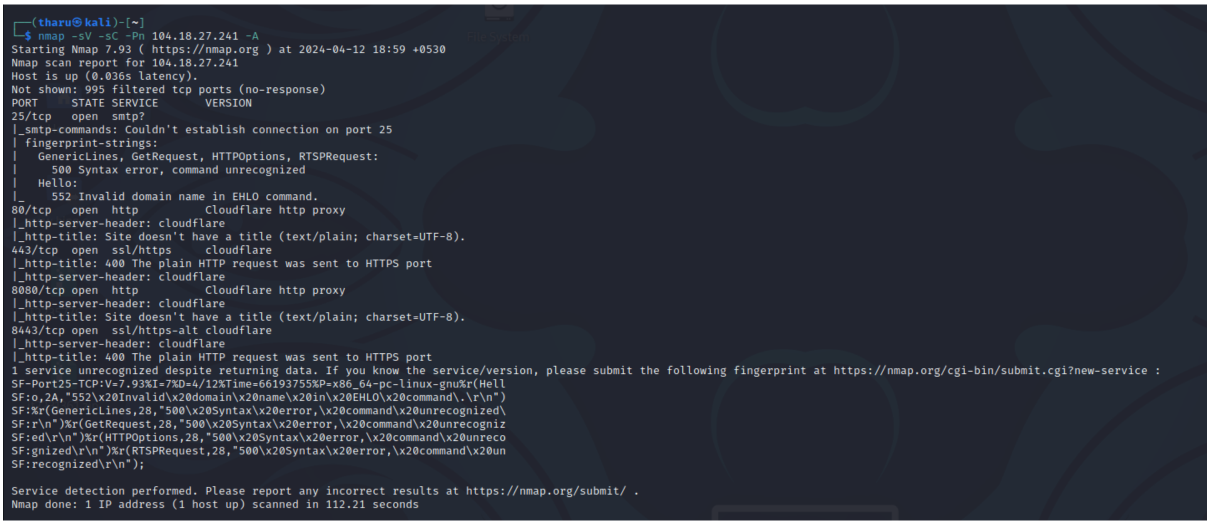


```
┌──(tharu㉿kali)-[~]
└─$ nslookup media.nexuzhealth.be
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   media.nexuzhealth.be
Address: 104.18.27.241
Name:   media.nexuzhealth.be
Address: 104.18.26.241
Name:   media.nexuzhealth.be
Address: 2606:4700::6812:1bf1
Name:   media.nexuzhealth.be
Address: 2606:4700::6812:1af1
```

1.4 Port scanning

Tool - nmap

Command – nmap -sV -sC -Pn 104.18.27.241 -A

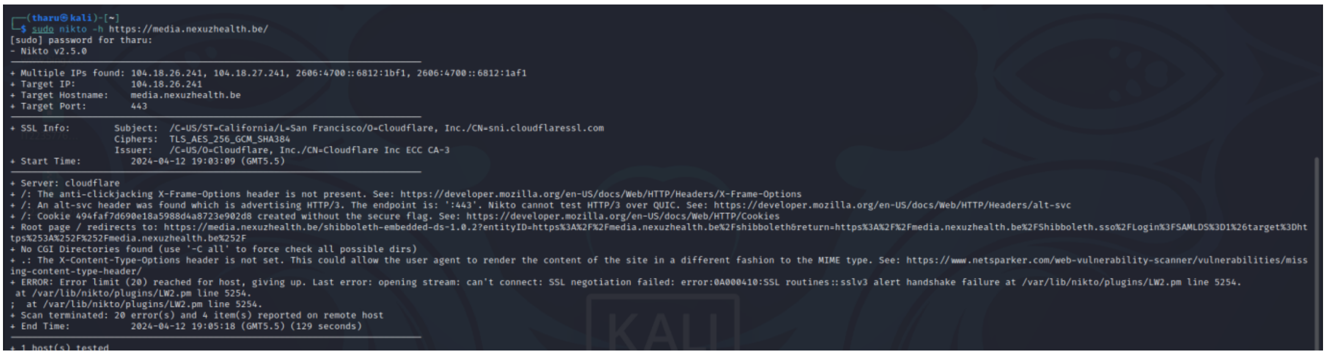


```
┌──(tharu㉿kali)-[~]
└─$ nmap -sV -sC -Pn 104.18.27.241 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-12 18:59 +0530
Nmap scan report for 104.18.27.241
Host is up (0.036s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions, RTSPRequest:
|     500 Syntax error, command unrecognized
|   Hello:
|_    552 Invalid domain name in EHLO command.
80/tcp   open  http          Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Site doesn't have a title (text/plain; charset=UTF-8).
443/tcp  open  ssl/https     cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
|_http-server-header: cloudflare
8080/tcp open  http          Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Site doesn't have a title (text/plain; charset=UTF-8).
8443/tcp open  ssl/https-alt cloudflare
|_http-server-header: cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.93%I=7%D=4/12%Time=66193755%P=x86_64-pc-linux-gnu%r(Hell
SF:o,2A,"552\x20Invalid\x20domain\x20name\x20in\x20EHLO\x20command\.\r\n")
SF:%r(GenericLines,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\
SF:r\n")%r(GetRequest,28,"500\x20Syntax\x20error,\x20command\x20unrecogniz
SF:ed\r\n")%r(HTTPOptions,28,"500\x20Syntax\x20error,\x20command\x20unreco
SF:gnized\r\n")%r(RTSPRequest,28,"500\x20Syntax\x20error,\x20command\x20un
SF:recognized\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 112.21 seconds
```

1.5 Nikto scanning

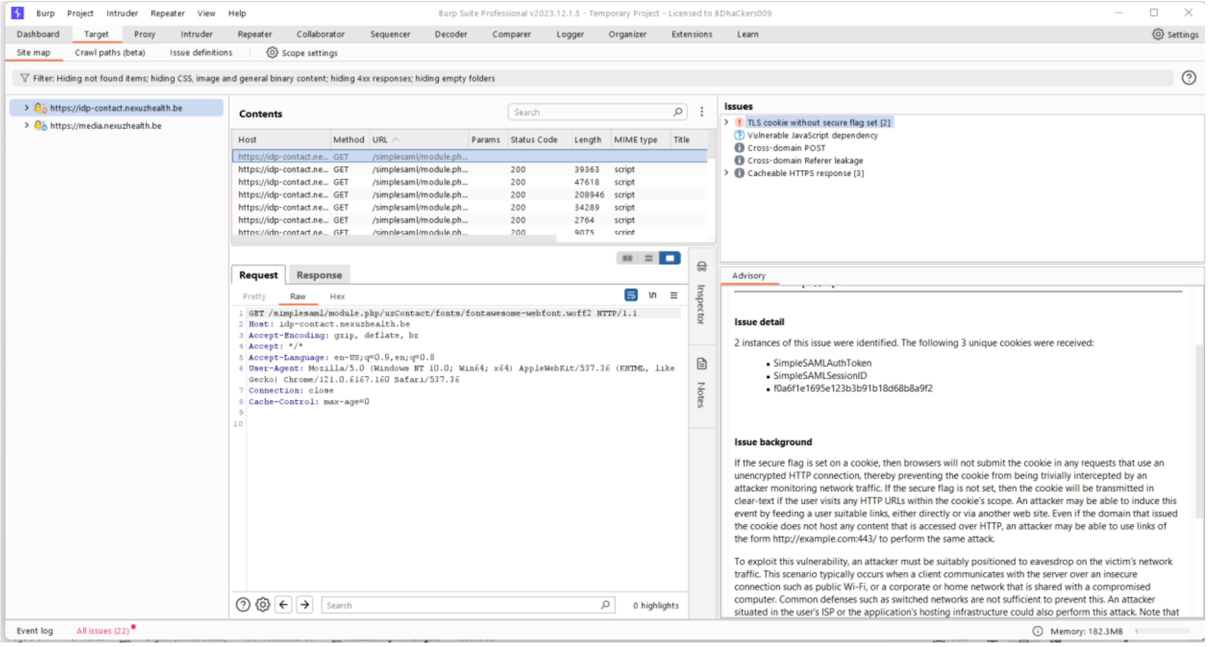
Tool – Nikto

Command - sudo nikto -h media.nexuzhealth.be



```
┌──(tharu㉿kali)-[~]
└─$ sudo nikto -h https://media.nexuzhealth.be/
[sudo] password for tharu:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.18.26.241, 104.18.27.241, 2606:4700::6812:1bf1, 2606:4700::6812:1af1
+ Target IP:          104.18.26.241
+ Target Hostname:    media.nexuzhealth.be
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=San Francisco/O=Cloudflare, Inc./CN=sni.cloudflaressl.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Cloudflare, Inc./CN=Cloudflare Inc ECC CA-3
+ Start Time:         2024-04-12 19:03:09 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: Cookie 494faf7d690e18a5988d4a8723e902d8 created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Root page / redirects to: https://media.nexuzhealth.be/shibboleth-embedded-ds-1.0.2?entityID=https%3A%2F%2Fmedia.nexuzhealth.be%2Fshibboleth&return=https%3A%2F%2Fmedia.nexuzhealth.be%2FShibboleth.sso%2FLogin%3FSAMLDS%3D1%26target%3Dht
tps%253A%252F%252Fmedia.nexuzhealth.be%252F
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ .: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::sslv3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time:           2024-04-12 19:05:18 (GMT5.5) (129 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

1.6 Burpsuite scanning


Burp Project Intruder Repeater View Help
Burp Suite Professional v2023.12.1.5 - Temporary Project - Licensed to BDhaCkers009
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Site map
Crawl paths (beta)
Issue definitions
Scope settings
Search
Request
Response
Pretty
Raw
Hex
Inspector
Notes
Advisory
Event log
All issues (22)
0 highlights
Memory: 182.3MB

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://idp-contact.nexuzhealth.be
- https://media.nexuzhealth.be

Contents

Host	Method	URL	Params	Status Code	Length	MIME type	Title
https://idp-contact.ne...	GET	/simplesaml/module.ph...					
https://idp-contact.ne...	GET	/simplesaml/module.ph...		200	39363	script	
https://idp-contact.ne...	GET	/simplesaml/module.ph...		200	47618	script	
https://idp-contact.ne...	GET	/simplesaml/module.ph...		200	208946	script	
https://idp-contact.ne...	GET	/simplesaml/module.ph...		200	34289	script	
https://idp-contact.ne...	GET	/simplesaml/module.ph...		200	2764	script	
https://idp-contact.ne...	GET	/simplesaml/module.ph...		200	9075	script	

```
GET /simplesaml/module.php/uzContact/fonts/fontawesome-webfont.woff2 HTTP/1.1
Host: idp-contact.nexuzhealth.be
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.6167.160 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

Issues

- TLS cookie without secure flag set [2]
- Vulnerable JavaScript dependency
- Cross-domain POST
- Cross-domain Referer leakage
- Cacheable HTTPS response [3]

Issue detail

2 instances of this issue were identified. The following 3 unique cookies were received:

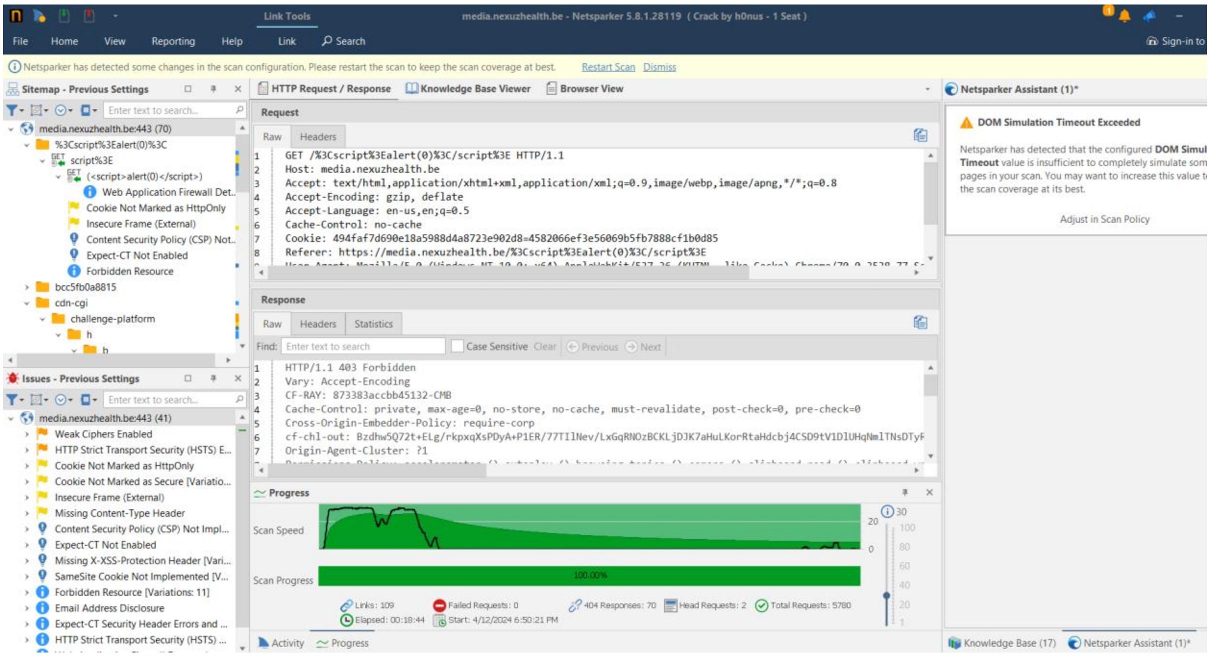
- SimpleSAMLAuthToken
- SimpleSAMLSessionID
- f0a6f1e1695e123b3b91b18d68b8a9f2

Issue background

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form http://example.com:443/ to perform the same attack.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that

1.7 Netspaker scan



Netsparker has detected some changes in the scan configuration. Please restart the scan to keep the scan coverage at best.

- media.nexuzhealth.be:443 (70)
  - %3Cscript%3Ealert(0)%3C
    - script%3E
      - (<script>alert(0)</script>)
        - Web Application Firewall Det...
        - Cookie Not Marked as HttpOnly
        - Insecure Frame (External)
        - Content Security Policy (CSP) Not...
        - Expect-CT Not Enabled
        - Forbidden Resource
  - bcc5fb0a8815
  - cdn-cgi
    - challenge-platform
      - h
        - h

- media.nexuzhealth.be:443 (41)
  - Weak Ciphers Enabled
  - HTTP Strict Transport Security (HSTS) E...
  - Cookie Not Marked as HttpOnly
  - Cookie Not Marked as Secure [Variatio...
  - Insecure Frame (External)
  - Missing Content-Type Header
  - Content Security Policy (CSP) Not Impl...
  - Expect-CT Not Enabled
  - Missing X-XSS-Protection Header [Vari...
  - SameSite Cookie Not Implemented [V...
  - Forbidden Resource [Variations: 11]
  - Email Address Disclosure
  - Expect-CT Security Header Errors and ...
  - HTTP Strict Transport Security (HSTS) ...

```
GET /%3Cscript%3Ealert(0)%3C/script%3E HTTP/1.1
Host: media.nexuzhealth.be
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 494faf7d690e18a5988d4a8723e902d8=4582066ef3e56069b5fb7888cf1b0d85
Referer: https://media.nexuzhealth.be/%3Cscript%3Ealert(0)%3C/script%3E
```

```
HTTP/1.1 403 Forbidden
Vary: Accept-Encoding
CF-RAY: 873383accbb45132-CMB
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Cross-Origin-Embedder-Policy: require-corp
cf-chl-out: Bzdhw5Q72t+ELg/rkpxqXsPDyA+P1ER/77TIlNev/LxGqRNOzBCKLjDJK7aHuLKorRtaHdcbj4CSD9tV1DlUHqNmlTNsDTyF
Origin-Agent-Cluster: ?1
```

Links: 109 Failed Requests: 0 404 Responses: 70 Head Requests: 2 Total Requests: 5780
Elapsed: 00:18:44 Start: 4/12/2024 6:50:21 PM

Netsparker Assistant (1)*

DOM Simulation Timeout Exceeded

Netsparker has detected that the configured **DOM Simul Timeout** value is insufficient to completely simulate som pages in your scan. You may want to increase this value t the scan coverage at its best.

Adjust in Scan Policy

1.8 Vulnerabilities

Vulnerability Title: TLS Cookie Without Secure Flag Set

Vulnerability Description: The website "https://idp-contact.nexuzhealth.be" is generating TLS cookies without enabling the secure flag. This presents a security vulnerability because these cookies can be sent via unencrypted HTTP connections, which might potentially enable attackers to intercept them and compromise user sessions.

Affected Components:

- /simplesaml/module.php/uzContact/uzContact.php
- /simplesaml/saml2/idp/SSOService.php

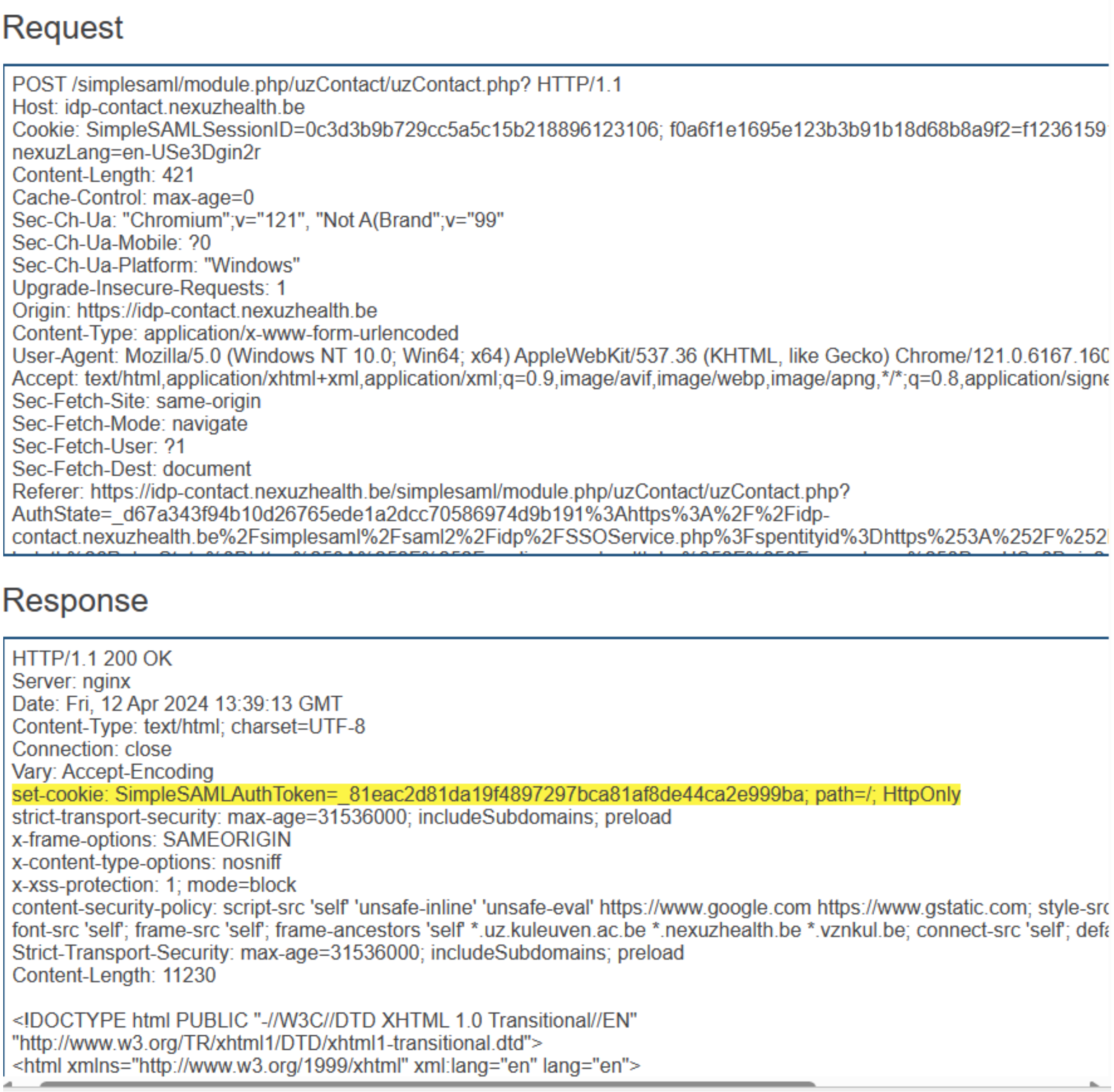
Impact Assessment: Impact of vulnerability includes,

- Intercept cookies
- Session hijacking
- Unauthorized access

Steps to Reproduce:

1. Navigate to the affected URL: https://idp-contact.nexuzhealth.be/simplesaml/module.php/uzContact/uzContact.php and https://idp-contact.nexuzhealth.be/simplesaml/saml2/idp/SSOService.php seperately.
2. Observe the cookies being set without the secure flag.

Proof of concept:

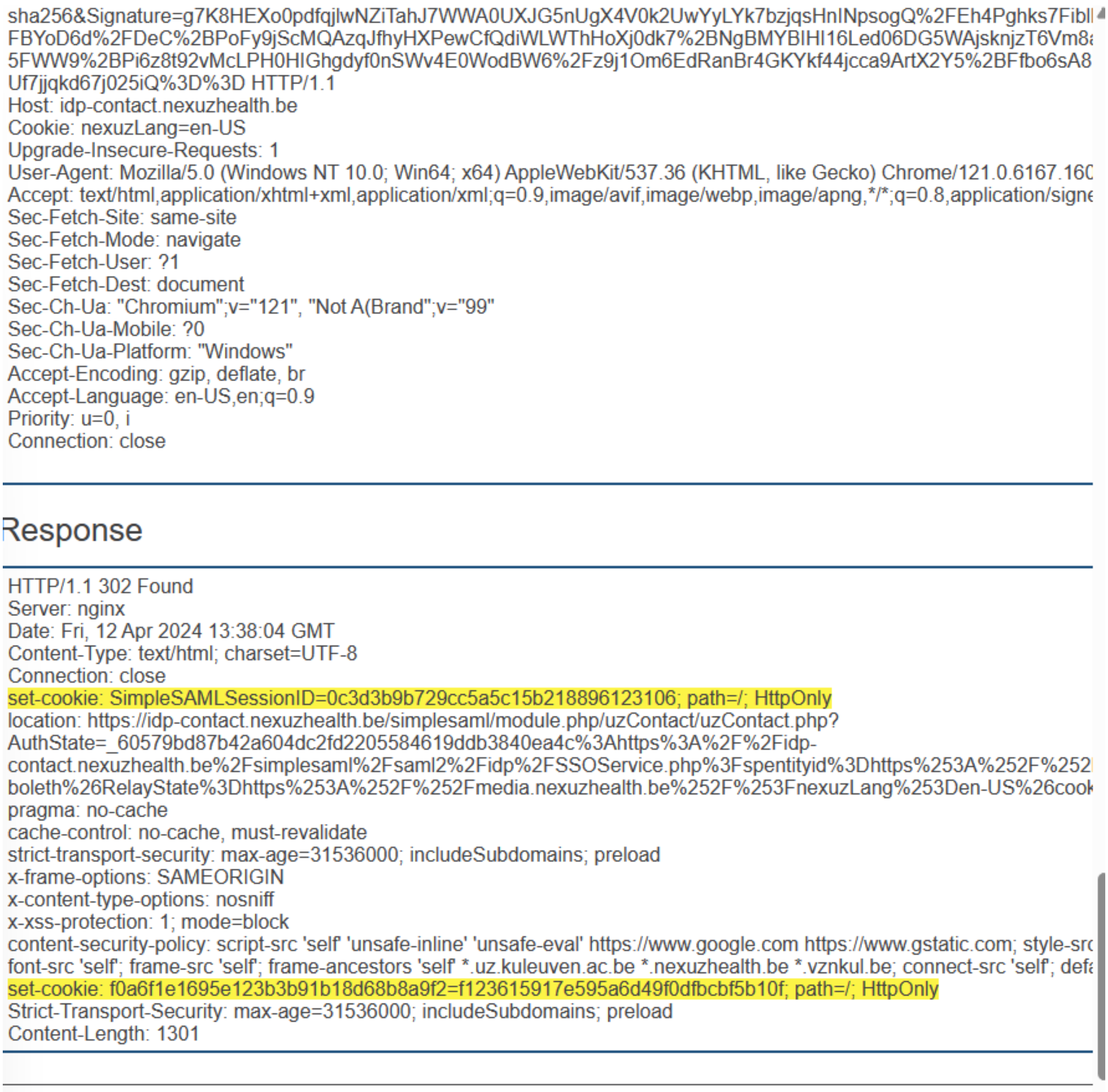


Request

```
POST /simplesaml/module.php/uzContact/uzContact.php? HTTP/1.1
Host: idp-contact.nexuzhealth.be
Cookie: SimpleSAMLSessionID=0c3d3b9b729cc5a5c15b218896123106; f0a6f1e1695e123b3b91b18d68b8a9f2=f1236159
nexuzLang=en-USe3Dgin2r
Content-Length: 421
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://idp-contact.nexuzhealth.be
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.16
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://idp-contact.nexuzhealth.be/simplesaml/module.php/uzContact/uzContact.php?
AuthState=_d67a343f94b10d26765ede1a2dcc70586974d9b191%3Ahttps%3A%2F%2Fidp-
contact.nexuzhealth.be%2Fsimplesaml%2Fsaml2%2Fidp%2FSSOService.php%3Fspentityid%3Dhttps%253A%252F%252
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 12 Apr 2024 13:39:13 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
set-cookie: SimpleSAMLAuthToken=_81eac2d81da19f4897297bca81af8de44ca2e999ba; path=/; HttpOnly
strict-transport-security: max-age=31536000; includeSubdomains; preload
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
content-security-policy: script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google.com https://www.gstatic.com; style-src
font-src 'self'; frame-src 'self'; frame-ancestors 'self' *.uz.kuleuven.ac.be *.nexuzhealth.be *.vznkul.be; connect-src 'self'; def
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Content-Length: 11230

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
```



```
sha256&Signature=g7K8HEXo0pdfqjlwNZiTahJ7WWA0UXJG5nUgX4V0k2UwYyLYk7bzjqsHnINpsogQ%2FEh4Pghks7Fibl
FBYoD6d%2FDeC%2BPoFy9jScMQAzqJfhyHXPewCfQdiWLWThHoXj0dk7%2BNgBMYBIHI16Led06DG5WAjsknjzT6Vm8
5FWW9%2BPi6z8t92vMcLPH0HIGhgdyf0nSWv4E0WodBW6%2Fz9j1Om6EdRanBr4GKYkf44jcca9ArtX2Y5%2BFfbo6sA8
Uf7jjqkd67j025iQ%3D%3D HTTP/1.1
Host: idp-contact.nexuzhealth.be
Cookie: nexuzLang=en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.16
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: close
```

Response

```
HTTP/1.1 302 Found
Server: nginx
Date: Fri, 12 Apr 2024 13:38:04 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
set-cookie: SimpleSAMLSessionID=0c3d3b9b729cc5a5c15b218896123106; path=/; HttpOnly
location: https://idp-contact.nexuzhealth.be/simplesaml/module.php/uzContact/uzContact.php?
AuthState=_60579bd87b42a604dc2fd2205584619ddb3840ea4c%3Ahttps%3A%2F%2Fidp-
contact.nexuzhealth.be%2Fsimplesaml%2Fsaml2%2Fidp%2FSSOService.php%3Fspentityid%3Dhttps%253A%252F%252
boleth%26RelayState%3Dhttps%253A%252F%252Fmedia.nexuzhealth.be%252F%253FnexuzLang%253Den-US%26cook
pragma: no-cache
cache-control: no-cache, must-revalidate
strict-transport-security: max-age=31536000; includeSubdomains; preload
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
content-security-policy: script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google.com https://www.gstatic.com; style-sr
font-src 'self'; frame-src 'self'; frame-ancestors 'self' *.uz.kuleuven.ac.be *.nexuzhealth.be *.vznkul.be; connect-src 'self'; def
set-cookie: f0a6f1e1695e123b3b91b18d68b8a9f2=f123615917e595a6d49f0dfbcbf5b10f; path=/; HttpOnly
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Content-Length: 1301
```

Proposed Mitigation or Fix: It is necessary to enable the secure flag on any cookies that are utilized for transmitting sensitive information while browsing material using HTTPS. If cookies are utilized for transmitting session tokens, it is imperative that the sections of the application accessed via HTTPS implement their own session management system. Furthermore, the session tokens employed should never be communicated through unencrypted connections.

1.8.1 Other vulnerabilities

1. Weak Ciphers Enabled
2. Missing Content-Type Header
3. Cookie Not Marked as HttpOnly
4. Cookie Not Marked as Secure
5. Insecure Frame (External)
6. Content Security Policy (CSP) Not Implemented
7. Expect-CT Not Enabled
8. Missing X-XSS-Protection Header
9. SameSite Cookie Not Implemented
10. Email Address Disclosure
11. HTTP Strict Transport Security (HSTS) Max-Age Value Too Low
12. Web Application Firewall Detected
13. Forbidden Resource