Sri Lanka Institute of Information Technology

Web Security – IE2062

Web Application Security Audit Report
(www.myndr.nl)

Submitted by:

IT19010236
Kajanthan.B

Weekday 14.1

Domain Details

Domain Name: www.myndr.nl

No of sub domains:

Source Where I found(Domain): www.hackerone.com

Confidential

The substance of this document shall be confidential and may be accessed only without authorization by parties.

This paper provides classified and exclusive information about https:/www.myndr.nl/ security and SLIIT. Before circulating copies of this document or the extracted contents of this document, strict caution should be taken. Our myndr contact point is approved by SLIIT. View this document and disseminate it in compliance with its policies and procedures on myndr data management. This paper should be branded as 'CONFIDENCIAL,' so that it is disseminated on a 'need for information' basis. Address questions regarding the proper and legitimate use of this document to: SLIIT Malabe Campus, New Kandy Rd, Malabe 10115

Disclaimers

The data contained in this document is given as is and without warranty. Vulnerability analyses are a "time-by-time" review. As such, something may have changed in the environment since the tests reflected in this report have been conducted. It is also likely that there could have been new vulnerabilities after the checks have been conducted. This study should therefore be viewed as a reference rather than a 100% risk representation threatening your systems, networks and applications.

Data on records and controls

Document Name : Web Application Security Audit Report of SLIIT

Client Name : Myndr

Audit Duration :

Initial Report Date :

Status Report Date : NA

Closing Report Date : NA

Hand Over To : Dr. Lanessha Rukgahakotuwa

Auditor Name : Kajanthan.B IT19010236

Reviewed By : Ms. Lanessha Rukgahakotuwa Ms. Chathu Udagedara

Purpose

Myndr has asked SLIIT to perform a detailed security examination of their web application. The security evaluation of the https:/www.myndr.nl/ application was requested to examine vulnerable. The purpose of this evaluation is to identify web application vulnerabilities and to indicate the corresponding level of risk associated with the vulnerabilities.

This web called Myndr make sure your internet at home is more suited to your actual needs. This research effort took place in October 2nd 2020 and ended on 24 October 2020 respectively. Separate coverage was given for some tentative reports, and this study is being presented to explain the full effects of our research activities and to make suggestions where appropriate.

Application Credentials and URL

Credentials and URLs of the application The security evaluation was carried out on the following URL https://www.myndr.nl/

Tools and Methods Used In Vulnerable Evaluation

- **Nmapper (Online tool to check instant report of Sub Domain)**
- **Sublister**
- **Zoom**
- **Dmitry**
- **Nmap**
- **Skip Fish**
- **Nikto**
- **OWASP ZAP**
- **Sqlmap**
- **NetSparker**

Data on risk levels and appropriate actions

The vulnerabilities found are correlated with a risk level that shows how serious the vulnerability is and allows application owners / development teams to prioritize the vulnerabilities and select an effective mitigation method.

Risk Level	Appropriate actions
High	The high level of risk demonstrates the highest risk for a certain instance of vulnerability. This vulnerability could allow an attacker to successfully exploit the underlying application and its data and to compromise the application and its data partially or entirely to change the behavior of the application to become different from its original intended intent. It is recommended that the vulnerability labelled "Extreme Risk" be treated with extreme priority
Medium	The medium risk level demonstrates substantial risks associated with a particular instance of vulnerability. This vulnerability can allow an attacker to exploit a specific level of the underlying application and data so that the attacker can obtain low-level information on the application. The attacker could use this information to make more precise attacks based on the collected information. Early on or soon after "High Danger" vulnerabilities should be mitigated the vulnerability labelled with "low risk"
Low	The low level of risk shows the lowest risk in relation to a particular instance of vulnerability. Such a weakness may allow an attacker to obtain some details concerning the application not otherwise known. The intruder will not be able to use tactics based on the knowledge the device reveals. Soon after high and medium risk vulnerabilities have been mitigated, the vulnerability described as "low risk."

OWASP Top 10 Vulnerability Threats for Applications

The open web Application Security Project (OWASP) is a global, non-profit humanitarian association focusing on strengthening application information security. A common knowledge guide for developers and web application protection is the OWASP Top 10. It reflects a broad consensus on the most important threats to web apps for stability. If we found any OWASP vulnerable we need to focus and we need to take immediate action towards the vulnerable.Those top 10 vulnerable are

1. **Injection.**

Injection errors, such as injection of SQL, NoSQL, OS, and LDAP, exist when untrusted data is sent as part of a command or query to an interpreter. The hostile data of the intruder will trick the interpreter without proper permission into performing unwanted commands or accessing data.

2. **The Authentication Broken.**

Authentication and session management related program features are frequently inappropriately configured, enabling attackers to steal passwords, keys, or session tokens or manipulate other design vulnerabilities to briefly or permanently assume the identity of other users.

3. **Exposure to confidential details.**

Often web apps and APIs don't protect confidential data properly, for example banking, healthcare and PII. Attackers may intercept or alter such weakly secured information to commit fraud on credit cards, stealing of identification or other crimes. Without additional security, confidential data such as rest or transit cryptography may be hacked, and special safeguards are needed for browser exchange.

4. **XML Persons Foreign (XXE).**

Many older or poorly built XML processors use XML document to determine external object references. The internal file handler, internal file transfers, internal port scanning, remote code installation and denial of service attacks may be used in external organizations to communicate internal data.

5. **Broken Access Control.**

Restrictions are also not adequately applied on what authenticated users are authorized to do. These vulnerabilities can be abused by attackers to access unauthorized functions and/or data, such as accessing the accounts of other users, viewing confidential files, altering the data of other users, changing access privileges, etc.

6. Misconfiguring Security.

The most widely seen concern is security misconfiguration. Incomplete or ad hoc implementations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing confidential information are usually the product of unsafe default configurations. It is not only necessary to safely configure all operating systems, frameworks, libraries, and programs, but to patch them in a timely manner.

7. XSS Cross-Site Scripting.

XSS vulnerabilities occur if an application uses a browser API that can build HTML or JavaScript to contain untrusted data in a new web page without sufficient authentication or escape , or update an existing web page with user-supplied data. In the victim's browser, XSS enables attackers to execute scripts that can hijack user sessions, deface websites, or send the user to malicious pages.

8. Insecure Deserialization.

Unsure deserialization also contributes to execution of remote code. Even if deserialization vulnerabilities should not lead to remote execution, threats, replay attacks, insertion attacks, and elevation of privilege can be used.

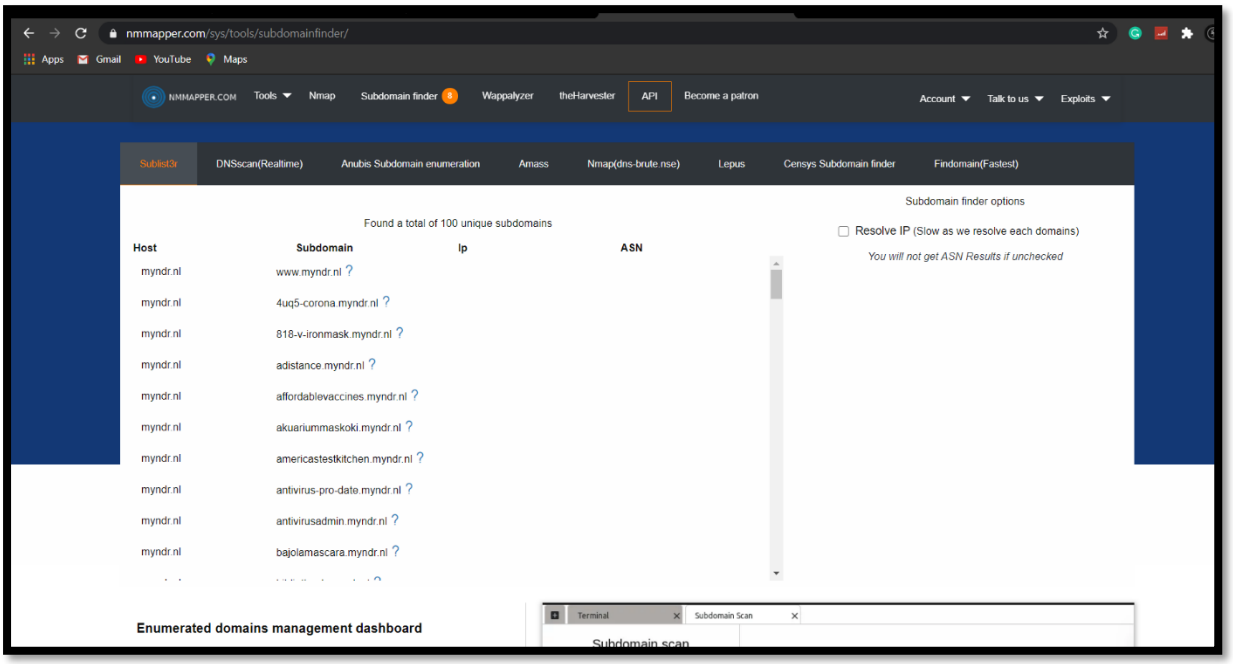
9. Using Components with Known Vulnerabilities.

The same rights occur for elements, such as databases, frames, and other program units. If a vulnerable part is used, a significant data failure or server capture can be enabled. Applications and APIs with known vulnerability components may weaken the protections of the framework and allow for different attacks.

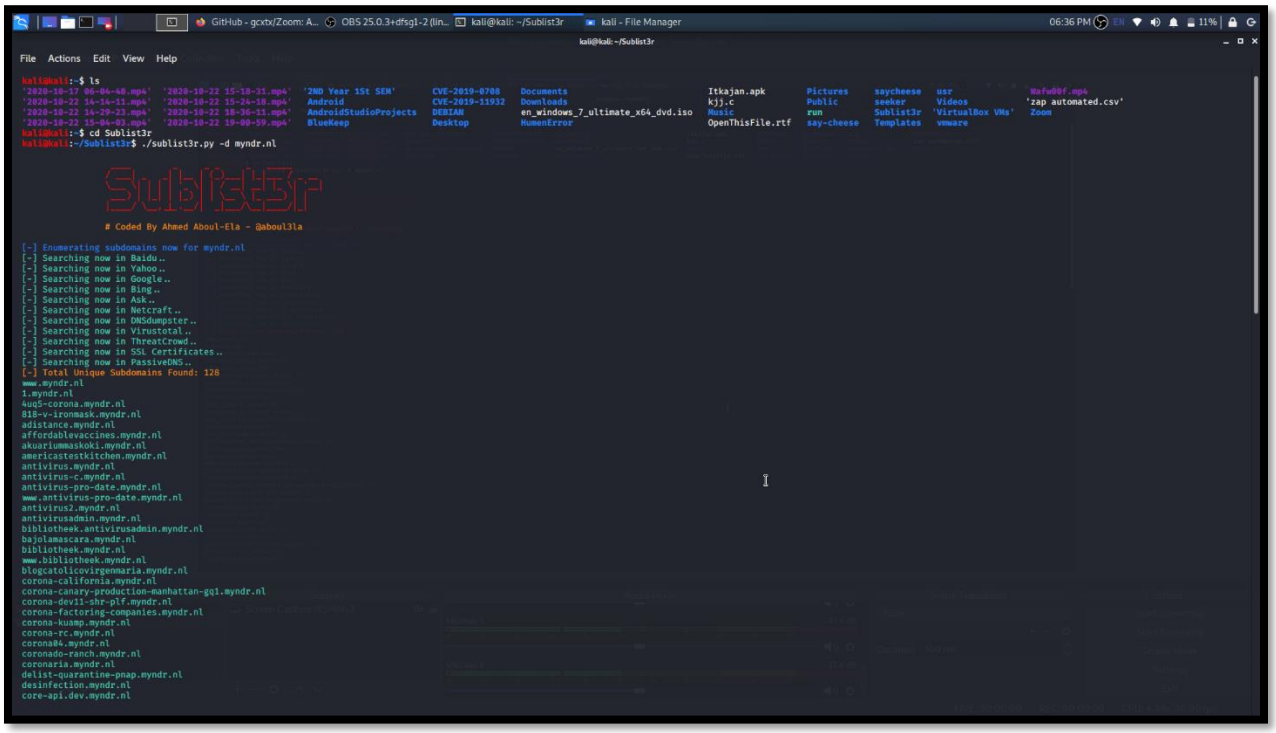
10. Logging & Tracking insufficient.

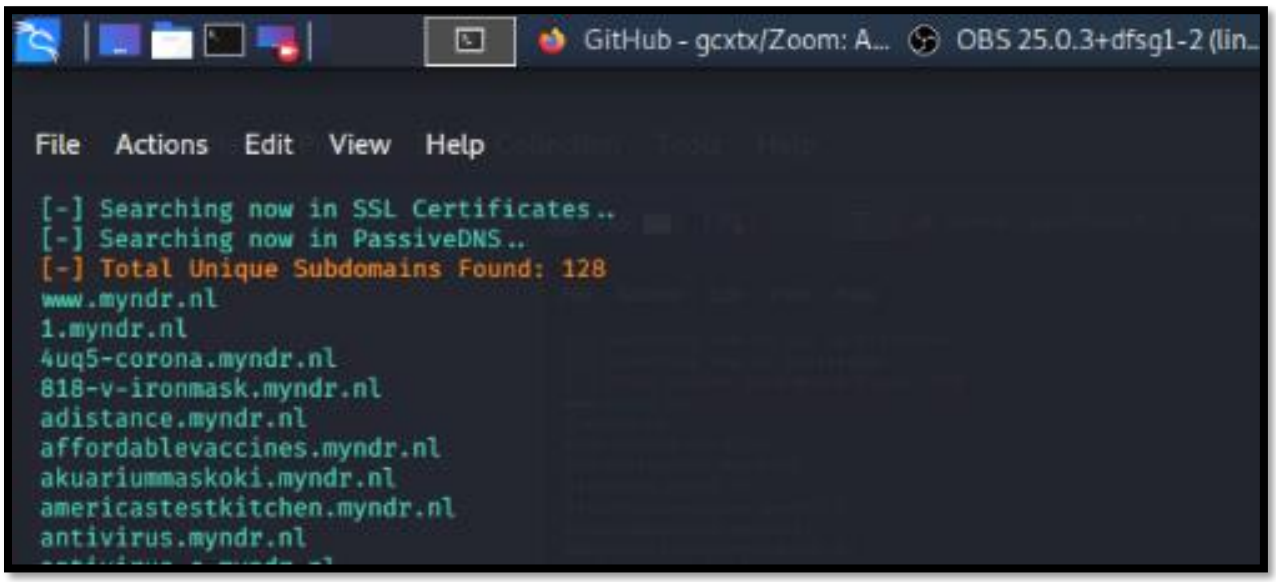
Logging and tracking insufficient, combined with lack or unsuccessful interplay with incident response enables attackers to continue to strike, sustain persistence, pivot more networks, and exploit, collect or kill data. Most of the infringement studies suggest that the time taken for detecting an infringement approaches 200 days.

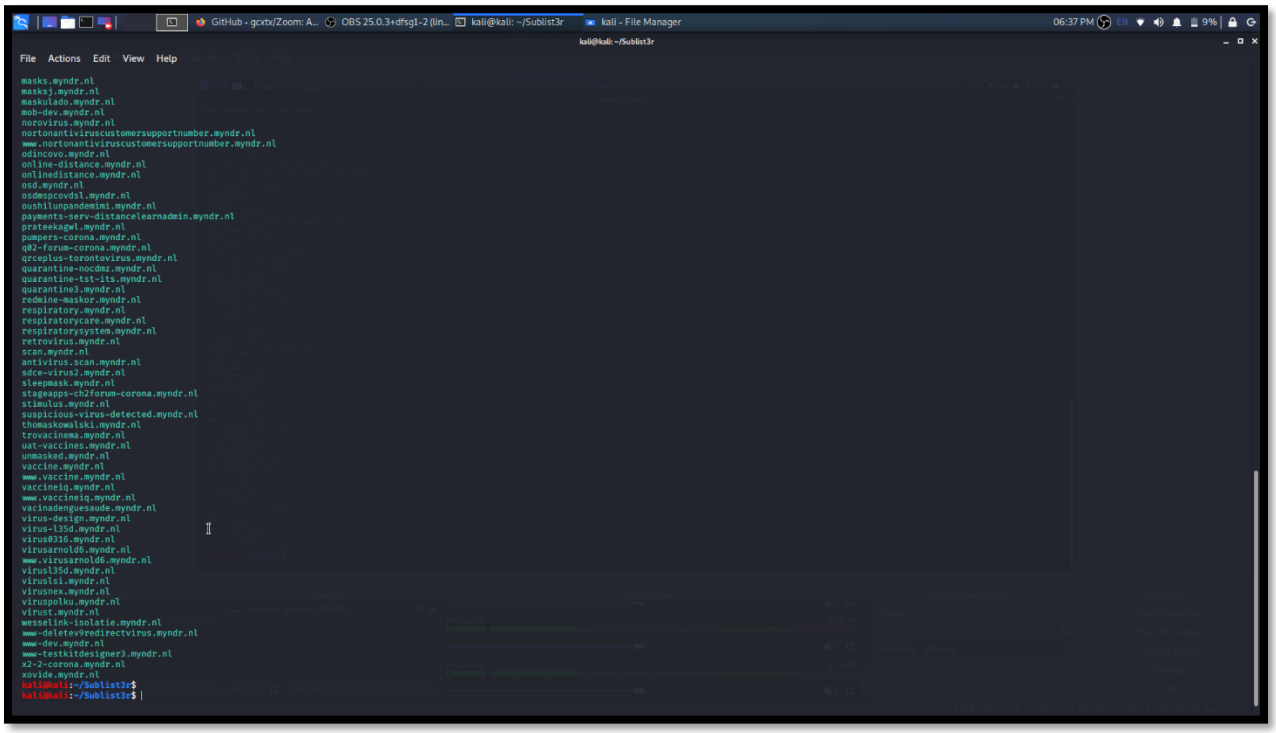
I've got almost **100** sub domains, according to the online subdomain finder named (nmmapper). In this article, I have added a screenshot of the relevant findings of the website. I used the online method to make the subdomain report accessible to a specific domain automatically. So we need to select a domain that includes more than 50 subdomains. Mi.com and www.myndr.nl have been chosen by me. Between these two choices, I prefer www.myndr.nl. I then registered with courseweb.sliit.lk.



There are several resources used for domain checking and counting. I choose sublister to count no subdomain of www.myndr.nl among others. It gives a subdomain number out of **128**. Here's the screen shot of the one coming down.


GitHub - gcxtx/Zoom: A...
OBS 25.0.3+dfsg1-2 (lin...
kali@kali: ~/Sublist3r
kali - File Manager
06:36 PM
kali@kali: ~/Sublist3r
File Actions Edit View Help
kali@kali:~$ ls
'2020-10-17 06-04-48.mp4' '2020-10-22 15-18-31.mp4' '2ND Year 1St SEM' CVE-2019-0708 Documents Itkajan.apk Pictures saycheese usr Wafw00f.mp4
'2020-10-22 14-14-11.mp4' '2020-10-22 15-24-18.mp4' Android CVE-2019-11932 Downloads kjj.c Public seeker Videos 'zap automated.csv'
'2020-10-22 14-29-23.mp4' '2020-10-22 18-36-11.mp4' AndroidStudioProjects DEBIAN en_windows_7_ultimate_x64_dvd.iso Music run Sublist3r 'VirtualBox VMs' Zoom
'2020-10-22 15-04-03.mp4' '2020-10-22 19-00-59.mp4' BlueKeep Desktop HumanError OpenThisFile.rtf say-cheese Templates vmware
kali@kali:~$ cd Sublist3r
kali@kali:~/Sublist3r$ ./sublist3r.py -d myndr.nl
Sublist3r
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for myndr.nl
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 128
www.myndr.nl
1.myndr.nl
4uq5-corona.myndr.nl
818-v-ironmask.myndr.nl
adistance.myndr.nl
affordablevaccines.myndr.nl
akuariummaskoki.myndr.nl
americastestkitchen.myndr.nl
antivirus.myndr.nl
antivirus-c.myndr.nl
antivirus-pro-date.myndr.nl
www.antivirus-pro-date.myndr.nl
antivirus2.myndr.nl
antivirusadmin.myndr.nl
bibliotheek.antivirusadmin.myndr.nl
bajolamascara.myndr.nl
bibliotheek.myndr.nl
www.bibliotheek.myndr.nl
blogcatolicovirgenmaria.myndr.nl
corona-california.myndr.nl
corona-canary-production-manhattan-gq1.myndr.nl
corona-dev11-shr-plf.myndr.nl
corona-factoring-companies.myndr.nl
corona-kuamp.myndr.nl
corona-rc.myndr.nl
corona04.myndr.nl
corona40-ranch.myndr.nl
coronaria.myndr.nl
delist-quarantine-pnap.myndr.nl
desinfection.myndr.nl
core-api.dev.myndr.nl


GitHub - gcxtx/Zoom: A...
OBS 25.0.3+dfsg1-2 (lin...
File Actions Edit View Help
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 128
www.myndr.nl
1.myndr.nl
4uq5-corona.myndr.nl
818-v-ironmask.myndr.nl
adistance.myndr.nl
affordablevaccines.myndr.nl
akuariummaskoki.myndr.nl
americastestkitchen.myndr.nl
antivirus.myndr.nl



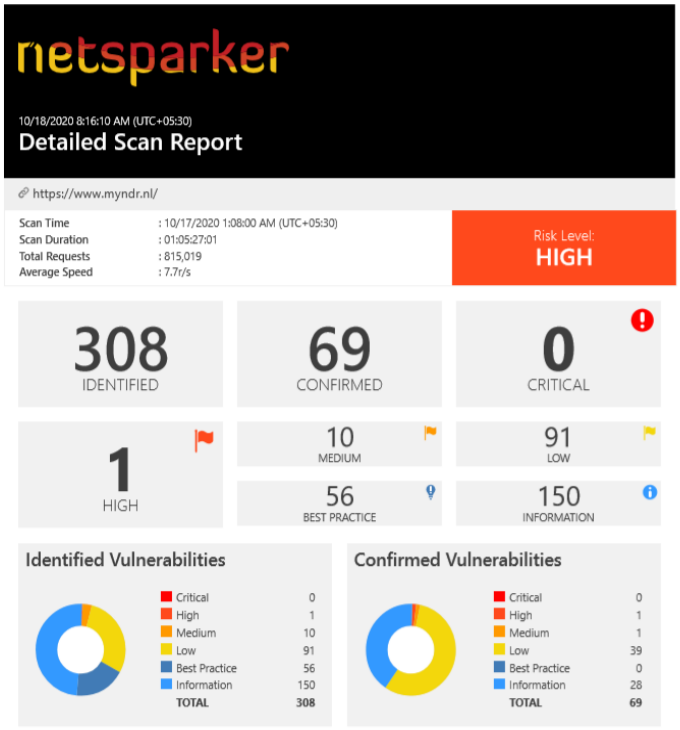
Vulnerability Details.

1) NetSparker

Netsparker is a web application protection scanner that helps you to search and detect websites , web apps and web services and protection bugs, automatic but completely configurable. No matter what the platform or the languages in which they are designed, Netsparker will search all forms of web applications.

It took nearly 48 hours to scan whole domain. In the video Documentary I skip unwanted parts and I uploaded; you can view it using the link which available in the last page of this document.

It generates the report according to Critical, high, medium, low levels vulnerable with graphical view. we identified 308 among that 69 confirmed. There is no critical vulnerability, 1 is high, 10 medium , and 91 law vulnerabilities we found. Here is the graphical view of screen shot.



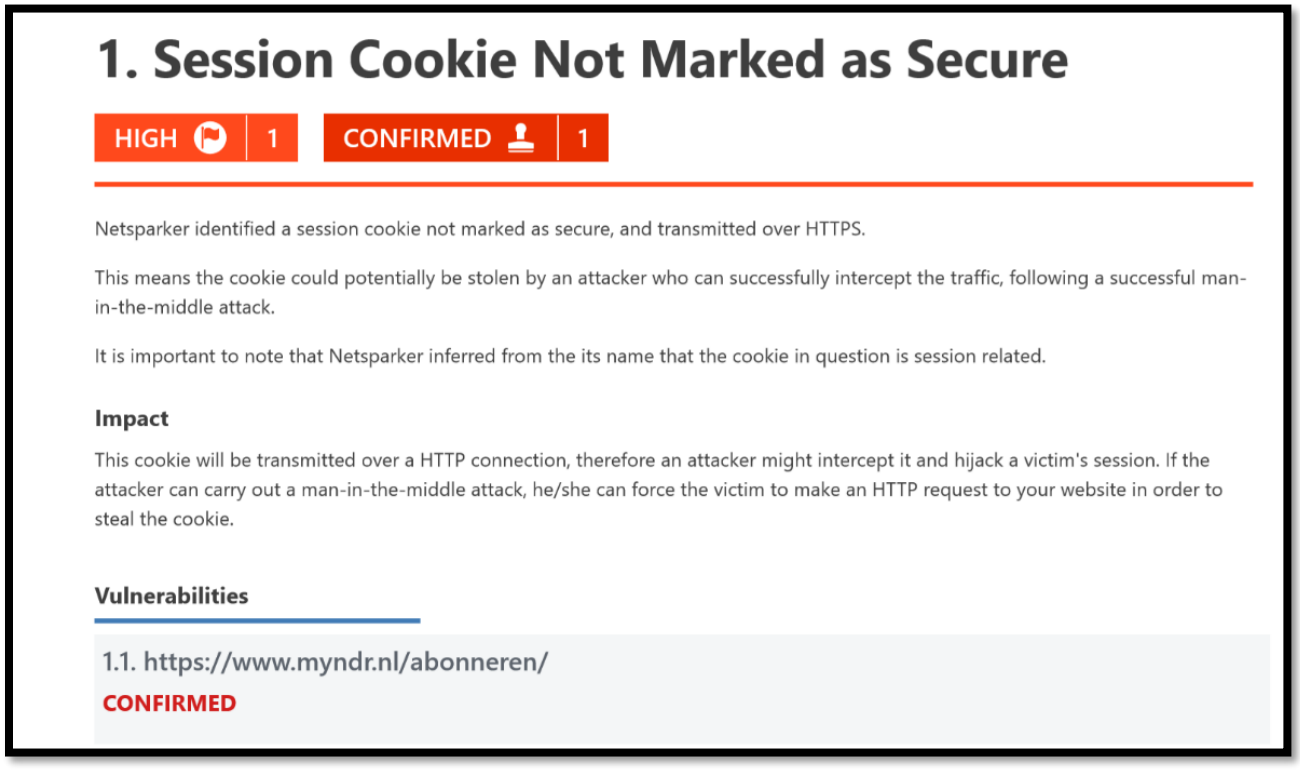
Among all we found one High Risk Level vulnerability called session cookie not marked as secure and we found 10 Medium Risk Level vulnerabilities such as HTTP Strict Transport Security (HSTS) Errors and Warnings, Out-of-date Version (jQuery), Weak Ciphers Enabled, [Possible] Cross-site Request Forgery, [Possible] Internal IP Address Disclosure, [Possible] Phishing by Navigating Browser Tabs, Apache Multi Views Enabled, Cookie Not Marked as Http Only, Cookie Not Marked as Secure, Insecure Frame (External).

High Risk Level. 1.[Session cookie not marked as secure].

Netsparker identified a session cookie not marked as secure, and transmitted over HTTPS. This means the cookie could potentially be stolen by an attacker who can successfully intercept the traffic, following a successful manin-the-middle attack. It is important to note that Netsparker inferred from the its name that the cookie in question is session related.

Sub Domain - https://www.myndr.nl/abonneren/

Impact - This cookie will be transmitted over a HTTP connection, therefore an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to your website in order to steal the cookie.



Vulnerabilities

1.1. https://www.myndr.nl/abonneren/

CONFIRMED

Method	Parameter	Value
GET	param1	abonneren

Identified Cookie(s)

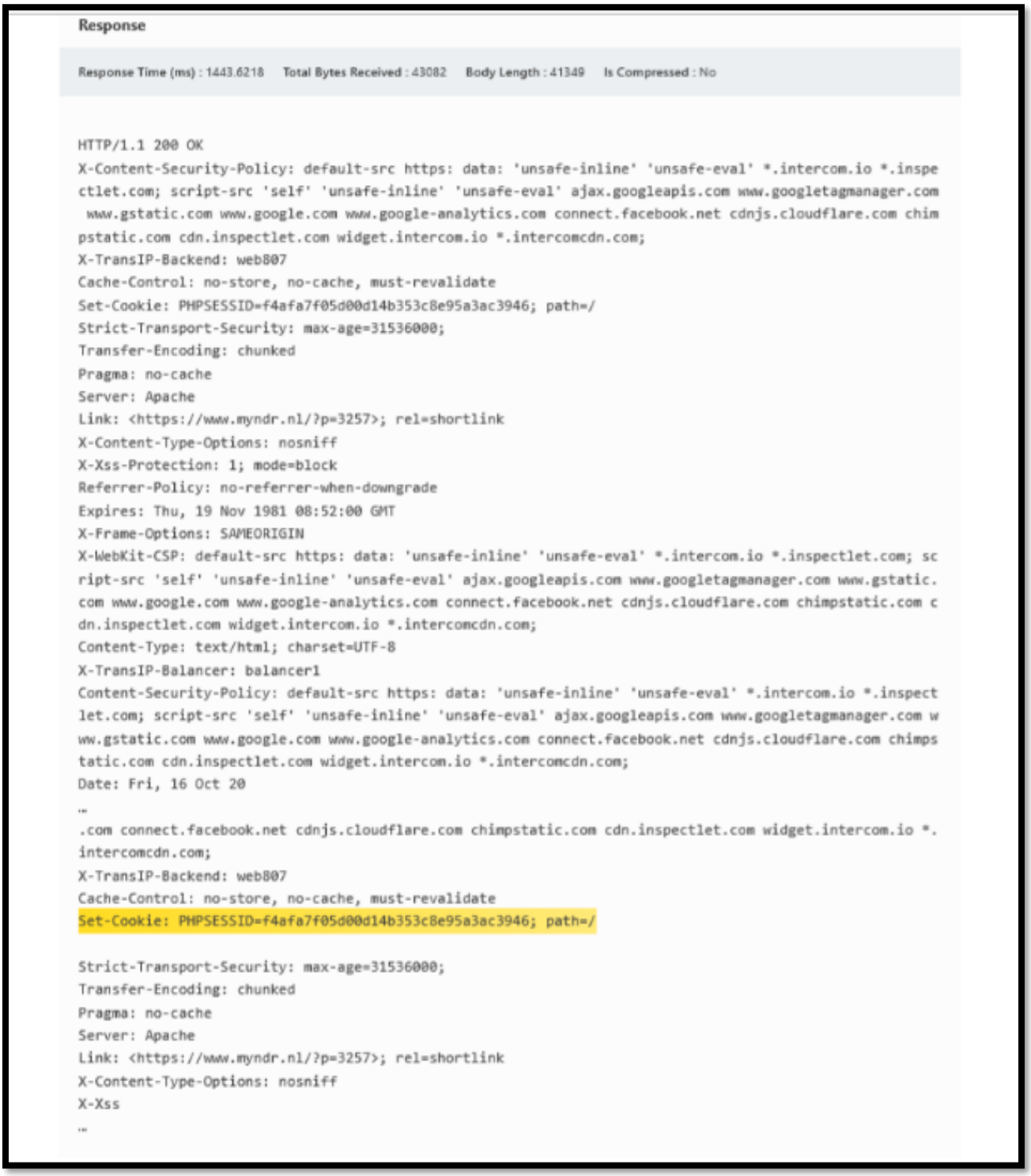
- PHPSESSID

Cookie Source

- HTTP Header

Request

```
GET /abonneren/ HTTP/1.1
Host: www.myndr.nl
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: intercom-id-i93abyr7=2b271df9-8920-4d51-860b-493b5d0de4b3; intercom-session-i93abyr7=; myndr-co
okies=2; pll_language=nl
Referer: https://www.myndr.nl/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```



Response

Response Time (ms) : 1443.6218 Total Bytes Received : 43082 Body Length : 41349 Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspe
ctlet.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com
 www.gstatic.com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chim
pstatic.com cdn.inspectlet.com widget.intercom.io *.intercomcdn.com;
X-TransIP-Backend: web807
Cache-Control: no-store, no-cache, must-revalidate
Set-Cookie: PHPSESSID=f4afa7f05d00d14b353c8e95a3ac3946; path=/
Strict-Transport-Security: max-age=31536000;
Transfer-Encoding: chunked
Pragma: no-cache
Server: Apache
Link: <https://www.myndr.nl/?p=3257>; rel=shortlink
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Frame-Options: SAMEORIGIN
X-WebKit-CSP: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspectlet.com; sc
ript-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com www.gstatic.
com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chimpstatic.com c
dn.inspectlet.com widget.intercom.io *.intercomcdn.com;
Content-Type: text/html; charset=UTF-8
X-TransIP-Balancer: balancer1
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspect
let.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com w
ww.gstatic.com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chimps
tatic.com cdn.inspectlet.com widget.intercom.io *.intercomcdn.com;
Date: Fri, 16 Oct 20
…
.com connect.facebook.net cdnjs.cloudflare.com chimpstatic.com cdn.inspectlet.com widget.intercom.io *.
intercomcdn.com;
X-TransIP-Backend: web807
Cache-Control: no-store, no-cache, must-revalidate
Set-Cookie: PHPSESSID=f4afa7f05d00d14b353c8e95a3ac3946; path=/

Strict-Transport-Security: max-age=31536000;
Transfer-Encoding: chunked
Pragma: no-cache
Server: Apache
Link: <https://www.myndr.nl/?p=3257>; rel=shortlink
X-Content-Type-Options: nosniff
X-Xss
…
```

Actions to Take

1. See the remedy for solution.

2. Mark all cookies used within the application as secure. (If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)

Remedy

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to understand layer 2 and have gained access to a system between the victim and the web server.

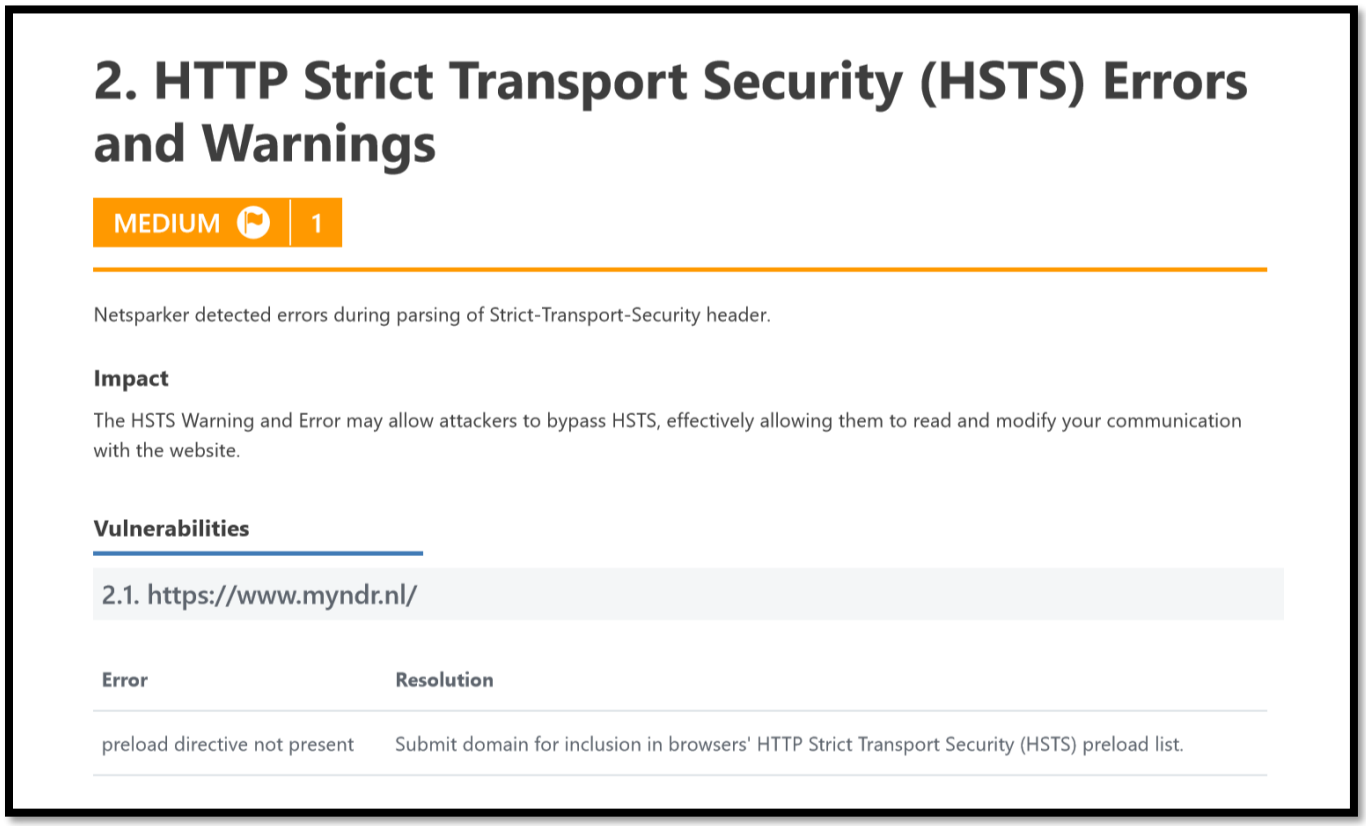
External References

- NET Cookie
- Secure Property How to Create Totally Secure Cookies
- Netsparker - Security Cookies - Secure Flag

Medium Risk Level. 1.[HTTP Strict Transport Security (HSTS) Errors and Warnings].

Netsparker detected errors during parsing of Strict-Transport-Security header.

Impact- The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.



2. HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM | 1

Netsparker detected errors during parsing of Strict-Transport-Security header.

Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Vulnerabilities

2.1. https://www.myndr.nl/

Error	Resolution
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

Request

```
GET / HTTP/1.1
Host: www.myndr.nl
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 698.5259 Total Bytes Received : 49039 Body Length : 47385 Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Type-Options: nosniff
Content-Type: text/html; charset=UTF-8
Server: Apache
Referrer-Policy: no-referrer-when-downgrade
X-TransIP-Backend: web807
Transfer-Encoding: chunked
X-Xss-Protection: 1; mode=block
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspect
let.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com w
ww.gstatic.com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chimps
tatic.com cdn.inspectlet.com widget.intercom.io *.intercomcdn.com;
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000;
X-Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspe
ctlet.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com
 www.gstatic.com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chim
pstatic.com cdn.inspectlet.com widget.intercom.io *.intercomcdn.com;
Set-Cookie: pll_language=nl; expires=Sat, 16-Oct-2021 19:38:58 GMT; Max-Age=31536000; path=/; secure
X-WebKit-CSP: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspectlet.com; sc
ript-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com www.gstatic.
com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chimpstatic.com c
dn.inspectlet.com widget.intercom.io *.intercomcdn.com;
X-TransIP-Balancer: balancer7
Date: Fri, 16 Oct 2020 19:38:57 GMT
Link: <https://www.myndr.nl/>; rel=shortlink

<!DOCTYPE html>
<html lang="nl-NL" class="no-js">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="http://gmpg.org/xfn/11">

<title>Myndr: word de baas over je aandacht</title>

<!-- The SEO Framework door Sybre Waaijer -->
<meta name="robots" content="max-snippet:
…
```

Remedy

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
    - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
    - The max-agemust be at least 31536000 seconds (1 year)
    - The includeSubDomainsdirective must be specified
    - The preloaddirective must be specified If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

External References

- HTTP Strict Transport Security (HSTS) HTTP Header
- Wikipedia - HTTP Strict Transport Security Implementation
- Check HSTS Preload status and eligibility

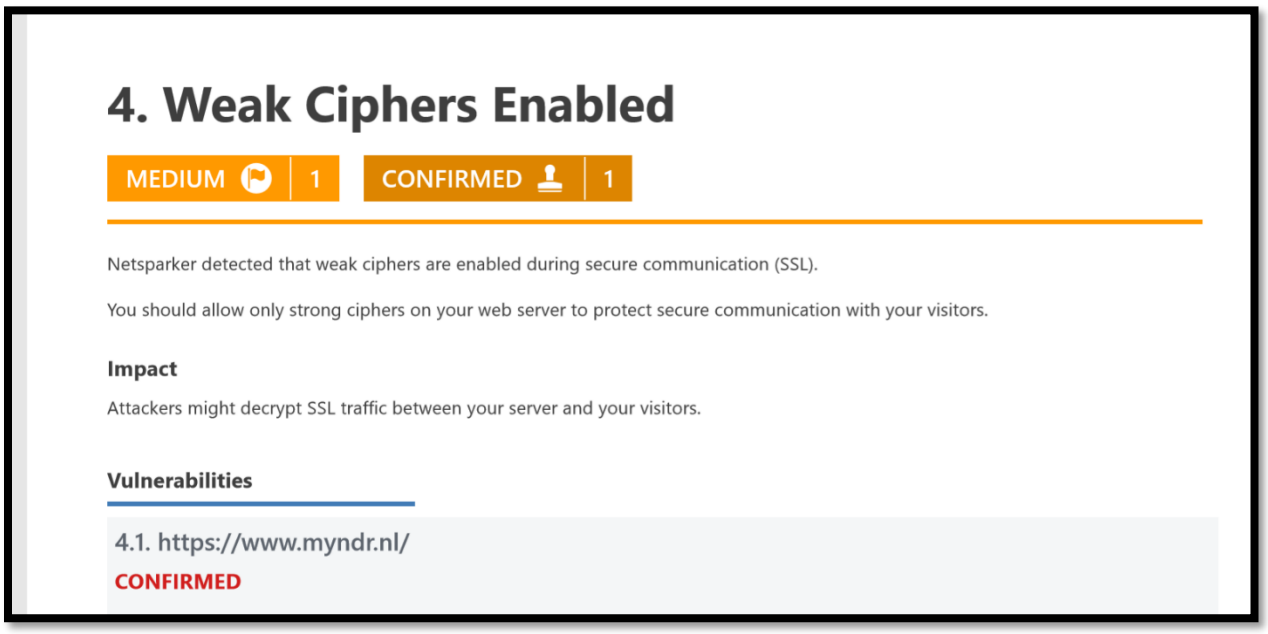
Medium Risk Level. 2.[Weak Ciphers Enabled].

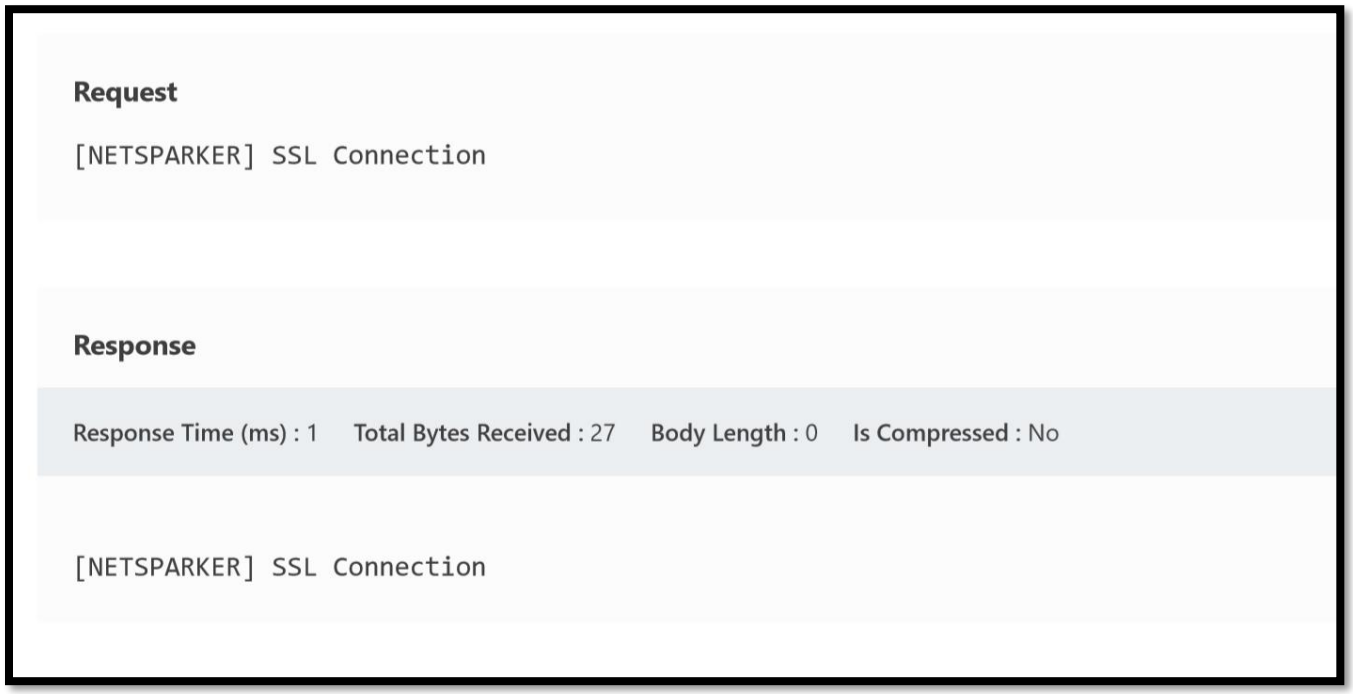
Netsparker detected that weak ciphers are enabled during secure communication (SSL). You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact - Attackers might decrypt SSL traffic between your server and your visitors.

List of Supported Weak Ciphers

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(0x006B)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA(0x0039)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(0xC028)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)





Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4

2. Lighttpd:

ssl.honor-cipher-order = "enable"

ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer**.

a. Click Start, click Run, type regedt32or type regedit, and then click OK.

b. In Registry Editor, locate the following registry key:

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

c. Set "Enabled" DWORD to "0x0" for the following registry keys:

SCHANNEL\Ciphers\DES 56/56

SCHANNEL\Ciphers\RC4 64/128

SCHANNEL\Ciphers\RC4 40/128

SCHANNEL\Ciphers\RC2 56/128

SCHANNEL\Ciphers\RC2 40/128

SCHANNEL\Ciphers\NULL

SCHANNEL\Hashes\MD5

Remedy

Configure your web server to disallow using weak ciphers.

External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- Zombie Poodle - Golden Doodle (CBC)
- Mozilla SSL Configuration Generator
- Strong Ciphers for Apache, Nginx and Lighttpd

Low Risk Level. 3.[[Possible] Cross-site Request Forgery].

Netsparker identified a possible Cross-Site Request Forgery. CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact- Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

Form Name(s)

- mc-embedded-subscribe-form

1. **https://www.myndr.nl/**

Request

```
GET / HTTP/1.1
Host: www.myndr.nl
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

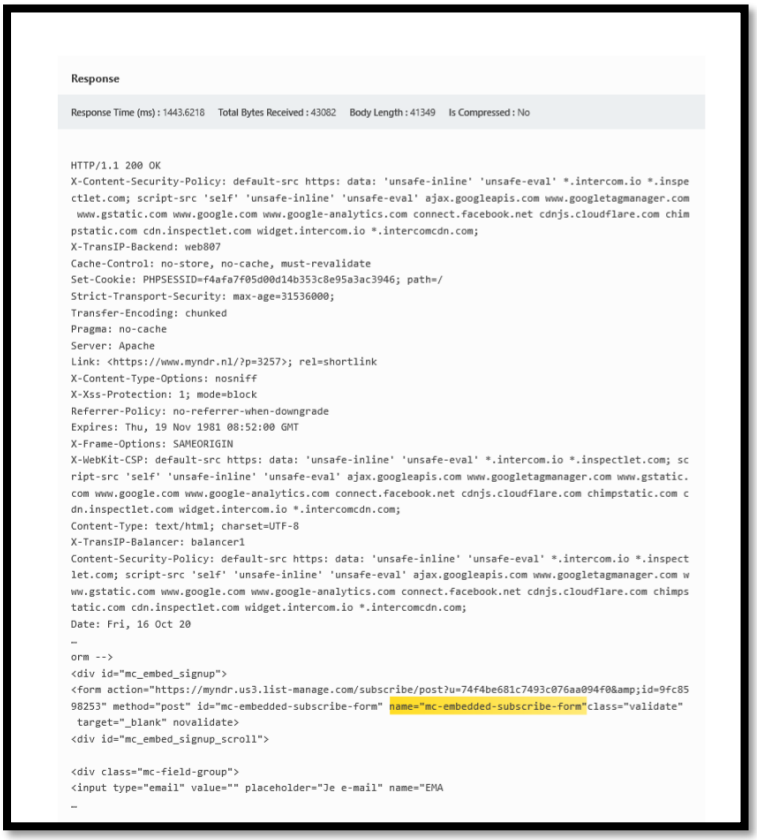
```
HTTP/1.1 200 OK
X-Content-Type-Options: nosniff
Content-Type: text/html; charset=UTF-8
Server: Apache
Referrer-Policy: no-referrer-when-downgrade
X-TransIP-Backend: web807
Transfer-Encoding: chunked
X-Xss-Protection: 1; mode=block
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspect
let.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com w
ww.gstatic.com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chimps
tatic.com cdn.inspectlet.com widget.intercom.io *.intercomcdn.com;
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000;
X-Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspe
ctlet.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com
 www.gstatic.com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chim
pstatic.com cdn.inspectlet.com widget.intercom.io *.intercomcdn.com;
Set-Cookie: pll_language=nl; expires=Sat, 16-Oct-2021 19:38:06 GMT; Max-Age=31536000; path=/; secure
X-WebKit-CSP: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspectlet.com; sc
ript-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com www.gstatic.
com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chimpstatic.com c
dn.inspectlet.com widget.intercom.io *.intercomcdn.com;
X-TransIP-Balancer: balancer7
Date: Fri, 16 Oct 2020 19:38:06 GMT
Link: <https://www.myndr.nl/>
…
orm -->
<div id="mc_embed_signup">
<form action="https://myndr.us3.list-manage.com/subscribe/post?u=74f4be681c7493c076aa094f0&amp;id=9fc85
98253" method="post" id="mc-embedded-subscribe-form" name="mc-embedded-subscribe-form"class="validate"
 target="_blank" novalidate>
<div id="mc_embed_signup_scroll">

<div class="mc-field-group">
<input type="email" value="" placeholder="Je e-mail" name="EMA
…
```

2. https://www.myndr.nl/abonneren/

Request

```
GET /abonneren/ HTTP/1.1
Host: www.myndr.nl
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: intercom-id-i93abyr7=2b271df9-8920-4d51-860b-493b5d0de4b3; intercom-session-i93abyr7=; myndr-co
okies=2; pll_language=nl
Referer: https://www.myndr.nl/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```



Response

Response Time (ms) : 1443.6218 Total Bytes Received : 43082 Body Length : 41349 Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspe
ctlet.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com
 www.gstatic.com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chim
pstatic.com cdn.inspectlet.com widget.intercom.io *.intercomcdn.com;
X-TransIP-Backend: web807
Cache-Control: no-store, no-cache, must-revalidate
Set-Cookie: PHPSESSID=f4afa7f05d00d14b353c8e95a3ac3946; path=/
Strict-Transport-Security: max-age=31536000;
Transfer-Encoding: chunked
Pragma: no-cache
Server: Apache
Link: <https://www.myndr.nl/?p=3257>; rel=shortlink
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Frame-Options: SAMEORIGIN
X-WebKit-CSP: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspectlet.com; sc
ript-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com www.gstatic.
com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chimpstatic.com c
dn.inspectlet.com widget.intercom.io *.intercomcdn.com;
Content-Type: text/html; charset=UTF-8
X-TransIP-Balancer: balancer1
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspect
let.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com w
ww.gstatic.com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chimps
tatic.com cdn.inspectlet.com widget.intercom.io *.intercomcdn.com;
Date: Fri, 16 Oct 20
…
orm -->
<div id="mc_embed_signup">
<form action="https://myndr.us3.list-manage.com/subscribe/post?u=74f4be681c7493c076aa094f0&amp;id=9fc85
98253" method="post" id="mc-embedded-subscribe-form" name="mc-embedded-subscribe-form"class="validate"
 target="_blank" novalidate>
<div id="mc_embed_signup_scroll">

<div class="mc-field-group">
<input type="email" value="" placeholder="Je e-mail" name="EMA
…
```

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.

    - For native XMLHttpRequest (XHR) object in JavaScript

      xhr = new XMLHttpRequest();
      xhr.setRequestHeader('custom-header', 'valueNULL');

    - For JQuery, if you want to add a custom header (or set of headers) to

      a. individual request

```
$.ajax({     url: 'foo/bar',     headers: { 'x-my-custom-header': 'some value' } });
```

      b. every request

```
$.ajaxSetup({
        headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
        beforeSend: function(xhr)
                {  xhr.setRequestHeader('x-my-custom-header', 'some value');
                }

    });
```

External References

- OWASP Cross-Site Request Forgery (CSRF)

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

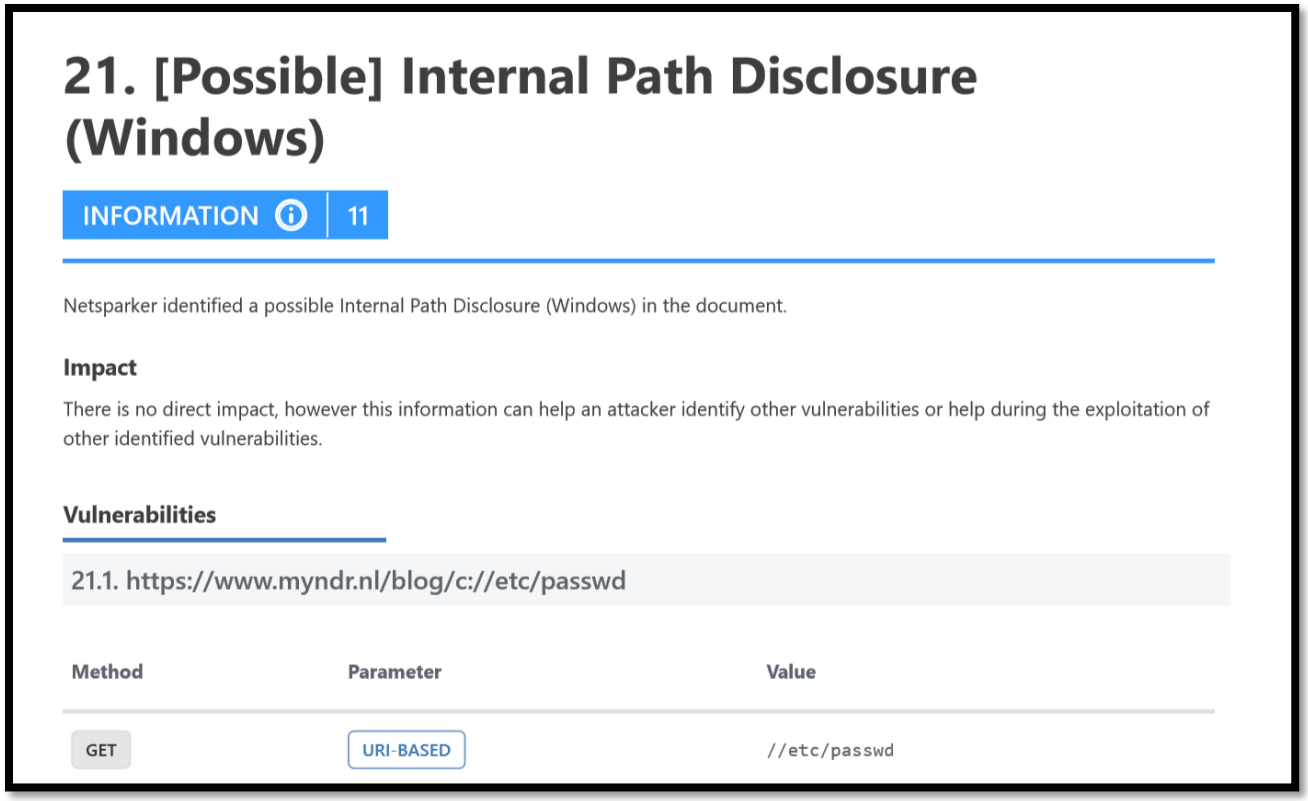
Informational. [[Possible] Internal Path Disclosure (Windows)].

Netsparker identified a possible Internal Path Disclosure (Windows) in the document.

Impact- There is no direct impact, however this information can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.

CustomField_CustomField_IdentifiedInternalPaths

- c:/etc/passwd



Request

```
GET /blog/c://etc/passwd HTTP/1.1
Host: www.myndr.nl
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
Connection: Keep-Alive
Cookie: PHPSESSID=f4afa7f05d00d14b353c8e95a3ac3946; pll_language=nl; intercom-id-i93abyr7=2b271df9-8920
-4d51-860b-493b5d0de4b3; intercom-session-i93abyr7=; myndr-cookies=261
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3181.756 Total Bytes Received : 1691 Body Length : 0 Is Compressed : No

```
HTTP/1.1 301 Moved Permanently
X-Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspe
ctlet.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com
 www.gstatic.com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chim
pstatic.com cdn.inspectlet.com widget.intercom.io *.intercomcdn.com;
X-TransIP-Backend: web807
Location: https://www.myndr.nl/blog/c:/etc/passwd
Cache-Control: no-cache, must-revalidate, max-age=0
Strict-Transport-Security: max-age=31536000;
Transfer-Encoding: chunked
X-Redirect-By: WordPress
Server: Apache
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade
Expires: Wed, 11 Jan 1984 05:00:00 GMT
X-Frame-Options: SAMEORIGIN
X-WebKit-CSP: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspectlet.com; sc
ript-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com www.gstatic.
com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chimpstatic.com c
dn.inspectlet.com widget.intercom.io *.intercomcdn.com;
Content-Type: text/html; charset=UTF-8
X-TransIP-Balancer: balancer2
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval' *.intercom.io *.inspect
let.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' ajax.googleapis.com www.googletagmanager.com w
ww.gstatic.com www.google.com www.google-analytics.com connect.facebook.net cdnjs.cloudflare.com chimps
tatic.com cdn.inspectlet.com widget.intercom.io *.intercomcdn.com;
Date: Fri, 16 Oct 2020 21:59:01 GMT
```

Remedy

Ensure this is not a false positive. Due to the nature of the issue, Netsparker could not confirm that this file path was actually the real file path of the target web server. Error messages should be disabled. Remove this kind of sensitive data from the output.

External References

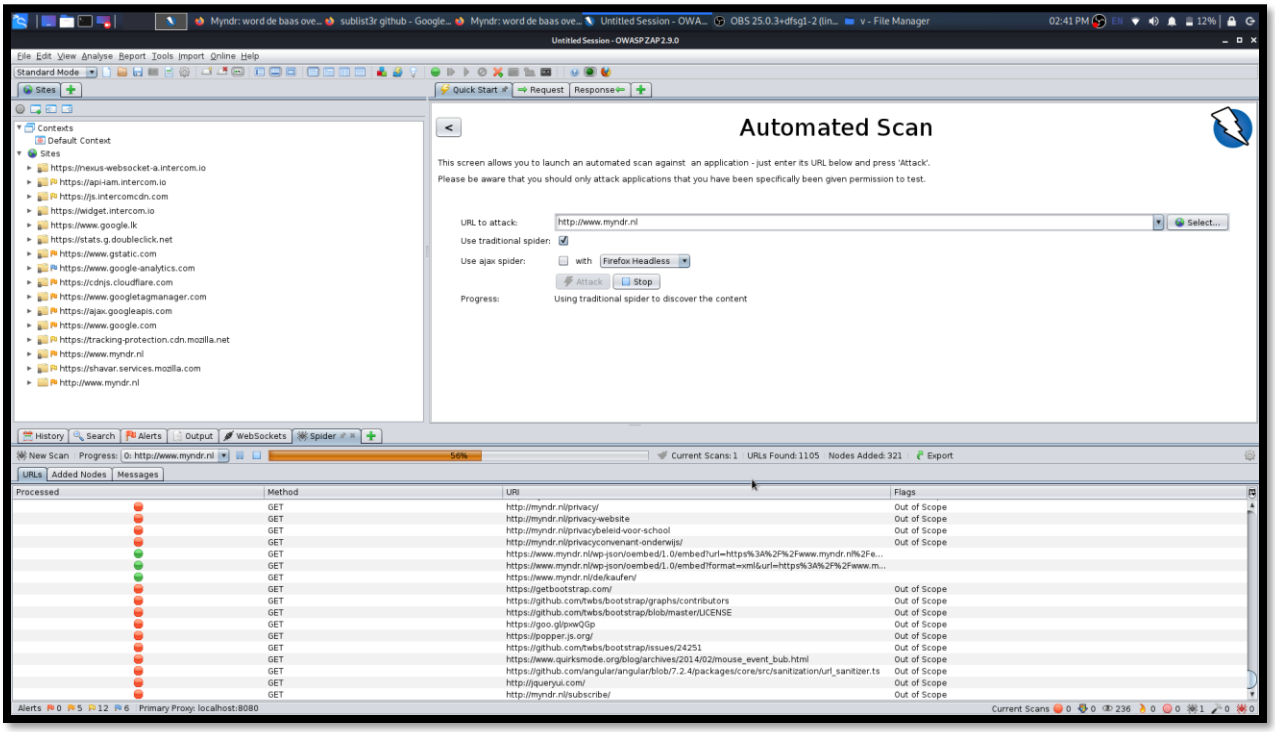
- OWASP - Full Path Disclosure

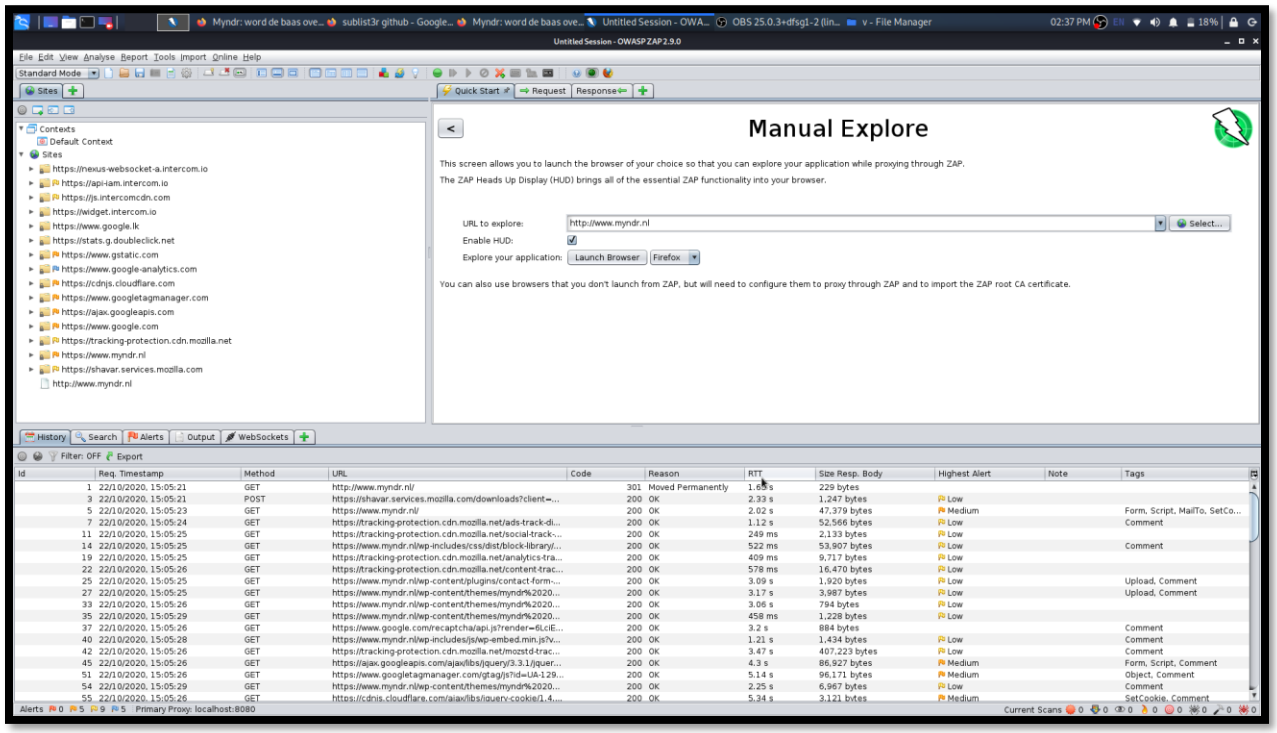
2. OWASP ZAP

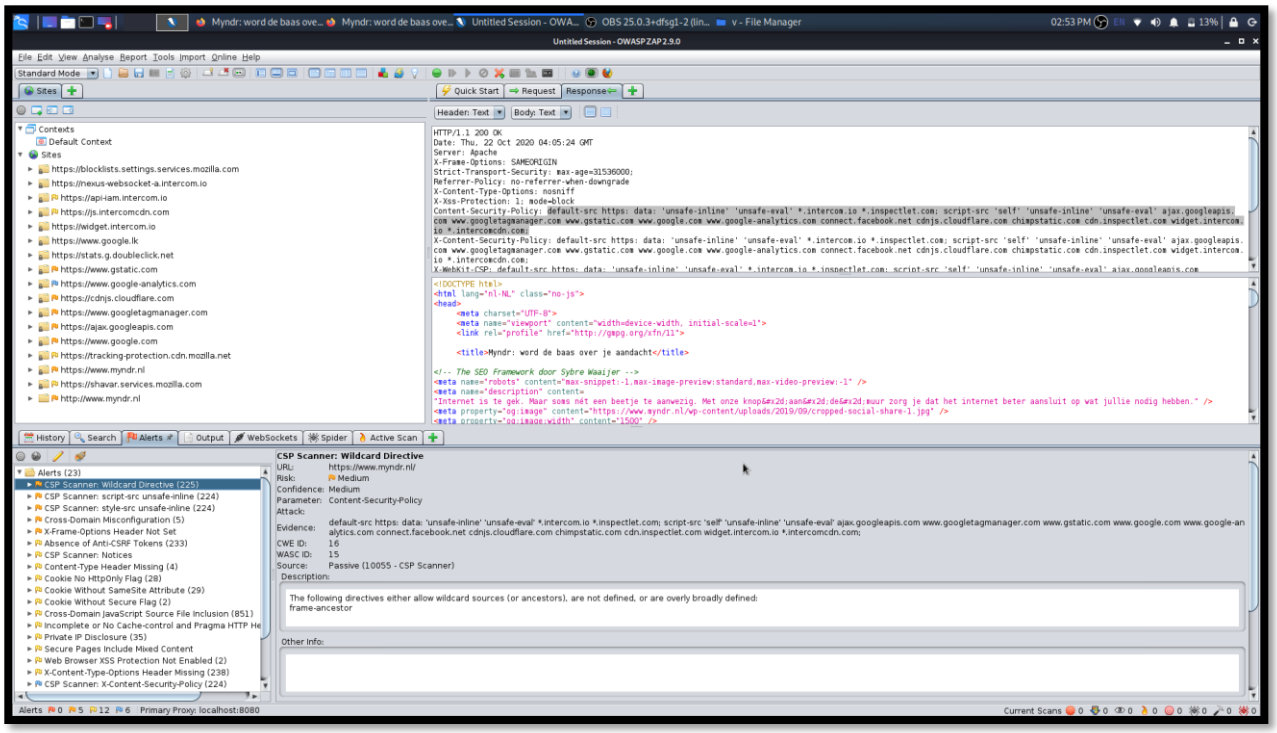
OWASP ZAP (short for Zed Attack Proxy) is an open-source web application security scanner. It helps the user to manage all the traffic going through it, including traffee uses https and used as a proxy server. The daemon mode can also be executed that is then managed through the REST API.

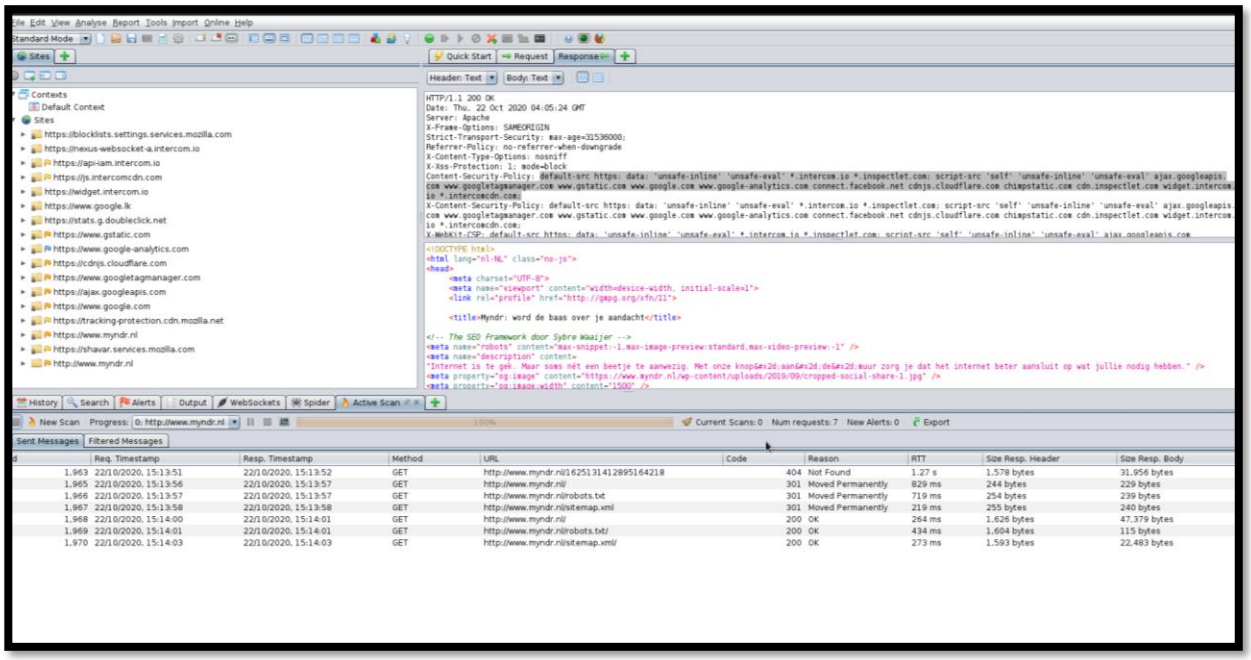
It took less than 30 minutes to scanned fully using ZAP tool which already built in kali2020. It generate a report under the category of Medium and Low level.

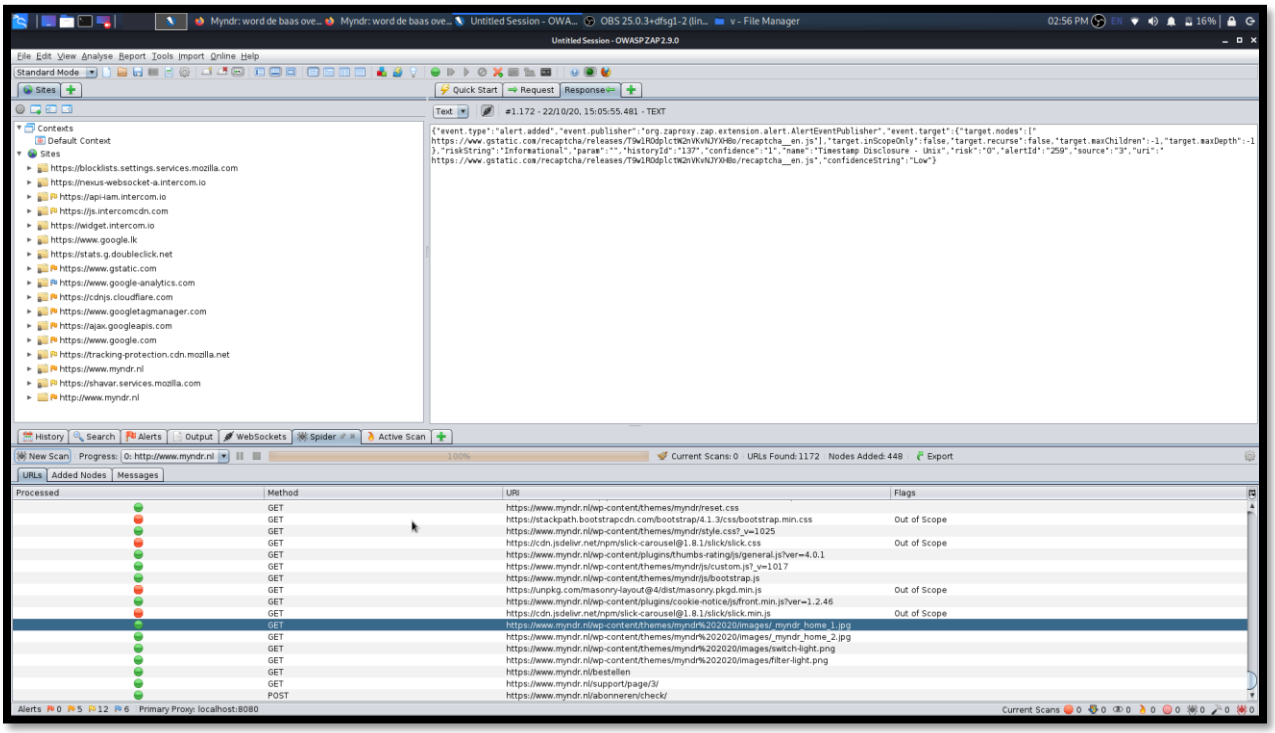
The Below Screen shots shows the out put and it vulnerabilities what we found using ZAP tool.

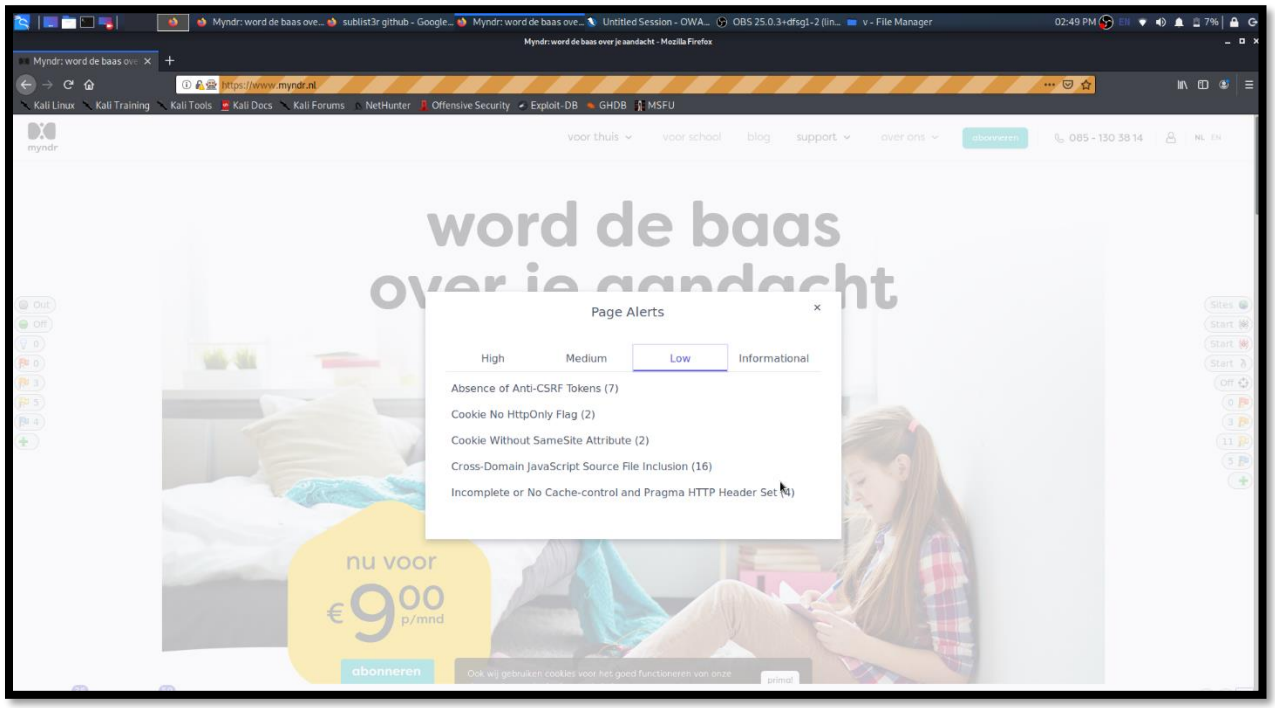


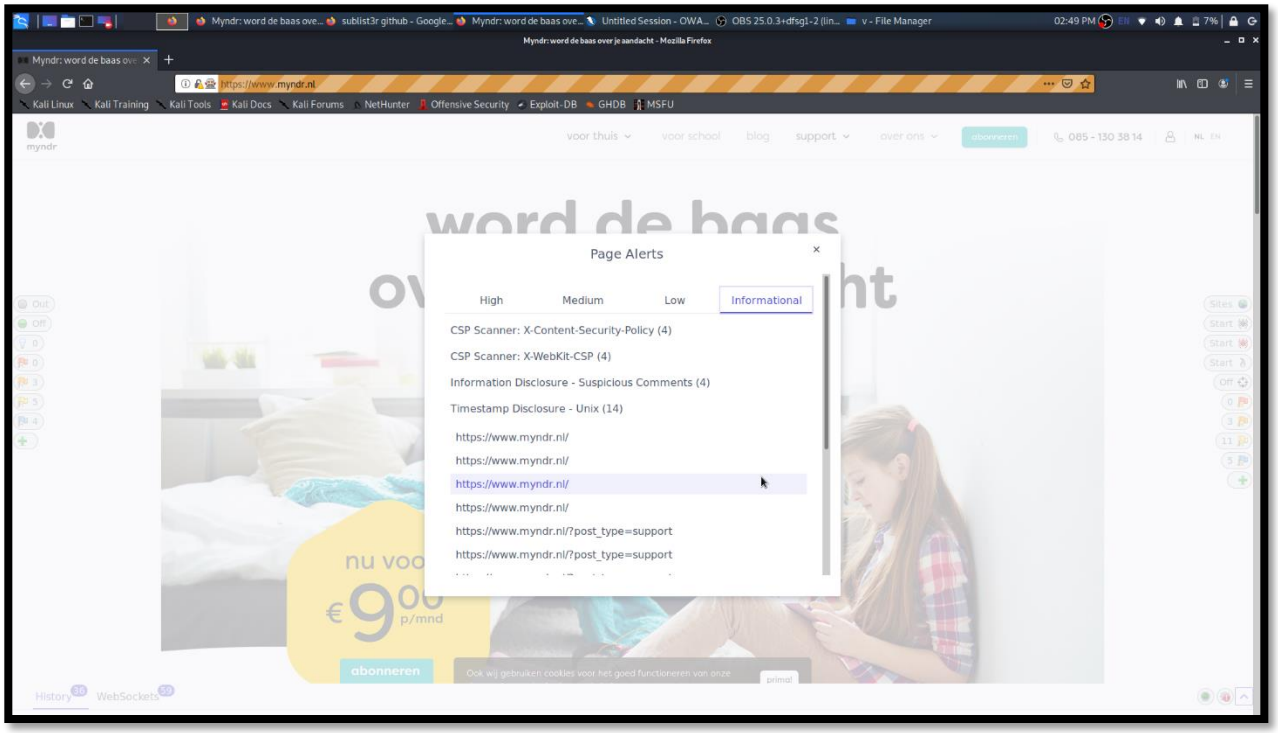

Untitled Session - OWASP ZAP 2.9.0
Manual Explore
This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.
The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.
URL to explore:
http://www.myndr.nl
Enable HUD:
Explore your application:
Launch Browser
Firefox
You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.

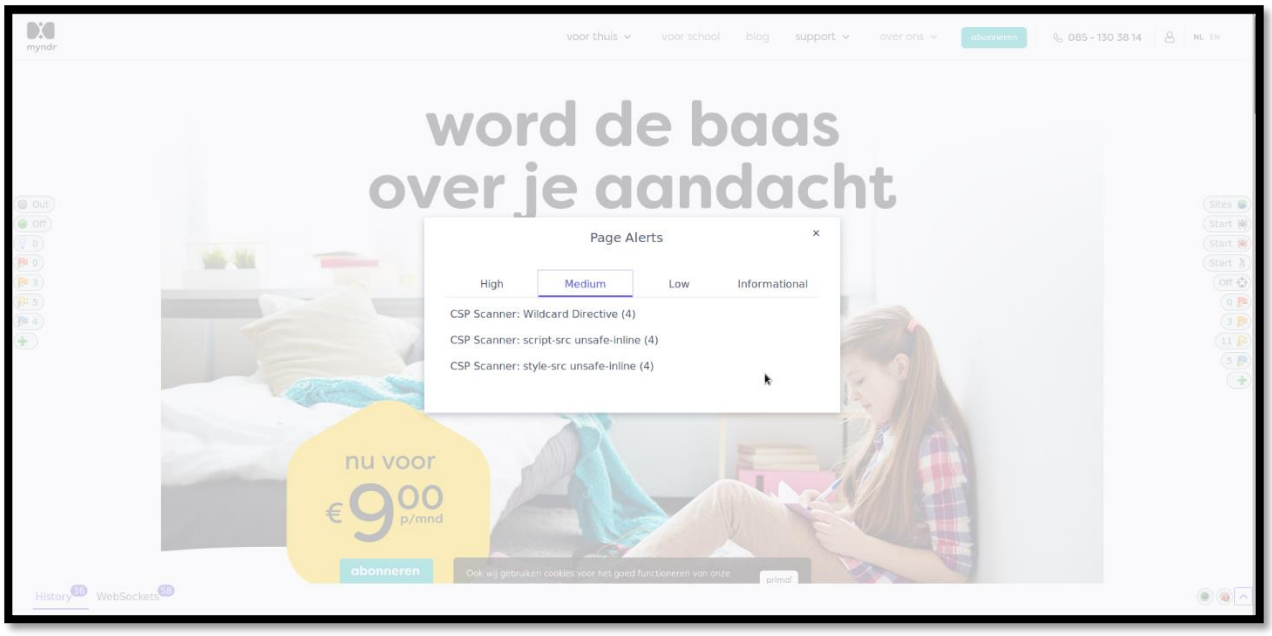

Untitled Session - OWASP ZAP 2.9.0
CSP Scanner: Wildcard Directive
URL: https://www.myndr.nl/
Risk: Medium
Confidence: Medium
Parameter: Content-Security-Policy
Attack:
CWE ID: 16
WASC ID: 15
Source: Passive (10055 - CSP Scanner)
Description:
The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined:
frame-ancestor
Other Info:






Page Alerts
High
Medium
Low
Informational
Absence of Anti-CSRF Tokens (7)
Cookie No HttpOnly Flag (2)
Cookie Without SameSite Attribute (2)
Cross-Domain JavaScript Source File Inclusion (16)
Incomplete or No Cache-control and Pragma HTTP Header Set (4)

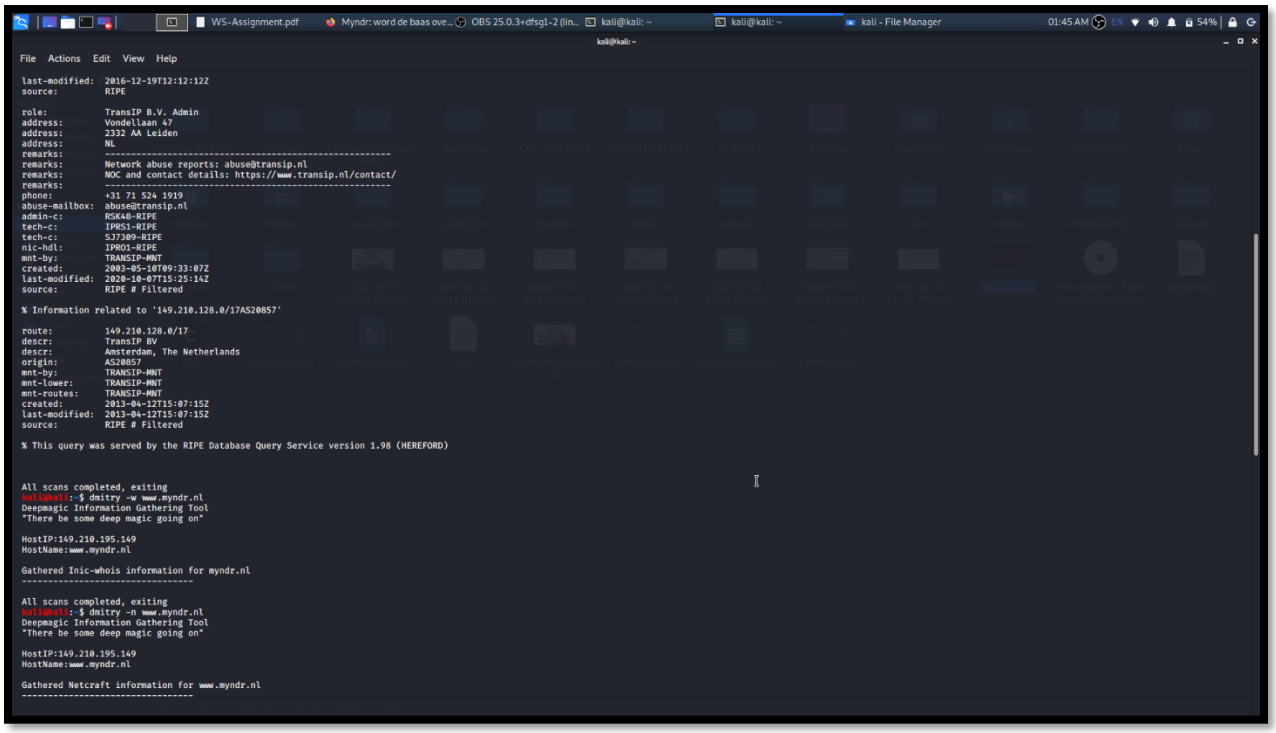

Page Alerts
High
Medium
Low
Informational
CSP Scanner: X-Content-Security-Policy (4)
CSP Scanner: X-WebKit-CSP (4)
Information Disclosure - Suspicious Comments (4)
Timestamp Disclosure - Unix (14)
https://www.myndr.nl/
https://www.myndr.nl/
https://www.myndr.nl/
https://www.myndr.nl/
https://www.myndr.nl/?post_type=support
https://www.myndr.nl/?post_type=support

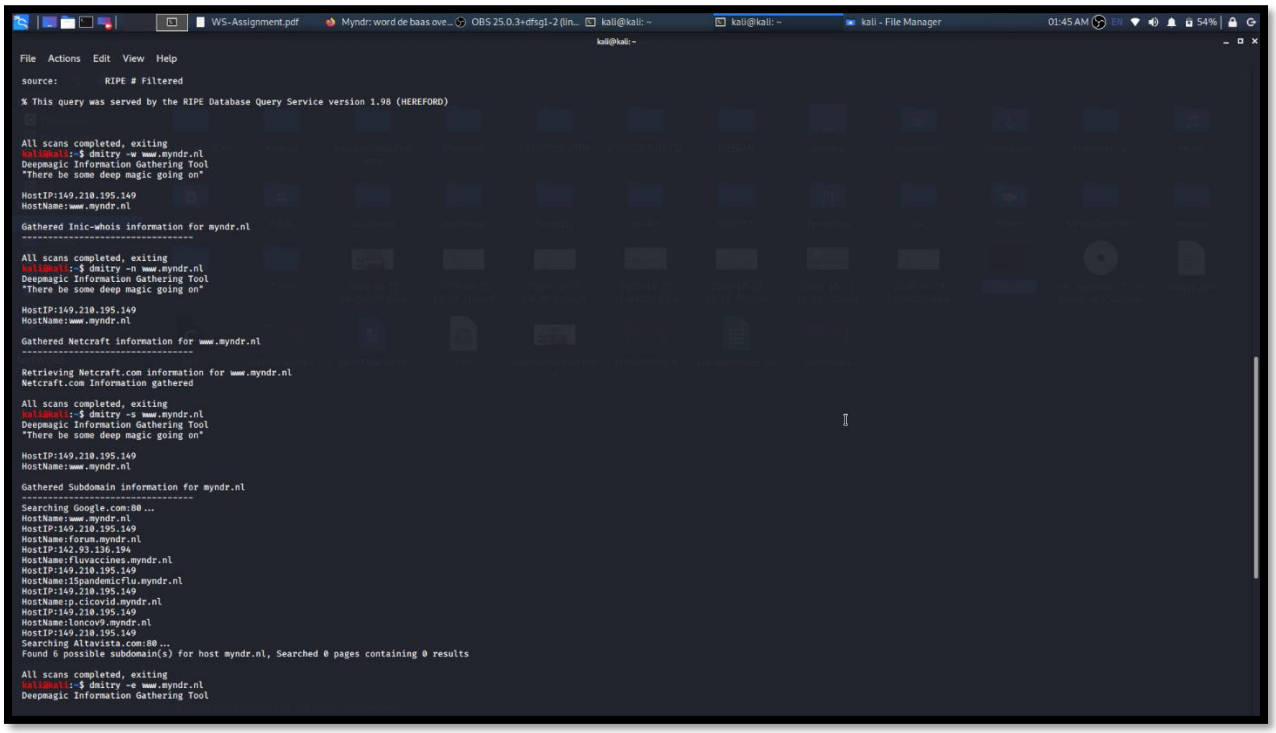

word de baas
over je aandacht
Page Alerts
High
Medium
Low
Informational
CSP Scanner: Wildcard Directive (4)
CSP Scanner: script-src unsafe-inline (4)
CSP Scanner: style-src unsafe-inline (4)
nu voor
€ 9 00
p/mnd
abonneren

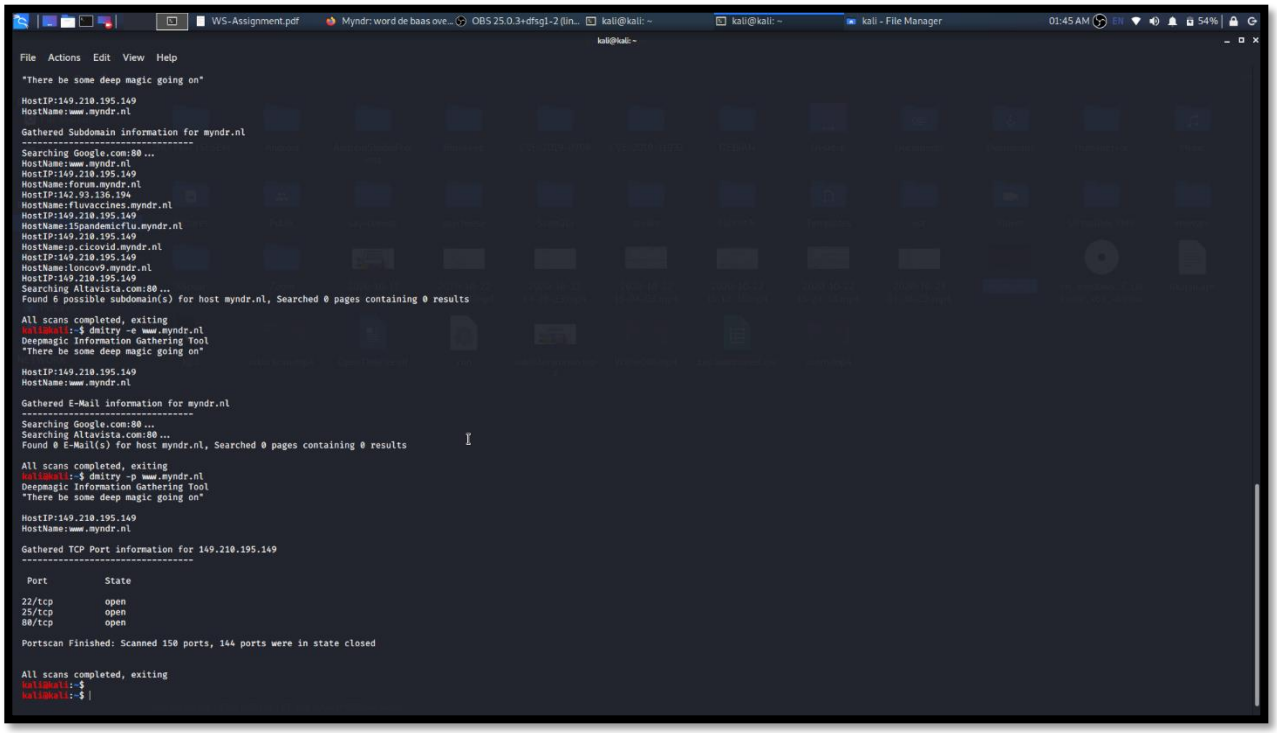
3. Dmitry

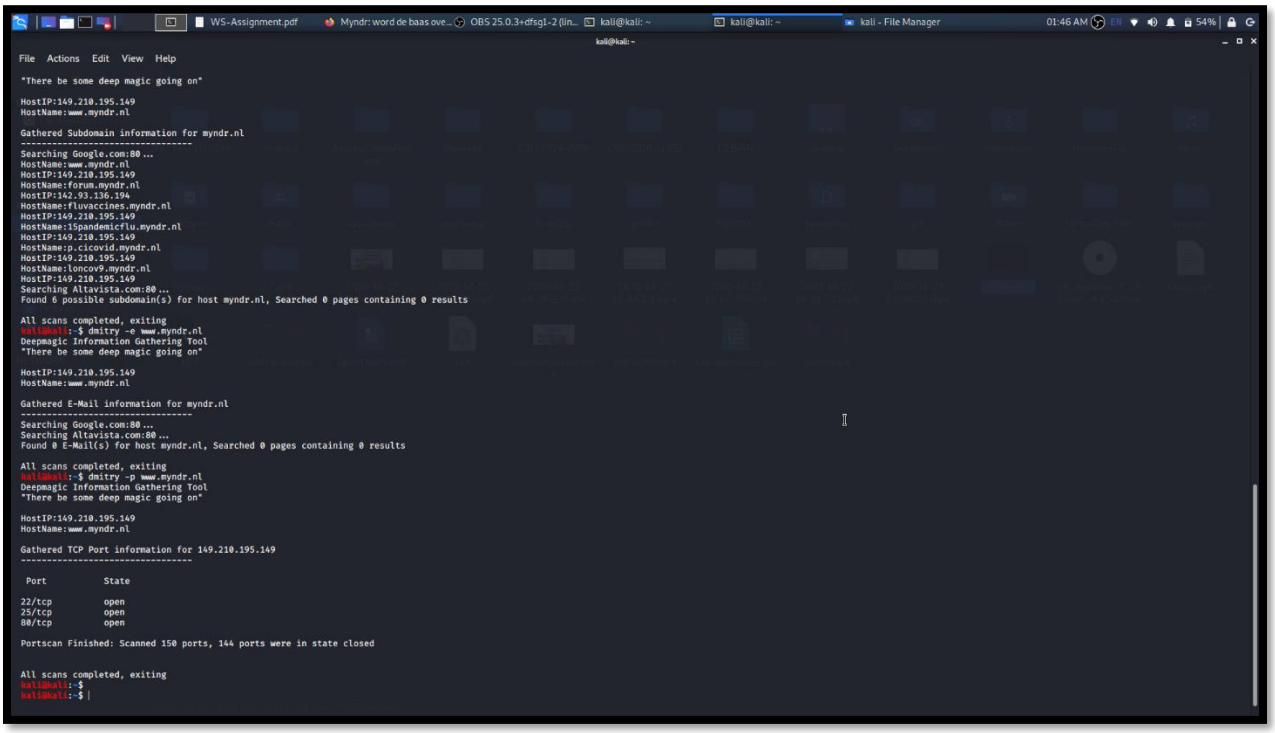
Dmitry is a command line utility included in Kali Linux, or Deep magic Information Collection Tool. It is designed so that a person can gather information on a target host for the public. It may be used to compile a collection of useful information items such as: who is of the host 's information.

It took few minutes only to scan domain. The following screen shot will demonstrate it.




WS-Assignment.pdf
Myndr: word de baas ove...
OBS 25.0.3+dfsg1-2 (lin...
kali@kali: ~
kali@kali: ~
kali - File Manager
01:45 AM
54%
kali@kali: ~
File Actions Edit View Help
source: RIPE # Filtered
% This query was served by the RIPE Database Query Service version 1.98 (HEREFORD)
All scans completed, exiting
kali@kali:~$ dmitry -w www.myndr.nl
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:149.210.195.149
HostName:www.myndr.nl
Gathered Inic-whois information for myndr.nl
All scans completed, exiting
kali@kali:~$ dmitry -n www.myndr.nl
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:149.210.195.149
HostName:www.myndr.nl
Gathered Netcraft information for www.myndr.nl
Retrieving Netcraft.com information for www.myndr.nl
Netcraft.com Information gathered
All scans completed, exiting
kali@kali:~$ dmitry -s www.myndr.nl
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:149.210.195.149
HostName:www.myndr.nl
Gathered Subdomain information for myndr.nl
Searching Google.com:80 ...
HostName:www.myndr.nl
HostIP:149.210.195.149
HostName:forum.myndr.nl
HostIP:142.93.136.194
HostName:fluvaccines.myndr.nl
HostIP:149.210.195.149
HostName:15pandemicflu.myndr.nl
HostIP:149.210.195.149
HostName:p.cicovid.myndr.nl
HostIP:149.210.195.149
HostName:loncov9.myndr.nl
HostIP:149.210.195.149
Searching Altavista.com:80 ...
Found 6 possible subdomain(s) for host myndr.nl, Searched 0 pages containing 0 results
All scans completed, exiting
kali@kali:~$ dmitry -e www.myndr.nl
Deepmagic Information Gathering Tool


WS-Assignment.pdf
Myndr: word de baas ove...
OBS 25.0.3+dfsg1-2 (lin...
kali@kali: ~
kali@kali: ~
kali - File Manager
01:45 AM
54%
kali@kali: ~
File Actions Edit View Help
"There be some deep magic going on"
HostIP:149.210.195.149
HostName:www.myndr.nl
Gathered Subdomain information for myndr.nl
Searching Google.com:80 ...
HostName:www.myndr.nl
HostIP:149.210.195.149
HostName:forum.myndr.nl
HostIP:142.93.136.194
HostName:fluvaccines.myndr.nl
HostIP:149.210.195.149
HostName:15pandemicflu.myndr.nl
HostIP:149.210.195.149
HostName:p.cicovid.myndr.nl
HostIP:149.210.195.149
HostName:loncov9.myndr.nl
HostIP:149.210.195.149
Searching Altavista.com:80 ...
Found 6 possible subdomain(s) for host myndr.nl, Searched 0 pages containing 0 results
All scans completed, exiting
kali@kali:~$ dmitry -e www.myndr.nl
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:149.210.195.149
HostName:www.myndr.nl
Gathered E-Mail information for myndr.nl
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host myndr.nl, Searched 0 pages containing 0 results
All scans completed, exiting
kali@kali:~$ dmitry -p www.myndr.nl
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:149.210.195.149
HostName:www.myndr.nl
Gathered TCP Port information for 149.210.195.149
Port State
22/tcp open
25/tcp open
80/tcp open
Portscan Finished: Scanned 150 ports, 144 ports were in state closed
All scans completed, exiting
kali@kali:~$
kali@kali:~$

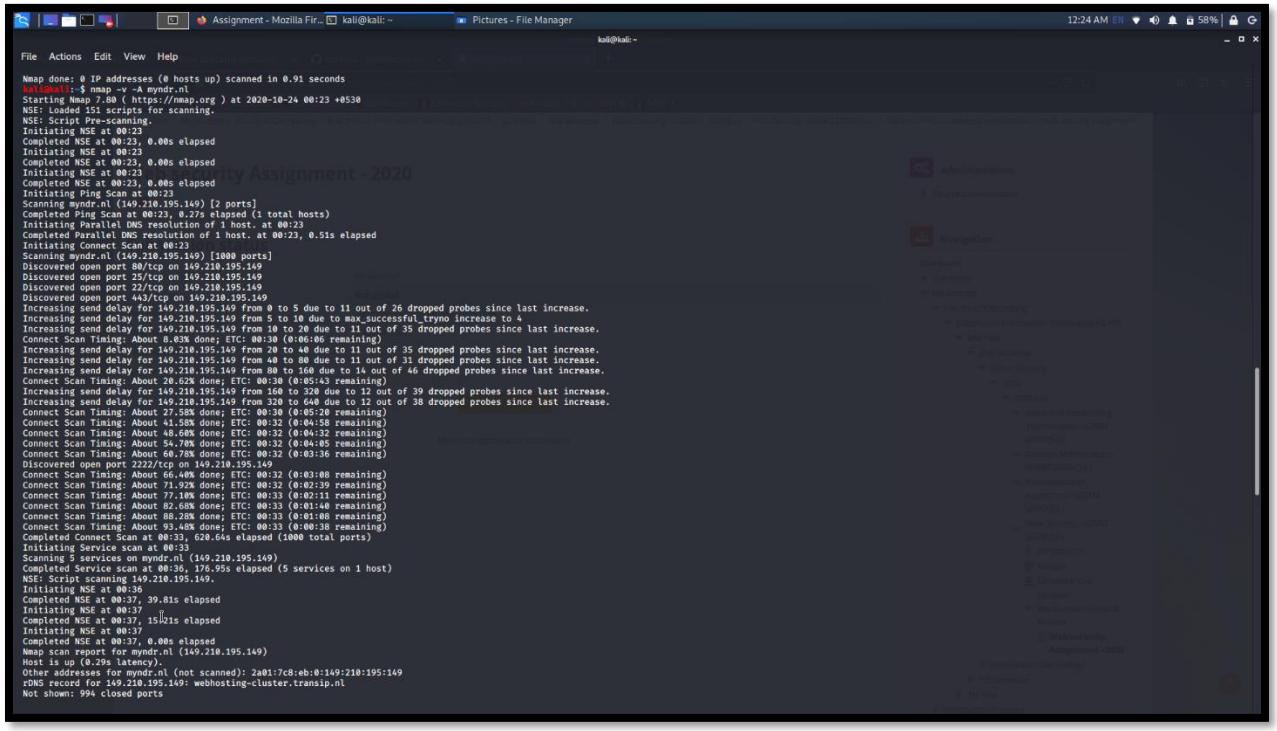

WS-Assignment.pdf
Myndr: word de baas ove...
OBS 25.0.3+dfsg1-2 (lin...
kali@kali: ~
kali@kali: ~
kali - File Manager
01:46 AM
54%
kali@kali: ~
File Actions Edit View Help
"There be some deep magic going on"
HostIP:149.210.195.149
HostName:www.myndr.nl
Gathered Subdomain information for myndr.nl
Searching Google.com:80 ...
HostName:www.myndr.nl
HostIP:149.210.195.149
HostName:forum.myndr.nl
HostIP:142.93.136.194
HostName:fluvaccines.myndr.nl
HostIP:149.210.195.149
HostName:15pandemicflu.myndr.nl
HostIP:149.210.195.149
HostName:p.cicovid.myndr.nl
HostIP:149.210.195.149
HostName:loncov9.myndr.nl
HostIP:149.210.195.149
Searching Altavista.com:80 ...
Found 6 possible subdomain(s) for host myndr.nl, Searched 0 pages containing 0 results
All scans completed, exiting
kali@kali:~$ dmitry -e www.myndr.nl
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:149.210.195.149
HostName:www.myndr.nl
Gathered E-Mail information for myndr.nl
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host myndr.nl, Searched 0 pages containing 0 results
All scans completed, exiting
kali@kali:~$ dmitry -p www.myndr.nl
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:149.210.195.149
HostName:www.myndr.nl
Gathered TCP Port information for 149.210.195.149
Port State
22/tcp open
25/tcp open
80/tcp open
Portscan Finished: Scanned 150 ports, 144 ports were in state closed
All scans completed, exiting
kali@kali:~$
kali@kali:~$

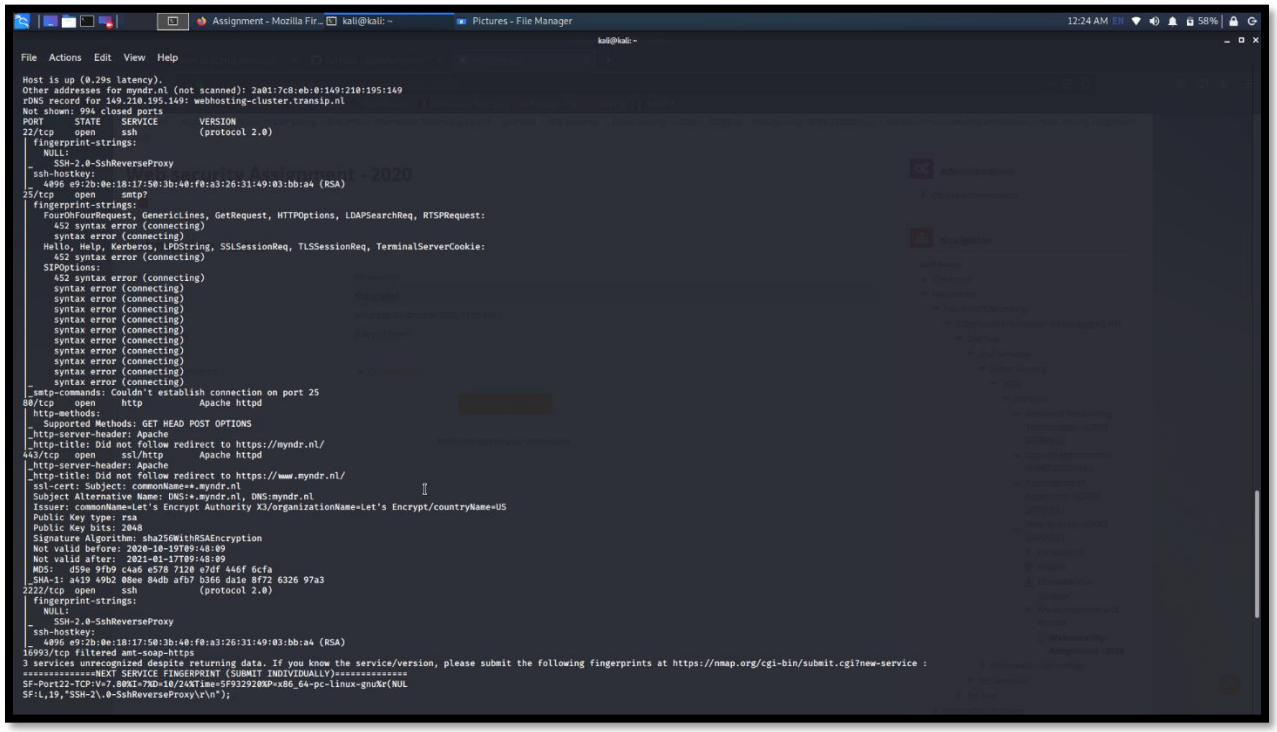
4.Nikto Tool

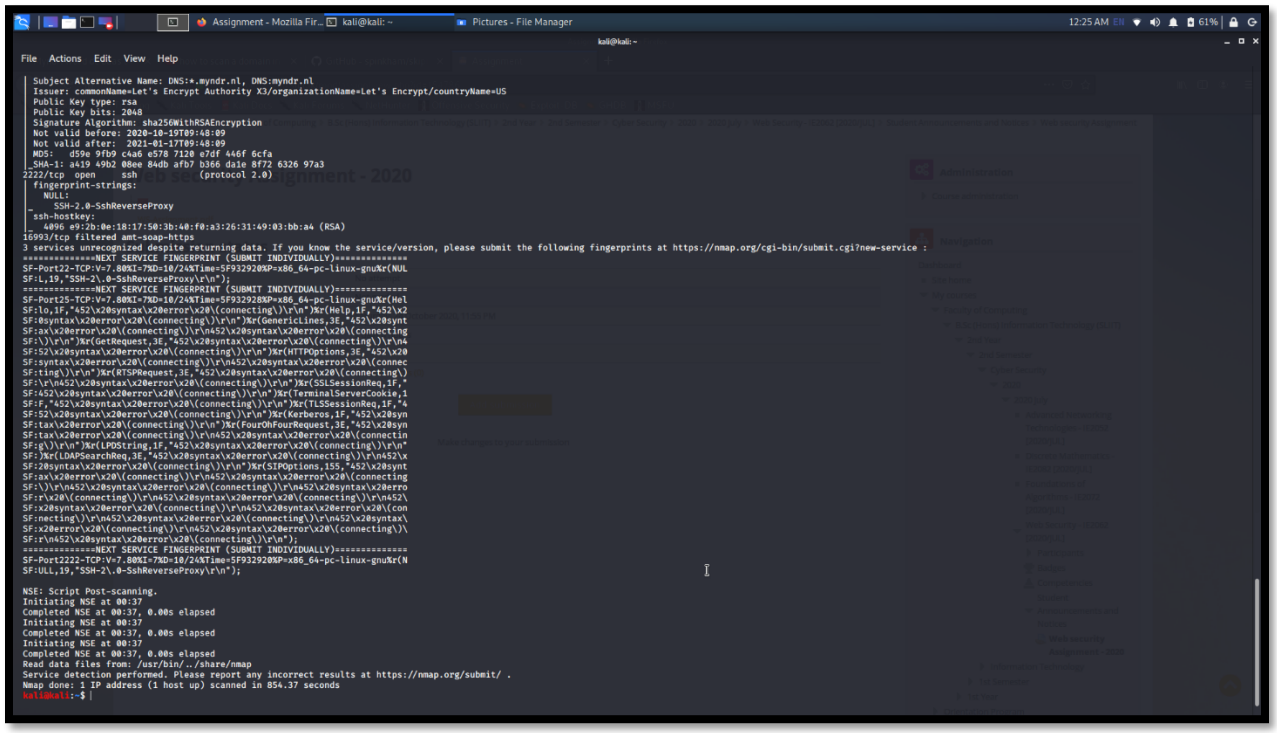
Nikto is a command-line vulnerability scanner free software, which checks web servers for unsafe data, obsolete server software, and other issues. Generic and server-specific controls are performed. It also gathers the collected cookies and prints them.

To scan you need to type **nikto -host https://www.myndr.nl/ .** It will generate the report with in few minutes such as Target IP address of the domain , target host name, target port, and starting name then some other information about vulnerabilities and their suggestion. Like in the screen shot below.

5.Namp Nmap is a network mapper that has emerged as one of the most freely accessible resources on the market for network exploration. There was a mistake. The software can be used to locate network live hosts, search the port, ping sweeps, detect the OS and detect the version.

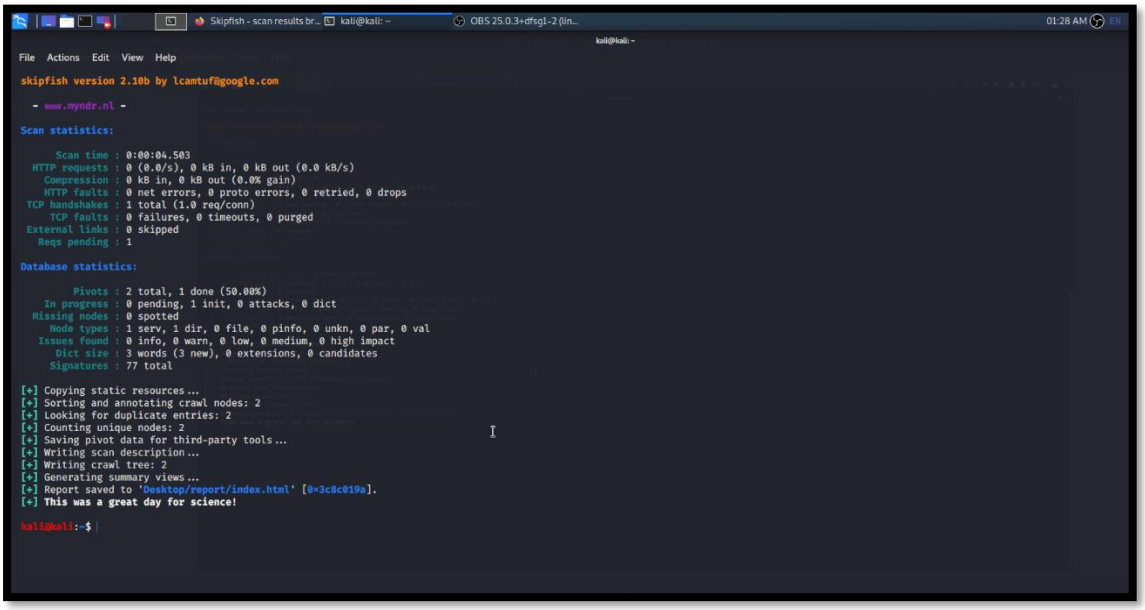


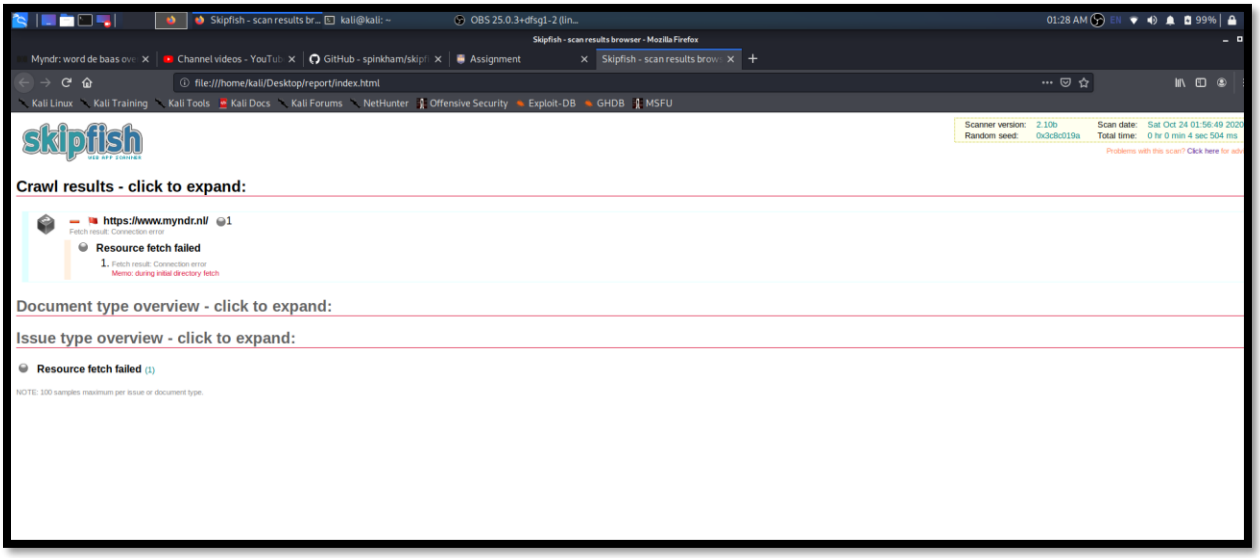



Assignment - Mozilla Fir...
kali@kali: ~
Pictures - File Manager
12:25 AM
61%
kali@kali: ~
File Actions Edit View Help
| Subject Alternative Name: DNS:*.myndr.nl, DNS:myndr.nl
| Issuer: commonName=Let's Encrypt Authority X3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-10-19T09:48:09
| Not valid after: 2021-01-17T09:48:09
| MD5: d59e 9fb9 c4a6 e578 7120 e7df 446f 6cfa
|_SHA-1: 4419 49b2 08ee 84db afb7 b366 da1e 8f72 6326 97a3
2222/tcp open ssh (protocol 2.0)
| fingerprint-strings:
| NULL:
|_ SSH-2.0-SshReverseProxy
| ssh-hostkey:
|_ 4096 e9:2b:0e:18:17:50:3b:40:f0:a3:26:31:49:03:bb:a4 (RSA)
16993/tcp filtered amt-soap-https
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port22-TCP:V=7.80%I=7%D=10/24%Time=5F932920%P=x86_64-pc-linux-gnu%r(NUL
SF:L,19,"SSH-2\.0-SshReverseProxy\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port25-TCP:V=7.80%I=7%D=10/24%Time=5F932928%P=x86_64-pc-linux-gnu%r(Hel
SF:lo,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(Help,1F,"452\x2
SF:0syntax\x20error\x20\(connecting\)\r\n")%r(GenericLines,3E,"452\x20synt
SF:ax\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connecting
SF:\)\r\n")%r(GetRequest,3E,"452\x20syntax\x20error\x20\(connecting\)\r\n4
SF:52\x20syntax\x20error\x20\(connecting\)\r\n")%r(HTTPOptions,3E,"452\x20
SF:syntax\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connec
SF:ting\)\r\n")%r(RTSPRequest,3E,"452\x20syntax\x20error\x20\(connecting\)
SF:\r\n452\x20syntax\x20error\x20\(connecting\)\r\n")%r(SSLSessionReq,1F,"
SF:452\x20syntax\x20error\x20\(connecting\)\r\n")%r(TerminalServerCookie,1
SF:F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(TLSSessionReq,1F,"4
SF:52\x20syntax\x20error\x20\(connecting\)\r\n")%r(Kerberos,1F,"452\x20syn
SF:tax\x20error\x20\(connecting\)\r\n")%r(FourOhFourRequest,3E,"452\x20syn
SF:tax\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connectin
SF:g\)\r\n")%r(LPDString,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n"
SF:)%r(LDAPSearchReq,3E,"452\x20syntax\x20error\x20\(connecting\)\r\n452\x
SF:20syntax\x20error\x20\(connecting\)\r\n")%r(SIPOptions,155,"452\x20synt
SF:ax\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connecting
SF:\)\r\n452\x20syntax\x20error\x20\(connecting\)\r\n452\x20syntax\x20erro
SF:r\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connecting\)\r\n452\
SF:x20syntax\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(con
SF:necting\)\r\n452\x20syntax\x20error\x20\(connecting\)\r\n452\x20syntax\
SF:x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connecting\)\
SF:r\n452\x20syntax\x20error\x20\(connecting\)\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port2222-TCP:V=7.80%I=7%D=10/24%Time=5F932920%P=x86_64-pc-linux-gnu%r(N
SF:ULL,19,"SSH-2\.0-SshReverseProxy\r\n");
NSE: Script Post-scanning.
Initiating NSE at 00:37
Completed NSE at 00:37, 0.00s elapsed
Initiating NSE at 00:37
Completed NSE at 00:37, 0.00s elapsed
Initiating NSE at 00:37
Completed NSE at 00:37, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 854.37 seconds
kali@kali:~$

6.SkipFish

Skipfish is an active vulnerability identification framework for web applications. It prepares an interactive map for the web in which a recursive crawl and dictionary-based samples are carried out. The performance from a series of successful (but preferably non-disruptive) safety checks would then be annotated.

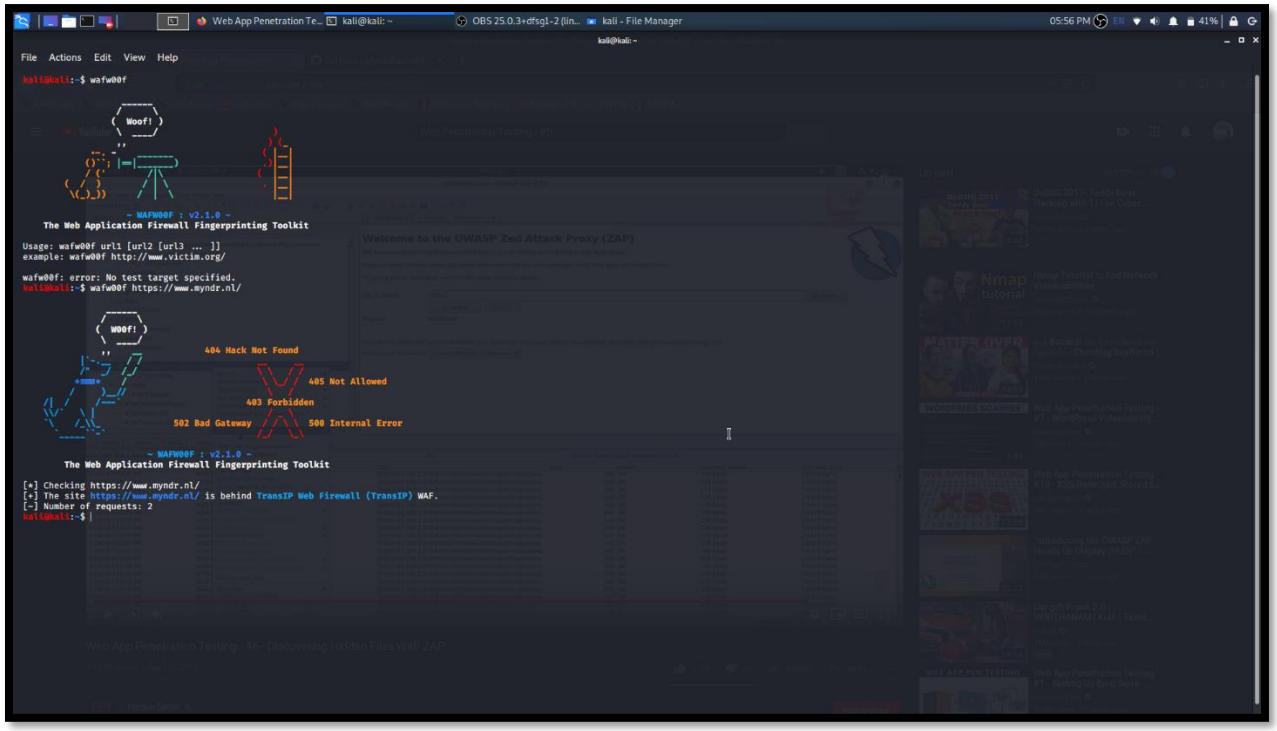




These things explained briefly in the video Documentary.

7.WafW00f

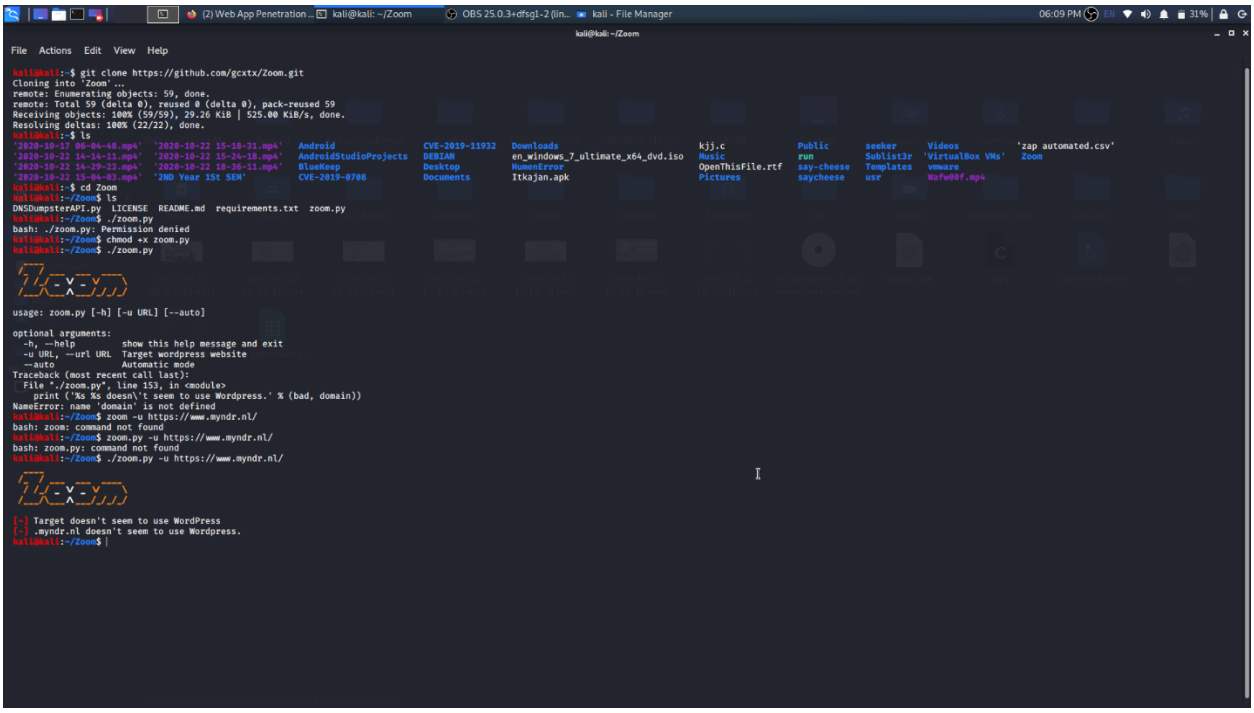
Wafw00f is just a program that automates a sequence of methods used to locate a WAF. A Site server with HTTP queries and approaches can only be queried. Wafw00f. It analyzes the answers and senses the internal firewall.



8.Sql Map

Sql map is an open source method used to find and manipulate SQL injection vulnerabilities in penetration tests. Sql map dynamically detects and uses SQL injection. Attacks by SQL Injection will take possession of SQL databases. There was a mistake. This weakness can be supported by Sql map.

9.Zoom


kali@kali: ~/Zoom
File Actions Edit View Help
kali@kali:~$ git clone https://github.com/gcxtx/Zoom.git
Cloning into 'Zoom'...
remote: Enumerating objects: 59, done.
remote: Total 59 (delta 0), reused 0 (delta 0), pack-reused 59
Receiving objects: 100% (59/59), 29.26 KiB | 525.00 KiB/s, done.
Resolving deltas: 100% (22/22), done.
kali@kali:~$ ls
'2020-10-17 06-04-48.mp4' '2020-10-22 15-18-31.mp4' Android CVE-2019-11932 Downloads kjj.c Public seeker Videos 'zap automated.csv'
'2020-10-22 14-14-11.mp4' '2020-10-22 15-24-18.mp4' AndroidStudioProjects DEBIAN en_windows_7_ultimate_x64_dvd.iso Music run Sublist3r 'VirtualBox VMs' Zoom
'2020-10-22 14-29-23.mp4' '2020-10-22 18-36-11.mp4' BlueKeep Desktop HumenError OpenThisFile.rtf say-cheese Templates vmware
'2020-10-22 15-04-03.mp4' '2ND Year 1St SEM' CVE-2019-0708 Documents Itkajan.apk Pictures saycheese usr Wafw00f.mp4
kali@kali:~$ cd Zoom
kali@kali:~/Zoom$ ls
DNSDumpsterAPI.py LICENSE README.md requirements.txt zoom.py
kali@kali:~/Zoom$ ./zoom.py
bash: ./zoom.py: Permission denied
kali@kali:~/Zoom$ chmod +x zoom.py
kali@kali:~/Zoom$ ./zoom.py
usage: zoom.py [-h] [-u URL] [--auto]
optional arguments:
-h, --help show this help message and exit
-u URL, --url URL Target wordpress website
--auto Automatic mode
Traceback (most recent call last):
File "./zoom.py", line 153, in <module>
print ('%s %s doesn\'t seem to use Wordpress.' % (bad, domain))
NameError: name 'domain' is not defined
kali@kali:~/Zoom$ zoom -u https://www.myndr.nl/
bash: zoom: command not found
kali@kali:~/Zoom$ zoom.py -u https://www.myndr.nl/
bash: zoom.py: command not found
kali@kali:~/Zoom$ ./zoom.py -u https://www.myndr.nl/
[-] Target doesn't seem to use WordPress
[-] .myndr.nl doesn't seem to use Wordpress.
kali@kali:~/Zoom$

Video Link:

Microsoft Teams Link >>>

https://teams.microsoft.com/_#/school/files/General?threadId=19%3Af6b3392a86254253b3a5f4500490ddd8%40thread.tacv2&ctx=channel&context=General&rootfolder=%252Fsites%252FIT19010236WSAssignment%252FShared%2520Documents%252FGeneral

Share Point Link:

https://mysliit.sharepoint.com/sites/IT19010236WSAssignment/Shared%20Documents/General

Google Drive Video >>>

https://drive.google.com/file/d/1P76DQgBwwdhDNnbbyV_70Laqbbfhn3ai/view?usp=sharing

References

- https://hackerone.com/picsart?type=team
- https://www.nmmapper.com/sys/tools/subdomainfinder/
- https://www.myndr.nl/
- https://www.youtube.com/watch?v=YKILueSxLR0&t=236s
- https://www.youtube.com/watch?v=2kaha1J-cQo
- https://www.youtube.com/watch?v=EmWXfq51pE0
- https://www.youtube.com/watch?v=GH9qn_DBzCk&t=564s
- https://www.youtube.com/watch?v=_js8PWU9t1k&t=217s