

Sri Lanka Institute of Information Technology



Individual Assignment

## **Bug Bounty Report**

**Web Security - IE2062**

BSc Honors in Information Technology Specializing in Cyber Security

<b>CASE STUDY NAME</b>	BUG BOUNTY Report 10
<b>CAMPUS/CENTER</b>	SLIIT KANDY UNI

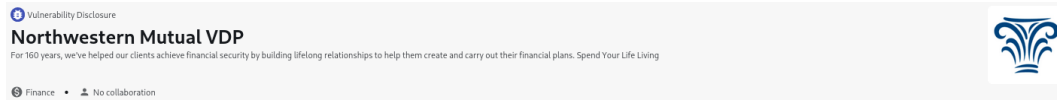
**Student Details**

	<b>Student Registration Number</b>	<b>Student Name</b>
<b>1</b>	IT23222854	JAYASINGHE B. I

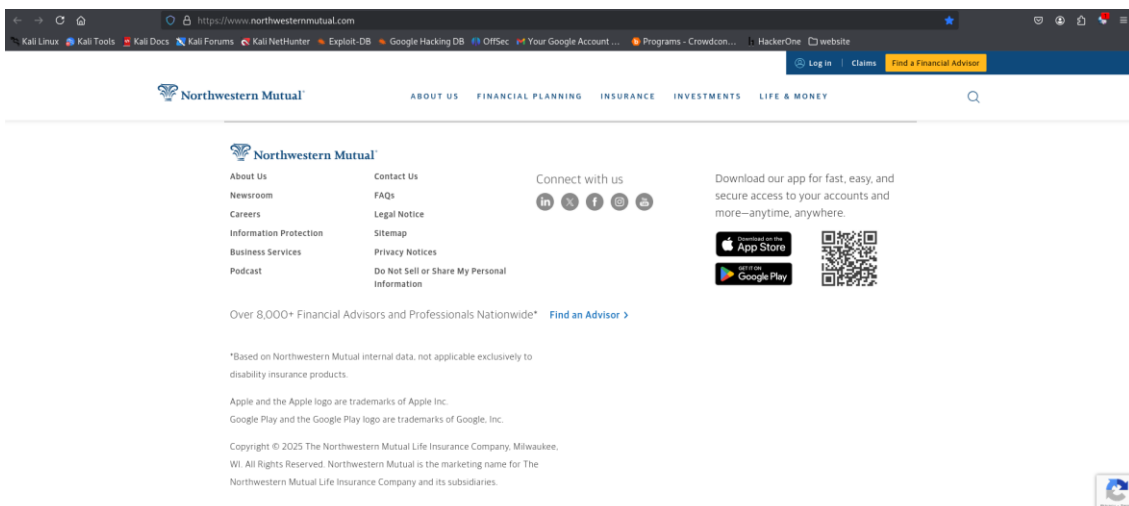
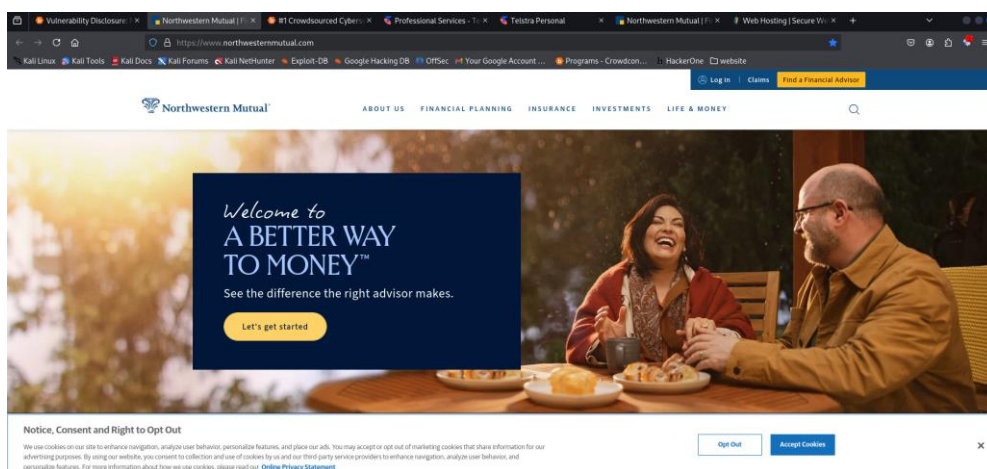
## Table of Contents

<b>Domain – <a href="https://www.northwesternmutual.com/">https://www.northwesternmutual.com/</a></b>	<b>4</b>
<b>1.Sensitive data Exposure</b>	<b>5</b>
1.1. nslookup & whois Enumeration	5
1.2 Retire.js	6
Summary fo the above vulnerabilities.	6
1.3 Wappalyzer	6
1.4 Netcraft	7
1.5 Katana	10
1.6 SecretFinder	10
<b>2. Firewall Detection</b>	<b>11</b>
2.1. Wafw00f	11
<b>3. Multi tool web Vulnerability Scanning</b>	<b>11</b>
3.1 Rapidscan	11
<b>4. OWASP ZAP</b>	<b>12</b>
<b>5. Injection</b>	<b>13</b>
5.1 Uniscan	13
<b>6. Using Components with Known Vulnerabilities</b>	<b>15</b>
6.1. Nmap	15
<b>Mitigation methods</b>	<b>16</b>

Domain – <https://www.northwesternmutual.com/>



- Link - <https://www.northwesternmutual.com/>
- Category – Vulnerability Disclosure Program (VDP)
- Type – Financial planning and life insurance company.



## 1. Sensitive data Exposure

### 1.1. nslookup & whois Enumeration

```
(binesh@BINZ) ~/Desktop/WS Assignment/Tools
$ nslookup northwesternmutual.com
Server:      10.0.2.3
Address:     10.0.2.3#53

Non-authoritative answer:
Name:   northwesternmutual.com
Address: 216.20.178.205
```

```
(binesh@BINZ) ~/Desktop/WS Assignment/Tools
$ whois northwesternmutual.com

Domain Name: NORTHWESTERNMUTUAL.COM
Registry Domain ID: 393329.DOMAIN.COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdn.com
Updated Date: 2025-04-23T01:13:48Z
Creation Date: 1995-04-26T00:00:00Z
Registry Expiry Date: 2027-04-27T00:00:00Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887882723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: AUTH01.NS.UU.NET
Name Server: NS1.NORTHWESTERNMUTUAL.COM
Name Server: NS2.NORTHWESTERNMUTUAL.COM
Name Server: NS6.NORTHWESTERNMUTUAL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-24T07:49:30Z <<<
```

```
Domain Name: northwesternmutual.com
Registry Domain ID: 393329.DOMAIN.COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2025-04-23T01:13:48Z
Creation Date: 1995-04-26T00:00:00Z
Registrar Registration Expiration Date: 2027-04-27T00:00:00Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887882723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Northwestern Mutual Life Insurance Company
Registrant Street: 720 East Wisconsin Avenue
Registrant City: Milwaukee
Registrant State/Province: WI
Registrant Postal Code: 53202
Registrant Country: US
Registrant Phone: +1.4146651444
Registrant Phone Ext:
Registrant Fax: +1.4146652467
Registrant Fax Ext:
Registrant Email: webmaster@northwesternmutual.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: The Northwestern Mutual Life Insurance Company
Admin Street: 720 East Wisconsin Avenue
Admin City: Milwaukee
Admin State/Province: WI
Admin Postal Code: 53202
Admin Country: US
Admin Phone: +1.4146651444
Admin Phone Ext:
Admin Fax: +1.4146652467
Admin Fax Ext:
Admin Email: webmaster@northwesternmutual.com
```

```
Tech Name: Domain Administrator
Tech Organization: The Northwestern Mutual Life Insurance Company
Tech Street: 720 East Wisconsin Avenue
Tech City: Milwaukee
Tech State/Province: WI
Tech Postal Code: 53202
Tech Country: US
Tech Phone: +1.4146651444
Tech Phone Ext:
Tech Fax: +1.4146652467
Tech Fax Ext:
Tech Email: webmaster@northwesternmutual.com
Name Server: ns6.northwesternmutual.com
Name Server: auth01.ns.uu.net
Name Server: ns2.northwesternmutual.com
Name Server: auth61.ns.uu.net
Name Server: ns1.northwesternmutual.com
DNSSEC: Unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2025-04-23T01:13:48Z <<<
```

The nslookup and whois information that have gathered provides insight into the website's domain and the associated IP address.

Here's how this information could potentially be used by malicious actors.

- Information disclosure
- DNS-related attacks
- Phishing
- Network reconnaissance
- IP address blocking

These are some remedies.

- Ensure that sensitive information such as server IP addresses, software versions, and network configurations are not publicly disclosed.
- Implement DNS security best practices.
- Educate users about phishing techniques and encourage them to verify the authenticity of emails and websites before providing sensitive information.
- Regularly audit your network for vulnerabilities.
- Implement firewall rules and other security measures.

### 1.2 Retire.js

#### Retire.js


☒ Enabled ☐ Show unknown

axios	1.6.8	Found in <a href="https://www.northwesternmutual.com/react-assets/templates/vendors~main.df7b945e.js">https://www.northwesternmutual.com/react-assets/templates/vendors~main.df7b945e.js</a> - Vulnerability info:  High Server-Side Request Forgery in axios CVE-2024-39338 GHSA-8hc4-vh64-cxmj  High axios Requests Vulnerable To Possible SSRF and Credential Leakage via Absolute URL CVE-2025-27152 GHSA-jr5f-v2jv-69x6	<a href="#">[1]</a> <a href="#">[2]</a> <a href="#">[3]</a> <a href="#">[4]</a> <a href="#">[5]</a> <a href="#">[6]</a> <a href="#">[7]</a> <a href="#">[8]</a> <a href="#">[9]</a> <a href="#">[10]</a> <a href="#">[1]</a> <a href="#">[2]</a> <a href="#">[3]</a> <a href="#">[4]</a> <a href="#">[5]</a> <a href="#">[6]</a> <a href="#">[7]</a>
-------	-------	--	--

Summary for the above vulnerabilities.

Library	Version	Found at URL	Vulnerability Description	Severity	Reference (CVE/GHSA)
Axios	1.6.8	<a href="#">Vendors Main JS</a>	Server-Side Request Forgery (SSRF) vulnerability	High	CVE-2024-39338, GHSA-8hc4-vh64-cxmj
Axios	1.6.8	<a href="#">Vendors Main JS</a>	Requests Vulnerable to SSRF & Credential Leakage via Absolute URL	High	CVE-2023-27152, GHSA-jr5f-v2jv-69x6

### 1.3 Wappalyzer


Wappalyzer - Techn...

#### Analytics

- [Pinterest Conversion Tag](#)
- [Dynatrace](#)
- [Adobe Analytics](#)
- [Heap](#) 4.23.6
- [Google Analytics](#)
- [Facebook Pixel](#)
- [LinkedIn Insight Tag](#)
- [Google Ads Conversion Tracking](#)

#### Advertising

- [Google Ads](#)
- [Twitter Ads](#)
- [Microsoft Advertising](#)
- [DoubleClick Floodlight](#)

#### JavaScript frameworks

- [React](#)
- [styled-components](#) 5.3.1
- [Adobe Client Data Layer](#) 2.0.2

#### Development

- [styled-components](#) 5.3.1
- [core-js](#) 3.32.2

#### Tag managers

- [Adobe Experience Platform Launch](#)
- [Google Tag Manager](#)

#### Security

- [reCAPTCHA](#)

#### Font scripts

- [Adobe Fonts](#)

#### Cookie compliance

- [OneTrust](#)

#### A/B testing

- [Adobe Target](#) 2.11.7

#### Personalisation

- [Adobe Target](#) 2.11.7

#### Customer data platform

- [Adobe Experience Platform Identity Service](#)

#### Miscellaneous

- [PWA](#)
- [Open Graph](#)
- [Webpack](#)
- [ServiceNow](#)

Check for exposed tracking IDs, misconfigured scripts, and excessive data collection that may lead to privacy issues.

Review JavaScript injections, third-party cookie risks, and improper iframe handling.

## Web Security - IE2062

Year 2 Semester 2 - 2025

Identify outdated versions, vulnerable dependencies, and potential supply chain risks.  
 Ensure proper implementation of reCAPTCHA, CSP headers, and anti-CSRF tokens.

### 1.4 Netcraft

Background

Site title	Northwestern Mutual   Financial Planning & Life Insurance Company	Date first seen	October 2012
Site rank	31085	Primary language	English
Description	Not Present		

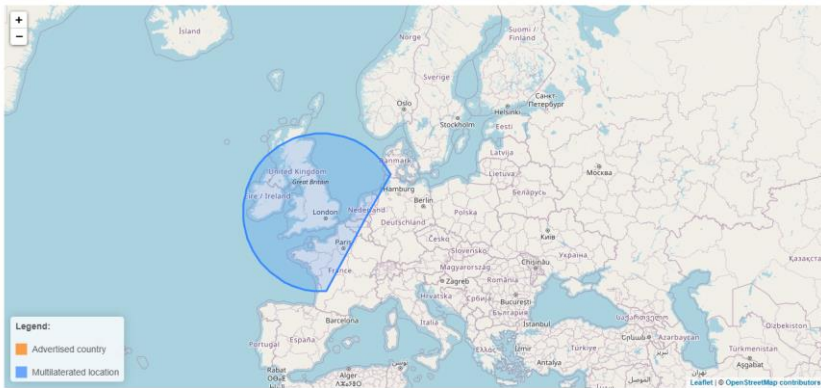
Network

Site	https://www.northwesternmutual.com/	Domain	northwesternmutual.com
Netblock Owner	Amazon.com, Inc.	Nameserver	fk1-26-ib-internet.northwesternmutual.com
Hosting company	Amazon	Domain registrar	corporatedomains.com
Hosting country	US	Nameserver organisation	whois.corporatedomains.com
IPv4 address	13.224.68.30 (Winseal US)	Organisation	Northwestern Mutual Life Insurance Company, 720 East Wisconsin Avenue, Milwaukee, 53202, US
IPv4 autonomous systems	AS16509	DNS admin	hostmaster@nsdc.ho.nmfc.com
IPv6 address	2600:900c:21c:bc00:fad9:ce00:93a1	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	AS16509	DNS Security Extensions	Enabled
Reverse DNS	server-13-224-68-30.dub2.r.cloudfront.net		

IP delegation

IP Geolocation

We use multilateration to independently determine the location of a server. [Read more.](#)



SSL/TLS

Assurance	Organisation validation	Perfect Forward Secrecy	Yes
Common name	northwesternmutual.com	Supported TLS Extensions	<a href="#">RFC4446</a> <a href="#">RFC4446</a> <a href="#">RFC4366</a> <a href="#">RFC4366</a> <a href="#">RFC3731</a>
Organisation	Northwestern Mutual Life Insurance	Application Layer Protocol Negotiation	h2
State	Wisconsin	Next Protocol Negotiation	Not Present
Country	US	Issuing organisation	SSL Corporation
Organisational unit	Not Present	Issuer common name	Entrust OV TLS Issuing RSA CA 1
Subject Alternative Name	<a href="#">northwesternmutual.com</a> , <a href="#">www.northwesternmutual.com</a> , <a href="#">lifeinsurance.com</a> , <a href="#">www.lifeinsurance.com</a>	Issuer unit	Not Present
Validity period	From Jan 9 2025 to Feb 8 2026 (12 months, 4 weeks, 1 day)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	US
Server	AmazonS3	Issuer state	Not Present
Public key algorithm	rsaEncryption	Certificate Revocation Lists	<a href="#">http://crls.ssl.com/Entrust-OV-TLS-1-R1.crl</a>
Protocol version	TLSv1.3	Certificate Hash	4A9dHfAe5nftzaQDQXQADyypQ
Public key length	2048	Public Key Hash	c92bd07f0c42340a80e022b09dcb8e9f22c376e863e890a022c14e954e88
Certificate check	OK	OCSP servers	<a href="#">http://ocsp.ssl.com</a>
Signature algorithm	sha256WithRSAEncryption	OCSP stapling response	No response received
Serial number	0x1c46c8e84b3772405e108dad1e698459		
Cipher	TLS_AES_128_GCM_SHA256		

**Web Security - IE2062****Year 2 Semester 2 - 2025****Certificate Transparency****Signed Certificate Timestamps (SCTs)**

Source	Log	Timestamp	Signature Verification
Certificate	Unknown ZBHEKQ57K3HKEICLQ8q88089q6Se6v7VA819zfa+	2025-01-09 17:31:11	Unknown
Certificate	Unknown 6YD0xy1q0/6A294K08K8A1OLKXD67000BBL5VWQ9+	2025-01-09 17:31:11	Unknown
Certificate	Unknown 016vPOuq74G0y/2B7P3K8v-buJ10VLSK8K1rGHT1E+	2025-01-09 17:31:11	Unknown

**SSLv3/POODLE**

This site does not support the SSL version 3 protocol.

[More information about SSL version 3 and the POODLE vulnerability.](#)

**SSL Certificate Chain**

Common name	SSL.com TLS RSA Root CA 2022
Organisational unit	Not Present
Organisation	SSL Corporation
Validity period	From 2022-08-25 to 2046-08-19
↓	
Common name	Entrust OV TLS Issuing RSA CA 1
Organisational unit	Not Present
Organisation	SSL Corporation
Validity period	From 2024-08-22 to 2027-08-22

**Sender Policy Framework**

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of [rules](#). Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see [open-spf.org](#).

Warning: It appears that this host does not have an SPF record. There may be an SPF record on [northwesternmutual.com](#). Check the [site report](#).

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any [mail-enabled subdomains](#). It is recommended to add an SPF record to any subdomain with an MX record.

**Web Trackers**

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

4 known trackers were identified.

**Companies****Categories**

Company	Primary Category	Tracker	Popular Sites with this Tracker
Adobe	Analytics	Adobe marketingcloud	<a href="#">www.canada.ca</a> , <a href="#">www.ibm.com</a> , <a href="#">www.dhl.de</a>
	CDN	Adobe TypeKit Web Fonts	<a href="#">www.newsnow.com</a> , <a href="#">www.kaldata.com</a> , <a href="#">www.compia.org</a>
Google	Widget	Google widget	<a href="#">www.iffatoquotidiano.it</a> , <a href="#">www.behance.net</a> , <a href="#">www.kaggle.com</a>
Heap	Analytics	Heap	

**Site Technology** (fetched today)

**Cloud & PaaS**

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service.

Technology	Description	Popular sites using this technology
Amazon Web Services - S3	Cloud storage service (Simple Storage Service)	<a href="#">www.eccouncil.org</a> , <a href="#">www.xike.com</a> , <a href="#">www.techtarget.com</a>
Amazon Web Services - CloudFront	Amazon Content Delivery Network	<a href="#">www.imdb.com</a> , <a href="#">www.primevideo.com</a> , <a href="#">www.wappalizer.com</a>

**Server-Side**

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	

**Client-Side**

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	<a href="#">www.drepl.com</a> , <a href="#">www.netflix.com</a> , <a href="#">www.amazon.com</a>
Asynchronous JavaScript	No description	<a href="#">www.microsoft.com</a> , <a href="#">www.sitok.com</a> , <a href="#">www.virustotal.com</a>



## Web Security - IE2062

Year 2 Semester 2 - 2025

### Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
Adobe TypeKit Web Fonts	No description	<a href="http://www.behance.net">www.behance.net</a> , <a href="http://www.kaldata.com">www.kaldata.com</a> , <a href="http://www.newsnow.co.uk">www.newsnow.co.uk</a>

### Content Delivery Network

A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.

Technology	Description	Popular sites using this technology
Cloudfront	No description	<a href="http://www.crunchyroll.com">www.crunchyroll.com</a> , <a href="http://www.amazon.es">www.amazon.es</a> , <a href="http://www.amazon.fr">www.amazon.fr</a>

### Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	<a href="http://www.twitch.tv">www.twitch.tv</a> , <a href="http://www.amazon.de">www.amazon.de</a> , <a href="http://discord.com">discord.com</a>

### HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encode	Gzip HTTP Compression protocol	<a href="http://www.jobthal.com">www.jobthal.com</a> , <a href="http://www.amazon.co.jp">www.amazon.co.jp</a> , <a href="http://www.espedia.com">www.espedia.com</a>

### Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
X-Content-Type-Options	Browser MIME type sniffing is disabled	<a href="http://docs.google.com">docs.google.com</a> , <a href="http://mail.google.com">mail.google.com</a>
Document Compatibility Mode	A meta-tag used in Internet Explorer 8 to enable compatibility mode	<a href="http://erp.fxpro.com">erp.fxpro.com</a> , <a href="http://chat.deepseek.com">chat.deepseek.com</a> , <a href="http://app.powerbi.com">app.powerbi.com</a>
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	
X-XSS-Protection Block	Block pages on which cross-site scripting is detected	<a href="http://teams.microsoft.com">teams.microsoft.com</a>
Referrer Policy	Restrict referrer information included in subsequent requests	<a href="http://www.perplexity.ai">www.perplexity.ai</a> , <a href="http://www.startpage.com">www.startpage.com</a> , <a href="http://paragon-fe.amazon.com">paragon-fe.amazon.com</a>
Strict-Transport-Security (including subdomains)	No description	

### Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	<a href="http://www.linkedin.com">www.linkedin.com</a> , <a href="http://webmail.vincichoteles.com">webmail.vincichoteles.com</a> , <a href="http://accounts.google.com">accounts.google.com</a>

### HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	<a href="http://chatgpt.com">chatgpt.com</a>

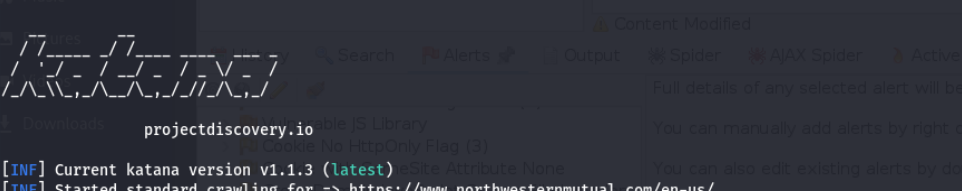
### CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	<a href="http://stackoverflow.com">stackoverflow.com</a> , <a href="http://mail.yahoo.com">mail.yahoo.com</a>

### 1.5 Katana

```
(binosh@BINZ)-[~/Desktop/WS_Assignment/Tools]
$ katana -u "https://www.northwesternmutual.com/en-us/" -jc -d 2 | grep "js$" | uniq | sort > ~/gapnic/katana.txt
```



### 1.6 SecretFinder

```
(secretfinder_env)-(binosh@BINZ)-[~/Desktop/WS_Assignment/Tools/SecretFinder]
$ echo "https://www.northwesternmutual.com/en-us/" | while read url; do python3 SecretFinder.py -i "$url" -o cli >> ~/north/SecretFinder.txt; done
```

```
(secretfinder_env)-(binosh@BINZ)-[~/Desktop/WS_Assignment/Tools/SecretFinder]
$ cat ~/north/SecretFinder.txt
[ + ] URL: https://www.northwesternmutual.com/en-us
google_api -> AIzaSyDoQaSL4iGvxiUrd4qNm2AzJob3SPNpkeI
google_captcha -> 6LfrTNgUAAAAAH5PukGUXA8sfC54GhFvd6fPyr8e
google_captcha -> 6LfDgz8UAAAAAH5YaeXLoogd944BheK0b2VZoRr
twilio_account_sid -> ACgCAYAAADw66xhAAACXB1WQMAAFiVAAB
twilio_app_sid -> ApygXOE0kkkLkoVbBU5dojkuWntC6yblL2
possible_Creds -> PwDDOuWcta9uJmR/oJaoJM5Kp0ynUJhgbfFn0/YkH7VstK9uBmRvntmgJFY6mtHIYJ5vLFQw6hLQs8nTpEuEzhTSLb/LvCPNGhnmkmc0b0SXebJgnLHrHw1Pme0qS3t7MPZQUX1Wm+uyS2Yvmq
a4BG1mtINZOHZZRzyF8MYySWYzgkfIVERf55dss+o961Wxaa3YI78JNC7wCvQ2XHsCIIadpleguLu8zeMjKvUp2+V0Ubgucu8wz5PuAG6dyLkvrFqVLCub1Djh57I5Ye0TpfYewreUqNNN16C6TfL/qh4CVzWdXAaku1s/LidJQ
FAj5YmtYhe4NlFwvNadYiKZqtAfe0Eoxd5qftbHyd851J4S2YEBa9hLurTAQA/wPEZbLaEef7VgAAAAABJR5UerKJggg=="</image><circle
```

**cat ~/ north /katana.txt | while read url; do python3 SecretFinder.py -i \$url -o cli  
>> ~/north/SecretFinder.txt; done**

The aim of using this tool is to read URLs from the katana.txt file and then utilize SecretFinder.py to find sensitive data in those URLs and output them into the SecretFinder.txt file.

**python3 SecretFinder.py -i "\$url" -o cli >> ~/north/SecretFinder.txt** → To run SecretFinder.py for each URL (\$url), specifying the input URL with -i, output format as CLI with -o cli, and appends the output to SecretFinder.txt.

```
(secretfinder_env)-(binosh@BINZ)-[~/Desktop/WS_Assignment/Tools/SecretFinder]
$ cat ~/north/SecretFinder.txt
[ + ] URL: https://www.northwesternmutual.com/en-us
google_api -> AIzaSyDoQaSL4iGvxiUrd4qNm2AzJob3SPNpkeI
google_captcha -> 6LfrTNgUAAAAAH5PukGUXA8sfC54GhFvd6fPyr8e
google_captcha -> 6LfDgz8UAAAAAH5YaeXLoogd944BheK0b2VZoRr
twilio_account_sid -> ACgCAYAAADw66xhAAACXB1WQMAAFiVAAB
twilio_app_sid -> ApygXOE0kkkLkoVbBU5dojkuWntC6yblL2
possible_Creds -> PwDDOuWcta9uJmR/oJaoJM5Kp0ynUJhgbfFn0/YkH7VstK9uBmRvntmgJFY6mtHIYJ5vLFQw6hLQs8nTpEuEzhTSLb/LvCPNGhnmkmc0b0SXebJgnLHrHw1Pme0qS3t7MPZQUX1Wm+uyS2Yvmq
a4BG1mtINZOHZZRzyF8MYySWYzgkfIVERf55dss+o961Wxaa3YI78JNC7wCvQ2XHsCIIadpleguLu8zeMjKvUp2+V0Ubgucu8wz5PuAG6dyLkvrFqVLCub1Djh57I5Ye0TpfYewreUqNNN16C6TfL/qh4CVzWdXAaku1s/LidJQ
FAj5YmtYhe4NlFwvNadYiKZqtAfe0Eoxd5qftbHyd851J4S2YEBa9hLurTAQA/wPEZbLaEef7VgAAAAABJR5UerKJggg=="</image><circle
```

Potential SIDs were detected. Need to validate them before utilizing them.

## **2. Firewall Detection**

### **2.1. Wafw00f**

```
(binosh@BINZ)-[~/Desktop/WS Assingment/Tools]
$ wafw00f https://www.northwesternmutual.com/

      ?  ??
    ( )  ;  )  .  "
  ( )  ;  ( " )  ;  ( ( ;  " )
  /  /  /  /  /  /  /  /  /  /
  \  \  \  \  \  \  \  \  \  \

~ WAFW00F : v2.3.1 ~
~ Sniffing Web Application Firewalls since 2014 ~

[*] Checking https://www.northwesternmutual.com/
[+] The site https://www.northwesternmutual.com/ is behind AWS Elastic Load Balancer (Amazon) WAF.
[~] Number of requests: 2
```

AWS Elastic Load Balancer (Amazon) was detected as the firewall that is being used. There is a single known vulnerability in AWS Elastic Load Balancer (Amazon). Need to be cautious about it and regular updates are a necessity.

## **3. Multi tool web Vulnerability Scanning**

### **3.1 Rapidscan**

```
(binosh@BINZ)-[~/Desktop/WS Assingment/Tools/rapidscan]
$ python3 rapidscan.py -u "https://www.gapinc.com/en-us/"
```





















Doesn't have IPv6 Address

```
Vulnerability Threat Level
Info Does not have an IPv6 Address. It is good to have one.
Vulnerability Definition
Not a vulnerability, just an informational alert. The host does not have IPv6 support. IPv6 provides more security as IPSec (responsible for CIA - Confidentiality, Integrity, and Availability) is incorporated into this model. So it is good to have IPv6 support.
Vulnerability Remediation
It is recommended to implement IPv6. More information on how to implement IPv6 can be found from this resource. https://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/IPv6-Implementation-CS.html
```

An RDP server was detected over UDP, posing a high-risk vulnerability that could allow attackers to exploit remote access, crash the service, or attempt brute-force authentication. Restricting access and securing configurations is strongly advised.

```
Vulnerability Threat Level
High RDP Server Detected over UDP.
Vulnerability Definition
Attackers may launch remote exploits to either crash the service or tools like ncrack to try brute-forcing the password on the target.
Vulnerability Remediation
It is recommended to block the service to outside world and made the service accessible only through the a set of allowed IPs only really necessary. The following resource provides insights on the risks and as well as the steps to block the service. https://www.perspectiverisk.com/remote-desktop-service-vulnerabilities/
```


### 4. OWASP ZAP

- >  Vulnerable JS Library (3)
- >  Absence of Anti-CSRF Tokens
- >  Content Security Policy (CSP) Header Not Set
- >  Cross-Domain Misconfiguration (9)
- >  Vulnerable JS Library
- >  Cookie No HttpOnly Flag (3)
- >  Cookie with SameSite Attribute None
- >  Cross-Domain JavaScript Source File Inclusion
- >  Server Leaks Information via "X-Powered-By"
- >  Server Leaks Version Information via "Server"
- >  Strict-Transport-Security Header Not Set (26)
- >  Timestamp Disclosure - Unix (132)
- >  X-Content-Type-Options Header Missing (10)
- >  Cookie Poisoning (29)
- >  Information Disclosure - Suspicious Comment
- >  Loosely Scoped Cookie (15)
- >  Modern Web Application (4)
- >  Re-examine Cache-control Directives (54)
- >  Retrieved from Cache (47)
- >  Session Management Response Identified (16)

There are 1 high risk alert and 4 medium ,8 low risk alerts shown above.

**Vulnerable JS Library**

URL: <https://www.northwesternmutual.com/react-assets/templates/vendors~main.df7b945e.js>

Risk:  High

Confidence: Medium

Parameter: |

Attack:

Evidence: return"[Axios v1.6.8] Transitional

CWE ID: 1395

WASC ID:

Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))

Input Vector:

Description:

The identified library appears to be vulnerable.

Other Info:

The identified library axios, version 1.6.8 is vulnerable.

CVE-2024-39338

**Absence of Anti-CSRF Tokens**

URL: <https://www.northwesternmutual.com/private-wealth-management/>

Risk:  Medium

Confidence: Low

Parameter:

Attack:

Evidence: <form class="sc-ijUvQt bfmjQS sc-ixNrWi eksAjh" method="POST" id="private-wealth-management-pcg-directory-form" action=""/>

CWE ID: 352

WASC ID: 9

Source: Passive (10202 - Absence of Anti-CSRF Tokens)

Input Vector:

Description:

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable

Other Info:

No known Anti-CSRF token [anticsrf, CSRFToken, RequestVerificationToken, csrfmiddlewaretoken, authenticity\_token,

**Content Security Policy (CSP) Header Not Set**

URL: <https://www.northwesternmutual.com/>

Risk:  Medium

Confidence: High

Parameter:

Attack:

Evidence:

CWE ID: 693

WASC ID: 15

Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)

Alert Reference: 10038-1


Input Vector:

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers

## Web Security - IE2062

Year 2 Semester 2 - 2025

**Cross-Domain Misconfiguration**  
 URL: <https://use.typekit.net/typ5dev.css>  
 Risk:  Medium  
 Confidence: Medium  
 Parameter:  
 Attack:  
 Evidence: Access-Control-Allow-Origin: \*  
 CWE ID: 264  
 WASC ID: 14  
 Source: Passive (10098 - Cross-Domain Misconfiguration)  
 Input Vector:  
 Description:  
 Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**Vulnerable JS Library**  
 URL: <https://www.northwesternmutual.com/template/assets/3.10.9/js/nmx-template.js>  
 Risk:  Medium  
 Confidence: Medium  
 Parameter:  
 Attack:  
 Evidence: /\*! @license DOMPurify 3.1.5  
 CWE ID: 1395  
 WASC ID:  
 Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))  
 Input Vector:  
 Description:  
 The identified library appears to be vulnerable.  
 Other Info:  
 The identified library DOMPurify, version 3.1.5 is vulnerable.  
 CVE-2025-26791

## 5. Injection

### 5.1 Uniscan

```
(binosh@BINZ)-[~/Desktop/WS Assingment/Tools]
$ sudo su
(root@BINZ)-[/home/binosh/Desktop/WS Assingment/Tools]
# uniscan -u https://www.northwesternmutual.com/en-us
#####
# Uniscan project #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 4-5-2025 12:13:58
```

With root privileges can start the scanning.

**uniscan -u <https://www.northwesternmutual.com/> -qd**  
**qd** → To enable directory and dynamic checks.

The scan results indicate that the crawler successfully found one URL during the crawling process. However, the scan did not find any vulnerabilities or issues related to FCKeditor File Upload, Web Backdoors, Source Code Disclosure, PHPinfo() Disclosure, E-mails, File Upload Forms, External Hosts, or Timthumb < 1.33 vulnerability.

**Web Security - IE2062**

**Year 2 Semester 2 - 2025**

```
Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 Loaded.
Plugin name: Blind SQL-injection tests v.1.3 Loaded.
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.2 Loaded.
Plugin name: SQL-injection tests v.1.2 Loaded.
Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
Plugin name: Web Shell Finder v.1.3 Loaded.
[+] 0 New directories added

FCKeditor tests:
Skipped because https://www.northwesternmutual.com/testing123 did not return the code 404

Timthumb < 1.33 vulnerability:
```

## 6. Using Components with Known Vulnerabilities

### 6.1. Nmap

Nmap can be used to find the servers running in the domain as well as their versions along with the port numbers.

**nmap -sV -v <https://www.northwesternmutual.com/>**

```
(binosh@BINZ)-[~/Desktop/WS Assignment/Tools]
$ nmap -sV -v northwesternmutual.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 12:20 SAST
NSE: Loaded 47 scripts for scanning.
Initiating Ping Scan at 12:20
Scanning northwesternmutual.com (216.20.178.205) [4 ports]
Completed Ping Scan at 12:20, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:20
Completed Parallel DNS resolution of 1 host. at 12:20, 0.35s elapsed
Initiating SYN Stealth Scan at 12:20
Scanning northwesternmutual.com (216.20.178.205) [1000 ports]
Discovered open port 25/tcp on 216.20.178.205
Discovered open port 80/tcp on 216.20.178.205
Discovered open port 443/tcp on 216.20.178.205
Discovered open port 80/tcp on 216.20.178.205
Discovered open port 443/tcp on 216.20.178.205
Completed SYN Stealth Scan at 12:20, 20.07s elapsed (1000 total ports)
Initiating Service scan at 12:20
Scanning 3 services on northwesternmutual.com (216.20.178.205)
Completed Service scan at 12:20, 16.07s elapsed (3 services on 1 host)
NSE: Script scanning 216.20.178.205.
Initiating NSE at 12:20
Completed NSE at 12:20, 1.59s elapsed
Initiating NSE at 12:20
Completed NSE at 12:20, 1.55s elapsed
Nmap scan report for northwesternmutual.com (216.20.178.205)
Host is up (0.025s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp?
80/tcp    open  http-proxy   F5 BIG-IP load balancer http proxy
443/tcp   open  ssl/http-proxy F5 BIG-IP load balancer http proxy
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=7.95%I=750-5/XTime=68173F6E3P=x86_64-pc-linux-gnu%r(Hello
SF:2A,"552%v2Invalid%v2domain%v20name%v20in%v20EHLO%v20command%v20\r\n");
Service Info: Device: load balancer

Read data files from: /usr/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 40.35 seconds
Raw packets sent: 3011 (132.416KB) | Rcvd: 17 (700B)
```

Even if the open ports are discovered the specific versions were not discoverable. One or more of the following factors could be the reason for it.

**Firewall Restrictions** – The target system may have a firewall that is blocking the version detection probes used by nmap.

**Service Configuration** – The service on the target system may be configured not to respond to version detection requests.

**Privilege Level** – The nmap scan may not have sufficient privileges to determine the service versions.

Even if, it is noticeable that the following ports are open.

1. Port 25 → SMTP
2. Port 80 → HTTP
4. Port 443 → HTTPS

And it is also notable that F5 BIG-IP load balancer http proxy is being used on HTTP processes. Despite conducting an aggressive Nmap scan, no results were obtained.

**nmap -A northwesternmutual.com**

**Mitigation methods**

- Use dependency management tools to monitor and patch vulnerabilities.
- Use dependency management tools to monitor and patch vulnerabilities.
- Implement CSRF protection mechanisms (e.g., synchronizer tokens or SameSite cookies).
- Use security frameworks that provide built-in CSRF defense.
- Define a strict CSP to control resource loading and mitigate XSS attacks.
- Limit script execution by enforcing **script-src 'self'** policy.
- Avoid exposing sensitive times timestamps in responses or metadata.
- Implement format standardization to reduce fingerprinting

**Proof of Report Submission**

**Northwestern Mutual VDP** has received  
**WS Assingment**

Thank you Binosh ,

We have received your Bugcrowd submission for engagement  
northwestern-vdp.

**Submission Details**

Submitted  
04 May 2025 19:37:30 UTC

Submission ID  
6b785ed0-3150-4965-9960-0623fbf99b26

VRT  
Cross-Site Request Forgery (CSRF) > CSRF Token Not Unique Per  
Request

[View Submission Details](#)