IE2062 [2023/JUL]- Web Security

Web Security BB Assignment

Report 05 – Axel Springer NM

Lecturer in charge – Ms. Chethana Liyanapathirana

IT21826368 – Nanayakkara Y.D.T.D

Contents

1. Axel Springer SE/Axel Springer National Media & Tech/Detail

Public Open

Axel Springer SE / Axel Springer National Media & Tech / Detail

1.1. Overview

Description

AS National Media & Tech (NMT) is a subsidiary of Axel Springer SE an international media and technology company.
NMT is responsible for all German news media websites, their web presence and continuous development. These websites reaches more than 50 million unique users per month.
By providing information across its diverse media brands Axel Springer SE empowers people to make free decisions for their lives.
Therefore, IT security of our websites and that of our customers is so important to us

Bounties

		Low 0.1 - 3.9	Medium 4.0 - 6.9	High 7.0 - 8.9	Critical 9.0 - 9.4	Exceptional 9.5 - 10.0
Tier 1	€	50	150	300	1,250	2,500
Tier 2	€	35	100	200	500	1,000
Tier 3	€	15	50	75	250	500

View changes

1.2.Scope

In scope

Introduction

We are happy to announce our program! We've done our best to clean up our known issues and now would like to request your help to spot the ones we missed!

Domain in Scope

In addition to the domains listed above, we provide a full **list of in scope sub-domains in the attachment**.
At some point in the future we will have all subdomains of our our main domains in scope, so stay tuned.

Our worst-case scenarios are:

- publish fake news in our website
- get sensitive user data
- command and execution on production service

Feedback

Would you like to help us improve our program or have some feedback to share, please send your anonymous feedback here:

Program feedback link

Please note this form will be checked periodically and **should not** be used for submission or support queries.

Hide attachments

NMT-DomainScopeBugBounty_10-2023.xlsx 10/5/2023, 1:54:53 AM

View changes

1.3. Out of Scope

Out of scope

Domains

- Any domain that is not listed in the Domains section including the attached full in scope domain list, is out of scope for this program.
- **Temporary out of scope:**

Application

- Wordpress usernames disclosure
- Pre-Auth Account takeover/OAuth squatting
- Self-XSS that cannot be used to exploit other users
- Verbose messages/files/directory listings without disclosing any sensitive information
- CORS misconfiguration on non-sensitive endpoints
- Missing cookie flags
- Missing security headers
- Cross-site Request Forgery with no or low impact
- Presence of autocomplete attribute on web forms
- Reverse tabnabbing
- Bypassing rate-limits or the non-existence of rate-limits.
- Best practices violations (password complexity, expiration, re-use, etc.)
- Clickjacking without proven impact/unrealistic user interaction
- CSV Injection
- Sessions not being invalidated (logout, enabling 2FA, etc.)
- Tokens leaked to third parties

General

- In case that a reported vulnerability was already known to the company from their own tests, it will be flagged as a duplicate
- Theoretical security issues with no realistic exploit scenario(s) or attack surfaces, or issues that would require complex end user interactions to be exploited
- Spam, social engineering and physical intrusion
- DoS/DDoS attacks or brute force attacks
- Vulnerabilities that only work on software that no longer receive security updates
- Attacks requiring physical access to a victim's computer/device, man in the middle or compromised user accounts
- Recently discovered zero-day vulnerabilities found in in-scope assets within 14 days after the public release of a patch or mitigation may be reported, but are usually not eligible for a bounty
- Reports that state that software is out of date/vulnerable without a proof-of-concept

View changes

1.4. Selected Domains

URL www.travelbook.de is used in this report

www.travelbook.de	Tier 3	URL

2. Information Gathering

2.1.Dmitry

First let's see the basic information on the given URL: www.travelbook.de using Dmitry.

```
┌──(user㉿user)-[~]
└─$ dmitry www.travelbook.de
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:173.222.27.208
HostName:www.travelbook.de

Gathered Inet-whois information for 173.222.27.208
---------------------------------------


inetnum:        173.214.204.0 - 173.234.15.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        -------------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        -------------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2019-08-26T14:46:25Z
last-modified:  2019-08-26T14:46:25Z
source:         RIPE

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
```

```
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2019-08-26T14:46:25Z
last-modified:  2019-08-26T14:46:25Z
source:         RIPE

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.108 (SHETLAND)



Gathered Inic-whois information for travelbook.de
---------------------------------------------------


Domain: travelbook.de
Nserver: a1-130.akam.net
Nserver: a11-67.akam.net
Nserver: a14-64.akam.net
Nserver: a16-65.akam.net
Nserver: a6-66.akam.net
Nserver: a7-67.akam.net
Nserver: ns21.netuse.de
Dnskey: 257 3 8 AwEAAb6wTnnGL+/OAsem8qerCOXCbx4tt+n+WI0C5TjB9ZY+vJ31fYa5J5BpLZz/3lAQM9i6lvx63DtXqy5h0l5AwGBlhjqii6x
Vh9ir4o2Ec5j6◆r◆◆U9U/)
'`K)UBeJfyfgbEi 3D◆◆UXa◆2D◆◆UTG◆◆◆◆◆FV0c48yNoiDTrhEieu◆C◆◆Uh2CEbIU2ROP◆◆◆◆C2ce
% available at the DENIC website:
% http://www.denic.de/en/domains/whois-service/web-whois.html
%
%

Domain: travelbook.de
Nserver: a1-130.akam.net
Nserver: a11-67.akam.net
Nserver: a14-64.akam.net
Nserver: a16-65.akam.net
Nserver: a6-66.akam.net
Nserver: a7-67.akam.net
Nserver: ns21.netuse.de
Dnskey: 257 3 8 AwEAAb6wTnnGL+/OAsem8qerCOXCbx4tt+n+WI0C5TjB9ZY+vJ31fYa5J5BpLZz/3lAQM9i6lvx63DtXqy5h0l5AwGBlhjqii6x
```

```
Vh9ir4o2Ec5j69U/BeJfyfgbEiXaTGFV0c48yNoiDTrhEieh2CEbIU2ROC2P/RNX73wBdgGD5sO9p9LrknWSoP/RNX73wBdgG+D5sO9p9L)
'◆◆◆◆rknWSoP/RNP◆◆◆◆X7◆◆◆◆3wD◆◆UBdgG+D5sO9◆◆◆◆◆p9◆◆C◆◆UL)de.whois-servers.net
*** stack smashing detected ***: terminated
zsh: IOT instruction  dmitry www.travelbook.de
```

2.2. Amass

```
┌──(user㉿user)-[~]
└─$ sudo amass enum -d travelbook.de
wetter.travelbook.de
travelzoo.travelbook.de
blogstars.travelbook.de
stage.travelbook.de
pur.travelbook.de
escapes.travelbook.de
www.escapes.travelbook.de
travelbook.de
image.travelbook.de
data-bb4ada6163.travelbook.de
backend.travelbook.de
data-9e4f40dc7c.travelbook.de
productstorybundles.travelbook.de
data.travelbook.de
m.purmail.travelbook.de
as.travelbook.de
kmp.travelbook.de
www.travelbook.de
cmp.travelbook.de
```

```
OWASP Amass v3.23.2                                https://github.com/owasp-amass/amass
___________________________________________________________________________________________

22 names discovered - archive: 8, cert: 13, scrape: 1
___________________________________________________________________________________________

ASN: 14061 - DIGITALOCEAN-ASN - DigitalOcean, LLC
        188.166.192.0/22        1    Subdomain Name(s)
ASN: 50018 - FLOWMAILER
        185.136.64.0/23         4    Subdomain Name(s)
ASN: 14618 - AMAZON-AES - Amazon.com, Inc.
        63.140.38.0/23          10   Subdomain Name(s)
ASN: 199236 - EMARSYS-AS
        217.175.192.0/23        1    Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
        13.248.160.0/20         2    Subdomain Name(s)
        76.223.48.0/20          2    Subdomain Name(s)
        18.155.128.0/22         8    Subdomain Name(s)
        13.33.88.0/22           8    Subdomain Name(s)
        34.240.0.0/12           1    Subdomain Name(s)
        54.64.0.0/12            2    Subdomain Name(s)
ASN: 5605 - NETUSE
        195.244.240.0/20        2    Subdomain Name(s)
ASN: 18001 - DIALOG-AS Dialog Axiata PLC.
        125.214.160.0/20        4    Subdomain Name(s)
ASN: 16276 - OVH
        178.32.0.0/15           2    Subdomain Name(s)
        51.89.0.0/16            1    Subdomain Name(s)
        51.77.0.0/16            1    Subdomain Name(s)
        54.36.0.0/14            1    Subdomain Name(s)
ASN: 29423 - GRIDSCALE
        185.102.92.0/22         2    Subdomain Name(s)
        185.201.144.0/22        2    Subdomain Name(s)
ASN: 4657 - STARHUB-INTERNET StarHub Ltd
        23.50.80.0/20           1    Subdomain Name(s)

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

2.3.Kockpy

```
┌──(user㉿user)-[~]
└─$ sudo knockpy travelbook.de

 _ __                _ |   v6.1.0
 | |/ /              | |
 | ' / _ __   ___   ___| | ___ __  _   _
 |  < | '_ \ / _ \ / __| |/ / '_ \| | | |
 | . \| | | | (_) | (__|   <| |_) | |_| |
 |_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                            | |     __/ |
                            |_|    |___/

local: 10757 | remote: 34

Wordlist: 10791 | Target: travelbook.de | Ip: 76.223.57.215

21:28:59

Ip address      Code Subdomain                                   Server                                   Real hostname

63.140.62.214   200  as.travelbook.de                           jag                                      travelbook.de.ssl.sc.omtrdc.net
13.33.88.126    200  ast.travelbook.de                          AmazonS3                                 ast.travelbook.de.greylabeldelivery.com
195.244.241.14  200  blogstars.travelbook.de                    nginx
52.98.66.104    200  autodiscover.travelbook.de                                                          autod.ms-acdc-autod.office.com
13.248.170.15        backend.travelbook.de                                                               travelbook-be.prod.mediasites.as-infra.de
65.8.11.73      403  cmp.travelbook.de                          AmazonS3                                 cdn-75.privacy-mgmt.com
125.214.166.51       embed.travelbook.de                                                                 a721.r.akamai.net
54.73.62.134    200  escapes.travelbook.de                      nginx                                    secretescapes.com
125.214.166.48  200  image.travelbook.de                        nginx                                    a987.r.akamai.net
185.136.65.6    200  m.purmail.travelbook.de                    nginx                                    web.flowmailer.net
173.222.27.208  200  www.travelbook.de                          nginx                                    e3537.f.akamaiedge.net
34.255.98.217        wetter.travelbook.de                                                                travelbook.wetterkontor.de

21:50:48

Ip address: 32 | Subdomain: 12 | elapsed time: 00:21:48
```

2.4.Sublist3r

```
┌──(user㉿user)-[~]
└─$ sudo sublist3r -d travelbook.de
[sudo] password for user:

                 ____        _      _ _     _ _____
                / ___| _   _| |__  | (_)___| |_   _|___ / _ __
                \___ \| | | | '_ \| | / __| __| | |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for travelbook.de
[-] 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..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 18
as.travelbook.de
ast.travelbook.de
cmp.travelbook.de
data-9e4f40dc7c.travelbook.de
data-bb4ada6163.travelbook.de
email.travelbook.de
escapes.travelbook.de
image.travelbook.de
kmp.travelbook.de
m.travelbook.de
link.mailer.travelbook.de
productstorybundles.travelbook.de
pur.travelbook.de
m.purmail.travelbook.de
ssl.travelbook.de
stage.travelbook.de
static.travelbook.de
wetter.travelbook.de
```

3. Scanning Vulnerability

3.1. Using Rapid scan

```
(The Multi-Tool Web Vulnerability Scanner)

Check out our new software, NetBot for simulating DDoS a
ttacks - https://github.com/skavngr/netbot
```

- Some Vulnerability Headers Exposed

```
Vulnerability Threat Level
        medium  Some vulnerable headers exposed.
Vulnerability Definition
        Attackers try to learn more about the target from the amount of information exposed in the headers. An attacker may know what type of tech stack a web application is emphasizing and many other information.
Vulnerability Remediation
        Banner Grabbing Should be restricted and access to the services from outside would should be made minimum.
```

- FREAK Vulnerability Detected

```
Vulnerability Threat Level
        high  FREAK Vulnerability Detected.
Vulnerability Definition
        Via this vulnerability the attacker will be able to perform a MiTM attack and thus compromising the confidentiality factor.
Vulnerability Remediation
        Upgrading OpenSSL to latest version will mitigate this issue. Versions prior to 1.1.0 is prone to this vulnerability. More information can be found in this resource. https://bobcares.com/blog/how-to-fix-sweet32-birthday-attacks-
vulnerability-cve-2016-2183/
```

- Does not have an IpV6 address. It is good to have one.

```
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 Availablity) is incorporated into this model. So
t 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
```

- Secure Client Initiated Renegotiation is supported.

```
Vulnerability Threat Level
        medium  Secure Client Initiated Renegotiation is supported.
Vulnerability Definition
        Otherwise termed as Plain-Text Injection attack, which allows MiTM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is process
ed retroactively by a server in a post-renegotiation context.
Vulnerability Remediation
        Detailed steps of remediation can be found from these resources. https://securingtomorrow.mcafee.com/technical-how-to/tips-securing-ssl-renegotiation/ https://www.digicert.com/news/2011-06-03-ssl-renego/
```

- X-XSS Protection is not present.

```
Vulnerability Threat Level
        medium  X-XSS Protection is not Present
Vulnerability Definition
        As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
Vulnerability Remediation
        Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.
```

- Subdomain Discovery with Dmirty and fierce.

```
Vulnerability Threat Level
        medium  Subdomains discovered with DMitry.
Vulnerability Definition
        Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the atta
cker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.
Vulnerability Remediation
        It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as at
tackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

```
Vulnerability Threat Level
        medium  Found Subdomains with Fierce.
Vulnerability Definition
        Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the atta
cker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.
Vulnerability Remediation
        It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as at
tackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

```
Scan Completed in 3s

[ Preliminary Scan Phase Completed. ]


[ Report Generation Phase Initiated. ]
        Complete Vulnerability Report for travelbook.de named rs.vul.travelbook.de.
        Total Number of Vulnerability Checks        : 80
        Total Number of Vulnerability Checks Skipped: 23
        Total Number of Vulnerabilities Detected    : 8
        Total Time Elapsed for the Scan             : 1h 46m 32s
```

3.2.Nmap

After we get the basic information, we can do a port scan using Nmap

```
┌──(user㉿user)-[~]
└─$ sudo nmap -sS 173.222.27.208
[sudo] password for user:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-29 16:31 EDT
Nmap scan report for a173-222-27-208.deploy.static.akamaitechnologies.com (173.222.27.208)
Host is up (0.028s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 10.59 seconds
```

4. Vulnerability description

- **Some Vulnerability Headers Exposed**:
  - The exposure of vulnerable headers indicates potential security weaknesses within the HTTP response headers. These headers might be misconfigured or contain security-related issues.
  -
- **Does Not Have an IPv6 Address**:
  - The absence of an IPv6 address may limit the website's compatibility with the next-generation Internet Protocol, IPv6, which is becoming increasingly important for network infrastructure.
  -
- **Secure Client-Initiated Renegotiation Supported**:
  - The support for Secure Client-Initiated Renegotiation may introduce security risks if not configured correctly. This can potentially facilitate man-in-the-middle attacks.
  -
- **X-XSS Protection is Not Present**:
  - The absence of the "X-XSS-Protection" header suggests a vulnerability to cross-site scripting (XSS) attacks. Malicious scripts could be injected into web pages, compromising user security and data.
  -
- Freak **Vulnerability**
  - The "FREAK" vulnerability, which stands for "Factoring attack on RSA-EXPORT Keys," is a security flaw that primarily affects the security of encrypted communications on the internet. It was discovered in 2015.
  - FREAK enabled a man-in-the-middle (MITM) attacker to intercept and potentially decrypt supposedly secure communications between a client (e.g., a web browser) and a server. This could expose sensitive information, such as login credentials, credit card numbers, and more.
  -
- **Subdomain Discovery with Dmitry and Fierce**:
  - Subdomains were discovered using the tools Dmitry and Fierce, potentially expanding the attack surface and uncovering additional potential vulnerabilities or entry points.

5. Affected components.

- **Some Vulnerability Headers Exposed**:
  - Affects the security and integrity of the exposed HTTP response headers.
- **Does Not Have an IPv6 Address**:
  - Impacts the website's network compatibility with IPv6.
- **Secure Client-Initiated Renegotiation Supported**:
  - Affects the server's SSL/TLS configuration and security.
- **X-XSS Protection is Not Present**:
  - Affects the entire website, potentially exposing user data to XSS attacks.
- **Subdomain Discovery with Dmitry and Fierce**:
  - Impacts the subdomains and their associated services and content.

6. Impact assessment

- **Some Vulnerability Headers Exposed**:
  - Low to moderate risk: Vulnerable headers may expose security weaknesses and should be reviewed and secured.
- **Does Not Have an IPv6 Address**:
  - Low risk: While IPv6 adoption is essential for future compatibility, the lack of an IPv6 address currently has limited security impact.
- **Secure Client-Initiated Renegotiation Supported**:
  - Moderate risk: If not properly configured, it could lead to SSL/TLS vulnerabilities.
- **X-XSS Protection is Not Present**:
  - Moderate risk: The absence of XSS protection headers increases the risk of successful XSS attacks, compromising user data and security.
- **Subdomain Discovery with Dmitry and Fierce**:
  - Moderate risk: The discovery of subdomains widens the attack surface and requires scrutiny for potential vulnerabilities.

7. Steps to reproduce.

- None

8. Proof of concept (if applicable)

- None

9. Proposed mitigation or fix

- Securing vulnerable headers
- Considering IPv6 adoption
- Configuring Secure Client-Initiated Renegotiation securely
- Implementing XSS protection
- Securing discovered subdomains.

10. Summary

- Finally, the assessment has unveiled several vulnerabilities and security concerns, including exposed vulnerable headers, the absence of IPv6 support, Secure Client-Initiated Renegotiation, missing XSS protection, and the discovery of subdomains. Addressing these findings is crucial to enhance the overall security and resilience of the target system. Mostly these vulnerabilities can be mitigated easily because they are in moderate severity.