IE2062 [2023/JUL]- Web Security

Web Security BB Assignment

Report 09 – Toyota Motor Europe

Lecturer in charge – Ms. Chethana Liyanapathirana

IT21826368 – Nanayakkara Y.D.T.D

Contents

1. Toyota Motor Europe/Toyota Motor Europe/Detail

1.1. Overview

Description

Toyota Motor Europe NV/SA (TME) oversees the wholesale sales and marketing of Toyota and Lexus vehicles, parts and accessories, and Toyota's European manufacturing and engineering operations. Toyota directly employs over 25,000 people in Europe and has invested over EUR 10 billion since 1990. Toyota's operations in Europe are supported by a network of 29 National Marketing and Sales Companies across 53 countries, a total of around 3,000 sales outlets, and nine manufacturing plants.

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 2	€	0	0	250	500	1,000

View changes

1.2.Scope

In scope

We are happy to announce our first bug bounty program!

We've done our best to clean most of our known issues and now would like to request your help to spot the ones we missed! We are specifically looking for

- leaking of personal data
- horizontal / vertical privilege escalation
- SQLi
- Log4Shell
- ...

We plan to update our scope every month so keep an eye on us or subscribe to our program to receive updates when we make changes!

shared codebase disclaimer
Some sites and applications share a codebase. If a vulnerability is present in multiple places, it will only be accepted as a valid subsmission once.

1.3.Out of Scope

Out of scope

Out of scope domains

- Any domain that is not listed in the Domains section, is out of scope for this program
- telematics.toyota-europe.com
- telematics.lexus-europe.com
- telematicsa.toyota-europe.com
- telematicsa.lexus-europe.com
- lexus.com
- toyota.com

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

www.toyota.fr	Tier 2	URL

- This URL www.toyota.fr Is used in this report.

2. Information Gathering

2.1. Using Dmitry.

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

ERROR: Unable to locate Host IP addr. for toyota.fe
Continuing with limited modules
HostIP:
HostName:toyota.fe

Gathered Inic-whois information for toyota.fe
---------------------------------
Error: Unable to connect - Invalid Host
ERROR: Connection to InicWhois Server fe.whois-servers.net failed

Gathered Netcraft information for toyota.fe
---------------------------------

Retrieving Netcraft.com information for toyota.fe
Netcraft.com Information gathered

Gathered Subdomain information for toyota.fe
---------------------------------
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 possible subdomain(s) for host toyota.fe, Searched 0 pages containing 0 results

Gathered E-Mail information for toyota.fe
---------------------------------
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host toyota.fe, Searched 0 pages containing 0 results

All scans completed, exiting
```

2.2.Using Knockpy

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

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

local: 10757 | remote: 115

Wordlist: 10872 | Target: toyota.fr | Ip: 195.177.80.76

12:28:02

Ip address      Code Subdomain                          Server                    Real hostname
52.210.74.165   404  brochure.toyota.fr                                           viewer.ipaper.io
161.71.146.9         bacs.toyota.fr                                              ukb.edge2.salesforce.com
40.99.10.40     200  autodiscover.toyota.fr                                      autod.ms-acdc-autod.office.com
185.2.52.20     200  collection.toyota.fr              nginx
212.3.255.31         contact.toyota.fr                                           buck.net7.be
161.71.33.242        crm.toyota.fr
52.84.251.84         csxd.toyota.fr                                              d34i2yvdqisvmz.cloudfront.net
212.3.255.39         datacapture.toyota.fr
108.143.11.25   200  facturations-recette.toyota.fr    Microsoft-IIS/10.0        ptoyweb02.westeurope.cloudapp.azure.com
13.81.82.55     200  facturations.toyota.fr            WebServer
213.41.115.210  200  gtw1.toyota.fr
94.130.186.250       garantiematoyota.toyota.fr
10.150.100.61        ixion3-dev.toyota.fr
195.177.83.78        ixion2.toyota.fr
195.177.83.73        ixion2-dev.toyota.fr
10.150.100.60        ixion3.toyota.fr
125.214.166.51  200  media.toyota.fr                                             a1894.b.akamai.net
194.177.36.54   403  reseau.toyota.fr                  Apache/2.2.16 (Debian)

12:56:08

Ip address: 28 | Subdomain: 18 | elapsed time: 00:28:05
```

- From found ports we can scan the ports and see them

3. Scanning Vulnerability

3.1. Using Nmap

```
┌──(user㉿user)-[~]
└─$ sudo nmap -sS 52.210.74.165
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 06:18 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds

┌──(user㉿user)-[~]
└─$ sudo nmap -sS 161.71.146.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 06:19 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.29 seconds

┌──(user㉿user)-[~]
└─$ sudo nmap -sS 40.99.10.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 06:19 PDT
Nmap scan report for 40.99.10.40
Host is up (0.82s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT    STATE  SERVICE
25/tcp  open   smtp
80/tcp  open   http
110/tcp closed pop3
143/tcp closed imap
443/tcp closed https
587/tcp closed submission
993/tcp closed imaps
995/tcp closed pop3s

Nmap done: 1 IP address (1 host up) scanned in 108.90 seconds
```

3.2.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
```

- No DNS/HTTP Based Load Balancers Found

```
Vulnerability Threat Level
        low  No DNS/HTTP based Load Balancers Found.
Vulnerability Definition
        This has nothing to do with security risks, however attackers may use this unavailability of load balancers as an advantage to leverage a denial of service attack on certain services or on the whole application itself.
Vulnerability Remediation
        Load-Balancers are highly encouraged for any web application. They improve performance times as well as data availability on during times of server outage. To know more information on load balancers and setup, check this resourc
e. https://www.digitalocean.com/community/tutorials/what-is-load-balancing
```

- Found Subdomains with fierce and amass.

```
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.
```

```
Vulnerability Threat Level
        medium  Found Subdomains with AMass
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.
```

- 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.
```

```
[ Report Generation Phase Initiated. ]
        Complete Vulnerability Report for toyota.fe named rs.vul.toyota.fe.
        Total Number of Vulnerability Checks        : 80
        Total Number of Vulnerability Checks Skipped: 19
        Total Number of Vulnerabilities Detected    : 4
        Total Time Elapsed for the Scan             : 2m 24s
```

4. Vulnerability description.

- **No DNS/HTTP-Based Load Balancers Found**:
  - The absence of DNS or HTTP-based load balancers indicates that the website may not have a mechanism to distribute incoming traffic across multiple servers for redundancy and load balancing.
  - This could impact on the website's availability during traffic spikes or server failures.
  -
- **Found Subdomains with Fierce and Amass**:
  - Subdomains were discovered using the tools Fierce and Amass, potentially revealing additional attack surfaces or potential points of vulnerability.
  - The presence of unmonitored or unsecured subdomains can pose security risks, including unauthorized access.
  -
- **X-XSS Protection is not Present**:
  - The absence of the "X-XSS-Protection" HTTP response header suggests a lack of protection against cross-site scripting (XSS) attacks.
  - This vulnerability can expose users to XSS attacks, where malicious scripts can be injected into web pages, potentially compromising user data and security.

5. Affected components.

- **No DNS/HTTP-Based Load Balancers Found**:
  - Affects the website's server infrastructure and overall availability.
  -
- **Found Subdomains with Fierce and Amass**:
  - Impacts the subdomains and their associated services and content.
  -
- **X-XSS Protection is not Present**:
  - Affects the entire website, potentially exposing user data and security.

6. Impact assessment.

- **No DNS/HTTP-Based Load Balancers Found**:
  - Moderate risk: The lack of load balancers could affect website availability during high traffic or server failures.
  -
- **Found Subdomains with Fierce and Amass**:
  - Moderate risk: The discovery of subdomains widens the attack surface and requires scrutiny for potential vulnerabilities.
  -
- **X-XSS Protection is not Present**:
  - Moderate risk: The absence of XSS protection headers increases the risk of successful XSS attacks, compromising user security and data.

7. Steps to reproduce

- None

8. Proof of concept (if applicable)

- None

9. Proposed mitigation or fix

- Implementing load balancers for availability.
- Reviewing and securing subdomains.
- Enabling XSS protection headers.

10. Summary

- Addressing these findings is crucial to enhance the overall security and availability of the target system. Immediate actions are recommended to implement load balancing and XSS protection, while thorough subdomain reviews are necessary to identify and mitigate potential risks associated with subdomains.