

1.1. Aufgabe 1: Advisory I (3 Punkte)

Am 28.3.2023 hat ein Security Forscher folgendes Security Advisory veröffentlicht.

**Sielco Analog FM Transmitter 2.12 'id' Cookie Brute Force Session Hijacking**  
  
Title: Sielco Analog FM Transmitter 2.12 'id' Cookie Brute Force Session Hijacking  
Advisory ID: [ZSL-2023-5758](#)  
Type: Local/Remote  
Impact: Security Bypass  
Risk: (4/5)  
Release Date: 28.03.2023

3 P.

Frage	Antwort	Punkte
Erklären Sie was mit Cookie Brute Force Session Hijacking gemeint ist		1
Schützt Sie 2FA vor diesem Angriff? Antwort mit Begründung.		1
Wie können Sie sich kurzfristig schützen, bis der Anbieter einen Security Patch bereitstellt (ohne den Service zu deaktivieren)		1

\_\_\_\_\_P.

## 1.2. Aufgabe 2: Advisory II (3 Punkte)

Am 28.3.2023 hat ein Security Forscher folgendes Security Advisory veröffentlicht.

```
#Exploit Title: X-Skipper-Proxy v0.13.237 - Server Side Request Forgery (SSRF)
#Date: 24/10/2022
#Exploit Author: Hosein Vita & Milad Fadavvi
#Vendor Homepage: https://github.com/zalando/skipper
#Software Link: https://github.com/zalando/skipper
#Version: < v0.13.237
#Tested on: Linux
#CVE: CVE-2022-38580
```

### Summary:

Skipper prior to version v0.13.236 is vulnerable to server-side request forgery (SSRF). An attacker can exploit a vulnerable version of proxy to access the internal metadata server or other unauthenticated URLs by adding an specific header (X-Skipper-Proxy) to the http request.

### Proof Of Concept:

- 1- Add header "X-Skipper-Proxy" to your request
- 2- Add the aws metadata to the path

```
GET /latest/meta-data/iam/security-credentials HTTP/1.1
Host: yourskipperdomain.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/105.0.0.0 Safari/537.36
X-Skipper-Proxy: http://169.254.169.254
Connection: close
```

3 P.

Frage	Antwort	Punkte
Erklären Sie den Begriff SSRF und die Gefahr die mit SSRF entsteht		1

Frage	Antwort	Punkte
Wie kann man sich grundsätzlich gegen SSRF schützen		1
Was müsste eine WAF tun, damit diese den Angriff verhindert und der Service trotzdem weiter nutzbar ist? Antwort mit Begründung.		1

\_\_\_\_\_P.

### 1.3. Aufgabe 3: Advisory III (3 Punkte)

cve.mitre.org hat folgende CVE veröffentlicht

CVE-ID	
<b>CVE-2021-35246</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption and use the application as a platform for attacks against its users.	

3 P.

Frage	Antwort	Punkte
Wie stellt man sicher, dass der Browser von sich aus immer eine Verbindung über TLS aufbaut, selbst wenn der User aus Versehen <b>http://</b> anstatt <b>https://</b> in den Browser eingibt?		1
Gibt es ein Restrisiko und was kann man technisch dagegen tun, um dies weiter zu reduzieren?		1
Warum sollten sensitive Daten immer mittels POST Methode übermittelt werden?		1

\_\_\_\_\_P.

#### 1.4. Aufgabe 4: Advisory IV (3 Punkte)

Am 26.1.2023 hat ein Security Forscher folgendes Security Advisory veröffentlicht.

Sielco PolyEco Digital FM Transmitter 2.0.6 Account Takeover / Lockout / EoP

Desc: The application suffers from an authentication bypass, account takeover/lockout and elevation of privileges vulnerability that can be triggered by directly calling the users object and effectively modifying the password of the two constants user/role (user/admin). This can be exploited by an unauthenticated adversary by issuing a single POST request to the vulnerable endpoint and gain unauthorized access to the affected device with administrative privileges.

```
# Change admin pwd
$ curl -X POST -F "pwd_admin=t00t" -F "pwd_user=" http://RADIOFM/protect/users.htm
```


3 P.

Frage	Antwort	Punkte
Zu welcher 2021 OWASP TOP 10 Kategorie gehört diese Vulnerability. Bitte begründen Sie Ihre Antwort		1
Was ist der Unterschied von einer CVE und CWE?		1
Nehmen Sie an, ein Tomcat Application Server wird mit den Default Apps betrieben und ein Hacker kann über diese Default Apps, die nichts mit der tatsächlichen App zu tun haben, einen Angriff lancieren.  In welche 2021 OWASP TOP 10 Kategorie würden Sie diesen Fall kategorisieren?		1

\_\_\_\_\_ P.

1.5. Aufgabe 5: Advisory V (4 Punkte)

Siehe die folgende CVE-ID 2022-1175

 **CVE-2022-1175 Detail**

Description

Improper neutralization of user input in GitLab CE/EE versions 14.4 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 allowed an attacker to exploit XSS by injecting HTML in notes.

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 **NIST: NVD**

**Base Score:**

6.1 MEDIUM

**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

 **CNA: GitLab Inc.**

**Base Score:**

8.7 HIGH

**Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N

CVSS v3.1 Severity and Metrics:

**Base Score:** 8.7 HIGH

**Vector:** AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N

**Impact Score:** 5.8

**Exploitability Score:** 2.3

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): Low

User Interaction (UI): Required

Scope (S): Changed

Confidentiality (C): High

Integrity (I): High

Availability (A): None

4 P.

Frage	Antwort	Punkte
Erklären Sie, was ein CVSS Score bedeutet.		1
NIST und CNA kommen auf unterschiedliche Werte (6.1 vs. 8.7)  Wie kommt dieser Unterschied zustande? Erklärung mit Begründung		1

Frage	Antwort	Punkte
Was muss der Entwickler des Produktes GitLab CE/EE tun, um die Schwachstelle im Code zu schliessen?		1
Was kann der Betreiber von diesem Produkt tun um sich gegen einen Angriff zu schützen, bis der Hersteller einen Patch bereitgestellt hat oder bis man das Update installiert hat?		1

\_\_\_\_P.

### 1.6. Aufgabe 6: Advisory VI (3 Punkte)

Web Sockets sind unterliegen **keiner** Same Origin Policy (SOP) oder CORS (Cross Origin Resource Sharing) Policy.

#### Securing WebSockets

Since SOP and CORS are ineffective for WebSockets, the server implementation should verify the `origin` header on the `Upgrade` request to prevent cross-site WS connections.

```
const io = require("socket.io")(httpServer, {
  allowRequest: (req, callback) => {
    const isOriginValid = check(req);
    callback(null, isOriginValid);
  }
});
```

Authentication/authorization should also be performed while establishing connection eg. via token.

As a developer, it is necessary to be aware of this attack and to know how to prevent it.

3 P.

Frage	Antwort	Punkte
Worin liegt das Problem? Oder anders gesagt, wie kann sich das ein Angreifer zunutze machen?		1
Was ist mit dem Satz «the server implementation should verify the Origin header on the Upgrade request to prevent cross-site WS connections» gemeint?  Wie wirkt der empfohlene Schutz mit dem obigen Satz? Warum bringt das was?		1



Frage	Antwort	Punkte
Würde SameSite=Strict das Problem nicht auch schon lösen? Antwort mit Begründung		1

\_\_\_\_P.

### 1.7. Aufgabe 6: Advisory VII (1 Punkte)

#### ## Description

SQL injection attacks can allow unauthorized access to sensitive data, modification of data and crash the application or make it unavailable, leading to lost revenue and damage to a company's reputation.

Path: /collection/all

GET parameter 'tag' is vulnerable to SQL Injection

[https://website/collection/all?tag=\[SQLi\]](https://website/collection/all?tag=[SQLi])

---

Parameter: tag (GET)

Type: time-based blind

Title: MySQL >= 5.0.12 time-based blind (query SLEEP)

Payload: tag=tshirt'XOR(SELECT(0)FROM(SELECT(SLEEP(6)))a)XOR'Z

---

1 P.

Frage	Antwort	Punkte
In welche 2021 OWASP TOP 10 Kategorie würden Sie diesen Fall kategorisieren?		1
<b>Bitte begründen Sie Ihre Wahl in einem kurzen Statement.</b>		

\_\_\_\_\_ P.