



## **A04:2021 – Insecure Design**

### **Issue Report**

Daniil Lebedev, AD1375, TTV22S2

Assignment report

Web Application Security TTC6500 / Joonatan Ovaska

02.03.2025

School of Technology / Information and Communication Technology

# 1 Main Target – Task 1

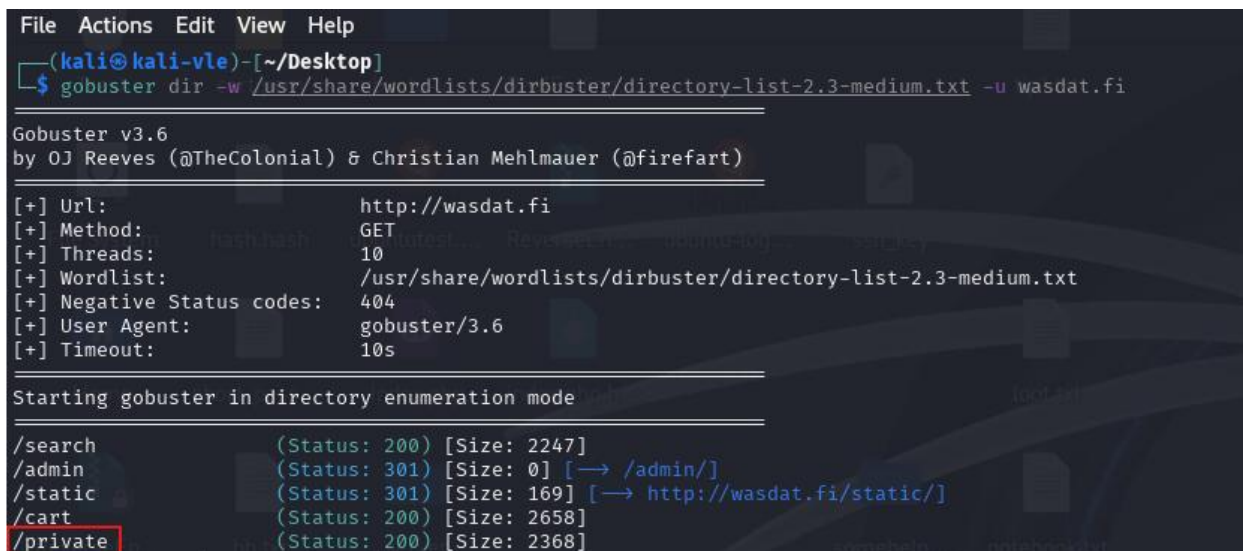
## 1.1 Coupon Codes Stored in Plain Text

Title: Website leaks sensitive discount codes in plain text.

Description: The target stores sensitive discount codes meant for staff only, which can be accessed and viewed by unauthorized user, without proper access controls or encryption.

Steps to Reproduce:

- Use subdirectory scanning tool to discover vulnerable directory (See Screenshot 1)



```
File Actions Edit View Help
(kali@kali-vle)-[~/Desktop]
$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u wasdat.fi

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

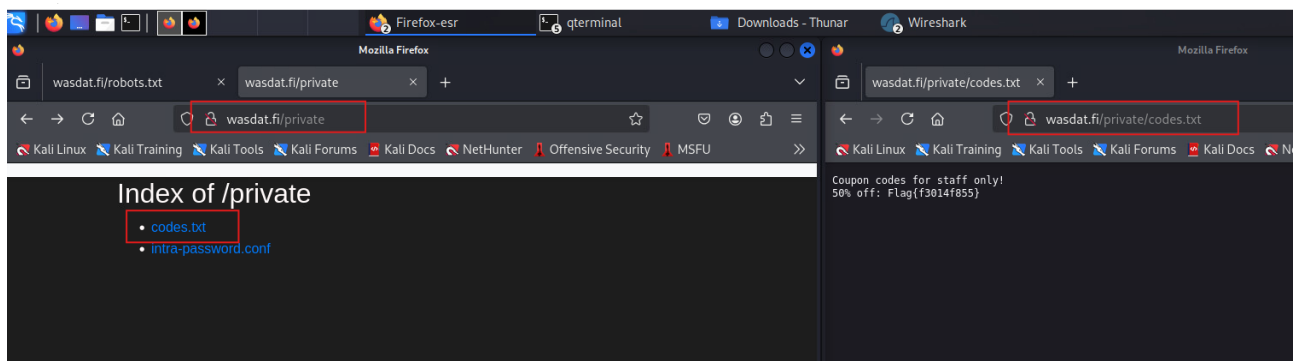
[+] Url: http://wasdat.fi
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/search (Status: 200) [Size: 2247]
/admin (Status: 301) [Size: 0] [→ /admin/]
/static (Status: 301) [Size: 169] [→ http://wasdat.fi/static/]
/cart (Status: 200) [Size: 2658]
/private (Status: 200) [Size: 2368]
```

Screenshot 1

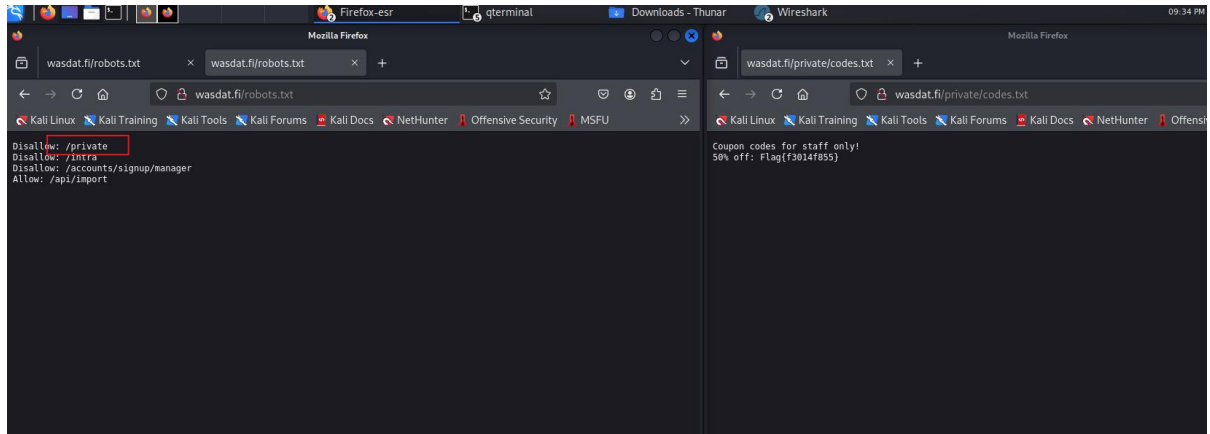
- Access improperly secured directory, containing discount coupons (See Screenshot 2)



Screenshot 2

OR

- Just by checking robots.txt of the target website you can discover some private subdirectory, which contains file with sensitive plain text information – no use of scanning tools is necessary (See Screenshot 3).



Screenshot 3

Impact estimation:

Medium to High:

Unauthorized users can easily exploit the leaked discount codes, resulting in potential financial losses for the company. The ease of exploitation, where even an unskilled attacker can simply access these discount coupons, further increases the risk.

Depending on usage limitations of the leaked coupon, this vulnerability could lead to substantial revenue loss, especially if attacker automate the process or distribute the codes publicly.

Mitigation:

- Restrict directory access by implementing proper authorization for directories with sensitive information
- Do not list sensitive directories in robots.txt. It does not provide any kind of protection over unauthorized access
- See <https://cwe.mitre.org/data/definitions/200.html>

## **2 Main target – Task 2**

### **2.1 Login Intra**

Title: Null byte injection leading to directory traversal and password exposure

Description: Website vulnerable to null byte injection, leading to directory traversal and exposing intranet login password to unauthorized user.

Steps to reproduce:

- Use subdirectory scanning tool to discover intranet login page and directory with password configuration file for it (See Screenshot 4 and see Screenshot 5)

```

(kali@kali-vle)-[~/Desktop]
$ dirb http://wasdat.fi

DIRB v2.223f19d48e13292c5e216e04ca339ea}
By The Dark Raver

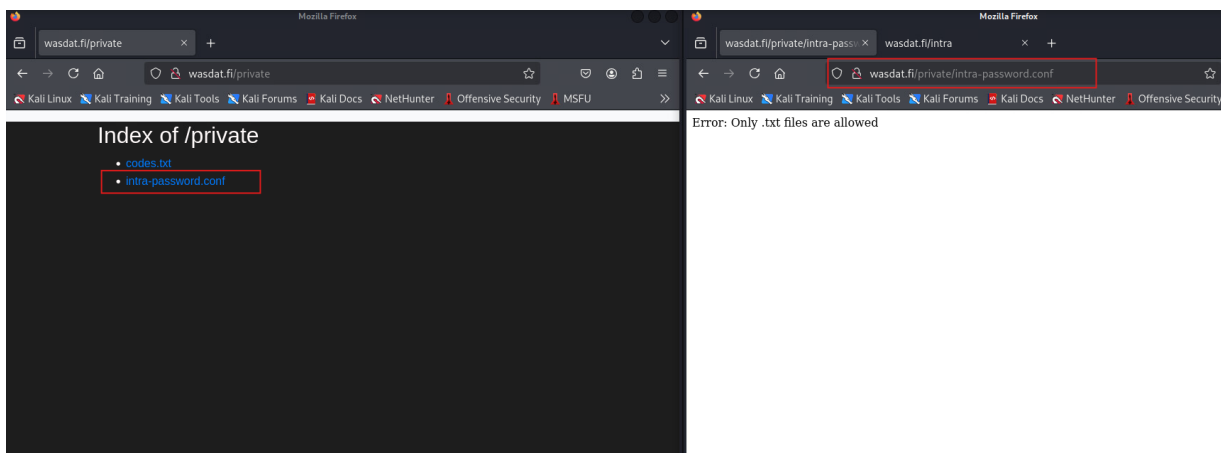
START_TIME: Sun Mar  2 22:11:06 2025
URL_BASE: http://wasdat.fi/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://wasdat.fi/ —
+ http://wasdat.fi/admin (CODE:301|SIZE:0)
+ http://wasdat.fi/cart (CODE:200|SIZE:2658)
+ http://wasdat.fi/intra (CODE:200|SIZE:2572)
+ http://wasdat.fi/private (CODE:200|SIZE:2368)
+ http://wasdat.fi/robots.txt (CODE:200|SIZE:89)
+ http://wasdat.fi/search (CODE:200|SIZE:2247)
=> DIRECTORY: http://wasdat.fi/static/

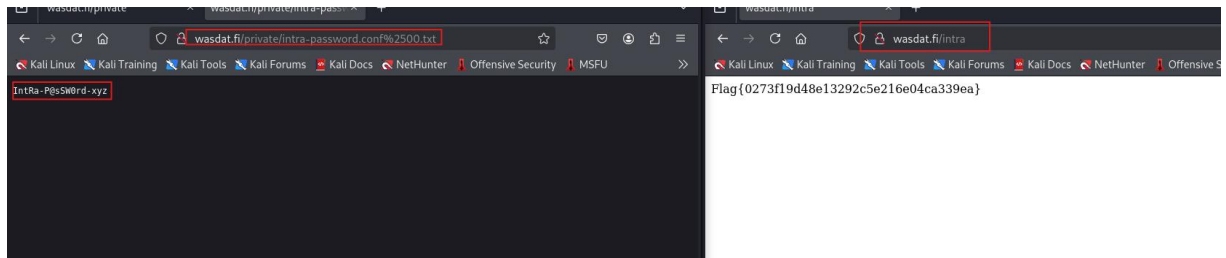
```

Screenshot 4



Screenshot 5

- Modify the request "http://wasdat.fi/private/intra-password.conf" to contain a null byte injection to bypass a requirement for .txt file and send it:  
**http://wasdat.fi/private/intra-password.conf%2500.txt**
- Access password for intranet and use it to login to intranet (See Screenshot 6 )



Screenshot 6

Impact estimation: Very high

Unauthorized users can exploit this vulnerability to access sensitive configuration file containing intranet login credentials and gain unauthorized access to intranet resources. This can lead to different severe consequences, including further privilege escalation or in worst case to full server compromise.

Mitigation:

- Proper input validation. Any input containing null bytes should be rejected.
- Restrict access to sensitive directories. Deny direct access to them from unauthorized users.
- Path Traversals – see [https://owasp.org/www-community/attacks/Path\\_Traversal](https://owasp.org/www-community/attacks/Path_Traversal)

### 3 Time management

Date	Used hours	Description
02.03.2025	1h	Reading chapter and watching recording
02.03.2025	0.5h	Exploiting the target weakness
02.03.2025	1h	Writing the documentation and finding the suitable resource recommendations
Total	2.5h	Finishing the assignment and reporting it