OWASP Top 5

Sl. No.	Name of Vulnerability	Reference CWE
1	Broken Access Control	CWE-377: Insecure Temporary File
2	Cryptographic Failures	CWE-331 Insufficient Entropy
3	Injection	CWE-184 Incomplete List of Disallowed Inputs
4	Insecure Design	CWE-269 Improper Privilege Management
5	Security Misconfiguration	CWE-315 Cleartext Storage of Sensitive Information in a Cookie

1. CWE-377: Insecure Temporary File

Description - Creating and using insecure temporary files can leave application and system data vulnerable to attack.
Business Impact - Some temporary files hold sensitive information like login credentials and payment details. Hackers can access this data if the files are not secure. By using this data, the attackers can gain access to the user's account and cause financial damage.
Example - https://hackerone.com/hacktivity/cve_discovery?id=CVE-2019-1010101

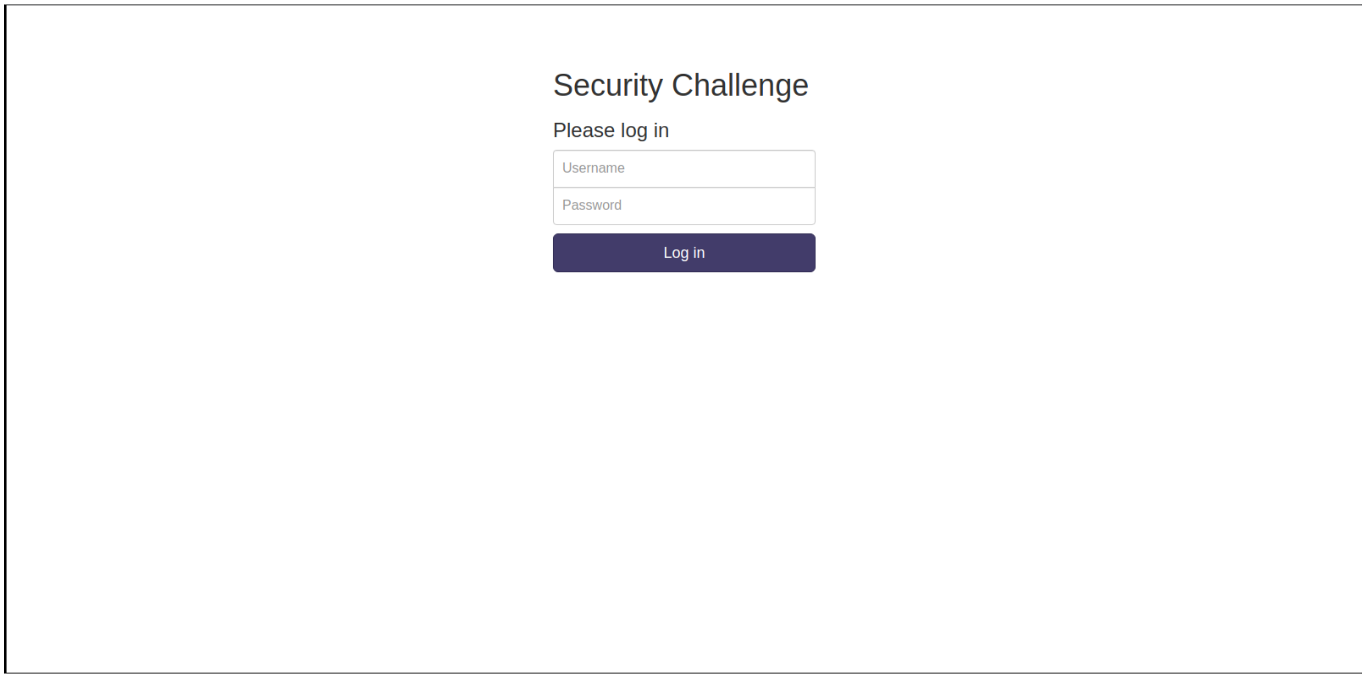
2. CWE-331 Insufficient Entropy

Description - The product uses an algorithm or scheme that produces insufficient entropy, leaving patterns or clusters of values that are more likely to occur than others.
Business Impact - Insufficient entropy leads to weak cryptographic protections. When encryption keys lack randomness, attackers can predict or guess them easily. This leads to data breaches.
Example - https://hackerone.com/hacktivity/cve_discovery?id=CVE-2021-22727

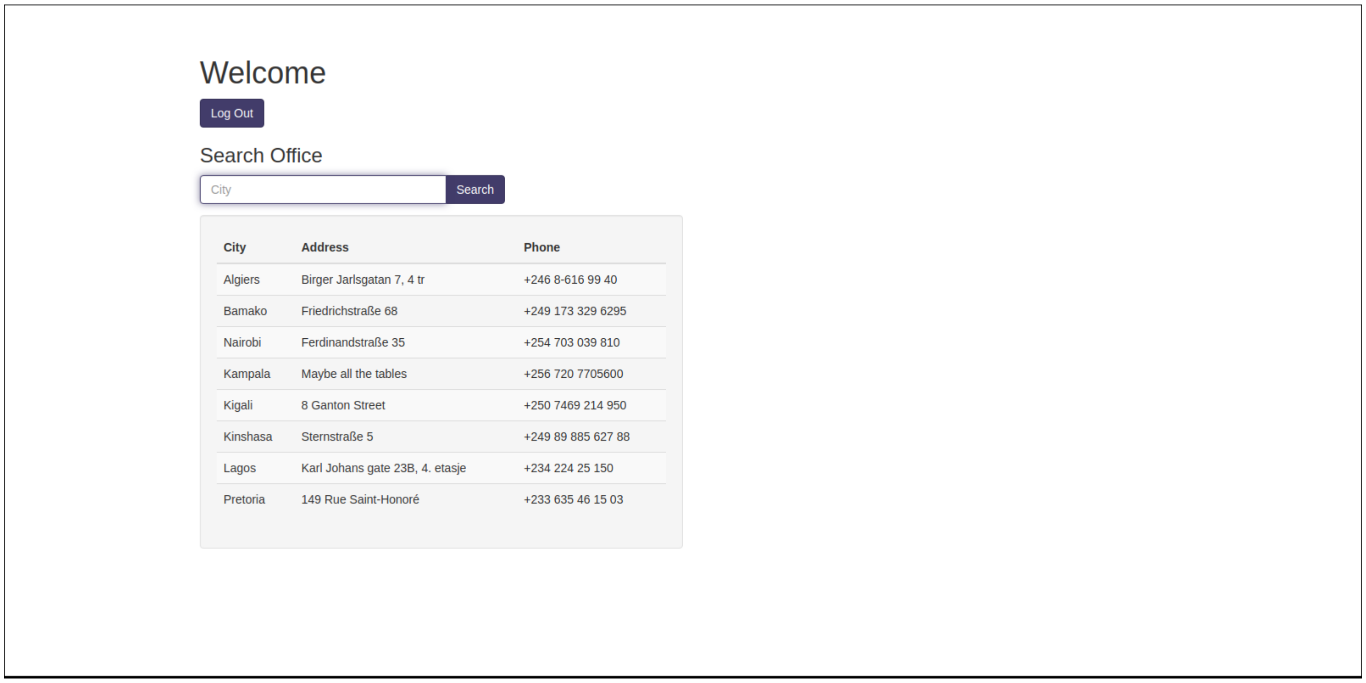
3. CWE-184 Incomplete List of Disallowed Inputs

Description - The product implements a protection mechanism that relies on a list of inputs (or properties of inputs) that are not allowed by policy or otherwise require other action to neutralise before additional processing takes place, but the list is incomplete, leading to resultant weaknesses.
Business Impact - Developers protect their products by banning inputs that invoke special commands. If the forbidden inputs are not properly blocked, attackers can inject data which won't be detected by the system (SQLi, XSS). This allows them to steal sensitive data which results in financial losses.

Example -



The inputs are not filtered properly so we can do some SQLi ('or 1=1;--) in the password field to get all the data on the website.



City	Address	Phone
Algiers	Birger Jarlsgatan 7, 4 tr	+246 8-616 99 40
Bamako	Friedrichstraße 68	+249 173 329 6295
Nairobi	Ferdinandstraße 35	+254 703 039 810
Kampala	Maybe all the tables	+256 720 7705600
Kigali	8 Ganton Street	+250 7469 214 950
Kinshasa	Sternstraße 5	+249 89 885 627 88
Lagos	Karl Johans gate 23B, 4. etasje	+234 224 25 150
Pretoria	149 Rue Saint-Honoré	+233 635 46 15 03

4. CWE-269 Improper Privilege Management

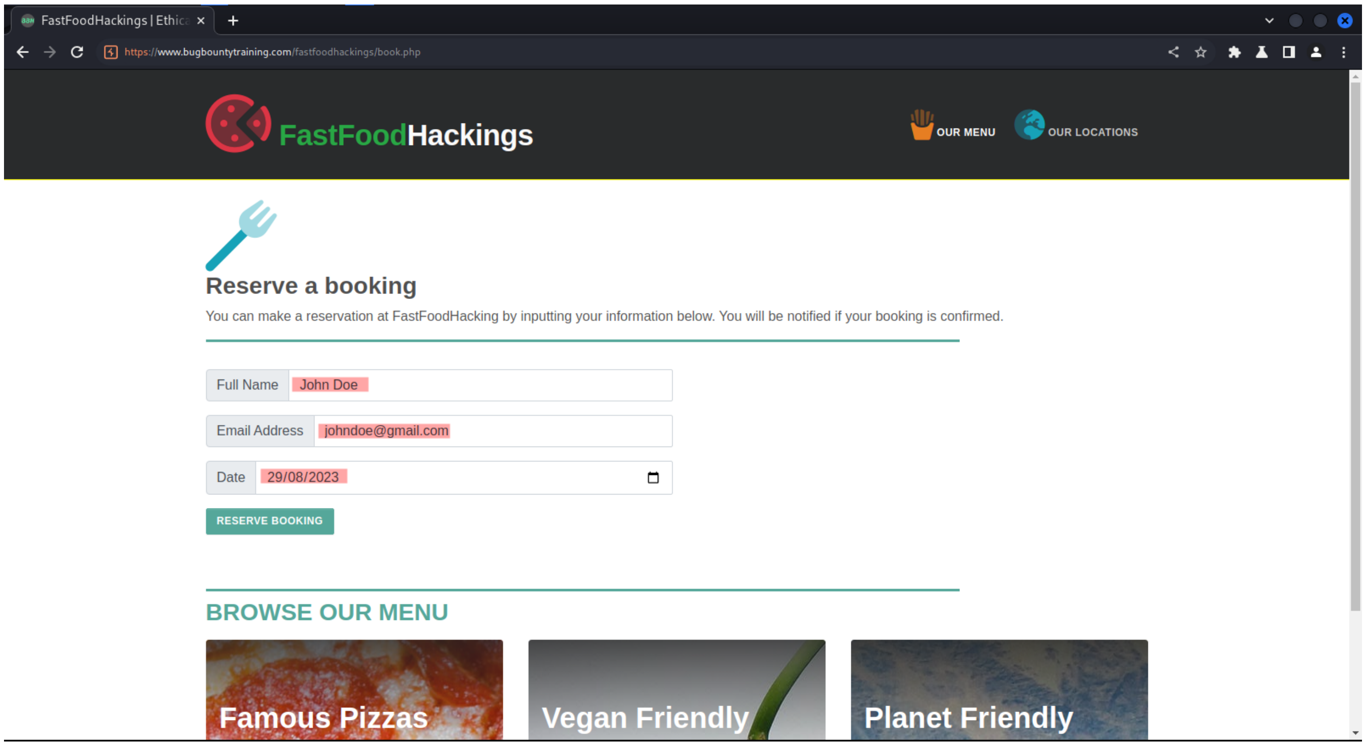
Description - The product does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor.
Business Impact - When user privileges are not configured/enforced properly, the users/attackers can easily escalate their privileges and manipulate the system. This can lead to data breaches, unauthorised system access or system alterations.
Example - https://hackerone.com/hacktivity/cve_discovery?id=CVE-2021-22801

5. CWE-315 Cleartext Storage of Sensitive Information in a Cookie

Description - Attackers can use widely-available tools to view the cookie and read the sensitive information. Even if the information is encoded in a way that is not human-readable, certain techniques could determine which encoding is being used, then decode the information.

Business Impact - Attackers can easily intercept unencrypted cookies containing sensitive information like login credentials. Using this data, they can gain access to user accounts compromising personal information or even escalating privileges. Individuals and businesses will face financial harm if such info is in the hands of an attacker.

Example -
On this website, we can order food by entering some details.

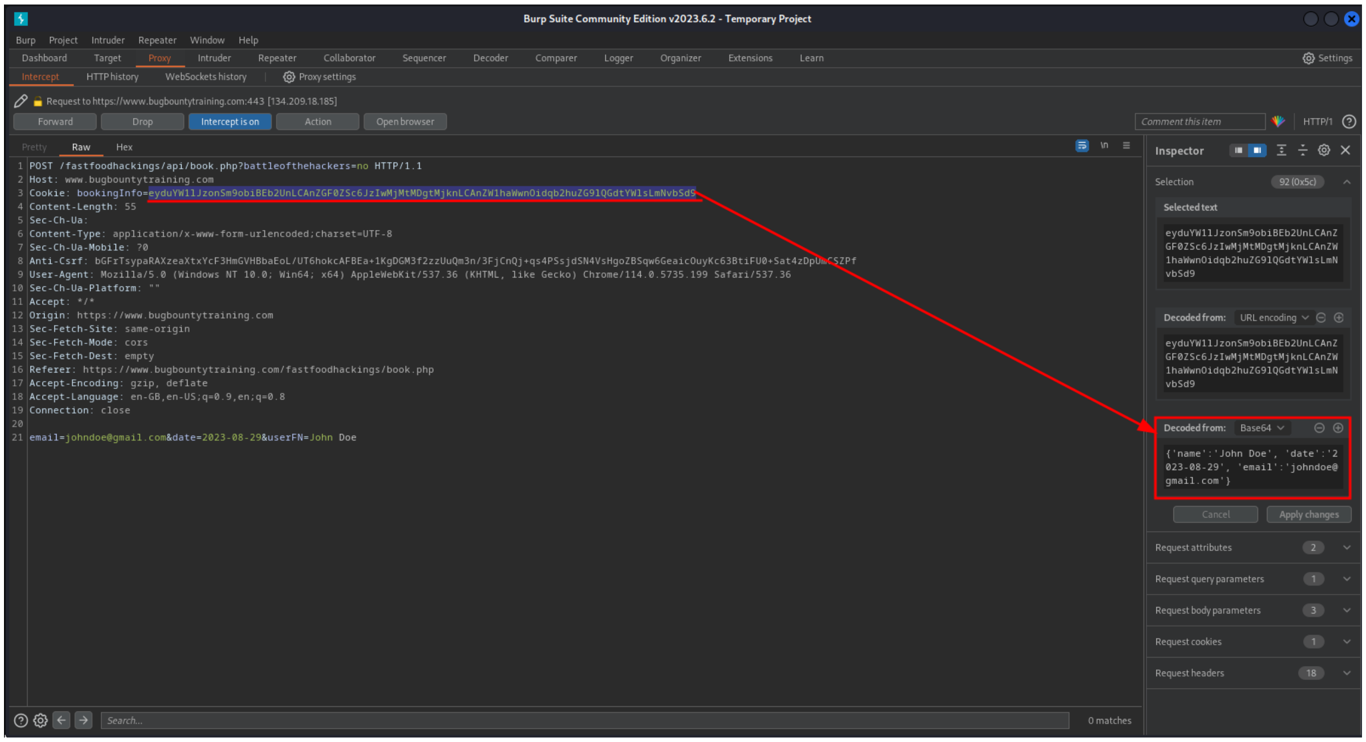


Reserve a booking

You can make a reservation at FastFoodHacking by inputting your information below. You will be notified if your booking is confirmed.

Full Name	John Doe
Email Address	johndoe@gmail.com
Date	29/08/2023

Using intercept mode on burpsuite, I interrupt the reservation request. Here we can easily decode the cookie using the built in base64 decoder to get back all the data.


Burp Suite Community Edition v2023.6.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Comment this item HTTP/1
Pretty Raw Hex
Inspector
Cancel Apply changes
Search... 0 matches

Request to https://www.bugbountytraining.com:443 [134.209.18.185]

```
POST /fastfoodhackings/api/book.php?battleofthehackers=no HTTP/1.1
Host: www.bugbountytraining.com
Cookie: bookingInfo=eyduYW1lJzonSm9obiBEb2UnLCAnZGF0ZSc6JzIwMjMtMDgtMjknLCAnZW1haWwnOidqb2huZG9lQGdtYWlsLmNvbSd9
Content-Length: 55
Sec-Ch-Ua:
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
Anti-Csrf: bGFrTsypaRAXzeaXtxYcF3HmGVHBbaEoL/UT6hokcAFBEa+1KgDGM3f2zzUuQm3n/3FjCnQj+qs4PSsjdSN4VsHgoZBSqw6GeaicOuyKc63BtiFU0+Sat4zDpUmCSZPf
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.199 Safari/537.36
Sec-Ch-Ua-Platform: ""
Accept: */*
Origin: https://www.bugbountytraining.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.bugbountytraining.com/fastfoodhackings/book.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

email=johndoe@gmail.com&date=2023-08-29&userFN=John Doe
```

Selection 92 (0x5c)

Selected text

```
eyduYW1lJzonSm9obiBEb2UnLCAnZ
GF0ZSc6JzIwMjMtMDgtMjknLCAnZW
1haWwnOidqb2huZG9lQGdtYWlsLmN
vbSd9
```

Decoded from: URL encoding

```
eyduYW1lJzonSm9obiBEb2UnLCAnZ
GF0ZSc6JzIwMjMtMDgtMjknLCAnZW
1haWwnOidqb2huZG9lQGdtYWlsLmN
vbSd9
```

Decoded from: Base64

```
{'name':'John Doe', 'date':'2
023-08-29', 'email':'johndoe@
gmail.com'}
```

Request attributes 2
Request query parameters 1
Request body parameters 3
Request cookies 1
Request headers 18