AICS TEAM 3.1

Vulnerability Report of Practice Website

Vulnerability Name: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

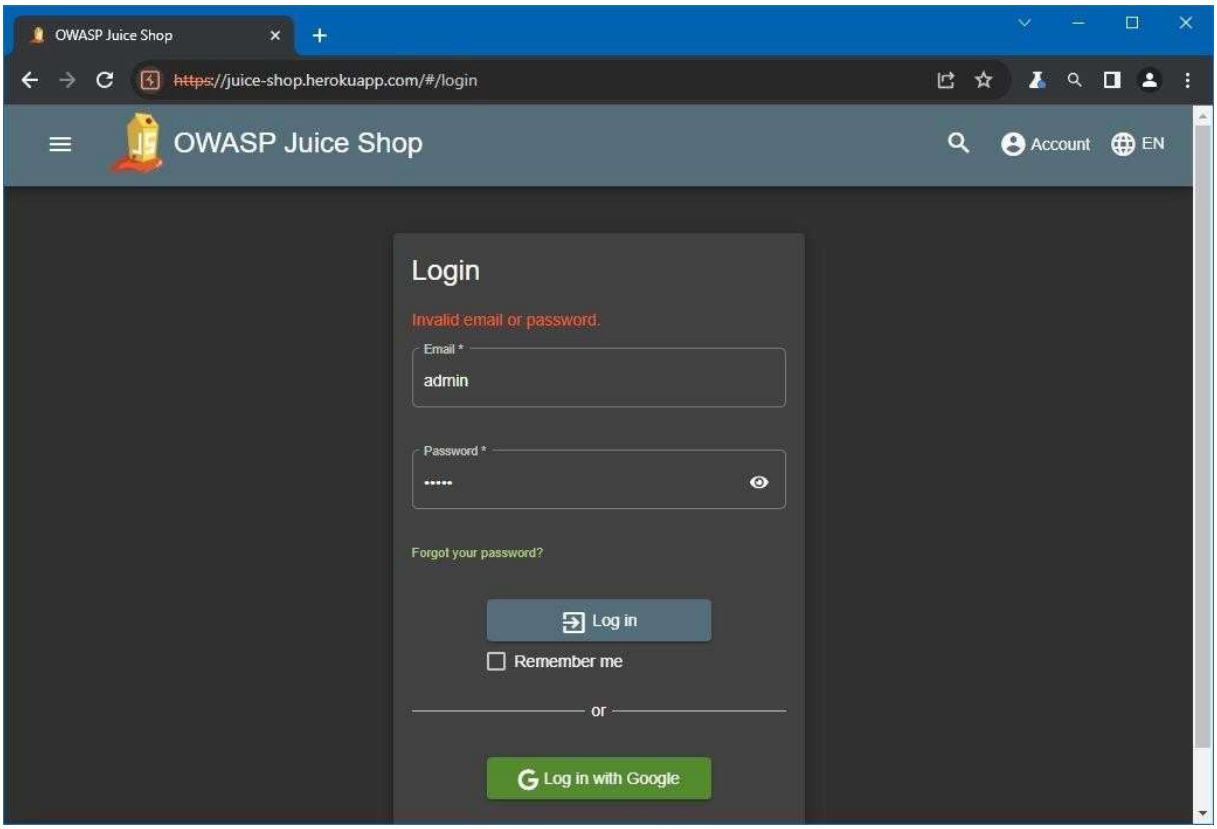
CWE: CWE-89

Description:

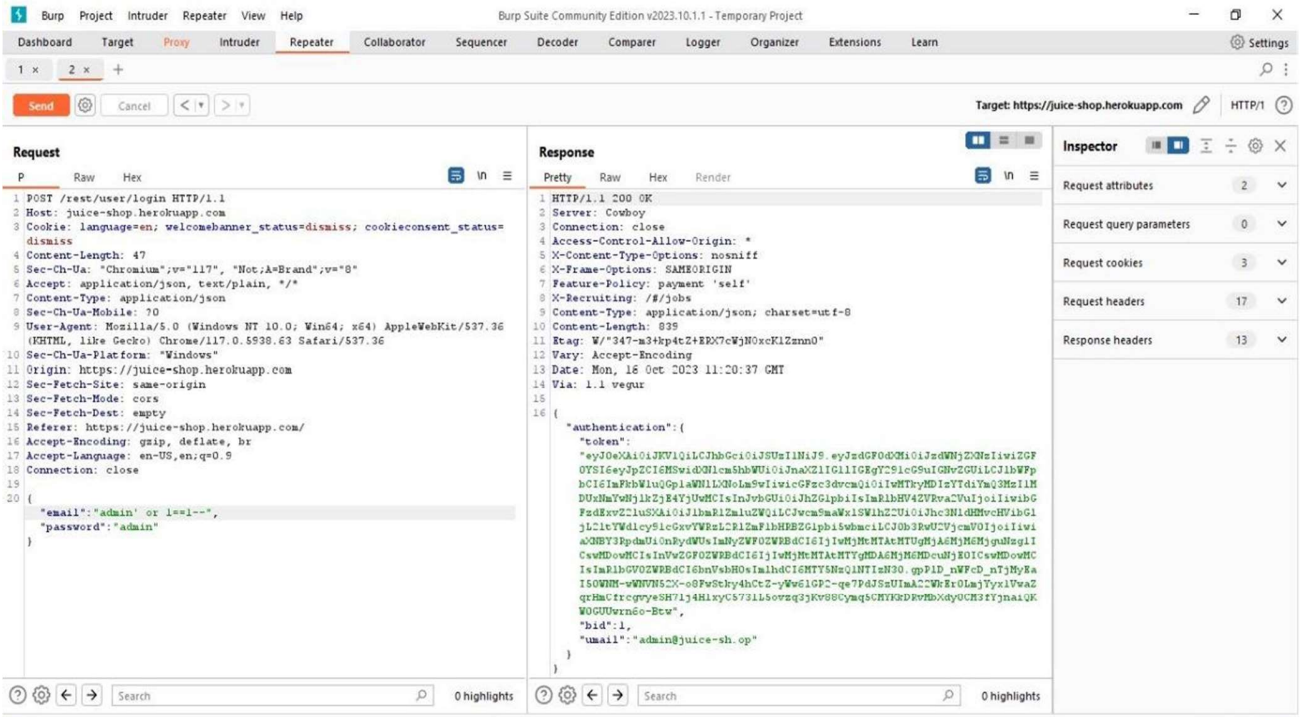
CWE-89, titled "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')," is a common software vulnerability that occurs when an application does not properly validate or sanitize user inputs before including them in SQL queries.

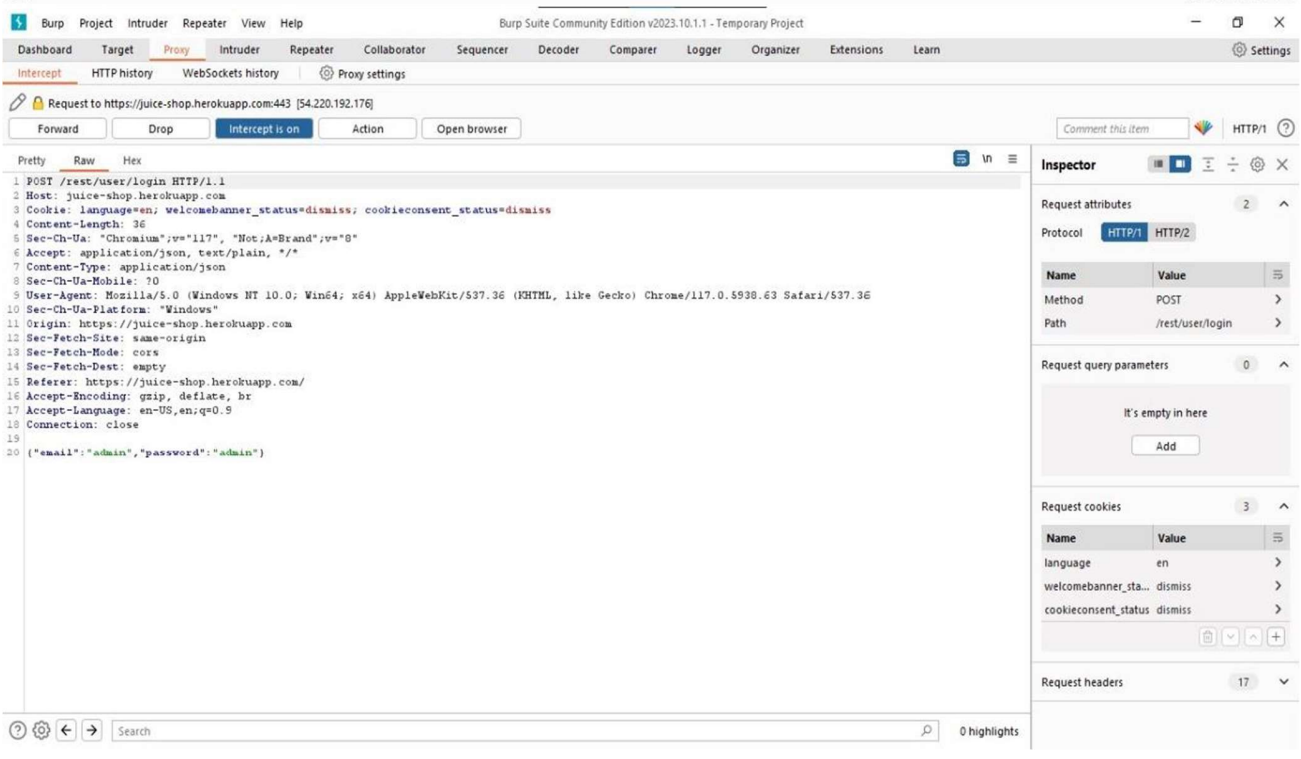
Business Impact:

CWE-89, or SQL injection, poses a severe business impact. This vulnerability can lead to data breaches, causing financial losses, legal repercussions, and reputational damage. Data theft compromises sensitive customer information and intellectual property, eroding trust and potentially triggering costly legal actions



AICS TEAM 3.1


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: https://juice-shop.herokuapp.com
HTTP/1
Request
Response
Inspector
Request attributes 2
Request query parameters 0
Request cookies 3
Request headers 17
Response headers 13
0 highlights
Done
1,229 bytes | 523 millis


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Intercept HTTP history WebSockets history Proxy settings
Request to https://juice-shop.herokuapp.com:443 [54.220.192.176]
Forward Drop Intercept is on Action Open browser
Inspector
Request attributes 2
Protocol HTTP/1 HTTP/2
Name Value
Method POST
Path /rest/user/login
Request query parameters 0
It's empty in here
Add
Request cookies 3
language en
welcomebanner_sta... dismiss
cookieconsent_status dismiss
Request headers 17
0 highlights

AICS TEAM 3.1

Vulnerability Name: Improper input validation

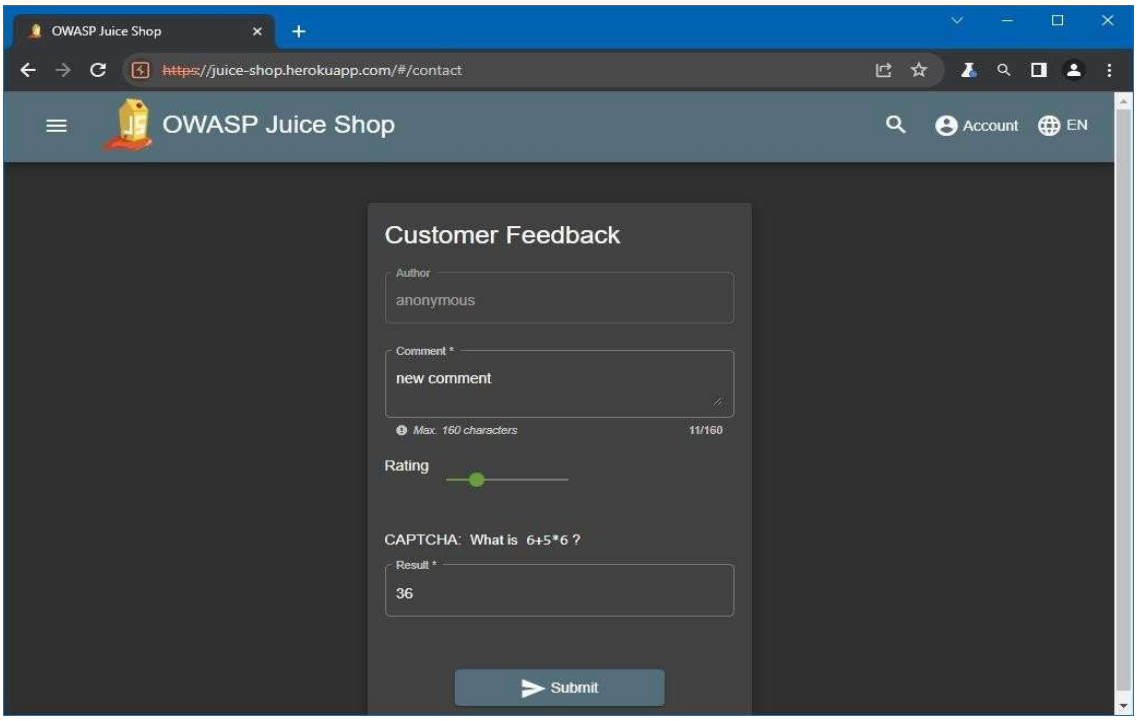
CWE: CWE 20

Description:

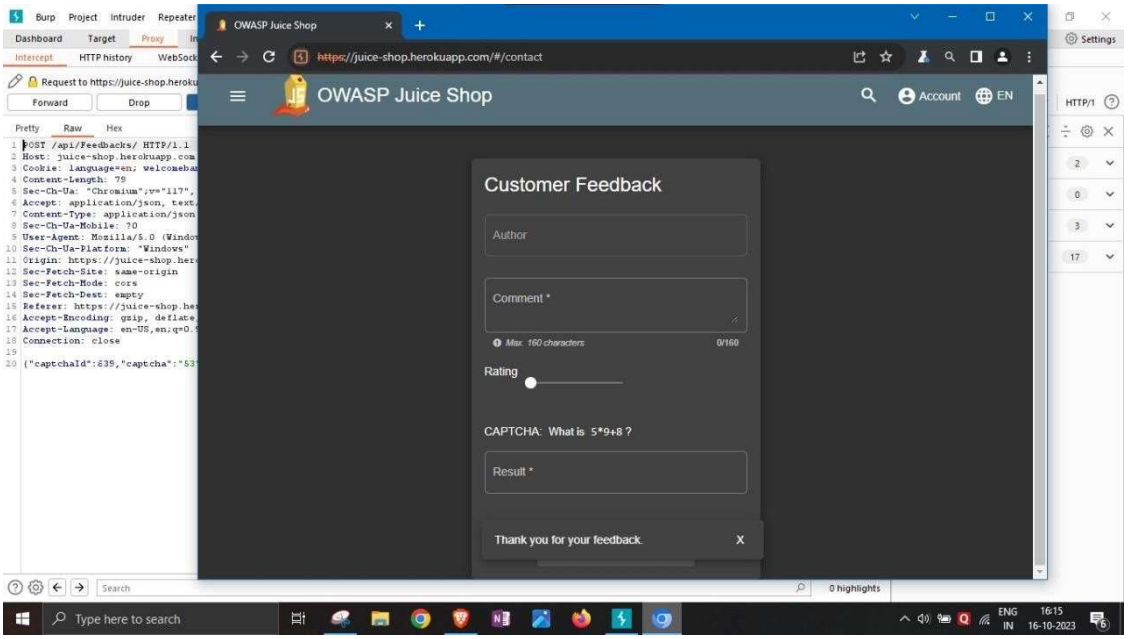
CWE-20, also known as "Improper Input Validation," is a software weakness that occurs when a program does not adequately validate and sanitize user inputs. This can lead to security vulnerabilities such as buffer overflows, SQL injection, and cross-site scripting.

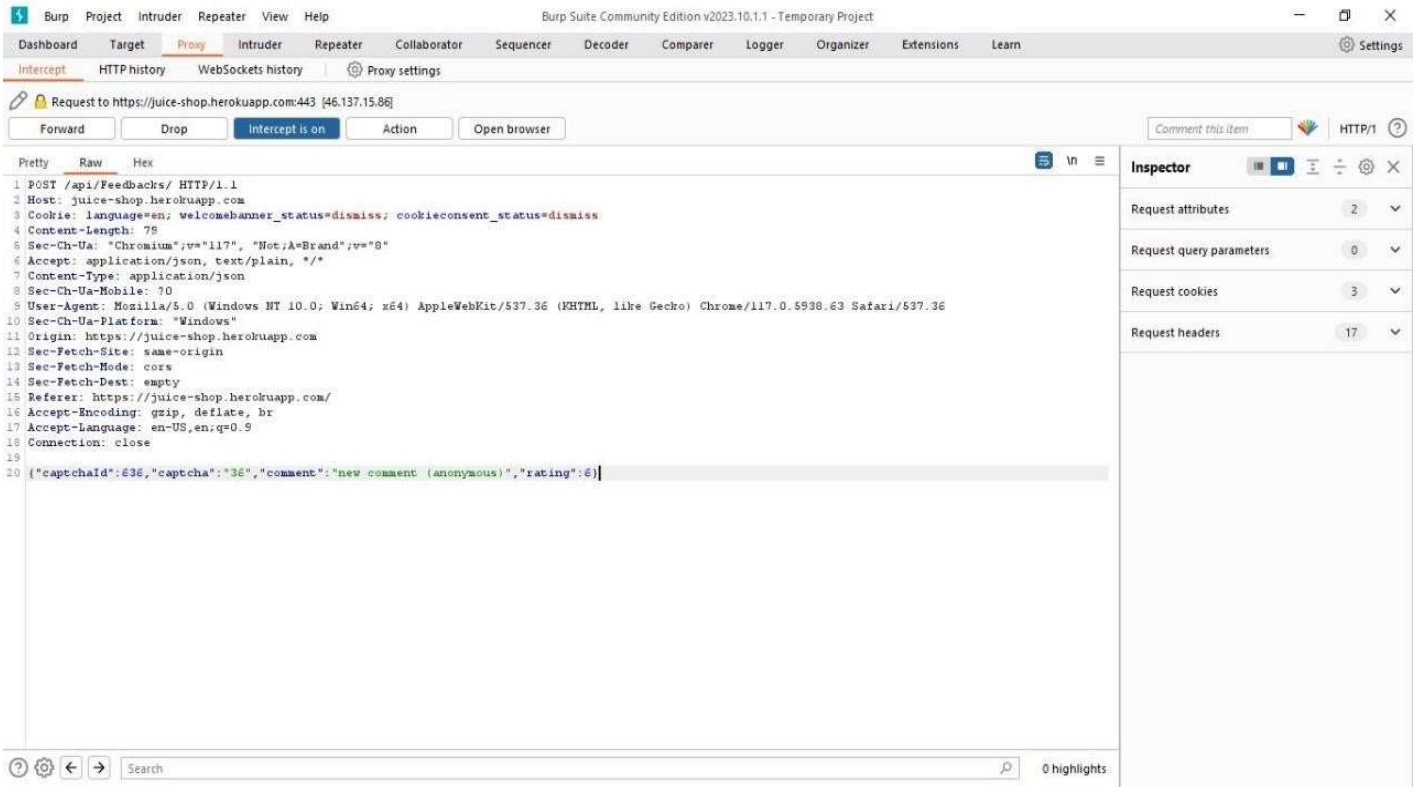
Business Impact:

CWE-20 can have a significant business impact, including data breaches, financial losses, reputation damage, and legal liabilities. Vulnerabilities arising from improper input validation can allow attackers to exploit software, leading to unauthorized access, data theft, and service disruptions, potentially resulting in customer trust erosion and costly remediation efforts.



AICS TEAM 3.1


Burp Project Intruder Repeater
OWASP Juice Shop
https://juice-shop.herokuapp.com/#/contact
OWASP Juice Shop
Account
EN
Customer Feedback
Author
Comment *
Max. 160 characters
0/160
Rating
CAPTCHA: What is 5*9+8 ?
Result *
Thank you for your feedback.
Type here to search
ENG
IN
16:15
16-10-2023


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to https://juice-shop.herokuapp.com:443 [46.137.15.86]
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
1 POST /api/Feedbacks/ HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
4 Content-Length: 79
5 Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8"
6 Accept: application/json, text/plain, */*
7 Content-Type: application/json
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.63 Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Origin: https://juice-shop.herokuapp.com
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://juice-shop.herokuapp.com/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20 {"captchaId":636,"captcha":"36","comment":"new comment (anonymous)","rating":6}
Inspector
Request attributes 2
Request query parameters 0
Request cookies 3
Request headers 17
Search
0 highlights

AICS TEAM 3.1

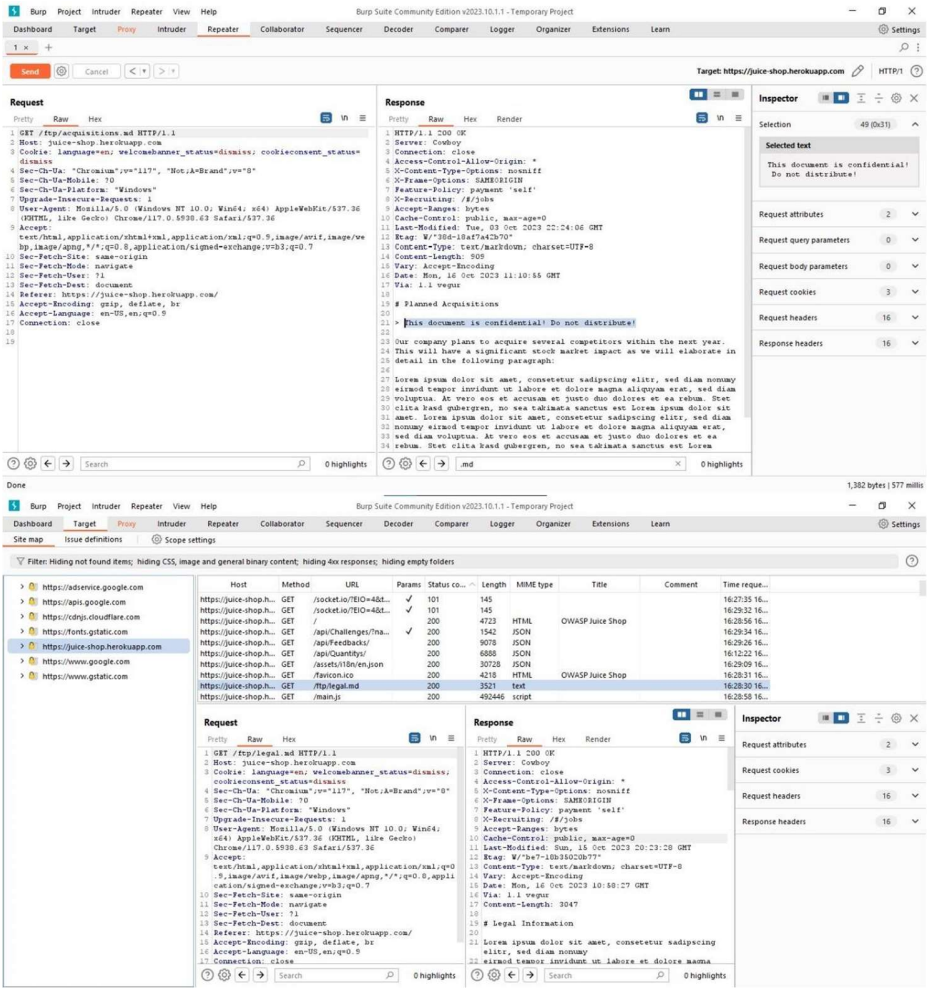
Vulnerability Name: Sensitive data exposure

CWE: CWE 200

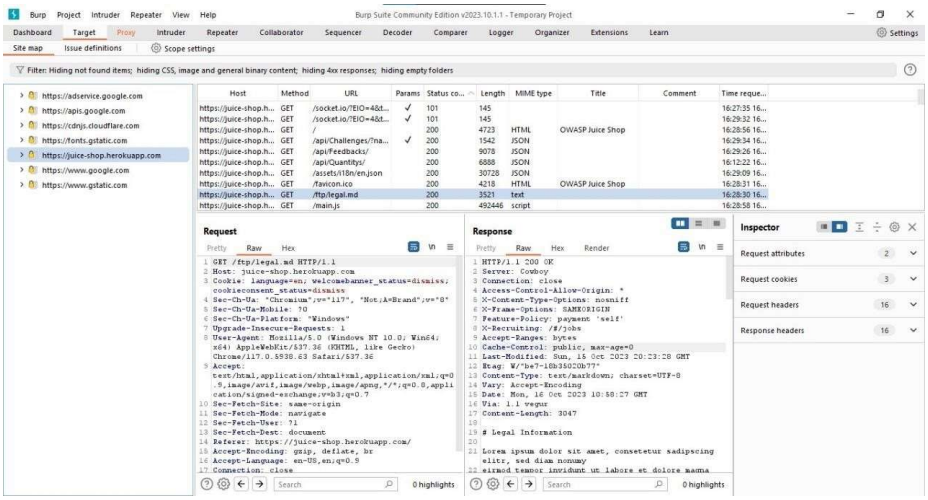
Description:
CWE-200, known as "Exposure of Sensitive Information to an Unauthorized Actor”

Business Impact:

CWE-200 can result in severe business consequences, including reputational damage, loss of customer trust, legal consequences, and financial losses.



AICS TEAM 3.1


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Site map
Issue definitions
Scope settings
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
https://adservice.google.com
https://apis.google.com
https://cdnjs.cloudflare.com
https://fonts.gstatic.com
https://juice-shop.herokuapp.com
https://www.google.com
https://www.gstatic.com
Host Method URL Params Status co... Length MIME type Title Comment Time reque...
https://juice-shop.h... GET /socket.io/?EIO=4&t... 101 145 16:27:35 16...
https://juice-shop.h... GET /socket.io/?EIO=4&t... 101 145 16:29:32 16...
https://juice-shop.h... GET / 200 4723 HTML OWASP Juice Shop 16:28:56 16...
https://juice-shop.h... GET /api/Challenges/?na... 200 1542 JSON 16:29:34 16...
https://juice-shop.h... GET /api/Feedbacks/ 200 9078 JSON 16:29:26 16...
https://juice-shop.h... GET /api/Quantitys/ 200 6888 JSON 16:12:22 16...
https://juice-shop.h... GET /assets/i18n/en.json 200 30728 JSON 16:29:09 16...
https://juice-shop.h... GET /favicon.ico 200 4218 HTML OWASP Juice Shop 16:28:31 16...
https://juice-shop.h... GET /ftp/legal.md 200 3521 text 16:28:30 16...
https://juice-shop.h... GET /main.js 200 492446 script 16:28:58 16...
Request
Pretty Raw Hex
GET /ftp/legal.md HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.63 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
Search
0 highlights
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Server: Cowboy
Connection: close
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Sun, 15 Oct 2023 20:23:28 GMT
Etag: W/"be7-18b3602bb77"
Content-Type: text/markdown; charset=UTF-8
Vary: Accept-Encoding
Date: Mon, 16 Oct 2023 10:58:27 GMT
Via: 1.1 vegur
Content-Length: 3047
Legal Information
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna
Search
0 highlights
Inspector
Request attributes 2
Request cookies 3
Request headers 16
Response headers 16

AICS TEAM 3.1

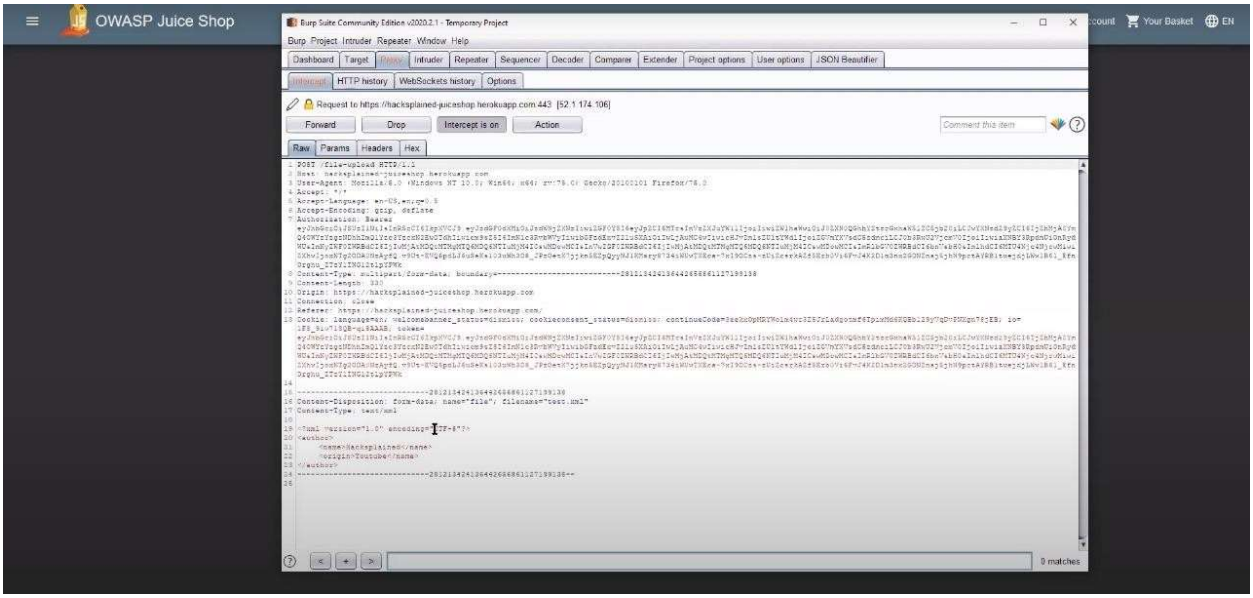
Vulnerability Name: Security misconfiguration

Description:

Security misconfiguration vulnerabilities occur when a system, application, or component is improperly set up, leaving it exposed to potential attacks. These weaknesses can lead to unauthorized access, data breaches, or other security incidents due to poorly configured permissions, default settings, or unnecessary features being enabled.

Business Impact:

Security misconfigurations can have significant business impacts, including data breaches, downtime, regulatory fines, and reputational damage. Improperly configured systems or applications can lead to unauthorized access, data exposure, and service disruptions. These incidents can result in financial losses, eroded customer trust, and legal consequences, affecting an organization's bottom line and market standing. Proper configuration management is essential to mitigate these risks.



AICS TEAM 3.1

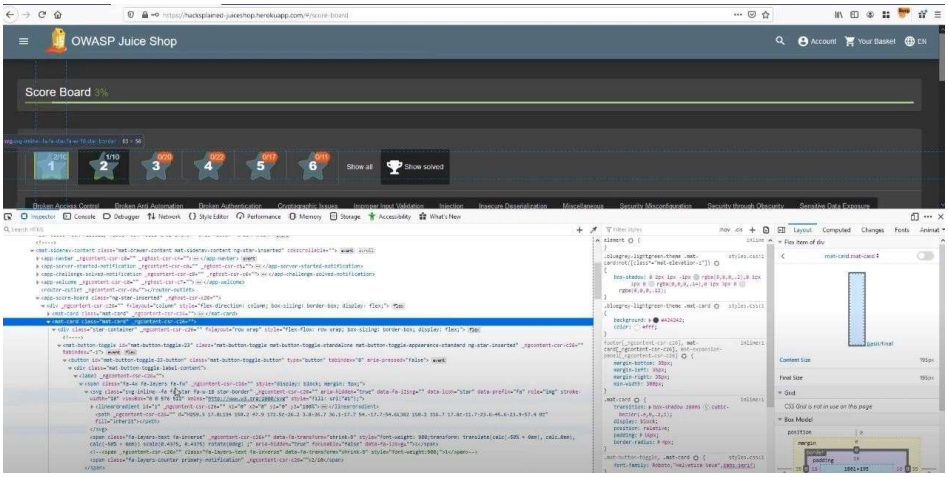
Vulnerability Name: Broken access control

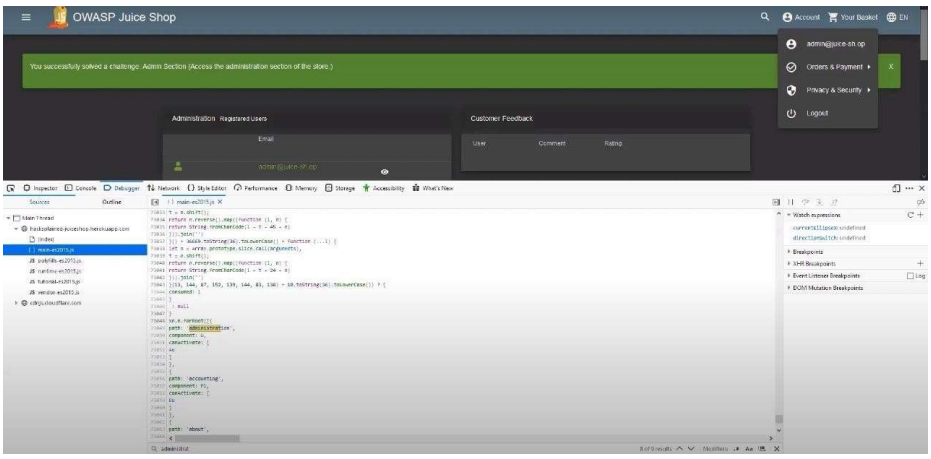
Description:

Broken access control is a security vulnerability that occurs when an application or system fails to enforce proper access restrictions. It allows unauthorized users to access sensitive data, perform actions, or modify resources they should not have permission to access. This issue can lead to unauthorized data exposure, data tampering, and pose significant security risks if not mitigated effectively through access control mechanisms.

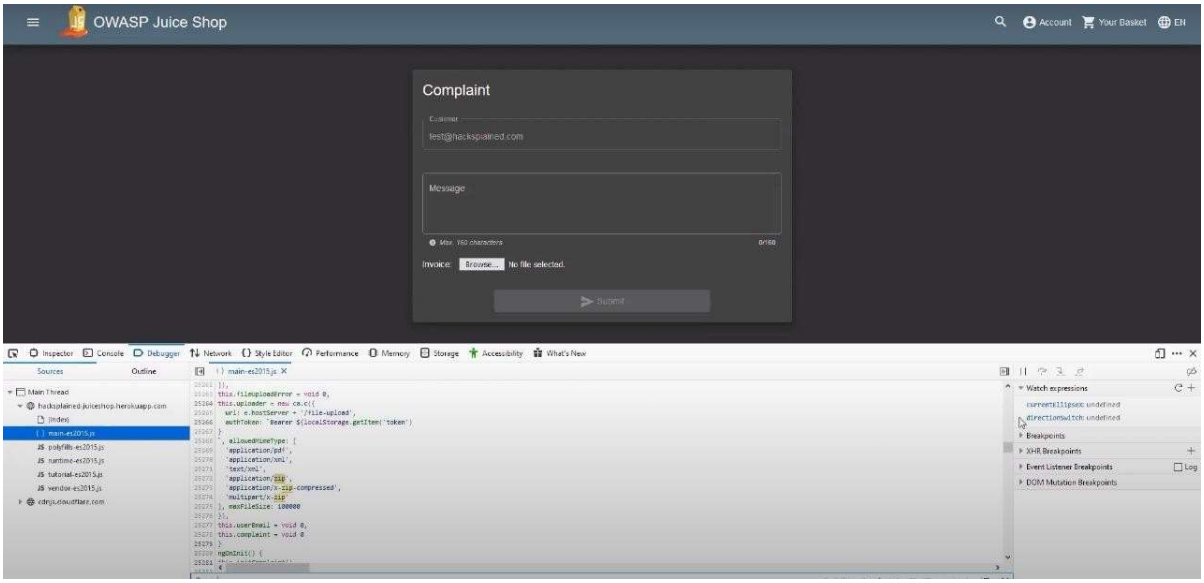
Business Impact:

Broken access control can have serious business impacts, including data breaches, compromised privacy, regulatory fines, and damage to reputation. Unauthorized users gaining access to sensitive data or functionality can lead to information theft, legal liabilities, and a loss of customer trust. This can result in financial losses, costs associated with investigations, and remediation efforts, ultimately affecting the organization's financial stability and brand image.





AICS TEAM 3.1


OWASP Juice Shop
Account
Your Basket
EN
Complaint
Customer
test@hackspalmed.com
Message
Max. 160 characters
0/160
Invoice:
Browse...
No file selected.
Submit
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
What's New
Sources
Outline
main-es2015.js
Watch expressions
Breakpoints
XHR Breakpoints
Event Listener Breakpoints
DOM Mutation Breakpoints

AICS TEAM 3.1

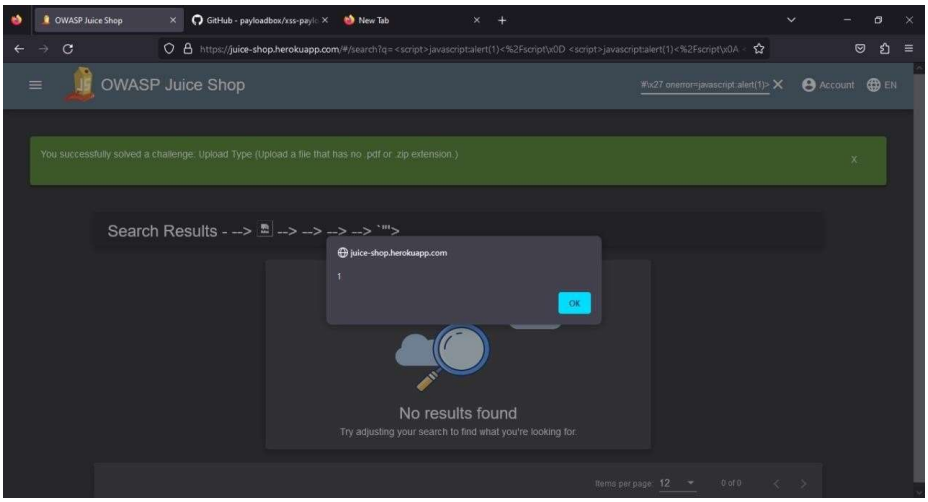
Vulnerability Name: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CWE: CWE 79

Description:

CWE-79, also known as "Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')," is a security vulnerability where an application includes untrusted data in web pages without proper validation. Attackers can inject malicious scripts, enabling them to steal data or perform actions on behalf of users, compromising their security and privacy.

Business Impact:
CWE-79 can have significant business impact, including reputation damage, data breaches, and financial losses. Cross-site scripting vulnerabilities allow attackers to steal sensitive data, compromise user accounts, and deface websites, eroding customer trust and potentially leading to regulatory fines. Organizations may also incur costs for incident response, legal liabilities, and remediation, affecting their bottom line and market standing.



AICS TEAM 3.1

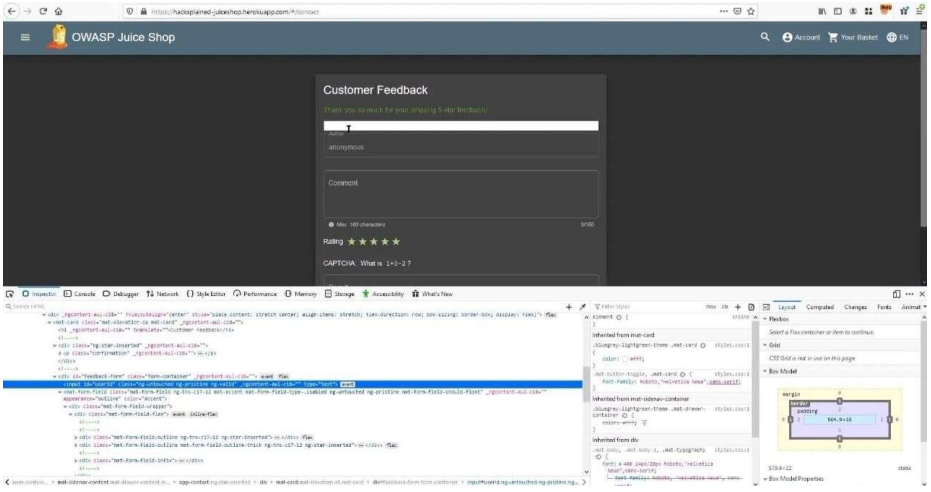
Vulnerability Name: Forged Feedback

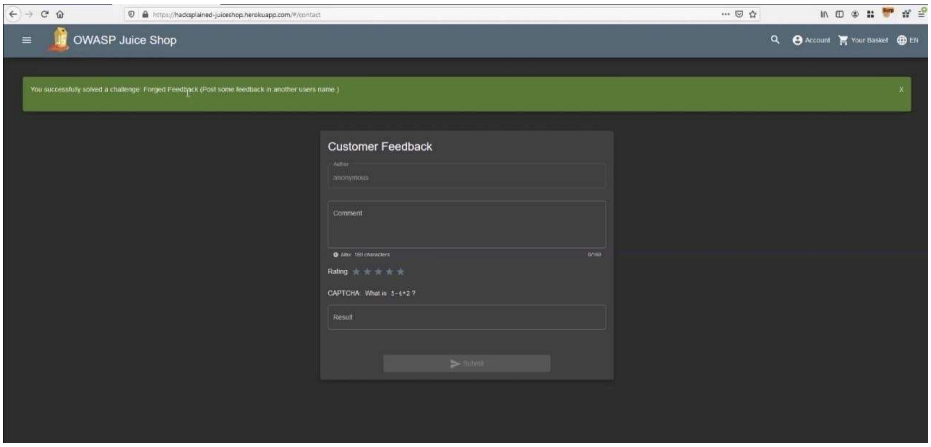
Description:

Forged feedback is a security vulnerability where attackers manipulate or counterfeit feedback or responses from a system to deceive users or systems. This can lead to misinformation, trust erosion, and potentially security breaches when users make decisions or take actions based on the fraudulent feedback provided.

Business Impact:

Forged feedback vulnerabilities can have a significant business impact, including damage to an organization's reputation, financial losses, and a potential loss of customer trust. Attackers exploiting these weaknesses can deceive users and may lead to actions that compromise security, result in data breaches, or tarnish an organization's image. This can result in costs for incident response, legal liabilities, and long-term harm to the organization's market standing.





AICS TEAM 3.1

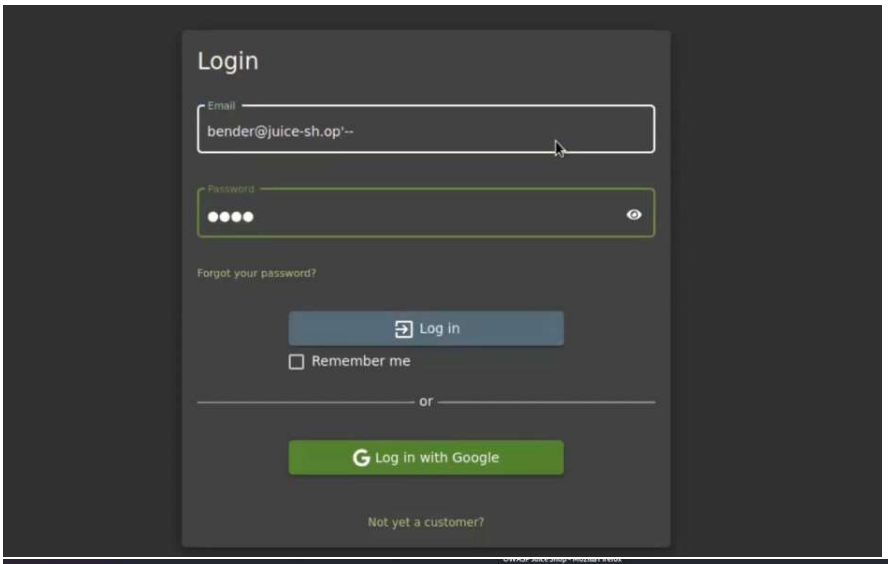
Vulnerability Name: Broken Authentication

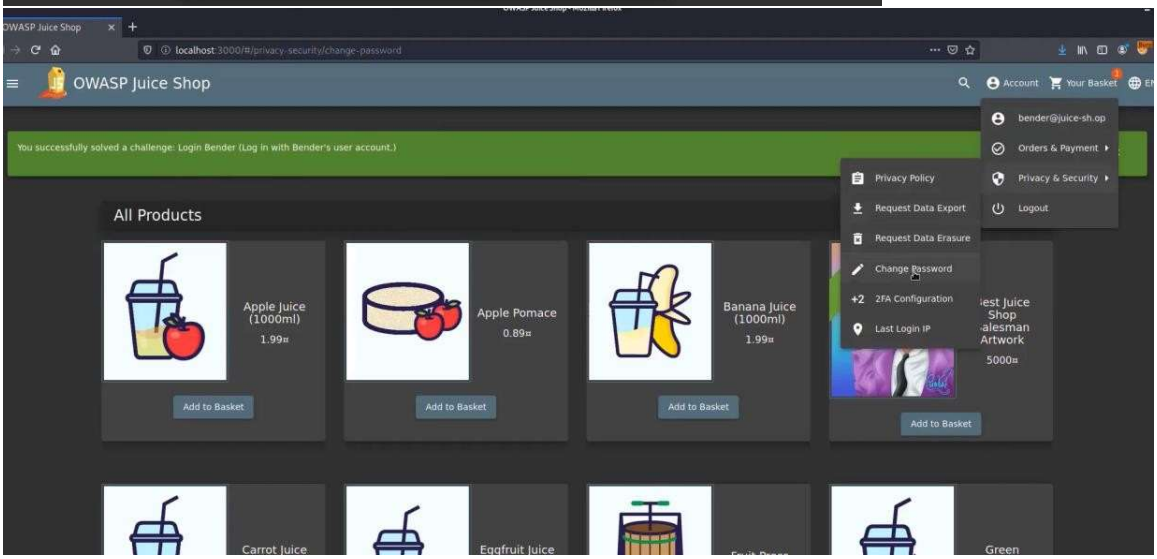
Description:

Broken authentication is a security issue where flawed or weak authentication and session management in an application enable unauthorized users to gain access to accounts and data. This can lead to data breaches, reputation damage, legal consequences, and financial losses.

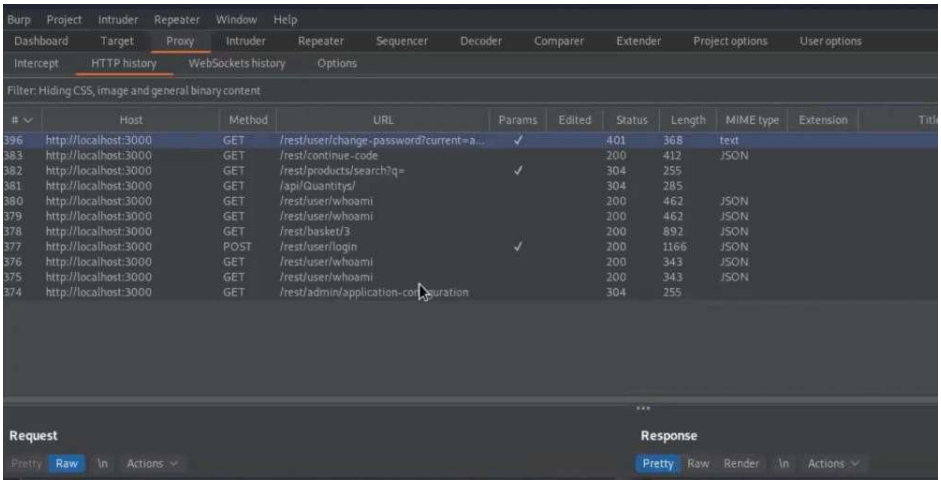
Business Impact:

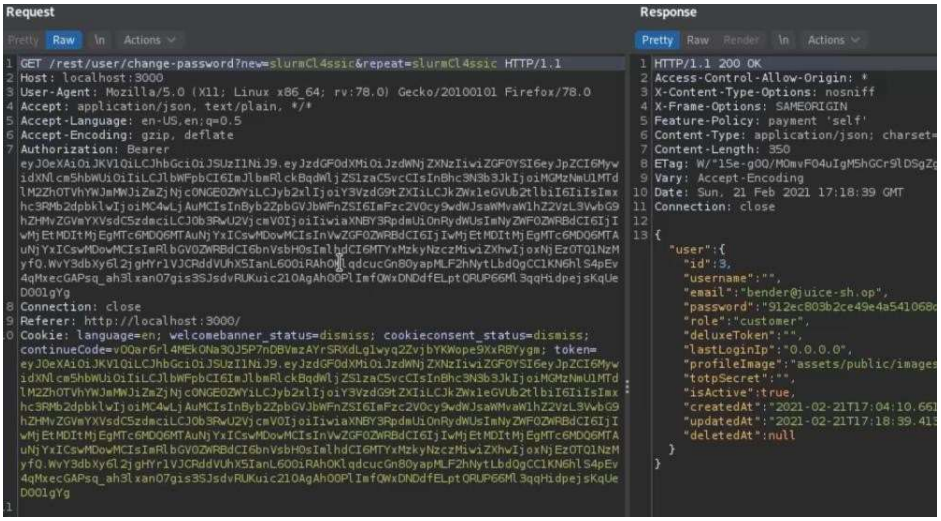
The business impact of broken authentication is significant. It can result in unauthorized access to user accounts and data, leading to data breaches and potentially severe financial losses. It also risks damaging a company's reputation and trust among its customers. Legal consequences and non-compliance with data protection regulations may further compound the impact, resulting in fines and legal actions.

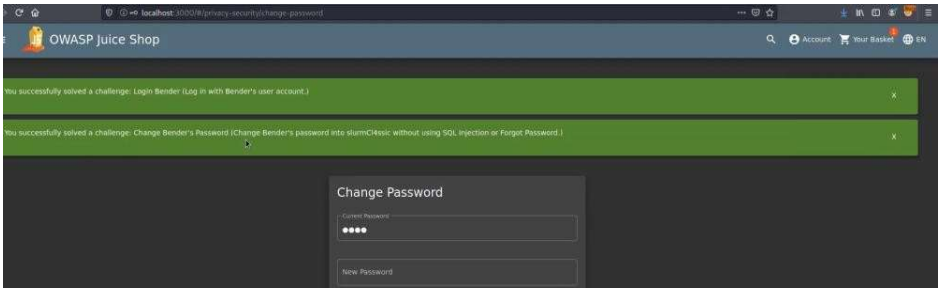




AICS TEAM 3.1


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension
396 http://localhost:3000 GET /rest/user/change-password?current=a... ✓ 401 368 text
383 http://localhost:3000 GET /rest/continue-code 200 412 JSON
382 http://localhost:3000 GET /rest/products/search?q= ✓ 304 255
381 http://localhost:3000 GET /api/Quantitys/ 304 285
380 http://localhost:3000 GET /rest/user/whoami 200 462 JSON
379 http://localhost:3000 GET /rest/user/whoami 200 462 JSON
378 http://localhost:3000 GET /rest/basket/3 200 892 JSON
377 http://localhost:3000 POST /rest/user/login ✓ 200 1166 JSON
376 http://localhost:3000 GET /rest/user/whoami 200 343 JSON
375 http://localhost:3000 GET /rest/user/whoami 200 343 JSON
374 http://localhost:3000 GET /rest/admin/application-configuration 304 255
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions


Request
Pretty Raw \n Actions
GET /rest/user/change-password?new=slurmCl4ssic&repeat=slurmCl4ssic HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
Response
Pretty Raw Render \n Actions
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=
Content-Length: 350
ETag: W/"15e-g0Q/MOmvF04uIgMShGCr9lDSgZ
Vary: Accept-Encoding
Date: Sun, 21 Feb 2021 17:18:39 GMT
Connection: close
{
"user":{
"id":3,
"username":"",
"email":"bender@juice-sh.op",
"password":"912ec803b2ce49e4a541068
"role":"customer",
"deluxeToken":"",
"lastLoginIp":"0.0.0.0",
"profileImage":"assets/public/images
"totpSecret":"",
"isActive":true,
"createdAt":"2021-02-21T17:04:10.661
"updatedAt":"2021-02-21T17:18:39.41
"deletedAt":null
}
}


OWASP Juice Shop
Account
Your Basket
EN
You successfully solved a challenge: Login Bender (Log in with Bender's user account.)
You successfully solved a challenge: Change Bender's Password (Change Bender's password into slurmCl4ssic without using SQL Injection or Forgot Password.)
Change Password
Current Password
New Password

AICS TEAM 3.1

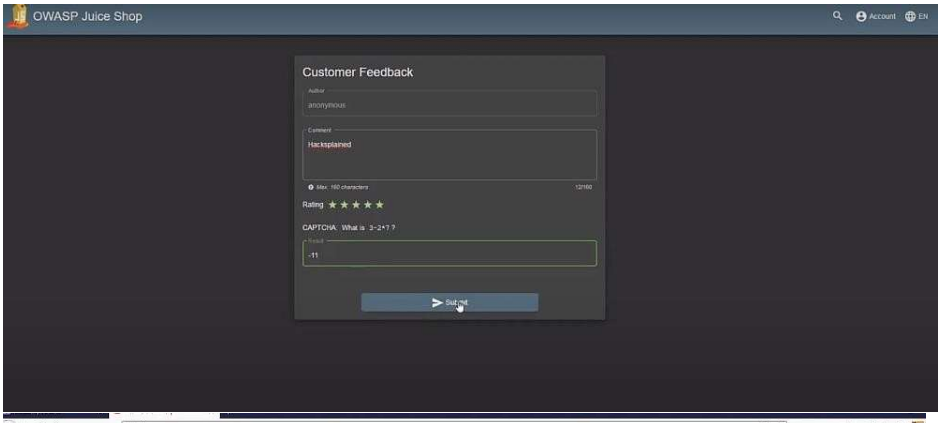
Vulnerability Name: Captcha Bypass(Broken Anti Authentication)

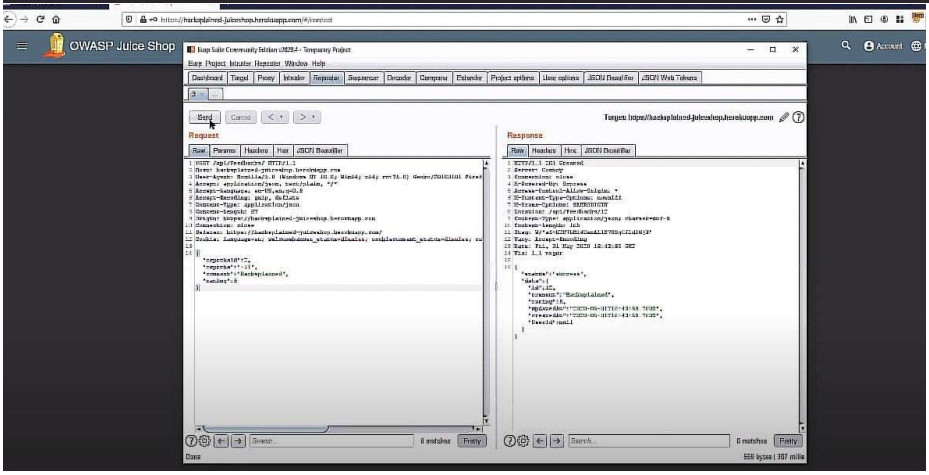
Description:

Captcha Bypass, a type of Broken Authentication, is a security vulnerability where automated scripts or attackers circumvent CAPTCHA challenges designed to prevent unauthorized access. By evading these safeguards, attackers can gain access to protected systems, potentially causing data breaches, fraud, or other malicious activities.

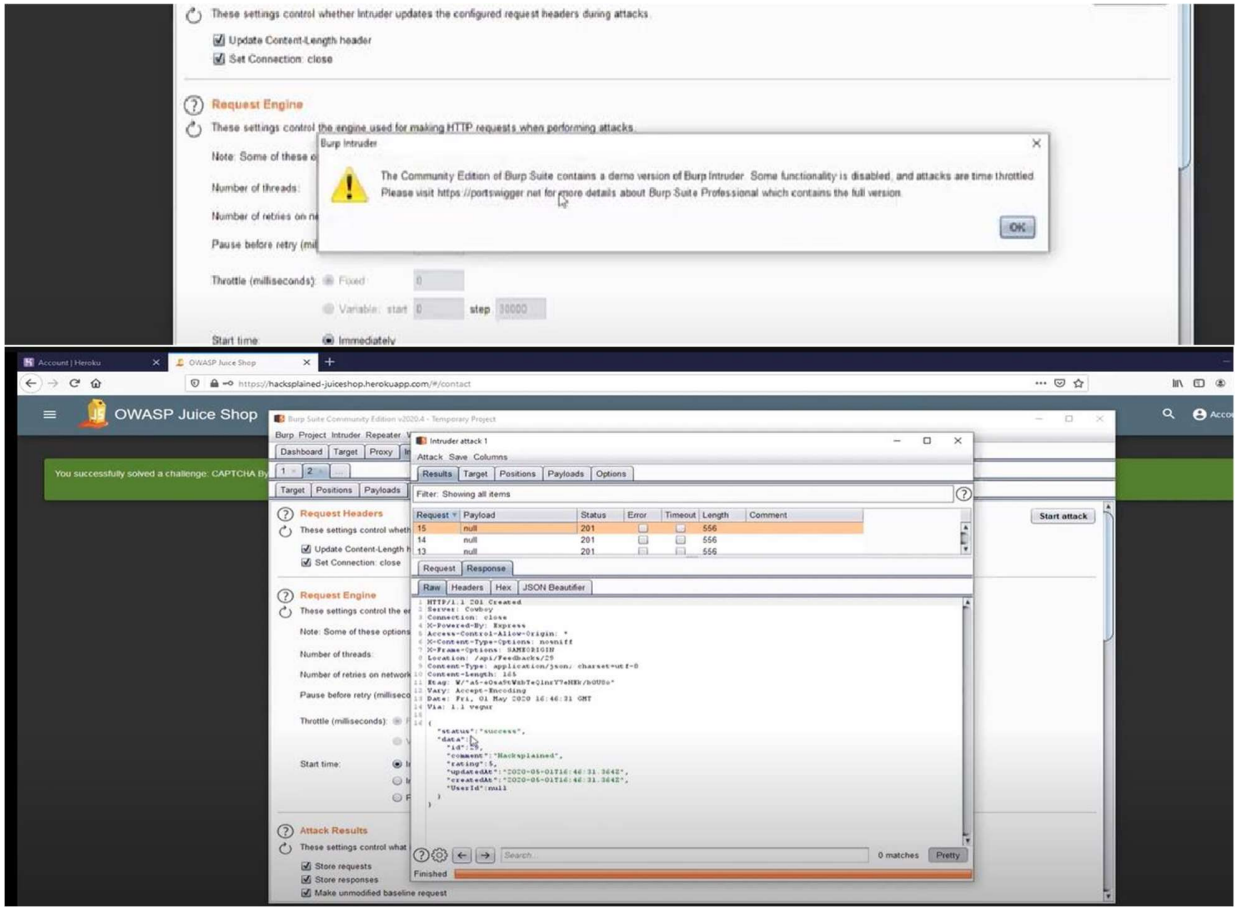
Business Impact:

Captcha Bypass, a form of Broken Authentication, can have serious business consequences. By allowing unauthorized users to evade CAPTCHA challenges, it can lead to unauthorized access, fraud, spam, and account takeovers. This undermines user trust, increases operational costs for dealing with fraudulent activities, and may result in reputational damage. Companies may also face legal and regulatory issues if they fail to protect user accounts and data adequate.





AICS TEAM 3.1


These settings control whether Intruder updates the configured request headers during attacks.
Update Content-Length header
Set Connection: close
Request Engine
These settings control the engine used for making HTTP requests when performing attacks.
Burp Intruder
The Community Edition of Burp Suite contains a demo version of Burp Intruder. Some functionality is disabled, and attacks are time-throttled.
Please visit https://portswigger.net for more details about Burp Suite Professional which contains the full version.
OK
Number of threads:
Pause before retry (mil
Throttle (milliseconds):
Fixed
Variable: start
step
Start time:
Immediately
OWASP Juice Shop
https://hacksplained-juiceshop.herokuapp.com/#/contact
You successfully solved a challenge: CAPTCHA By
Burp Suite Community Edition v2020.4 - Temporary Project
Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
15 null 201 556
14 null 201 556
13 null 201 556
Start attack
Request Response
Raw Headers Hex JSON Beautifier
Request Headers
Request Engine
Attack Results
Store requests
Store responses
Make unmodified baseline request
0 matches
Pretty
Finished