



The future of AppSec: PortSwigger's vision

PortSwigger is
on a mission to
enable the
world to secure
the web.

17k+

Customers

160+

Countries

200k+

Active users

1.4m+

Scans in 2025

Contents

01

AppSec in 2025+

02

Burp Suite DAST

03

Burp Suite Professional

04

Introducing Burp AI



AppSec

In 2025+

Application security is evolving



Software development is faster than ever

Continuous deployment.
AI-generated code.
API-first architectures.



Attackers are evolving just as quickly

Using automation & AI to find issues before you're aware of them.



Security teams are struggling to keep pace

Workload pressure leads to security trade-offs

Security teams are stretched thin.

We need smarter ways to work efficiently.

*"Not enough **time**  to test everything well."*

*"**Time**  constraint for testing applications."*

*"Lack of **time**  to go deep into manual testing due to workload pressure"*

*"Dividing my **time**  in testing for specific vulnerabilities"*

**More apps,
more APIs,
more risk.**

More complexity
means more gaps.

54%

Struggle with modern
application complexity

Shift-left alone isn't enough.

Security that works in
development but fails
in production isn't
security at all.



Prioritizing security
testing in the SDLC

Shift-left alone isn't enough.

Security that works in
development but fails
in production isn't
security at all.

*"The revival of HTTP request
smuggling has led to
devastating vulnerabilities
in our modern
application deployments"*

Bishop Fox

**More
signal, less
noise.**

Security teams need to
prioritize real risks, not
distractions.

63%

Of AppSec professionals
cite false positives as a
major frustration

AI is reshaping security.

AI will supercharge
human testers,
sharpening focus on
real threats.

70%

Are optimistic about
using AI for security

AI is reshaping security.

AI will supercharge
human testers,
sharpening focus on
real threats.

Zero

Believe AI can fully
replace manual testing

PortSwigger's vision for the future



**Keeping pace
with an
evolving web**



**Full-lifecycle
security
testing**



**Automation
fused with
human
insight**

**AI that
enhances,
not replaces
humans**



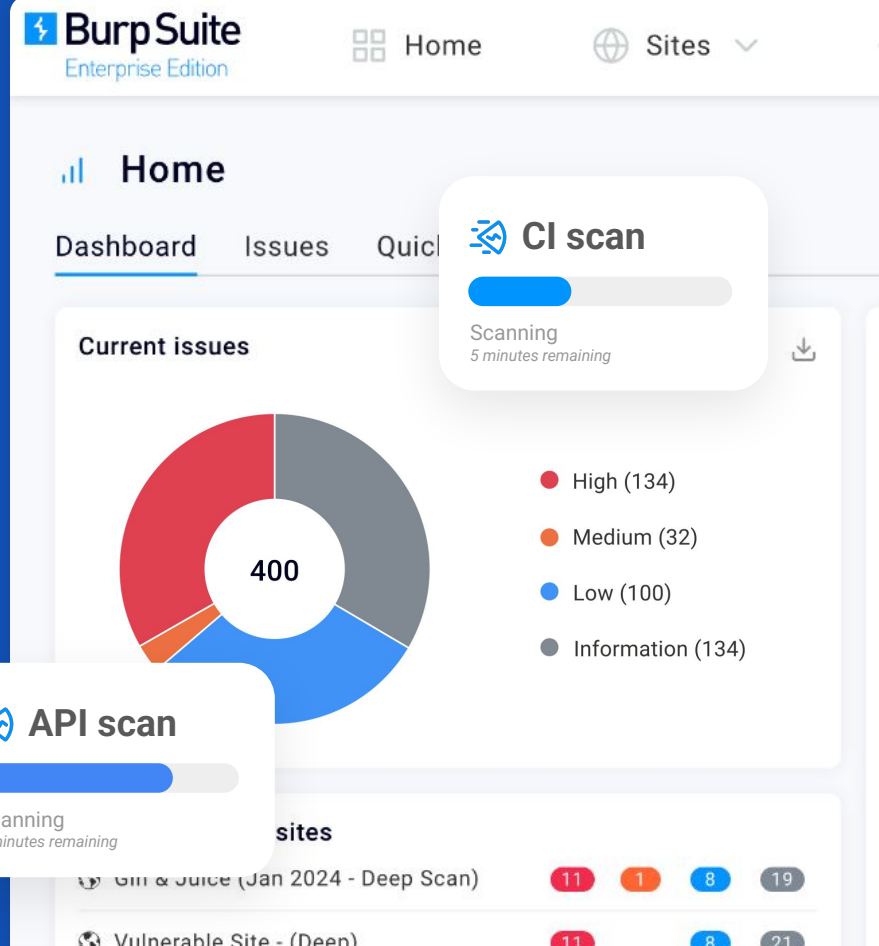
Burp Suite DAST

Best-in-class, enterprise-grade DAST scanning
from the leading authority on web security.

Trusted insights from Burp Suite's
industry-leading scanner.

Limitless scalability.

Secure your apps and APIs before
they hit production.



Battle-hardened Burp Suite technology your team already trusts

Harmonized experience across your
manual and automated testing.

Reduce the burden on
your manual testers.



Reuse your existing
configuration library.

Consistent scan results and issue
categorization.

**Automate
scans
wherever
and
whenever
you need to.**



PortSwigger Cloud



**On-premises &
private cloud**

E.g. AWS, Azure, GCP



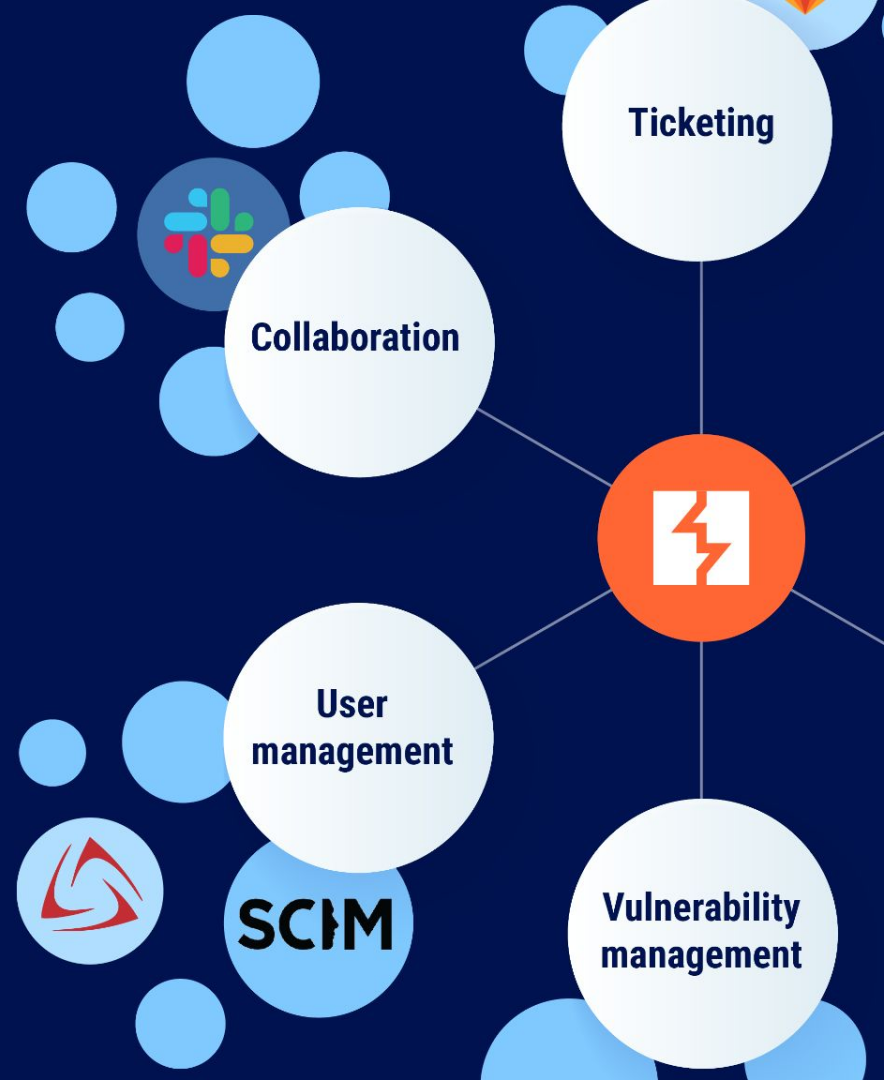
Kubernetes



CI/CD

E.g. GitLab, GitHub, Jenkins

**Integrate with
the systems
your teams
already rely on.**





Burp Suite DAST is trusted by global enterprises

"By partnering with PortSwigger and adopting Burp Suite DAST, we're able to satisfy our security requirements at scale, with the lowest false positives, ensuring we're able to improve our SAP solutions, while providing deeper technical insights to regional regulators."

Alijohn Ghassemloei

Senior Director of Engineering, Sovereign Cloud at SAP



New in Burp Suite DAST



Enhanced scalability

Performance improvements to handle vast estates

Bulk schedule scans

Customised CI-scans

Faster vulnerability detection



Native API scanning

Scan API targets via file upload or self hosted URL

Postman, OpenAPI, SOAP, GraphQL

Various auth methods including dynamic refresh tokens



Reporting & Integrations

Integration with Splunk

Enhanced crawl visibility

Enhanced issue management options

Enhanced Jira integration

2025 Roadmap

Scalability

Asset tagging

Scan freeze windows

Advanced scope control

Enhanced authentication

API scanning

Fast validation

API scanning a scale

Reporting & Integrations

Further Jira customisation

Full issue history

Advanced issue management



Burp Suite Professional

The gold-standard toolkit of choice for web app and API security testing.

Helps you test deeper, faster.

Automates the tedious.
Amplifies expertise.

Focuses your time where it matters most.

Dashboard Target Proxy Intruder Repeater Collaborator Decoder Sequencer Comparer Logger Organ

Tasks New scan New live task Filter Search

10. Crawl and audit of ginandjuice.shop
Crawl and Audit - Lightweight
Paused
Issues: 0 0 0 0

9. Crawl and audit of ginandjuice.shop
Crawl and Audit - Lightweight
Finished
Issues: 2 0 0 1

6. Crawl and audit of ginandjuice.shop
Crawl and Audit - Fast
Finished
Issues: 10 0 7 20

5. Crawl and audit of 0aac003d043a606186dd634000...
Crawl and Audit - Lightweight
Finished
Issues: 0 0 0 0

4. Crawl and audit of 0aac003d043a606186dd634000...
Crawl and Audit - Lightweight

6. Crawl and audit of ginandjuice.shop
Summary Audit items Issues Event log Logger

Most serious vulnerabilities found (live)

Issue type	Host
Cross-site scripting (reflected)	https://ginandjuice.
Cross-site scripting (reflected)	https://ginandjuice.
External service interaction (HTTP)	https://ginandjuice.
HTTP response header injection	https://ginandjuice.
Client-side template injection	https://ginandjuice.
Client-side template injection	https://ginandjuice.
Cross-site scripting (DOM-based)	https://ginandjuice.
Client-side desync	http://ginandjuice.s
SQL injection	https://ginandjuice.
SQL injection	https://ginandjuice.
Strict transport security not enforced	https://ginandjuice.
Link manipulation (reflected DOM-based)	https://ginandjuice.
Link manipulation (reflected DOM-based)	https://ginandjuice.
Link manipulation (reflected DOM-based)	https://ginandjuice.
Open redirection (DOM-based)	https://ginandjuice.
Open redirection (DOM-based)	https://ginandjuice.
Vulnerable JavaScript dependency	https://ginandjuice.
Backup file	https://ginandjuice.
Backup file	https://ginandjuice.
Cacheable HTTPS response	https://ginandjuice.
Cookie without HttpOnly flag set	https://ginandjuice.
Cookie without HttpOnly flag set	https://ginandjuice.
Cross-site scripting (reflected)	https://ginandjuice.
External service interaction (DNS)	https://ginandjuice.
Input returned in response (reflected)	https://ginandjuice.
Input returned in response (reflected)	https://ginandjuice.
Input returned in response (reflected)	https://ginandjuice.
Input returned in response (reflected)	https://ginandjuice.
Input returned in response (reflected)	https://ginandjuice.
TLS certificate	https://ginandjuice.
TLS cookie without secure flag set	https://ginandjuice.

The most powerful security testing toolkit for modern web applications and APIs



```
graph TD; Title[The most powerful security testing toolkit for modern web applications and APIs] --- Feature1[Rich message manipulation]; Title --- Feature2[Exploitation without restrictions]; Title --- Feature3[Advanced automation];
```

Rich message manipulation

Unmatched HTTP/1, HTTP/2, and WebSocket manipulation capabilities

Fine-grained configuration and full control

Exploitation without restrictions

Persistent connections

Hex editor and non-printing character injection

Native out-of-band testing with Burp Collaborator

Advanced automation

Best-of-breed scanner

Intruder

DOM Invader

**Unmatched
extensibility.
Customizable
to the core.
Powered by a
thriving
community.**



**Fully-featured API for deep
integration and customization**

Bambdas for lightweight automation

Custom scan checks

**Access to a powerful ecosystem of
community-created extensions**

**Powerful extensions created by the
PortSwigger research team**



Microsoft

*"I would be surprised if all penetration testers are not exclusively using Burp Suite... [at Microsoft] it's not even up for consideration. **Burp Suite is what you use.**"*

Taylor O'Dell

Security Engineer, Microsoft

New in Burp Suite Professional



Performance improvements

Faster load times for large responses and tables

Lower memory usage and improved stability across the Suite

Lag-busting upgrades across the UI



Expanded extensibility

Powerful new scripting capabilities through Bambdas

Bambda Library to manage and share

Continued evolution of the Montoya API




Modernised workflows & UI

Smoother, faster interactions across the suite

Polished UI and enhanced functionality across core tools


Fewer clicks. More flow.
Better focus.



 **Tib3rius** 30/08/2024 18:36
Updated to Burp Pro v2024.7.5 today. Project before upgrade was using ~4GB of memory. Project after is using ~700MB. 🙌
👍 4 🗨️

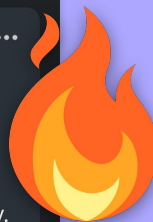


Comments Most relevant

 **Petr Juhaňák** · 3rd+ 1h (edited) ...
Penetration Tester - OSCP, BSCP, CISSP

I cannot imagine my job without Burp. The journey from WAHH paper book to Burp Academy along with the software improvements over time, UX redesign and constant research in web application security. This product and team effort stays in my heart. Thank you that you are here with us 🏆

Like Reply




NEW Thu Nov 7th · 16:00 89

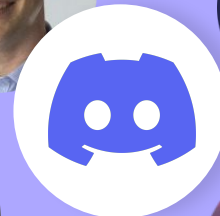
Discover Shazzer

Unlock the full potential of Shazzer and take your fuzzing skills to the next level!

In this talk, you'll discover why it was built and ...



🔊 spotlight-stage ... Share Interested



2025 Roadmap

Core tooling

Custom Actions in Repeater

Parallel Crawl & Audit

Strengthen core tools and workflows

Extensibility

Scan Checks

Easier Extensibility authorship & team management

Burp AI

70%

of hands-on security testers
feel optimistic or excited about
AI's growing role in AppSec.

Introducing

Burp AI

**Augmenting human
expertise, not
replacing it**



User control remains paramount

AI is an on-demand
assistant.



Trust through transparency

Data privacy & security
are key priorities.



Delivering real value, not superficial AI features

We prioritize meaningful
AI integrations over hype.



Need more confidence

in the accuracy of AI-led findings.

Scared

*of relying on AI
when I don't fully understand
the logic behind its decisions.*

Concerned

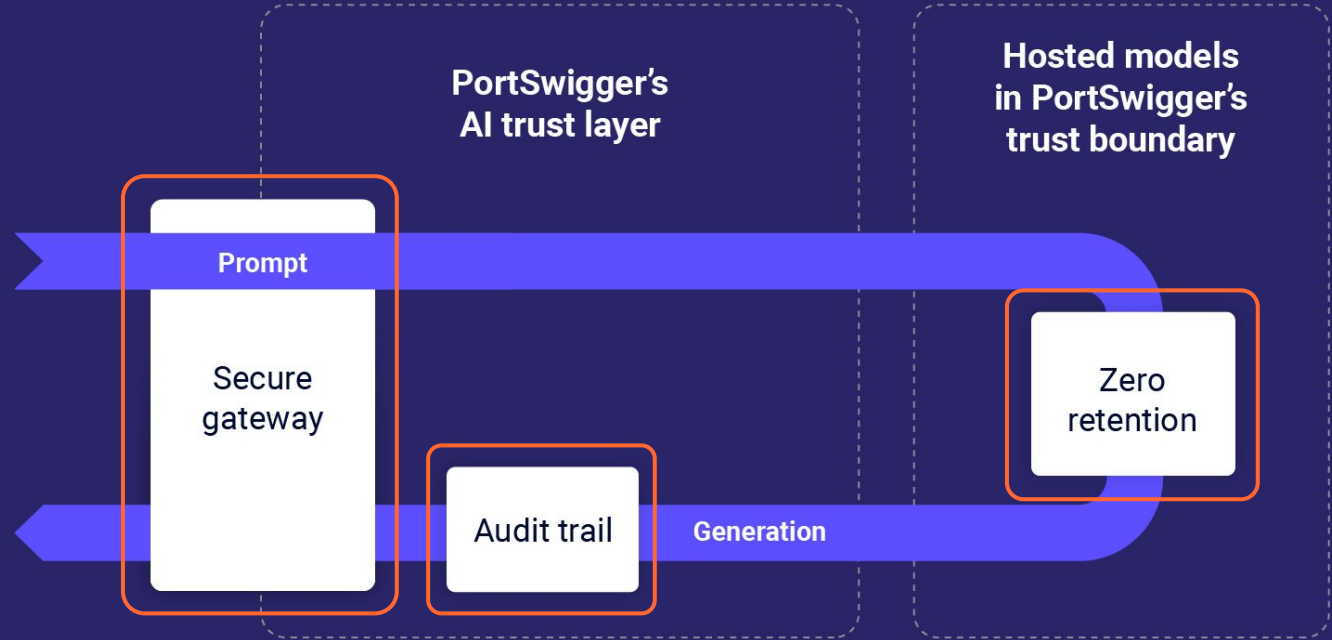
*about AI
hallucinations in security tools.*

*"I actively integrate AI into my
work, but I'm **cautious**
about trusting it too much."*

*"AI's usefulness in real-world security
testing is still **unproven** in
my experience."*

*A solution that leveraged that capability would have to prove its
effectiveness to **gain trust** before it could be relied upon.*

**Data from
Burp Suite**



AI timeline



Introducing

Explore Issue

The screenshot displays the Burp Suite Professional v2025.3-LOCALBUILD (Early Adopter) interface. The top navigation bar includes tabs for Dashboard, Target, Proxy, Logger, Extensions, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, and Organizer. The main window is divided into three panels.

Left Panel (Tasks): Shows a list of tasks. Task 3, "Crawl and audit of ginandjuice.shop", is highlighted. It has a status of "Finished" and shows 14 issues. Below this, Task 2, "Live audit from...", is shown with a status of "Capturing" and 0 issues. Task 1, "Live passive cr...", is also shown with a status of "Capturing" and 0 issues.

Right Panel (Issues): Displays a table of issues. The table has columns for Time, Source, Issue type, Host, and Path. The issues listed are:

Time	Source	Issue type	Host	Path
14:08:21 11 Mar 2025	Task 3	DOM data manipulation (reflected DOM-bas...	https://ginandjuice.shop	/login
14:08:20 11 Mar 2025	Task 3	Link manipulation (reflected DOM-based)	https://ginandjuice.shop	/catalog
14:08:20 11 Mar 2025	Task 3	DOM data manipulation (reflected DOM-bas...	https://ginandjuice.shop	/catalog
14:08:19 11 Mar 2025	Task 3	Link manipulation (reflected DOM-based)	https://ginandjuice.shop	/catalog
14:08:19 11 Mar 2025	Task 3	Link manipulation (reflected DOM-based)	https://ginandjuice.shop	/catalog
14:04:12 11 Mar 2025	Task 3	External service interaction (HTTP)	https://ginandjuice.shop	/resources/images/pineapple-can.png
14:04:12 11 Mar 2025	Task 3	External service interaction (HTTP)	https://ginandjuice.shop	/resources/images/pineapple-can.png
14:04:07 11 Mar 2025	Task 3	External service interaction (HTTP)	https://ginandjuice.shop	/image/scanme/blog/posts/1.jpg
14:04:07 11 Mar 2025	Task 3	External service interaction (DNS)	https://ginandjuice.shop	/resources/images/gin-and-juice-shop-logo
14:02:26 11 Mar 2025	Task 3	Backup file	https://ginandjuice.shop	/image/scanme/productcatalog/products/1
14:02:26 11 Mar 2025	Task 3	Backup file	https://ginandjuice.shop	/image/scanme/productcatalog/products/1
13:54:47 11 Mar 2025	Task 3	External service interaction (HTTP)	https://ginandjuice.shop	/resources/images/gin-and-juice-shop-logo
13:54:47 11 Mar 2025	Task 3	External service interaction (DNS)	https://ginandjuice.shop	/resources/images/gin-and-juice-shop-logo
13:50:23 11 Mar 2025	Task 3	External service interaction (HTTP)	https://ginandjuice.shop	/
13:50:23 11 Mar 2025	Task 3	External service interaction (DNS)	https://ginandjuice.shop	/

The bottom panel shows the details of a selected issue, "SQL injection". The severity is "High", the confidence is "Tentative", and the URL is "https://ginandjuice.shop/catalog". The issue detail section explains that the category parameter appears to be vulnerable to SQL injection attacks. The issue background section states that SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner.

Introducing

Explainer

Burp Suite Professional v2025.2-LOCALBUILD (Early Adopter) - Temporary Project - licensed to PortSwigger Web Security

Dashboard Target Proxy Logger Extensions Intruder Repeater Collaborator Sequencer Decoder Search Settings

1 x +

Send Cancel < >

Target: <https://ginandjuice.shop> HTTP/2

Request Response

Pretty Raw Hex

```
1 GET /catalog/product?productId=1 HTTP/2
2 Host: ginandjuice.shop
3 Cookie: session=U6J6dkSYqkQQLDV1F7w3xBiFQKfHG13; TrackingId=eyJ0eXBlijo1Y2xhc3M1LCJ2YWx1ZSI6Ik8xQmQ4a21zUVBoN0M4UWoiQ==;
  AWSALB=
  bZX0wo9Tzt1tfkRXdTr7MYAE/eyu+rnLDU9EVENAraHJBhIlhv6BLpzsQESn2cv6EdZHXBhBX080K/TPbSxyIL546IScULMMeo1Pb9a1rGYvpLNlVQKi+tvV/L7k;
  AWSALBCORS=
  bZX0wo9Tzt1tfkRXdTr7MYAE/eyu+rnLDU9EVENAraHJBhIlhv6BLpzsQESn2cv6EdZHXBhBX080K/TPbSxyIL546IScULMMeo1Pb9a1rGYvpLNlVQKi+tvV/L7k
4 Sec-Ch-UA: "Chromium";v="133", "Not(A:Brand";v="99"
5 Sec-Ch-UA-Mobile: 70
6 Sec-Ch-UA-Platform: "macOS"
7 Accept-Language: en-gb,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0
  Safari/537.36
10 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
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: 71
14 Sec-Fetch-Dest: document
15 Referer: https://ginandjuice.shop/catalog
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

Done 11,989 bytes | 22 ms

Introducing

False Positive Reduction: Broken Access Control

Dashboard Target Proxy Logger Extensions Intruder Repeater Collaborator Sequencer Decoder Compare

Tasks

New scan New live task

Filter Search

3. Crawl and audi...
Default configuration
Finished
Issues: 14 0 7 25

2. Live audit from...
Audit checks - passive
Capturing: ☒
Issues: 0 0 0 0

1. Live passive cr...
Add links. Add item itself, same domain and URLs in suite scope.
Capturing: ☒

3. Crawl and audit of ginandjuice.shop

Summary Audit items Issues Event log Logger Audit log Live crawl view

Filter

Time	Source	Issue type	Host
14:02:11 11 Mar 2025	Task 3	External service interaction (HTTP)	https://ginandjuice.shop
14:02:26 11 Mar 2025	Task 3	Backup file	https://ginandjuice.shop
13:54:47 11 Mar 2025	Task 3	Backup file	https://ginandjuice.shop
13:54:47 11 Mar 2025	Task 3	External service interaction (HTTP)	https://ginandjuice.shop
13:50:23 11 Mar 2025	Task 3	External service interaction (DNS)	https://ginandjuice.shop
13:50:23 11 Mar 2025	Task 3	External service interaction (HTTP)	https://ginandjuice.shop
13:50:23 11 Mar 2025	Task 3	External service interaction (DNS)	https://ginandjuice.shop
13:38:16 11 Mar 2025	Task 3	Vulnerable JavaScript dependency	https://ginandjuice.shop
13:38:15 11 Mar 2025	Task 3	Cacheable HTTPS response	https://ginandjuice.shop
13:38:15 11 Mar 2025	Task 3	Base64-encoded data in parameter	https://ginandjuice.shop
13:38:15 11 Mar 2025	Task 3	Cookie without HttpOnly flag set	https://ginandjuice.shop
13:38:15 11 Mar 2025	Task 3	Cookie without HttpOnly flag set	https://ginandjuice.shop
13:38:15 11 Mar 2025	Task 3	TLS cookie without secure flag set	https://ginandjuice.shop
13:38:14 11 Mar 2025	Task 3	Strict transport security not enforced	https://ginandjuice.shop
13:36:56 11 Mar 2025	Task 3	Broken access control	https://ginandjuice.shop
13:36:36 11 Mar 2025	Task 3	Broken access control	https://ginandjuice.shop

Advisory Request 1 Response 1 Request 2 Response 2 Path to issue

Broken access control

AI enhanced

Severity: High
Confidence: Firm
URL: https://ginandjuice.shop/order/details

AI summary

The image contains personal identifiable information (PII) such as a name, address, and payment details.

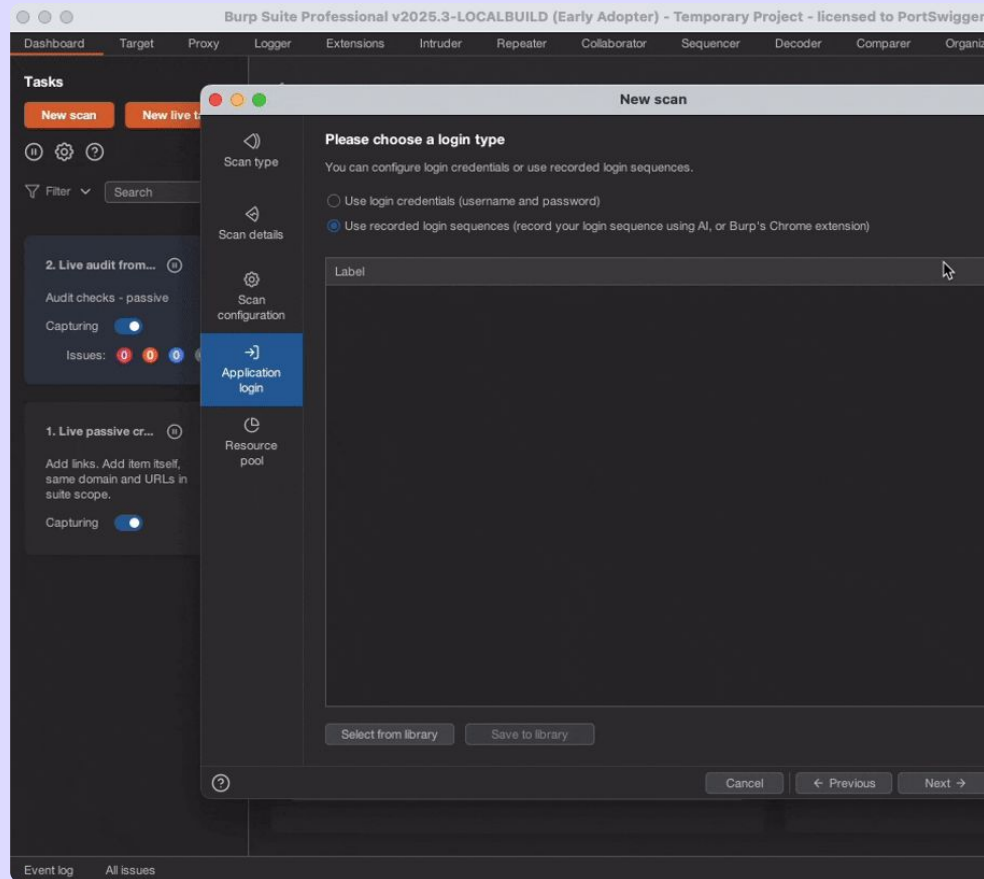
Issue detail

Unauthenticated users can access https://ginandjuice.shop/order/details by directly requesting it without authentication. The application only provides a link to https://ginandjuice.shop/order/details to authenticated users, suggesting a broken access control issue.

To confirm whether this is a vulnerability, review the unauthenticated response to see if it contains any PII.

Introducing

Recorded Login Sequences



What's next?



AI in Burp Suite Professional

Reduce the tedious

Bring enhancements to your
workflow

Even more AI-extensibility



AI in Burp Suite DAST

Reducing time-to-value

AI Enhancements to Burp
Scanner

Improving Accuracy



Thanks.