Antlion

Security assessment report

example.com

Sample report. The target, dates and findings are fictional. They show the format and depth of a real Antlion report.

Report ID	**ANT-SAMPLE-001**	Version	**1.0**
Assessment date	**14 November 2026**	Duration	**3 hours 42 minutes**
Assessment type	**External, automated, no credentials supplied**	Prepared by	**Antlion**

Contents

1. Executive summary
2. Scope and approach
3. Findings summary
4. Detailed findings
5. Remediation plan
6. Severity ratings
7. Limitations

1 Executive summary

Antlion assessed **example.com** from the public internet on 14 November 2026. The assessment ran for 3 hours 42 minutes in an isolated sandbox and identified 5 findings.

1	2	1	1
Critical	High	Medium	Low

Overall risk

Critical

The deployment panel and the database are both reachable from the internet, and the application's environment file can be downloaded by anyone. Together they give an attacker several direct routes to control of the server and its data.

What to do first

1. Block public access to the Dokploy panel (ANT-001).
2. Remove the exposed environment file and rotate every secret in it (ANT-002).
3. Stop publishing the PostgreSQL port (ANT-003).

2 Scope and approach

In scope	example.com and the services on the same server that are reachable from the internet
Out of scope	Subdomains, DDoS-style attacks, and systems the client does not own
Perspective	External attacker with no credentials and no prior knowledge of the system
Authorisation	Ownership of the domain was confirmed before the assessment started
Environment	An isolated sandbox, destroyed when the assessment ended
Test window	14 November 2026, 09:12 to 12:54 UTC

How the assessment ran

1. **Confirm.** Ownership of the domain is confirmed before any traffic is sent to it.
2. **Test.** Agents running Antlion's own pretrained models test the target in parallel for more than 25,000 recently disclosed vulnerabilities.
3. **Probe.** Further tools test the endpoints the server leaves open to the internet. No DDoS-style attacks are used.
4. **Report.** Each finding is written up with the evidence that demonstrates it and the steps to fix it, and the report is sent within 4 to 24 hours.

3 Findings summary

ID	Finding	Severity	Affected asset
ANT-001	Dokploy panel open to the internet	Critical	`example.com:3000`
ANT-002	Environment file readable from the browser	High	`https://example.com/.env`
ANT-003	PostgreSQL accepts remote connections	High	`example.com:5432`
ANT-004	Traefik dashboard has no login	Medium	`example.com:8080`
ANT-005	Server header reveals software version	Low	`https://example.com/`

4 Detailed findings

ANT-001

Dokploy panel open to the internet

Critical

Affected asset	Category
`example.com:3000`	Exposed administration interface

Description

The Dokploy administration panel answers on port 3000 from any address on the internet. The panel manages every application, database and domain on the server.

Evidence

```
GET / HTTP/1.1
Host: example.com:3000

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

<title>Dokploy</title>      (sign-in page returned)
```

Impact

An attacker can attack the sign-in page directly, by guessing passwords, reusing leaked ones or exploiting a flaw in the panel itself. A successful sign-in gives control of every application on the server and the secrets they use.

Remediation

1. Block port 3000 in the server firewall.
2. Reach the panel through an SSH tunnel or a VPN, or restrict it to trusted IP addresses.
3. Use a strong, unique password for every panel account, and turn on two-factor authentication where it is available.

How to confirm the fix

From a network outside the server, a request to http://example.com:3000/ should time out or be refused.

ANT-002

Environment file readable from the browser

High

Affected asset	Category
`https://example.com/.env`	Sensitive file exposure

Description

The application's environment file is served by the web server like any other static file. It can be downloaded without signing in.

Evidence

```
GET /.env HTTP/1.1
Host: example.com

HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 412

DATABASE_URL=postgres://app:[redacted]@db:5432/app
SESSION_SECRET=[redacted]
PAYMENT_API_KEY=[redacted]
```

Impact

Anyone who downloads the file obtains the database credentials and the application secrets. Combined with ANT-003, the database can be read and changed directly.

Remediation

1. Move the file out of the public folder and configure the web server to refuse requests for dotfiles.
2. Treat every secret in the file as compromised and rotate it.
3. Search the access logs for earlier requests to /.env to learn whether it has already been downloaded.

How to confirm the fix

A request to https://example.com/.env should return 403 or 404.

ANT-003

PostgreSQL accepts remote connections

High

Affected asset

`example.com:5432`

Category

Exposed database service

Description

The PostgreSQL database listens on its default port and accepts connections from the public internet. Only the database password stands between an attacker and the data.

Evidence

```
$ pg_isready -h example.com -p 5432
example.com:5432 - accepting connections
```

Impact

The database can be attacked directly by password guessing. With the credentials exposed in ANT-002, it can be accessed immediately.

Remediation

1. Remove the published port from the database container and let the application reach it over the internal network.
2. If remote access is needed, allow only specific IP addresses in the firewall or use an SSH tunnel.
3. Change the database password once the port is closed.

How to confirm the fix

From outside the server, a connection attempt to port 5432 should time out or be refused.

ANT-004

Traefik dashboard has no login

Medium

Affected asset	Category
`example.com:8080`	Missing authentication

Description

The Traefik dashboard and its API are reachable on port 8080 without any authentication.

Evidence

```
GET /api/http/routers HTTP/1.1
Host: example.com:8080

HTTP/1.1 200 OK
Content-Type: application/json

[{"name":"app@docker","rule":"Host(`example.com`)", ...}]
```

Impact

Anyone can list every route, service and internal hostname behind the proxy. This does not grant access by itself, but it gives an attacker a map of the server and makes further attacks easier to plan.

Remediation

1. Turn off the insecure API mode in the Traefik configuration.
2. If the dashboard is needed, publish it through a router protected by authentication and an IP allowlist.

How to confirm the fix

A request to http://example.com:8080/api/http/routers should be refused or require authentication.

ANT-005

Server header reveals software version

Low

Affected asset	Category
`https://example.com/`	Information disclosure

Description

Responses from the web server include the exact nginx version in the Server header.

Evidence

```
HTTP/1.1 200 OK
Server: nginx/1.18.0
```

Impact

Knowing the exact version lets an attacker look up the weaknesses that apply to it and skip the ones that do not.

Remediation

1. Set server_tokens off in the nginx configuration so the version is no longer sent.
2. Keep nginx on a supported, up-to-date release.

How to confirm the fix

The Server header should read nginx, with no version number.

5 Remediation plan

The actions below are ordered by how much risk each one removes.

When	Action	Finding
Today	Block public access to the Dokploy panel.	ANT-001
	Remove the exposed environment file and rotate every secret in it.	ANT-002
	Stop publishing the PostgreSQL port.	ANT-003
This week	Close or protect the Traefik dashboard.	ANT-004
Next maintenance window	Hide the nginx version and review the update schedule.	ANT-005

6 Severity ratings

Rating	What it means
Critical	A direct route to control of the server or its data. Fix immediately.
High	Likely to lead to compromise or data exposure, alone or combined with another finding. Fix within days.
Medium	Weakens the defences or gives an attacker useful information. Fix in the next planned cycle.
Low	Limited direct impact. Fix when convenient.

7 Limitations

This report describes the target as it was during the test window. Systems change, and new weaknesses are discovered over time, so a report with few findings is not a guarantee of security. Run a new assessment after significant changes to the server or the application.

Antlion only assesses domains whose owner has confirmed the request. Questions about this report can be sent to hello@antlion.dev.