intruder

Vulnerability report

Option to VAT Limited

24 July 2026

1 target scanned

Threat Level

All clear

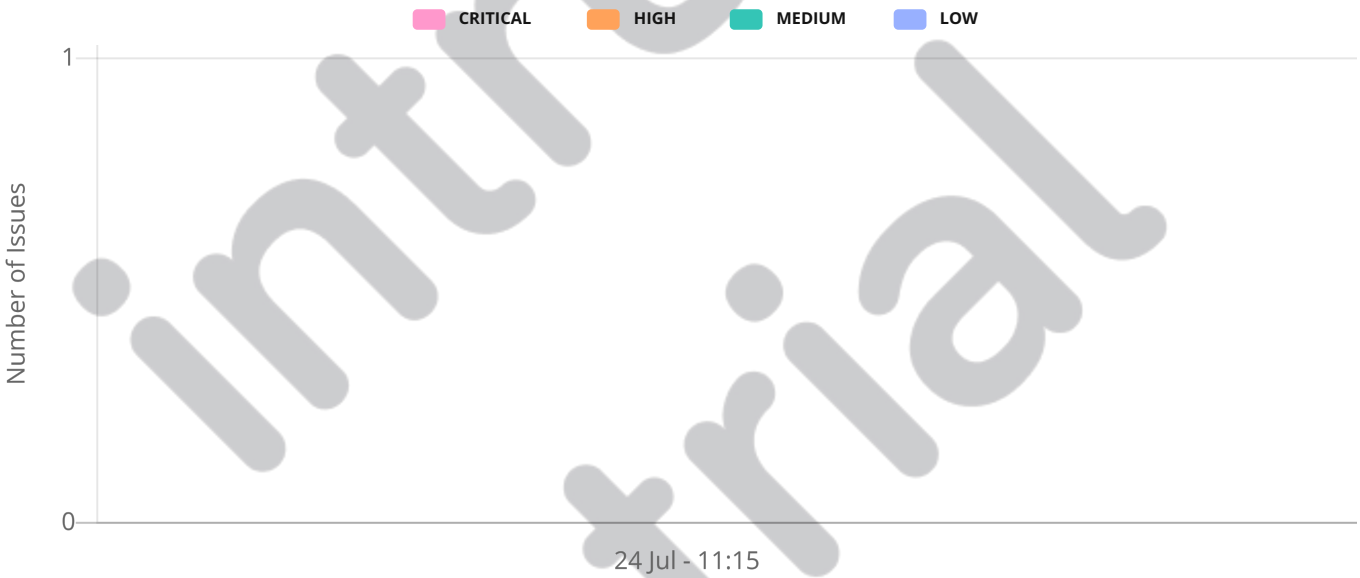
Target	Issues
1	0

Critical	High
0	0

Medium	Low
0	0

No issues were discovered that could lead to or increase the chances of a breach. While this is a good position to be in today, new weaknesses are discovered daily, and chang es are often made to systems that could reduce their security. Make sure to continue using ongoing security services to monitor your risk.

Exposure over time



Total checks

45,936

The types of areas we cover when reviewing your targets and their accessible web pages:

Vulnerable software & hardware

- Web servers, e.g. Apache, Nginx
- Mail servers, e.g. Exim
- Development software, e.g. PHP
- Network monitoring software, e.g. Zabbix, Nagios
- Networking systems, e.g. Cisco ASA
- Content management systems, e.g. Drupal, Wordpress
- Other well-known weaknesses, e.g. 'Log4Shell' and 'Shellshock'

Attack Surface Reduction

Our service is designed to help you reduce your attack surface and identify systems and software which do not need to be exposed to the Internet, such as:

- Publicly exposed databases
- Administrative interfaces
- Sensitive services, e.g. SMB
- Network monitoring software

Encryption weaknesses

Weaknesses in SSL/TLS implementations, such as:

- 'Heartbleed', 'CRIME', 'BEAST' and 'ROBOT'
- Weak encryption ciphers & protocols
- SSL certificate misconfigurations
- Unencrypted services such as FTP

Web Application Vulnerabilities

- Checks for multiple OWASP Top Ten issues
- SQL injection
- Cross-site scripting (XSS)
- XML external entity (XXE) injection
- Local/remote file inclusion
- Web server misconfigurations
- Directory/path traversal, directory listing & unintentionally exposed content

Information Leakage

Checks for information which your systems are reporting to end-users which should remain private. This information includes data which could be used to assist in the mounting of further attacks, such as:

- Local directory path information
- Internal IP Addresses

Common mistakes & misconfigurations

- VPN configuration weaknesses
- Exposed SVN/git repositories
- Unsupported operating systems
- Open mail relays
- DNS servers allowing zone transfer

Cloud Security

These checks assess your cloud environment for misconfiguration and accidental exposure including:

- Checks for misconfigured cloud settings
- Missing security controls and mitigations
- Insecure user roles and permissions
- Exposed services and overpermissive access controls

As a Cloud plan customer, you also have access to:

Emerging threats

The time between new vulnerabilities emerging and hackers exploiting them is now days, not weeks. For organizations who need a more mature approach to cyber security, our emerging threat scans detect critical threats to your systems without waiting for the next monthly check.

Issues

No issues were detected.

All selected active targets were scanned and no vulnerabilities were detected.

Target included in this scan

www.onesixth.app

Scan timings

This report includes last known scan data for your selected targets.

Company

Intruder Systems Ltd is an independent security advisory company, specialising in providing continuous security monitoring for internet-facing web applications and infrastructure.

Security team

Our consultants have delivered work for government agencies, international financial institutions, and global retail giants.

Intruder is a member of CREST

Monitored by Vanta for SOC 2 compliance

Intruder is a CREST accredited Vulnerability Assessment service

Intruder is a member of the Cyber-security Information Sharing Partnership

Intruder is Cyber Essentials certified

Compliance

Our reports are ISO 27001 and SOC 2 compliance ready.

contact@intruder.io