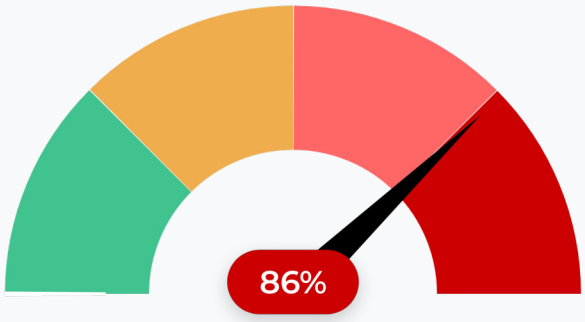
Your HackRisk Score Report



Critical

Your systems are at immediate risk of attack. The gaps in your security could be exploited with devastating effect. These issues demand immediate, top-priority attention to mitigate the threat and protect your organisation from an attack.

Warning

Failure to remedy these issues risks severe penalties including regulatory fines by the ICO of up to £17.5 million (€20 million) or 4% of global turnover under GDPR, DUAA, DORA, NIS2, Cyber Security and Resilience Act, the Computer Misuse Act 1990 and loss of CE/CE+ accreditation

Our recommendation is that this report is shared with your board member responsible for cyber risk.

Your Top Risks

The list below details the top 5 risks across all modules. You will find detailed breakdowns in the following pages.

Target	Description	Severity
pentest-ground.com	Oracle WebLogic Default Credentials	Critical
pentest-ground.com	Unsecured Redis Database Exposed	Critical
pentest-ground.com	Redis < 8.2.1 lua script - Integer Overflow	Critical

Target	Description	Severity
pentest-ground.com	Redis Lua Parser < 8.2.2 - Use After Free	Critical
oNDgTfiV@burpcollaborator.net	Dark Web Breach	Critical

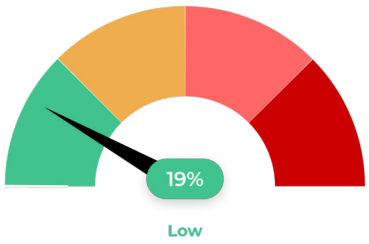
Your HackRisk Report

Summary

HackRisk.AI
Powered by CyberLab

Dark Web Monitor

Your organisation has a small footprint on the dark web, with limited data exposed. This poses no direct threat, but users should remain vigilant as exposed addresses may be targeted by phishing attempts.



Vulnerability Scan

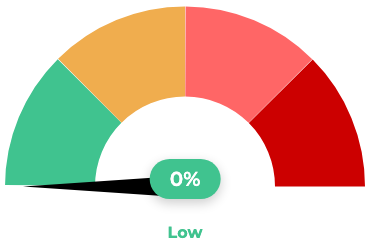
Your systems are at immediate risk of attack. The gaps in your security could be exploited easily, and with devastating effect. These issues demand immediate attention to mitigate the threat of an attack that could result in downtime or regulatory fines.

Recon Scan

Your infrastructure has critical vulnerabilities which need to be addressed immediately. You are at risk a large scale security breach of your systems. Consider disconnecting the at-risk endpoints from the internet while issues are resolved. A full review of your infrastructure configuration is recommended.

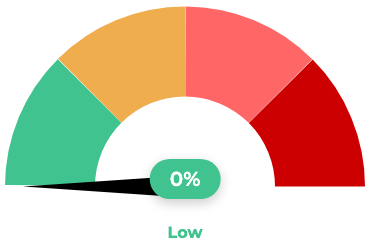
Security Awareness

Your users are completing there allocated security courses and scoring well. Users are generally aware of security risks they may encounter in the workplace and how to mitigate them.



Phishing Simulation

Your users are responding correctly to phishing emails and the risk of compromise is low. Ensure any new users are also educated on phishing prevention to maintain this standard.



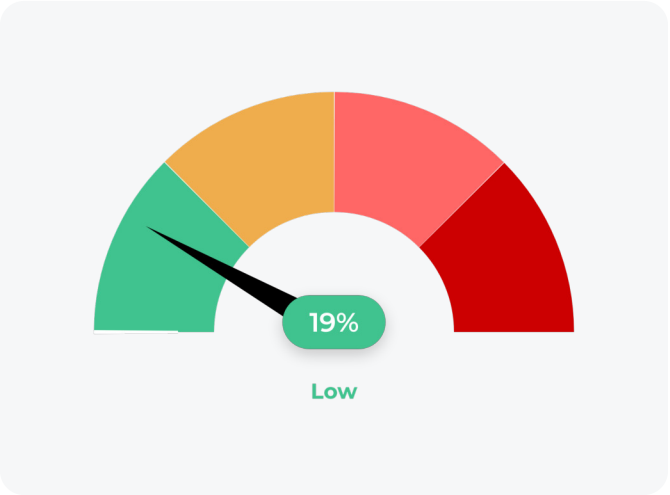
Your HackRisk Report

Dark Web Monitor

HackRisk.AI
Powered by CyberLab

Overall Dark Web Score: Low

Your organisation has a small footprint on the dark web, with limited data exposed. This poses no direct threat, but users should remain vigilant as exposed addresses may be targeted by phishing attempts.



Exposed passwords	61
Users at risk breaches	62
Total Breaches	82
Emails with breaches	259

Your Top Risks

Below are the top 5 risks identified based on breach severity and exposed data.

Email Address	Breach Score	Breaches	Passwords
oNDgTfiV@burpcollaborator.net	895	4	1
win.inioNDgTfiV@burpcollaborator.net	820	2	1
w1ym90hsf6yldbylhfeqtbljqaw3k6puhp5hs7gw@burpcollaborator.net	820	2	1
AJqinPcB@burpcollaborator.net	820	2	1
passwdoNDgTfiV@burpcollaborator.net	820	2	1

Our HackRisk Recommendation

Dark web breaches expose your credentials to cybercriminals. Take immediate action to secure compromised accounts and strengthen your password policies across your organisation.

Log in to your HackRisk Portal for detailed Dark Web Monitoring analysis and remediation guidance →

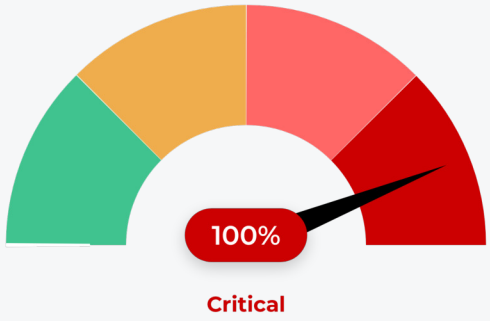
Your HackRisk Report

Vulnerability Scan

HackRisk.AI
Powered by CyberLab

Overall Vulnerability Score: Critical

Your systems are at immediate risk of attack. The gaps in your security could be exploited easily, and with devastating effect. These issues demand immediate attention to mitigate the threat of an attack that could result in downtime or regulatory fines.



Critical	2
High	2
Medium	2
Low	3

Your Top Risks

Below are the top 5 vulnerabilities identified based on severity.

Severity	Vulnerability	Occurrences	Targets
Critical	**Oracle WebLogic Default Credentials**	**1**	**1**
Critical	**Unsecured Redis Database Exposed**	**1**	**1**
High	**Arbitrary File Download**	**2**	**1**
High	**Unsupported Oracle WebLogic Version**	**1**	**1**
Medium	**Redis Database Exposed**	**1**	**1**

Our HackRisk Recommendation

Unpatched vulnerabilities are open invitations for cyberattacks. Prioritize remediation based on severity and exploitability to minimize your attack surface and protect critical assets.

Log in to your HackRisk Portal for detailed Vulnerability Scanning analysis and remediation guidance →

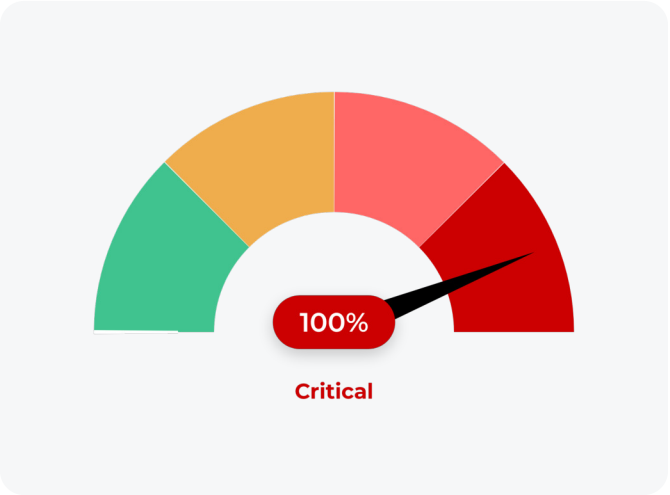
Your HackRisk Report

Recon Scan

HackRisk.AI
Powered by CyberLab

Overall Recon Scan Score: Critical

Your infrastructure has critical vulnerabilities which need to be addressed immediately. You are at risk a large scale security breach of your systems. Consider disconnecting the at-risk endpoints from the internet while issues are resolved. A full review of your infrastructure configuration is recommended.



Critical	2
High	4
Medium	0
Low	0

Your Top Risks

Below are the top 5 vulnerabilities identified during reconnaissance scans.

Vulnerability	Subdomain	Severity
Redis < 8.2.1 lua script - Integer Overflow	pentest-ground.com	Critical
Redis Lua Parser < 8.2.2 - Use After Free	pentest-ground.com	Critical
Redis < 8.2.1 Lua Long-String Delimiter - Out-of-Bounds Read	pentest-ground.com	High
Redis - Default Logins	pentest-ground.com	High
Redis Lua Sandbox < 8.2.2 - Cross-User Escape	pentest-ground.com	High

Our HackRisk Recommendation

Your external attack surface reveals what hackers see. open ports and services, misconfigurations and security gaps all put you at risk. Reduce your organisation's risk profile before attackers exploit them.

Log in to your HackRisk Portal for detailed Recon Scanning analysis and remediation guidance →

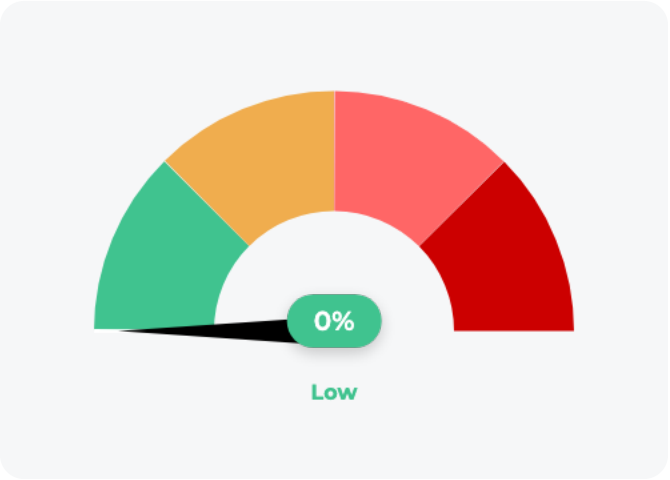
Your HackRisk Report

Security Awareness Training

HackRisk.AI
Powered by CyberLab

Overall Security Awareness Score: Low

Your users are completing there allocated security courses and scoring well. Users are generally aware of security risks they may encounter in the workplace and how to mitigate them.



Average score	-
Users without training	-
Users completed training	-
Modules Completed	-

Your Top Risks

Below are the top 5 users with the highest risk scores in security awareness training.

Learner	Score	Enrolled	Completed	Avg. Score
Ryan Hughes	940.00	12	1	72%
Matthew Harris	906.00	15	2	71%
Michael Thompson	825.00	13	3	76%
Benjamin Cox	799.00	18	5	73%
Andrew Cooper	797.00	19	5	78%

Our HackRisk Recommendation

Your employees are your first line of defense. Continuous security awareness training transforms them from potential vulnerabilities into human firewalls, reducing social engineering and phishing risks.

Log in to your HackRisk Portal for detailed Security Awareness Training analysis and remediation guidance →

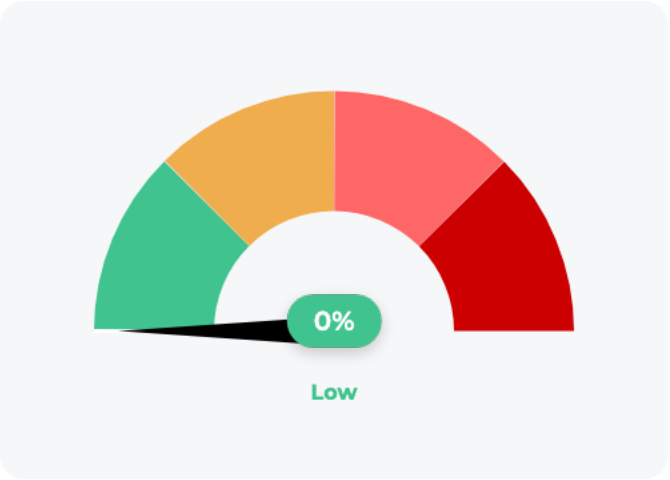
Your HackRisk Report

Phishing Simulation Reports

HackRisk.AI
Powered by CyberLab

Overall Phishing Simulation Score: Low

Your users are responding correctly to phishing emails and the risk of compromise is low. Ensure any new users are also educated on phishing prevention to maintain this standard.



Compromises	-
Links visited	-
Emails opened	-
Emails Sent	-

Your Top Risks

Below are the top 5 users with the highest risk scores in phishing simulations.

Learner	Score	Opened	Visited	Compromised
Michael Thompson	1000.00	Opened	Visited	Compromised
Olivia Scott	1000.00	Opened	Visited	Compromised
Charlotte Evans	1000.00	Opened	Visited	Compromised
David Chen	1000.00	Opened	Visited	Compromised
Jessica Park	1000.00	Opened	Visited	Compromised

Our HackRisk Recommendation

Phishing attacks are the leading cause of data breaches. Regular simulation testing identifies vulnerable users and reinforces security awareness, dramatically reducing your organisation's susceptibility to real attacks.

Log in to your HackRisk Portal for detailed Phishing Simulation analysis and remediation guidance →