

Is Your Business at Risk? Defend Against Cyber Threats

Are you protecting your company's assets with regular Customized Vulnerability Assessments, Pentesting and Ethical Hacking best practices?

Customized Vulnerability Assessments assess perimeters and applications for potential vulnerabilities that could expose critical systems, data and financial assets

Pentesting combines the tools and techniques used by malicious “hackers” with disciplined scientific procedures to provide unique insight into the state of security for Information Systems and network vulnerabilities from an external hacker’s perspective

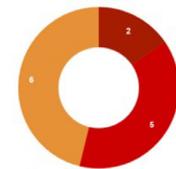
Ethical Hacking takes you to the next level! With certified Ethical Hackers added to your team, you can go beyond risk assessment and carry out the exploits using a wide range of techniques and attack vectors

Each report is customized and includes an executive summary that highlights the key security grading areas and risk profile of each.

ACCEDIAN

13 Summary of Findings
Our assessment of the CLIENT application revealed the following vulnerabilities:

Vulnerabilities by severity



● Critical ● High ● Medium ● Low ● Informational

Severity	Critical	High	Medium	Low	Informational
Number of issues	5	15	26	30	21

Severity scoring:

- Critical – Immediate threat to key business processes.
- High – Direct threat to key business processes.
- Medium – Indirect threat to key business processes or partial threat to business processes.
- Low – No direct threat exists. The vulnerability may be exploited using other vulnerabilities.
- Informational – This finding does not indicate vulnerability, but states a comment that notifies about design flaws and improper implementation that might cause a problem in the long run.

The exploitation of found vulnerabilities may cause full compromise of some services, stealing users' accounts, and gaining organization's and users' sensitive information.

Each area is highlighted and shows how many vulnerabilities there are by severity level.

All business risks are specifically called out showing what each risk means to the business

ACCEDIAN

Comprehensive
Organization External
& Internal Customized
Vulnerability
Assessment for
CLIENT NAME

Compliance with Accedian Certification
criteria: IEEE1 criteria
Prepared for:
John Doe
johndoe@corp.com>

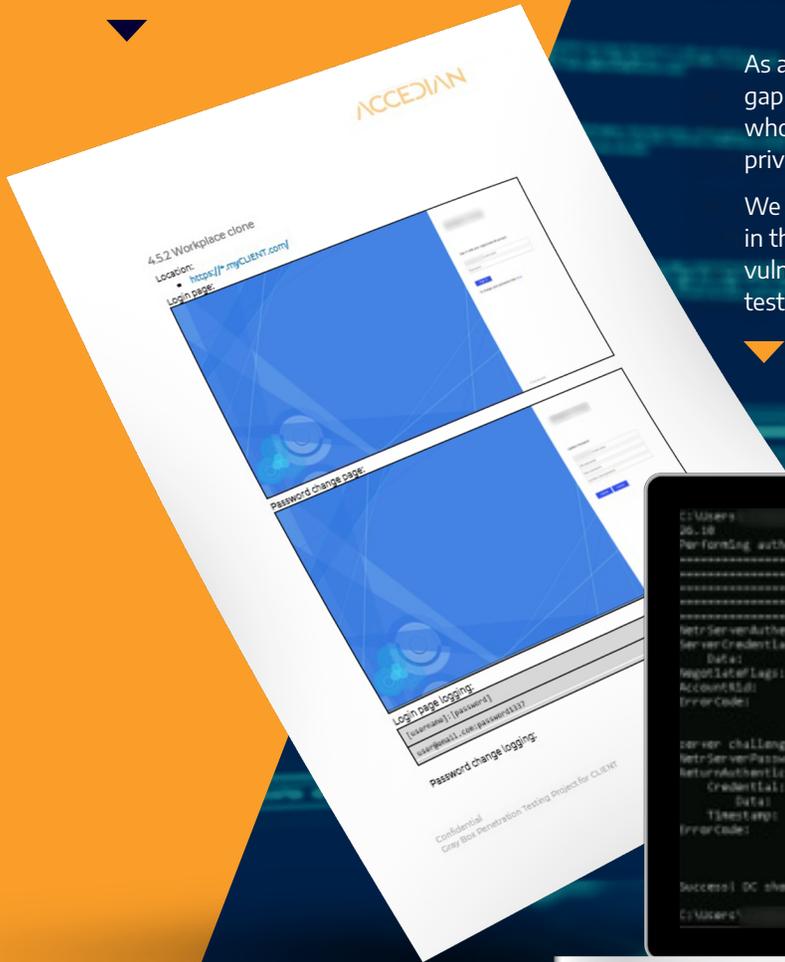
April 2021

Criteria	Grade	Security	Covered Description
Excellent	A	Excellent	The security exceeds industry best practice standards. The overall posture was found to be excellent with only a few low risk findings identified.
Good	B	Good	The security meets with accepted standards for industry best practice. The overall posture was found to be strong with only a handful of medium and low risk issues identified.
Fair	C	Fair	Current security posture covers areas of the enterprise (on security issues). However, changes are required to elevate the assessed areas to industry best practice standards.
Poor	D	Poor	Significant security deficiencies exist. Immediate attention should be given to the discussed issues to address exposures required. Major changes are required to elevate to industry best practice standards.
Inadequate	F	Inadequate	Serious security deficiencies exist. Shortcomings were identified throughout most or even all of the security controls. Improving security will require a major allocation of resources.

ACCEDIAN

In Social media, relevant information is used.

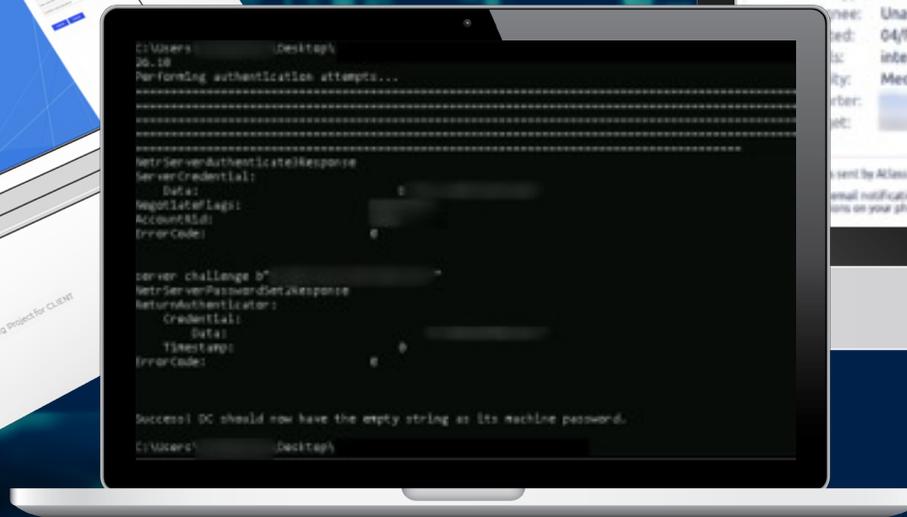
For example a workplace clone was created to try to get people to log in.



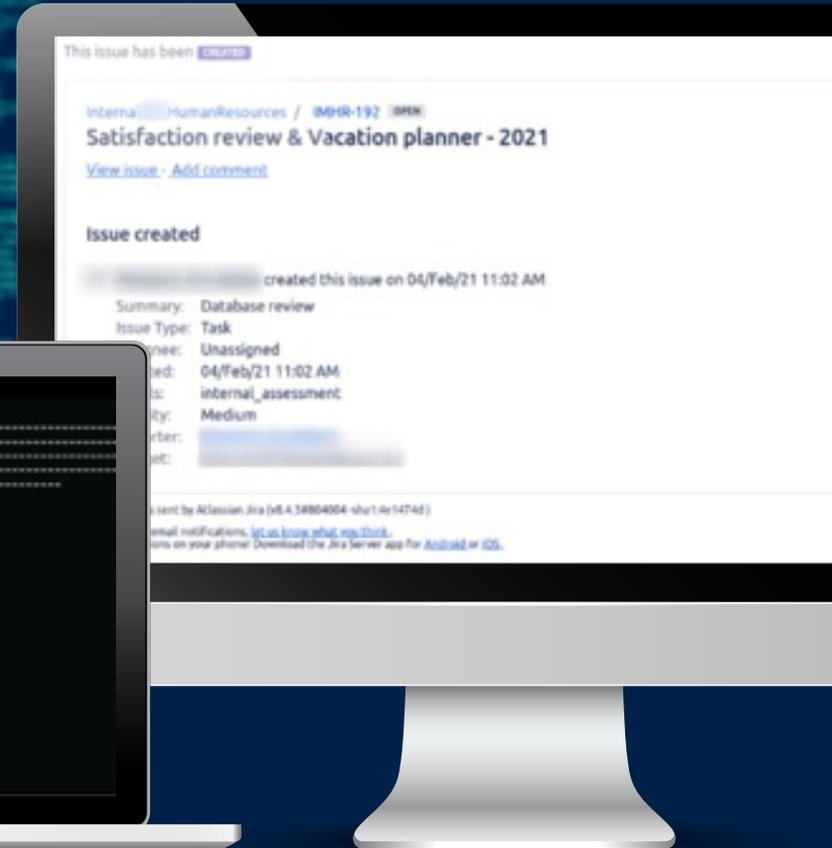
All infrastructure risks are called out with specific details to show all vulnerabilities.

As an example, this shows an open gap of an unauthenticated attacker who has the ability to take over full privilege access to full domain.

We also test and report on the gaps in the training of staff that lead to vulnerabilities with Social Engineering testing.



This shows phishing letters sent, including using Covid (relevant news information) to get people to click on links



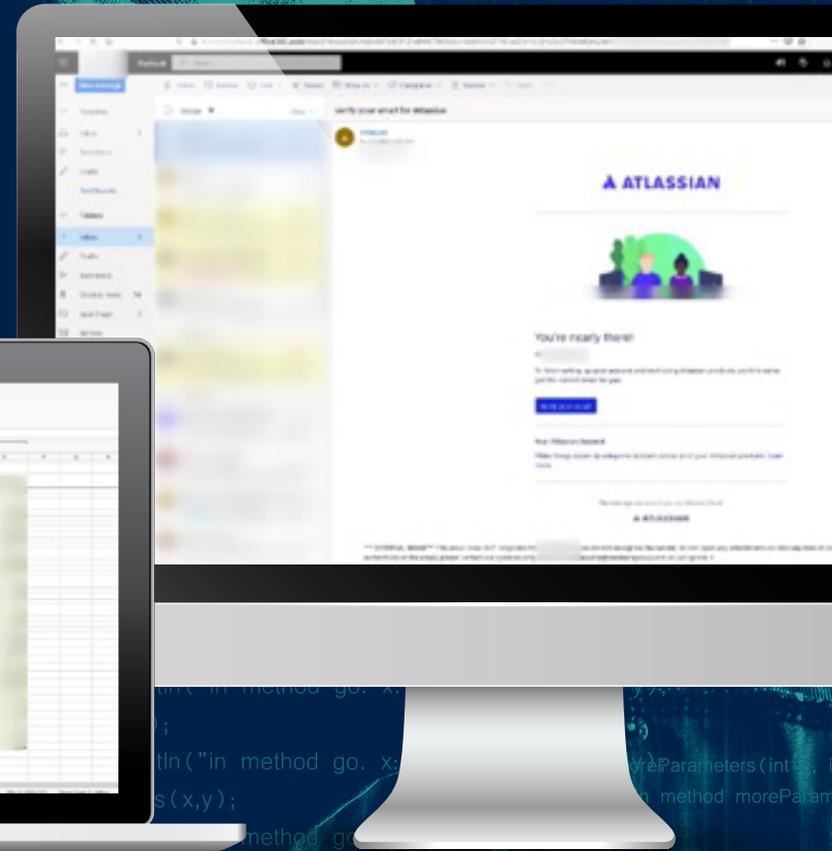
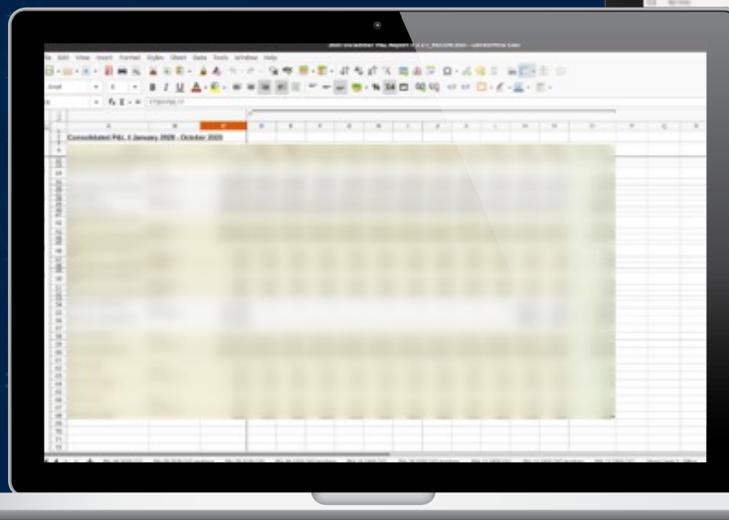


◀ We also test for open WiFi vulnerabilities.

This example shows how access to a live video feed was able to be captured via a workplace phishing letter.

These gaps in security also led to vulnerabilities ▶

in financial documentation access



An example of ethical hacking which was able to take over administration of Azure.

ACCEDIAN

Accedian | 2351 Blvd. Alfred Nobel, N-410 | Saint-Laurent, QC H4S 2A9 | 1 866-685-8181 | accedian.com

© 2021 Accedian Networks Inc. All rights reserved. Accedian, Skylight, Skylight Interceptor, per-packet intel, and the Accedian logo are trademarks or registered trademarks of Accedian Networks Inc. To view a list of Accedian trademarks visit: accedian.com/legal/trademarks