

From Findings to Fixed

The Real Value in a Penetration Test Report

Copyright © 2026 Secure Ideas LLC

Where We Are Going

1. **A report is five documents, not one**
   Five sections, and many people who need something from it

2. **What you lose reading only your section**
   Nine findings are usually three problems

3. **Two windows where it is still adjustable**
   The readout before it is final, the retest after

4. **A plan that survives leadership**
   Turning the document into something you can defend upward

Examples all come from one report. Mine.

Copyright © 2026 Secure Ideas LLC

Kathy Collins

Senior Security Consultant Secure Ideas, LLC

- Secure Ideas since 2021
- Based in Jacksonville, Florida
- CISSP, PCI QSA, ISO 27001 LA

Focus Areas

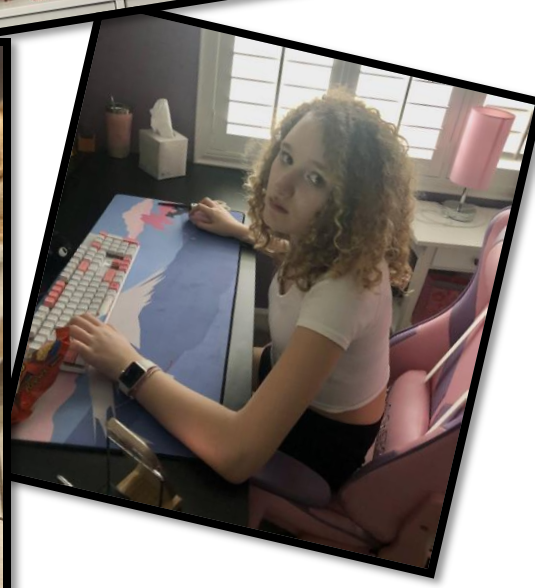
- Networks
- Web Applications
- PCI DSS
- Physical Assessments

Other Fun Facts

- Former Chef
- Mother of doggos (and a teenager)
- Horror Nerd
- BSides Jacksonville
- Costco Member





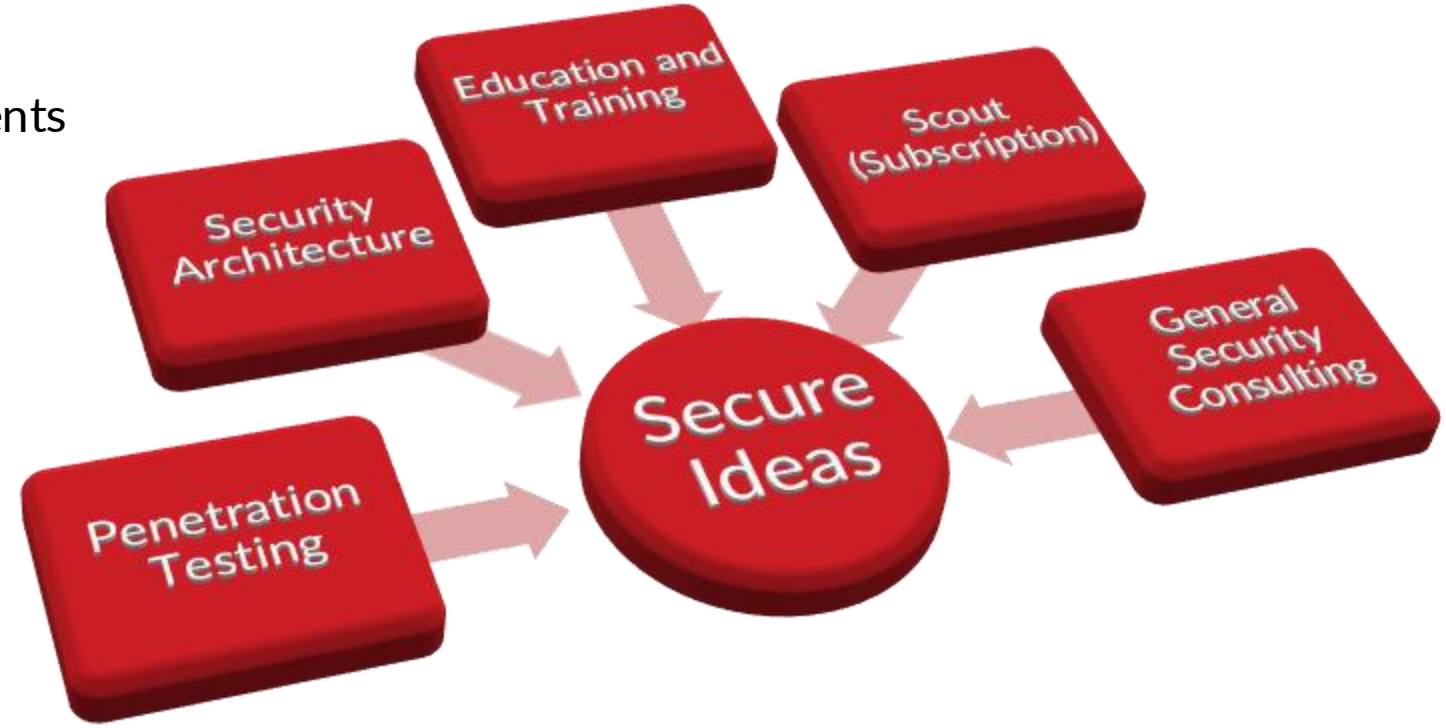


kathy.collins@secureideas.com

Copyright © 2026 Secure Ideas LLC

About Secure Ideas

- Founded in September 2010
  - Kevin Johnson: CEO, former SANS instructor and author
- Based in Jacksonville, FL
  - Consultants live around the country
- Expert Security Consultants
  - Penetration Testing & Vuln Assessments
  - Security Architecture Reviews
  - Education (training, conference talks)
- "Security Evangelists"
  - Open Source authors/contributors
  - Blogs (blog.secureideas.com)
  - "Heart of a Teacher"



Copyright © 2026 Secure Ideas LLC

What is "Professionally Evil"?

professionally evil®

We need to think "evil" so we can understand **how** an attacker will behave and **what** they will attack.

And we are Professional:

- Help companies improve their security posture
- Permission: Penetration Testing is always under contract
- Establish and follow rules of engagement



Copyright © 2026 Secure Ideas LLC



2001



2013

I made both of these

Copyright © 2026 Secure Ideas LLC



2001



2016

And these

Copyright © 2026 Secure Ideas LLC

OWASP Juice Shop Sample Report


Secure Ideas
professionally evil®

Web Application Penetration Test

Final Report

Prepared for: OWASP Juice Shop

June 16th, 2022

Reference: S-230616904

I wrote this one.

Nine findings. Published. You can go read it.

Copyright © 2026 Secure Ideas LLC

What I Would Change Now



- **The executive summary**
  It's a little long. Four paragraphs to get to what actually matters.
- **Strategic guidance**
  Advice written for a different engagement
- **Language that did not get caught**
  A duplicated verb and a broken sentence
- **Reproduction steps that do not reproduce**
  The payload I gave the reader will not run

None of these are disasters. All of them are things I only see now.

Copyright © 2026 Secure Ideas LLC

Same Executive Summary, Written Today

2022

Secure Ideas found multiple critical and high-rated vulnerabilities in the OWASP Juice Shop web application. These weaknesses are very concerning and, if leveraged, would decrease the security and usability of the application.

One of the most significant vulnerabilities Secure Ideas uncovered was the application's susceptibility to various injection-based attacks. To illustrate this vulnerability's severity, a simple SQL injection string was used, enabling Secure Ideas to log in as the application's administrator account without knowing the username or password. Other examples of injection flaws are the instances of Cross-Site Scripting vulnerabilities identified throughout the application. Cross-Site Scripting allows attackers to have malicious code run in the browsers of OWASP Juice Shop users.

Another significant issue discovered is in the form of an authorization bypass flaw. This security flaw allows an attacker to exploit the OWASP Juice Shop API to create a new user with any role, including ones having administrative privileges. This vulnerability stems from a lack of consistent authorization checking within the API. Consistency is important in authorization validation, and the application must enforce it across all interfaces to prevent resources from being unprotected.

These, and the other issues found are outlined in the report that follows. Secure Ideas appreciates the opportunity to work with OWASP Juice Shop to help improve its security posture.

Today

Secure Ideas found that the OWASP Juice Shop web application contains vulnerabilities that present critical risk. The most significant of these allow an unauthenticated attacker to take full administrative control of the application. In one case, a short string entered into the login form was sufficient to authenticate as the administrator. In another, the application's API accepted a request from an unauthenticated user to create an account with administrative privileges. Either issue on its own would give an attacker access to the application, its customer accounts, and its order data.

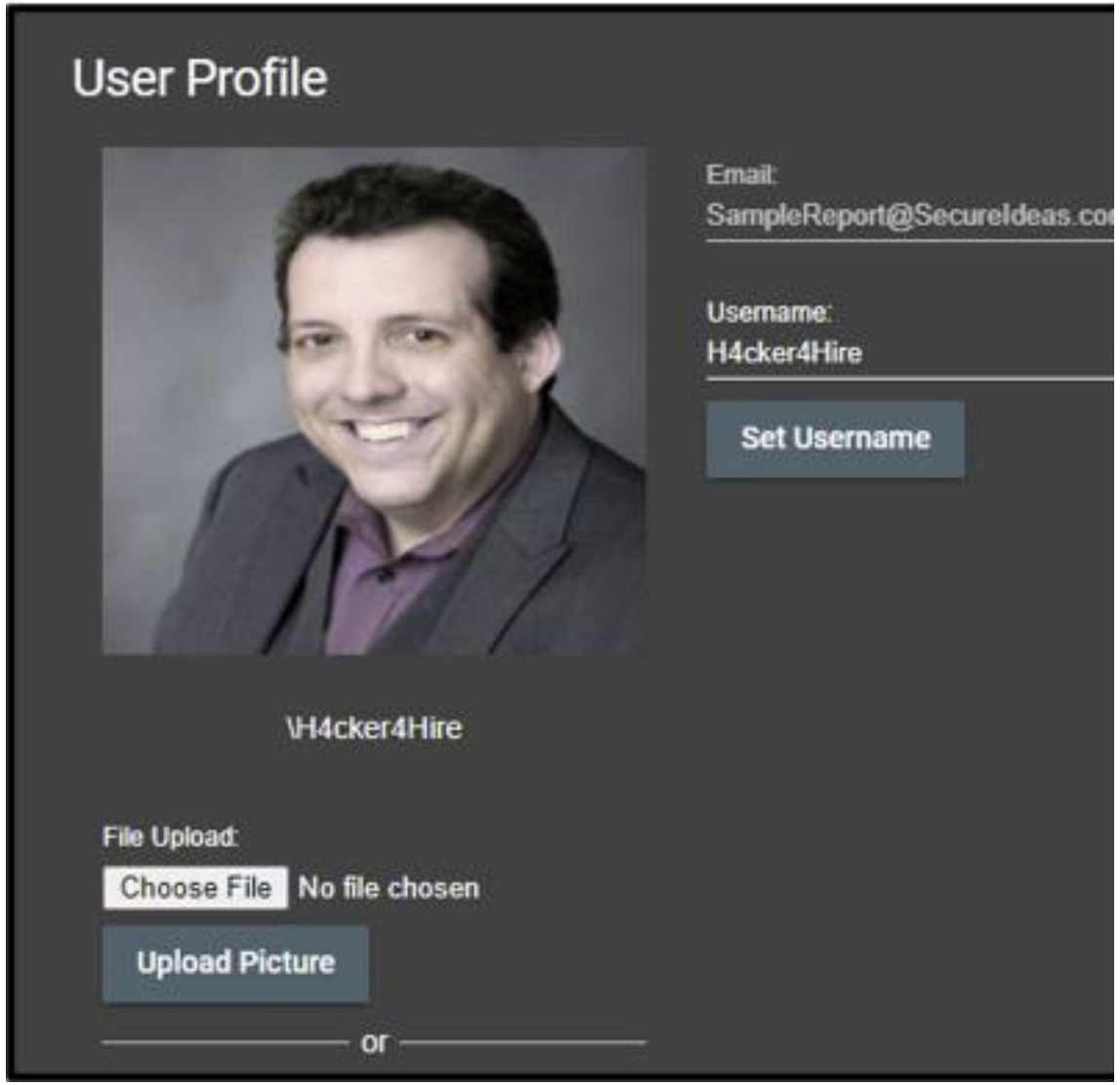
These flaws share a common cause. The application accepts input without validating it and does not consistently verify whether the requester is authorized to perform the requested action. Most of the remaining findings trace back to that same weakness.

Secure Ideas recommends remediating the two critical findings before this application is made available to untrusted users. Given the nature and number of issues identified, the overall risk to OWASP Juice Shop is rated Very High.

These, and the other issues found are outlined in the report that follows. Secure Ideas appreciates the opportunity to work with OWASP Juice Shop to help improve its security posture.

Copyright © 2026 Secure Ideas LLC

What I Would Keep



- I am not embarrassed by this report.
- But I would write it differently now, and in three years I will want to change whatever I write this month.
- The question is whether you go back and look.

Copyright © 2026 Secure Ideas LLC



Five Sections, Six Readers

Copyright © 2026 Secure Ideas LLC

It's Really Five Documents

Scope	Everyone
Executive summary	The people who fund things
Findings	The people who assign the work, and the people who do it
Narrative	Anyone who needs the story, not just the list
Strategic guidance	Whoever can fix the cause, not the instance
And a sixth reader	**with no section of their own.**

Copyright © 2026 Secure Ideas LLC

Scope and Executive Summary

Scope

Readers: Everyone. It is the only section with no specific audience, because it changes the meaning of all the others.

Executive Summary

Readers: The people weighing this against everything else it takes to operate a business.



Copyright © 2026 Secure Ideas LLC

Findings

FINDINGS SUMMARY

The following table summarizes the findings. Each finding is broken out in detail by risk immediately after the summary table.

Finding	Risk
1. SQL Injection Flaws	Critical
2. Authorization Bypass	Critical
3. Cross-Site Scripting Flaws	High
4. XML External Entity (XXE)	High
5. Improper Validation and Handling	High
6. Sensitive Information Disclosure	High
7. Weak Password Complexity Requirements	Medium
8. Username Harvesting	Medium
9. Lack of JavaScript Library Patching	Low

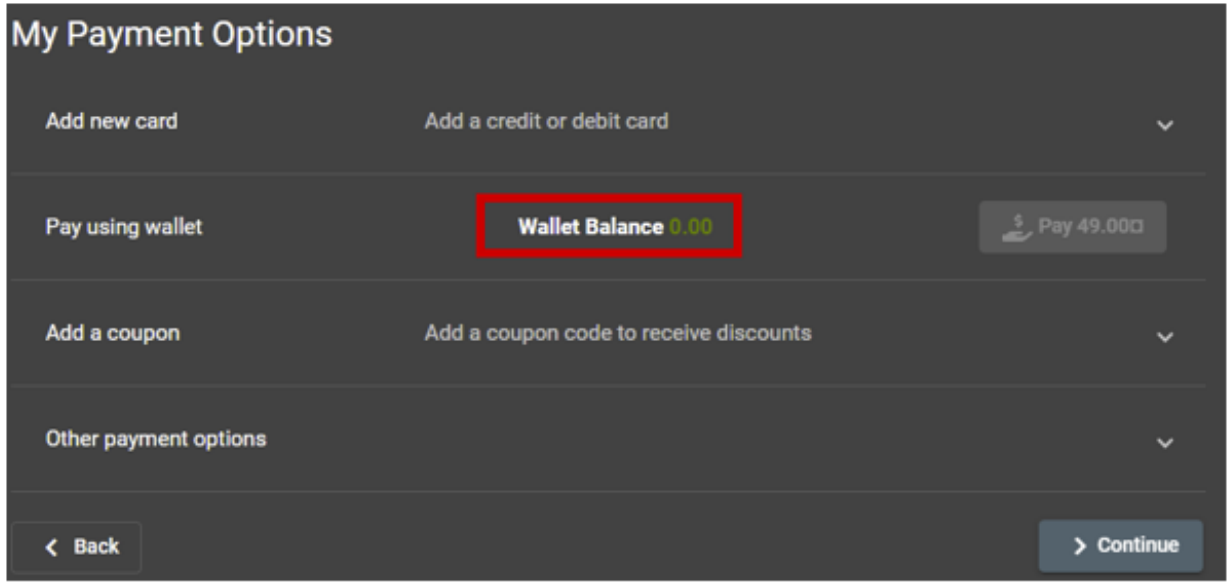
Copyright © 2026 Secure Ideas LLC

Findings

Finding

Secure Ideas has found that the OWASP Juice Shop application contains an improper validation and handling flaw. During testing, Secure Ideas found that a Deluxe Membership upgrade was possible without payment.

Initially, when browsing to *http://localhost:3000/#/payment/deluxe* the payment options were displayed correctly, with a noted account balance of $0 in the wallet, as seen in the accompanying screenshot.



Through an examination of the webpage using developer tools, Secure Ideas observed that the payment button attribute was set to "disabled=true", suggesting that the system was correctly disallowing payment attempts due to the absence of funds in the wallet. The relevant code snippet and the corresponding screenshot are included below.

The people who assign the work



The people who do the work

Copyright © 2026 Secure Ideas LLC

Narrative

The Findings Table lists nine findings. It does not show you how any of them connect.

PATH ONE

SQL injection
' or 1=1-- in the email field. No account needed.

→

Log in as anyone
Modify the query, walk down the user table.

→

Change Password
Button is gated client side. Enable it in dev tools.

PATH TWO

Unauthenticated POST to /api/Users
No login, no token, no cookie. Creates an account with the admin role.

↓

Either path, on its own: permanent control of any account

Copyright © 2026 Secure Ideas LLC

Narrative Before the Narrative

WE STOPPED AND CALLED. TWICE.

"Due to the criticality of the SQLi… Secure Ideas quickly reached out to the OWASP Juice Shop point of contact… and a meeting was requested to review the findings."

REMEDIATION STARTED BEFORE THE REPORT WAS DELIVERED.

"…OWASP Juice Shop's technical team was quick to respond… and have already begun a root cause analysis to determine how to best implement fixes."

Due to the critical nature of this authorization bypass, another email was sent to OWASP Juice Shop. A meeting was set up to go over these findings immediately as well as get additional direction on considerations for the remainder of this test. Secure Ideas then walked OWASP Juice Shop's technical team through the critical findings discovered, and discussed various options related to the risk and remediation of these items. OWASP Juice Shop's technical team was quick to respond to the input provided and have already begun a root cause analysis to determine how to best implement fixes in accordance with OWASP Juice Shop's internal policies and processes. Additional effort is going to be spent on reviewing, and determining the best way to address security concerns throughout the application's development process.

Can also include details about communication during the test, alerts, and interesting tidbits.

Copyright © 2026 Secure Ideas LLC

Strategic Guidance



Reader: whoever can change how the work gets done.

Secure coding training

Answers four of my nine findings at once

Formalize app security practices

A program change, not a ticket

Consider MFA

The boilerplate I showed you earlier

Findings tell you what to fix.

Strategic guidance tells you what to change.

Copyright © 2026 Secure Ideas LLC

The Sixth Reader

Governance, risk, compliance

There is no section written for them.

Which is where those OWASP and NIST tables come in.

2. Authorization Bypass

Industry Standards	
OWASP Top 10	*A1:2021: Broken Access Control*
NIST 800-53	*AC-3: Access Enforcement*

Copyright © 2026 Secure Ideas LLC



What You Lose Reading Only Your Section

Copyright © 2026 Secure Ideas LLC

What Each Reader Misses

Executive summary only	You cannot judge whether the spend is proportionate
Findings only	You fix instances and miss causes
Nobody reads scope	Everyone misreads everything

Copyright © 2026 Secure Ideas LLC

How to Tell When Nine Findings Are Three Problems

- Group by the fix, not the symptom
- Ask who would do the work
- Count the mistakes that repeat

Nine findings, three causes, three projects. Not nine tickets.



Copyright © 2026 Secure Ideas LLC

The Two Windows



Copyright © 2026 Secure Ideas LLC

Two Windows

The report changes twice. Different things change each time.

Before it is final
The readout

The findings are still in play.

- Severity can move
- A finding can be corrected or withdrawn
- Scope language can be clarified

After the retest
The status changes

The findings stay. Their status does not.

- Remediated findings are marked remediated
- The executive summary is updated to match
- Nothing is deleted

A remediated Critical is still a Critical that existed. Now shown as closed.

Copyright © 2026 Secure Ideas LLC

Two Ways a Readout Goes Flat

Accepting everything



Pushing back on everything



Copyright © 2026 Secure Ideas LLC

A Severity Rating Describes One Thing



- The vulnerability, in isolation
- The rating is accurate
- It's just not the entire picture

Copyright © 2026 Secure Ideas LLC

Window One: While It Is Still a Draft



A rating that moves after a conversation

A rating quietly overridden later

Same decision.

Completely different outcome the next time somebody asks why that Critical is now a Medium.

Tell us what we did not have visibility into while the draft is still a draft.

Copyright © 2026 Secure Ideas LLC

Window Two: The Retest

Retest terms live in the engagement agreement, not in the report.

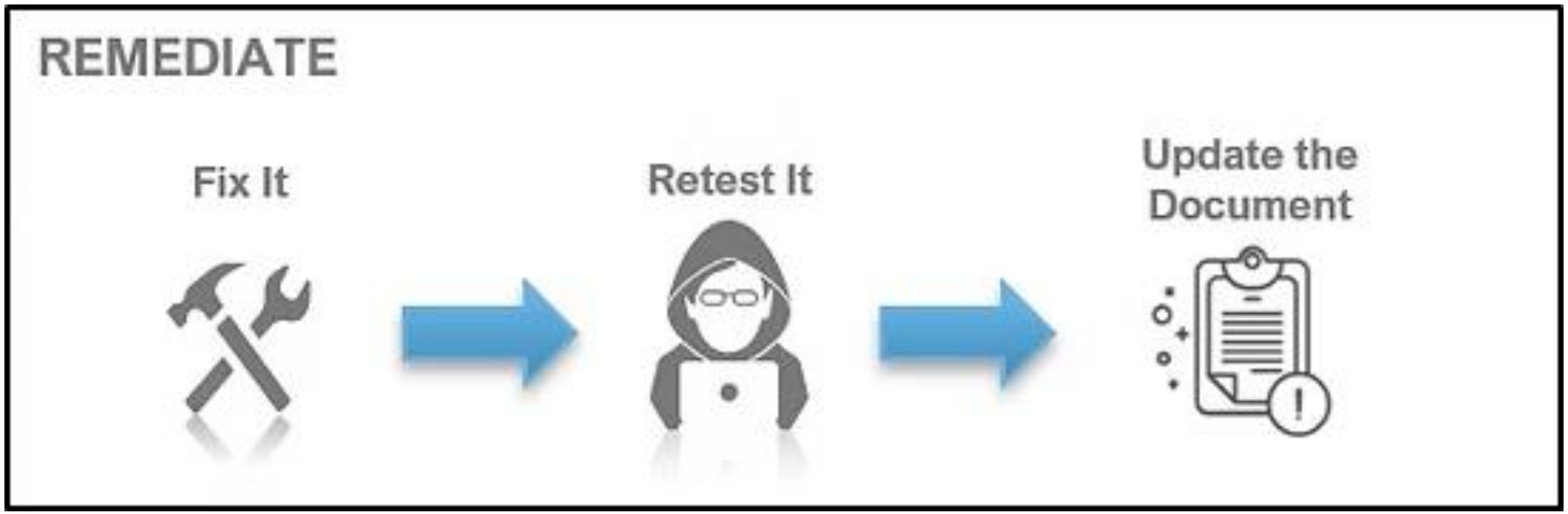
Covers the original findings

Often not much else

Ask what is included while you are still negotiating, not when you are ready to request it.

Copyright © 2026 Secure Ideas LLC

Our Window



- Our retest window is 90 days from final delivery.
- If you are outside it, ask anyway
- The answer is often yes

Copyright © 2026 Secure Ideas LLC



A Plan That Leadership Can Get Behind

Copyright © 2026 Secure Ideas LLC

Building the Plan



- GROUP BY ROOT CAUSE



- SEQUENCE RISK AGAINST EFFORT



- NAME AN OWNER AND A DATE



- DECIDE WHAT YOU ARE ACCEPTING

Copyright © 2026 Secure Ideas LLC

What Leadership Actually Needs



What could happen	What it costs to prevent	What we are choosing not to do	And why

Not a findings table. Not a count of reds. Not a forwarded PDF.

Copyright © 2026 Secure Ideas LLC

- Bring the people who own the fixes to the readout
- Read the section that was not written for you
- Tell us what we could not see while the draft is still a draft
- Know your retest window before you need it
- Group findings by cause before you schedule any of them

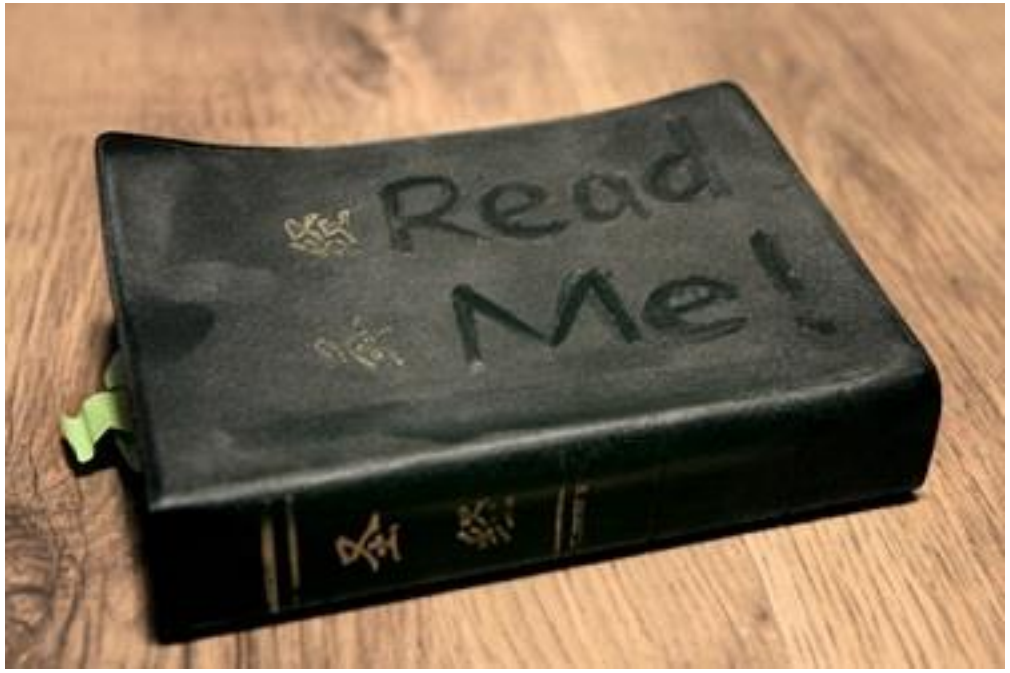


Copyright © 2026 Secure Ideas LLC

The report is the deliverable. A more secure environment is the goal.

The distance between them is covered by reading past your own section, talking to each other, and talking to us.

Before and After the engagement.



Copyright © 2026 Secure Ideas LLC



Questions?

Kathy.Collins@secureideas.com

linkedin.com/in/kathyvcollins/

Copyright © 2026 Secure Ideas LLC