ACCCF / अनुप्रयुक्त ज्ञान पुस्तकालय

09

प्राधिकरण, नियंत्रित परीक्षण और सत्यापनयोग्य सुधार

स्पेनिश संस्करण · 2026

खंड

प्रमाण-आधारित पेनटेस्ट पुस्तिका: संगठनों के लिए सत्यापन, परिहार और पुनःपरीक्षण

परीक्षण-संचालन नियम, निष्कर्ष, सीमांकित प्रभाव, सुधार और सत्यापन

सुरक्षा परीक्षण को अधिकृत और समीक्षा-योग्य प्रक्रिया बनाना, जिसमें प्रत्येक निष्कर्ष के साथ समानुपातिक प्रमाण हो और प्रत्येक सुधार की जाँच बिना दूसरी घटना पैदा किए की जा सके।

सुरक्षा और प्रौद्योगिकी टीमों, प्रबंधन, अनुपालन अधिकारियों, बीमाकर्ताओं, लेखापरीक्षकों और सेवा प्रदाताओं के लिए। इसमें शोषण के निर्देश नहीं हैं और यह स्पष्ट अनुमति के बिना किसी भी सिस्टम का परीक्षण करने का प्राधिकरण नहीं देता।

संपादकीय समन्वय: जोसान लैगुन · अमेरिकी साइबर सुरक्षा और फोरेंसिक कम्प्यूटिंग परिषद

सामान्य तकनीकी मार्गदर्शिका और खुली शैक्षिक सामग्री। यह कानूनी सलाह, विशेषज्ञ राय या बिना प्राधिकरण के सिस्टम तक पहुँचने के निर्देश नहीं है। उदाहरण और डेटा काल्पनिक हैं; आकृतियाँ संपादकीय पुनर्निर्माण हैं।

विषय-सूची

दिखाई देने वाला पृष्ठांकन PDF संस्करण से संबंधित है। Word दस्तावेज़ खोलते समय इस अनुक्रमणिका को अद्यतन कर सकता है; शीर्षक आंतरिक नेविगेशन बनाए रखते हैं।

प्रस्तावना: एक स्कैन हर महत्वपूर्ण बात सिद्ध नहीं करता 3

अध्याय 1. प्राधिकरण और नियम 3

- **1.1 बिना व्याख्या के क्रियान्वित किया जा सकने वाला दायरा** 3
- **1.2 परिचालन जोखिम और निकासी योजना** 4

अध्याय 2. तकनीकी तैयारी और सत्यापन 4

- **2.1 आर्किटेक्चर और सुरक्षा प्रश्न** 4
- **2.2 उपकरण और नियंत्रण डेटा** 5
- **2.3 रिकॉर्ड और सिंक्रोनाइज़ेशन** 5

अध्याय 3. सुरक्षित क्रियान्वयन और कार्यवाही-लॉग 5

- **3.1 प्रत्येक कार्रवाई का लॉग** 5
- **3.2 रोकना, एस्केलेशन और संचार** 6
- **3.3 प्राप्त जानकारी का प्रबंधन** 6

अध्याय 4. प्रत्येक निष्कर्ष का प्रमाण 6

- **4.1 दोहराने योग्य निष्कर्ष विवरण** 6
- **4.2 गलत सकारात्मक परिणाम और डुप्लिकेट** 6
- **4.3 प्रभाव और प्राथमिकता** 7

अध्याय 5. परिहार और जोखिम प्रबंधन 8

- **5.1 मूल कारण दूर करने वाला सुधार** 8
- **5.2 प्रभाव और निर्भरताओं के आधार पर योजना** 8
- **5.3 परिहार का प्रमाण** 8

अध्याय 6. पुनःपरीक्षण और समापन 8

- **6.1 तुलनीय परिस्थितियाँ दोहराना** 8
- **6.2 समापन स्थितियाँ** 9
- **6.3 अंतिम रिपोर्ट और प्राप्त सीख** 9

परिशिष्ट A. परीक्षण-संचालन नियम और निष्कर्ष विवरण 10

- **A.1 परीक्षण-संचालन नियम** 10
- **A.2 निष्कर्ष विवरण** 10
- **A.3 पुनःपरीक्षण रिपोर्ट** 11

परिशिष्ट B. कानूनी ढाँचा और अंतिम जाँच 11

प्रस्तावना: एक स्कैन हर महत्वपूर्ण बात सिद्ध नहीं करता

सैकड़ों अलर्ट वाली रिपोर्ट मूल प्रश्न अनुत्तरित छोड़ सकती है: कौन-सा जोखिम वास्तविक है, किस एसेट पर, किन परिस्थितियों में, क्या प्रभाव है और कैसे जाँचें कि सुधार काम कर गया। पेनेट्रेशन परीक्षण किसी भी कीमत पर पहुँच पाने की दौड़ नहीं है। यह अधिकृत मूल्यांकन है जो लोगों, डेटा या निरंतरता को नुकसान पहुँचाए बिना जोखिम घटाने का प्रमाण देता है।

NIST SP 800-115 कमज़ोरियों की समीक्षा, पहचान, विश्लेषण और सत्यापन की तकनीकों में अंतर करता है। स्कैनर इस प्रक्रिया का हिस्सा हो सकता है, लेकिन योजना, विश्लेषण या बाद के मूल्यांकन का स्थान नहीं लेता। विशेषज्ञ का मूल्य अधिक उपकरण चलाने में नहीं, बल्कि यह तय करने में है कि कौन-सा उपकरण आवश्यक है, किस दायरे में और कब रोकना है।[1]

परीक्षण से पहले प्रमाण की रूपरेखा तय करें। इससे एसेट, कॉन्फ़िगरेशन, परिस्थितियाँ, प्रक्रिया, परिणाम, प्रभाव और सीमाओं की समीक्षा संभव होनी चाहिए। यदि काल्पनिक डेटा, आंशिक प्रतिक्रियाओं या नियंत्रित वातावरण से बात सिद्ध की जा सके, तो वास्तविक रहस्यों के अस्तित्व को साबित करने के लिए उन्हें कैप्चर न करें। परिहार और पुनःपरीक्षण शुरुआत से कार्य-दायित्व का हिस्सा हैं; रिपोर्ट सौंपने के बाद इन्हें अचानक नहीं जोड़ा जाता।

> **मार्गदर्शक सिद्धांत**
> किसी चीज़ का परीक्षण कर सकना उसका प्राधिकरण नहीं है। प्राधिकरण में एसेट, तकनीकें, परीक्षण-विंडो, डेटा, संपर्क और रोकने के मानदंड तय होते हैं; पद्धति इन सीमाओं को बनाए रखती है।

अध्याय 1. प्राधिकरण और नियम

1.1 बिना व्याख्या के क्रियान्वित किया जा सकने वाला दायरा

प्राधिकरण दस्तावेज़ में डोमेन, पता, एप्लिकेशन, खाता, वातावरण और मालिक के अनुसार एसेट; अनुमत और निषिद्ध तकनीकें; तिथियाँ और समय क्षेत्र; परीक्षण डेटा; सूचना प्रबंधन; संपर्क; संचार; रोकने की शर्तें और डिलीवरी शामिल हों। “आप सब कुछ ऑडिट कर सकते हैं” यह स्पष्ट नहीं करता कि सोशल इंजीनियरिंग, सेवा-निषेध, शोषण, ब्रूट फ़ोर्स, भौतिक पहुँच या वास्तविक डेटा की समीक्षा की अनुमति है या नहीं।

तीसरे पक्ष और निर्भरताएँ पहचानें: क्लाउड, CDN, ईमेल प्रदाता, पेमेंट गेटवे, साझा सेवाएँ, बाहरी API और ग्राहक नेटवर्क। अधिकृत डोमेन किसी तीसरे पक्ष के बुनियादी ढाँचे पर हल हो सकता है जिसके लिए अलग प्राधिकरण चाहिए। खोज से परीक्षण का दायरा अपने आप नहीं बढ़ता: नया एसेट मिलने पर उसे दर्ज करें और उससे संवाद करने से पहले दायरा बढ़ाने का अनुरोध करें।

तत्व	जिस जानकारी का लिखित विवरण आवश्यक है	काल्पनिक उदाहरण
उद्देश्य	व्यावसायिक जोखिम और मूल्यांकन प्रश्न।	ग्राहक पोर्टल के पहुँच नियंत्रणों का सत्यापन करें।
एसेट	डोमेन, IP, एप्लिकेशन, खाते और वातावरण।	demo.empresa.invalid और दो काल्पनिक खाते।
तकनीकें	अनुमत, प्रतिबंधित और बाहर रखी गई।	सेवा-निषेध नहीं, ब्रूट फ़ोर्स नहीं, स्पैम नहीं।
परीक्षण-विंडो	प्रारंभ, समाप्ति, समय क्षेत्र और संपर्क समय।	10–12 नवंबर, 22:00–02:00 UTC।
डेटा	काल्पनिक डेटा, मास्किंग, प्रतिधारण और विलोपन।	वास्तविक डेटाबेस डाउनलोड न करें और रहस्य निकाल न करें।

[1] NIST SP 800-115. सूचना सुरक्षा परीक्षण और मूल्यांकन की तकनीकी मार्गदर्शिका: योजना, क्रियान्वयन और बाद का विश्लेषण। केवल स्वचालित स्कैन पेनेट्रेशन परीक्षण या पूर्ण सत्यापन नहीं है। आधिकारिक ऑनलाइन स्रोत

तत्व	जिस जानकारी का लिखित विवरण आवश्यक है	काल्पनिक उदाहरण
दायरा	खाते, उत्तरदायी व्यक्ति और सूचना देने का तरीका।	लिखित, तीसरे पक्ष तक अप्रत्याशित पहुँच की जानकारी दायरा।
डिलिवरी	प्रारूप, प्राप्तकर्ता, पैनल और विलोपन।	आवंटित संपर्क-व्यक्ति को एन्क्रिप्टेड रिपोर्ट भेजी।

1.2 परिचालन जोखिम और निकासी योजना

संभावित लॉकआउट, संसाधन खपत, लॉग, अलर्ट, स्थिति परिवर्तन, अवशिष्ट डेटा और उपयोगकर्ताओं पर प्रभाव की समीक्षा करें। योजना में आवश्यकता अनुसार बैकअप, तकनीकी संपर्क, कॉन्फ़िगरेशन रोलबैक, कार्य निलंबन और संचार शामिल हों। किसी ऐसे जोखिम को साबित करने के लिए अपरिवर्तनीय कार्रवाई न करें जिसे दूसरे तरीके से सिद्ध किया जा सके।

परीक्षण में अधिमानतः काल्पनिक खाते, रिकॉर्ड और ऑब्जेक्ट उपयोग करें। यदि अनधिकृत पहुँच दिखानी है, तो वास्तविक सामग्री देखने से पहले रोकने की शर्त तय करें। केवल न्यूनतम कैप्चर रखें: प्रतिक्रिया, कोड, संरचना और संदर्भ; ग्राहक डेटा साझा न करें। निष्कर्ष का प्रमाण दूसरा उल्लंघन नहीं बनना चाहिए।

> **शुरू करने का पूर्व-शर्त**
> यदि आप यह नहीं बता सकते कि प्राधिकरण कौन देता है, कौन-से एसेट शामिल हैं, कौन-सी कार्रवाइयाँ अनुमत हैं, किसे बुलाना है और कब रोकना है, तो परीक्षण अभी शुरू करने के लिए तैयार नहीं है।



चित्र 1. प्राधिकरण पद्धति का हिस्सा है। परीक्षण से पहले कार्रवाइयाँ और निकासी योजना तय की जाती है। संपादकीय पुनर्लिखित; वास्तविक प्रमाण नहीं।

अध्याय 2. तकनीकी तैयारी और सत्यापन

2.1 आर्किटेक्चर और सुरक्षा प्रश्न

आर्किटेक्चर, इन्वेंटरी, प्रमाणीकरण प्रवाह, भूमिकाएँ, लॉग, निर्भरताएँ, हाल के बदलाव और व्यावसायिक आवश्यकताएँ एकत्र करें। दस्तावेज़ समीक्षा से सेवा को छूए बिना कमज़ोरियाँ पता चल सकती हैं। आर्किटेक्चर प्राधिकरण, कॉन्फ़िगरेशन, सत्र प्रबंधन, डेटा एक्सपोज़र और एकीकरण नियंत्रणों के परीक्षण का मार्गदर्शन करता है। हर प्रश्न के लिए शोषण आवश्यक नहीं है।

योजना में प्रभाव और संभावना के आधार पर प्राथमिकता दें, शोषण की आसानी के आधार पर नहीं। डेटा रहित सेवा की चेतावनी की प्राथमिकता उस फ़ंक्शन से कम हो सकती है जो लाभार्थी बदलने देता है। मूल्यांकन तकनीकी जोखिम, वातावरण की स्थिति और व्यावसायिक परिणाम में अंतर करता है। एसेट का कार्य अज्ञात हो तो प्रभाव का दावा सीमित रखें।

2.2 उपकरण और नियंत्रण डेटा

ज्ञात लक्ष्यों और काल्पनिक डेटा पर उपकरणों का सत्यापन करें: पहचान, आउटपुट, सीमाएँ, दर, पुनःप्रयास, प्रारूप और लॉग पर प्रभाव। नाम, संस्करण, कॉन्फ़िगरेशन और परिणाम दर्ज करें। स्कैनर गलत सकारात्मक परिणाम दे सकता है या सामान्य प्रतिक्रिया का गलत अर्थ निकालकर कोई स्थिति छोड़ सकता है। समीक्षा के बिना आउटपुट रिपोर्ट में कॉपी न करें।

नियंत्रण डेटा से अपेक्षित और देखे गए व्यवहार की तुलना करें: बिना अनुमति वाला उपयोगकर्ता, सीमित भूमिका वाला उपयोगकर्ता, अपना संसाधन, किसी अन्य उपयोगकर्ता का काल्पनिक संसाधन, वैध अनुरोध और बदला हुआ अनुरोध। प्रतिक्रियाओं का अंतर संवेदनशील सामग्री पढ़े बिना स्थिति सिद्ध कर सकता है। यदि केवल प्रोडक्शन में परीक्षण संभव हो, तो अधिक सख्त सीमाएँ तय करें और उत्तरदायी व्यक्ति उपलब्ध रखें।

2.3 रिकॉर्ड और सिंक्रोनाइज़ेशन

परीक्षण से पहले जाँचें कि सिस्टम कौन-से लॉग बनाता है, कौन उन्हें देख सकता है और घड़ियाँ सिंक्रोनाइज़ हैं या नहीं। प्रत्येक स्रोत के यथावत टाइमस्टैम्प और समय क्षेत्र दर्ज करें। WAF अलर्ट, एप्लिकेशन घटना और परीक्षक के अनुरोध की घड़ियाँ अलग हो सकती हैं। सहसंबंध पहचानकर्ताओं से स्पष्ट करें, केवल समय की निकटता से नहीं।

> **गुणवत्ता नियंत्रण**
> यदि परीक्षण से समझने योग्य लॉग नहीं बनते, तो उसके बारे में दावे सीमित करें। समाधान पूरी घटनावली बनाना नहीं है; उपयुक्त स्रोत सक्षम करें या उनकी अनुपस्थिति बताएँ।

अध्याय 3. सुरक्षित क्रियान्वयन और कार्यवाही-लॉग

3.1 प्रत्येक कार्रवाई का लॉग

प्रत्येक कार्रवाई में तिथि और समय क्षेत्र, ऑपरेटर, एसेट, उपकरण और संस्करण, कॉन्फ़िगरेशन, उद्देश्य, अधिकृत अनुरोध या प्रक्रिया, प्रतिक्रिया, आर्टिफ़ैक्ट और प्रभाव दर्ज करें। कार्यवाही-लॉग में वास्तविक क्रेडेंशियल या टोकन न रखें। आउटपुट फ़ाइलों को मैनिफ़ेस्ट से जोड़ें और पहुँच सीमित करें। स्क्रीनशॉट केवल आवश्यक बात दिखाने के लिए लें, छवियाँ इकट्ठा करने के लिए नहीं।

कार्यवाही-लॉग में वे प्रयास भी रखें जो सफल नहीं हुए। दस्तावेज़ित परिस्थितियों में नकारात्मक परिणाम गलत जोखिम-दावे से बचा सकता है, लेकिन सार्वभौमिक अनुपस्थिति सिद्ध नहीं करता। उपकरण विफल होने पर संस्करण, त्रुटि और दायरा दर्ज करें। परीक्षण दोहराने पर नया संबंधित क्रियान्वयन बनता है; पिछला प्रयास मिटता नहीं।

फ़ील्ड	काल्पनिक उदाहरण	समीक्षा
कार्रवाई	सीमित सूची से DEMO-02 सत्यापन का अधिकृत अनुरोध।	दायरे के भीतर और काल्पनिक डेटा का उपयोग।
समय और समय क्षेत्र	2026-11-10T22:14:03+00:00.	यह रिकॉर्ड से मेल खाता है।
परिणाम	200 प्रतिक्रिया, जिसमें किसी अन्य उपयोगकर्ता का परीक्षण संसाधन की संरचना है।	वास्तविक डेटा पढ़ा बिना अनधिकृत पहुँच का प्रदर्शन।
प्रमाण	अनुरोध, आंशिक प्रतिक्रिया, पहचानकर्ता और स्क्रीनशॉट कैप्चर।	कोई टोकन या व्यक्तिगत डेटा नहीं।

फ़ील्ड	काल्पनिक उदाहरण	समीक्षा
प्रमाण	कोई स्थिति परिवर्तन या सर्वर पर दृश्यमान प्रभाव नहीं।	निगरानी और सर्वर की पुष्टि की गई है।
निर्णय	परीक्षण-पथ रोकें और निष्कर्ष दस्तावेज़ित करें।	अन्य वास्तविक रिकॉर्ड तक पहुँच न बढ़ाएँ।

3.2 रोकना, एस्केलेशन और संचार

गिरावट, अप्रत्याशित प्रभाव, अनिश्चित दायरा, योजना से बाहर वास्तविक डेटा, प्रतिक्रिया माँगने वाला सुरक्षा अलर्ट या अधिकृत संपर्क का निर्देश होने पर रोकें। सूचना में एसेट, कार्रवाई, स्थिति, उपलब्ध प्रमाण और लंबित निर्णय शामिल हों। प्राधिकरण में न आने वाले अवसर का लाभ लेने के लिए परीक्षण जारी न रखें।

वास्तविक घटना को परीक्षण से अलग रखें। यदि टीम को अपने द्वारा उत्पन्न न की गई गतिविधि मिले, तो उसे स्वतंत्र निष्कर्ष के रूप में दर्ज करें और सुरक्षित चैनल से सूचित करें। उसे अपने आप पेनटेस्ट से न जोड़ें और न उसके निशान मिटाएँ। समयक्रम में स्पष्ट हो कि प्रत्येक कार्रवाई किसने की और साथ-साथ क्या घटित हुआ।

3.3 प्राप्त जानकारी का प्रबंधन

यदि परीक्षण के दौरान अप्रत्याशित डेटा मिले, तो अन्वेषण रोकें, अतिरिक्त सामग्री कॉपी किए बिना स्थिति दर्ज करें और प्राप्त डेटा का प्रबंधन कैसे करना है यह पूछें। एन्क्रिप्टेड चैनल से सीमित प्राप्तकर्ताओं को डिलीवरी करें। कुंजियाँ अलग चैनल से भेजें। परीक्षण फ़ाइलों के विलोपन का दायरा और सीमाएँ दस्तावेज़ित करें; सहमति के बिना कार्रवाई का प्रमाण न मिटाएँ।

> **न्यूनतम आवश्यक प्रमाण का सिद्धांत**
> यदि आंशिक प्रतिक्रिया और काल्पनिक पहचानकर्ता समस्या सिद्ध कर देते हैं, तो पूरा डेटाबेस डाउनलोड न करें। प्रमाण की मज़बूती उजागर किए गए डेटा की मात्रा से नहीं मापी जाती।

अध्याय 4. प्रत्येक निष्कर्ष का प्रमाण

4.1 दोहराने योग्य निष्कर्ष विवरण

निष्कर्ष विवरण में पहचानकर्ता, शीर्षक, एसेट, संस्करण, स्थिति, स्रोत, प्रक्रिया, परिणाम, प्रभाव, दायरा, सीमाएँ, सहमत गंभीरता, अनुशंसा और पुनःपरीक्षण मानदंड शामिल हों। परीक्षण का इतना विवरण दें कि अधिकृत व्यक्ति उसे दोहरा सके, लेकिन सामान्य रिपोर्ट में रहस्य या शोषण-पथ सार्वजनिक न हों जिससे निर्धारित प्राप्तकर्ताओं से बाहर जोखिम बढ़े।

प्रमाण अनुरोध और प्रतिक्रिया को सही एसेट से जोड़ना चाहिए। बिना URL या तिथि का स्क्रीनशॉट ऑब्जेक्ट की पहचान नहीं करता। त्रुटि संदेश शोषण सिद्ध नहीं करता। स्कैनर के “गंभीर” लेबल से व्यावसायिक प्रभाव सिद्ध नहीं होता। विशेषज्ञ समीक्षा करके बताता है कि क्या किया गया और कौन-सा प्रभाव वास्तव में प्रदर्शित हुआ।

4.2 गलत सकारात्मक परिणाम और डुप्लिकेट

गलत सकारात्मक परिणाम अनुमानित संस्करण, अनुकूलित प्रतिक्रिया, प्रॉक्सी, कॉन्फ़िगरेशन या स्कैनर के गलत सिग्नेचर के कारण हो सकता है। उसे मैनुअल समीक्षा, लॉग और अपेक्षित व्यवहार से जाँचें। पुष्टि न होने पर उसे अपुष्ट चिह्नित करें और निष्कर्षों की कुल संख्या में न जोड़ें। एक ही मूल कारण वाले डुप्लिकेट को आपस में जोड़ें, प्रभावित एसेट छिपाए बिना।

स्थिति	पक्षीकरण प्रश्न	पढ़ न करें
अपुष्ट परिणाम	स्रोत, संस्करण और व्यवहार की समीक्षा करें, फिर घोषित करें।	इसे एक सिद्ध भेद्यता के रूप में प्रस्तुत करें।

स्थिति	पश्चातवर्ती प्रबंधन	यह न करें
कई एसेट में एक ही मूल कारण	कारण के अनुसार समूह बनाएं और प्रत्येक प्रभावित एसेट की कवरेज सूचीबद्ध करें।	एसेट छिपाना या संख्या बढ़ा-चढ़ाकर दिखाना।
जोखिम परिणाम	पारिस्थितियां, पुनः प्रयास और वातावरण का दस्तावेजीकरण।	केवल अनुकूल क्रियान्वयन चुनना।
अप्रमाणित प्रभाव	तकनीकी स्थिति और प्रमाणित परिणाम को अलग रखें।	सिस्टम का पूर्ण नियंत्रण मान लेना।
दायरे से बाहर का एसेट	रोकें और दायरा बढ़ाने का अनुरोध करें।	केवल संबंधित दिखने के कारण परीक्षण करना।

4.3 प्रभाव और प्राथमिकता

तकनीकी गंभीरता का मूल्यांकन एक्सपोज़र, विशेषाधिकार, डेटा, शोषण-योग्यता, प्रतिपूरक नियंत्रण और व्यावसायिक प्रभाव के साथ करें। महत्वपूर्ण एसेट में कठिनाई से शोषित होने वाली कमज़ोरी की प्राथमिकता पृथक वातावरण में आसानी से शोषित होने वाली कमज़ोरी से भिन्न हो सकती है। व्यावसायिक संबंधों के कारण जोखिम घटाकर दिखाने और प्रभाव डालने के लिए बढ़ाने, दोनों से बचें।

कार्यकारी सारांश बताता है कि क्या हो सकता है, कौन-से एसेट प्रभावित हैं, किन परिस्थितियों में और कौन-सा निर्णय चाहिए। इसमें संदर्भ रहित शब्दों की लंबी सूची न हो। तकनीकी परिशिष्ट में प्रमाण, लॉग और सीमाएँ सुरक्षित रहें। प्रबंधन को निर्णय, सुरक्षा टीम को पुनरुत्पादन के चरण और अनुपालन को अनुवर्ती कार्रवाई का प्रमाण मिलें।

> **काल्पनिक मामला**
> कोई फ़ंक्शन पहचानकर्ता बदलकर दूसरे उपयोगकर्ता का परीक्षण दस्तावेज़ देखने देता है। वास्तविक दस्तावेज़ों तक पहुँचने से पहले रोकें। निष्कर्ष काल्पनिक ऑब्जेक्ट पर ऑब्जेक्ट-स्तरीय प्राधिकरण विफलता दिखाता है। यह दावा नहीं करता कि सभी दस्तावेज़ उपलब्ध हैं या हमलावर ने डेटाबेस डाउनलोड किया: अतिरिक्त अधिकृत परीक्षणों से प्रभाव सीमांकित करें।



चित्र 2. निष्कर्ष विवरण से नुकसान दोहराए बिना समीक्षा संभव है। न्यूनतम प्रमाण, सीमांकित प्रभाव और सुधार का मार्ग। संपादकीय पुनर्निर्माण; वास्तविक प्रमाण नहीं।

अध्याय 5. परिहार और जोखिम प्रबंधन

5.1 मूल कारण दूर करने वाला सुधार

अनुशंसा उस स्थिति को पहचाने जिसे बदलना है, न कि केवल सामान्य अद्यतन को। प्राधिकरण की समस्या हो तो सर्वर-साइड सत्यापन और संसाधन से संबंध जाँचें; लिंक छिपाना समाधान नहीं है। कॉन्फ़िगरेशन की समस्या हो तो अन्य वातावरणों और घटकों पर प्रभाव जाँचें। सुधार में मालिक, लक्ष्य तिथि, निर्भरता, परीक्षण और संभावित रिग्रेशन शामिल हों।

यदि तुरंत सुधार संभव न हो, तो स्वीकृत जोखिम, अस्थायी शमन, उत्तरदायी व्यक्ति और समीक्षा तिथि दस्तावेज़ित करें। स्वीकृति को परिहार न कहें। WAF किसी पथ को सीमित कर सकता है, मूल कारण समाप्त नहीं करता; दोनों स्थितियों का प्रमाण रखें और जाँचें कि नियम वैध फ़ंक्शन को प्रभावित तो नहीं करता।

5.2 प्रभाव और निर्भरताओं के आधार पर योजना

कार्यवाई	उत्तरदायी व्यक्ति और तिथि	स्वीकृति मानदंड
अस्थायी शमन	[मालिक, क्रियान्वयन और पर्यवेक्षण-अवधि]	[संचालन बाधित किए बिना दुरुपयोग घटाए]
स्थायी सुधार	[परिवर्तन, संस्करण और तिथि]	[दोषर न मूल कारण समाप्त]
अन्य एसेट का समाधान	[एक ही पटल और कवरेज]	[कोई छिपा हुआ डुप्लिकेट नहीं]
रिग्रेशन परीक्षण	[महत्वपूर्ण फ्लो और यूनिट्स]	[कानूनी उपयोगकर्ताओं को कोई नुकसान नहीं]
दस्तावेज़ीय अद्यतन	[आरेख, कॉन्फ़िगरेशन और प्रक्रिया]	[वास्तविकता और दस्तावेज़ मेल खाते हैं]
अवशिष्ट जोखिम स्वीकृति	[नाम, कारण और समाप्ति तिथि]	[तकनीकी समापन से भ्रमित न करें]

5.3 परिहार का प्रमाण

कॉन्फ़िगरेशन परिवर्तन, संस्करण, तिथि, मालिक, डिप्लॉयमेंट, परीक्षण और प्रभाव सुरक्षित रखें। “अद्यतन” दिखने वाला डैशबोर्ड स्क्रीनशॉट सिद्ध नहीं करता कि पथ ठीक हो गया। एक से अधिक वातावरण हों तो दर्ज करें कि सुधार कहाँ लागू हुआ। निष्कर्ष मिटाने के लिए प्रारंभिक रिपोर्ट न बदलें: नया संबंधित मूल्यांकन जोड़ें।

> **ईमानदारी का सिद्धांत**
> “प्रदाता कहता है कि सुधार हो गया है” एक विवरण है, पुनःपरीक्षण नहीं। समापन के लिए तकनीकी सत्यापन या निर्धारित दायरे सहित अवशिष्ट जोखिम का स्पष्ट निर्णय आवश्यक है।

अध्याय 6. पुनःपरीक्षण और समापन

6.1 तुलनीय परिस्थितियाँ दोहराना

जहाँ संभव हो, पुनःपरीक्षण में उसी ऑब्जेक्ट, भूमिका, परिस्थितियों और प्रक्रिया का उपयोग करें, नए संस्करण और नई तिथि के साथ। पिछले प्रमाण बदले बिना परिणाम की तुलना मूल निष्कर्ष से करें। एप्लिकेशन या वातावरण बदला हो तो दर्ज करें, क्योंकि इससे अलग परिणाम की व्याख्या हो सकती है। नकारात्मक परिणाम केवल वर्तमान परीक्षण और कवरेज पर लागू होता है।

रिग्रेशन भी जाँचें: वैध उपयोगकर्ता काम कर सके और फ़ंक्शन अन्य डेटा उजागर न करे। दुर्भावनापूर्ण अनुरोध रुक जाए लेकिन सामान्य पहुँच टूट जाए, तो स्थिति आंशिक हो सकती है। सुधार केवल एक पथ पर काम करे और समकक्ष पथ मौजूद हों, तो उन्हें दायरे में जाँचें। समापन परीक्षण केवल वांछित त्रुटि के स्क्रीनशॉट तक सीमित न हो।

6.2 समापन स्थितियाँ

स्थिति	मानदंड	प्रमाण
सही किया गया।	दायरे में स्थिति दोहराई नहीं जा सकती और कोई रिग्रेशन नहीं देखा गया।	पुनः परीक्षण, तिथि, सत्यापन और पथ कवर।
आंशिक	कुछ एसेट या पथ में सुधार हुआ, लेकिन स्थिति बनी हुई है।	प्रत्येक एसेट का कवरेज और लंबित कार्य।
शमन किया गया।	जोखिम नियंत्रण एक्सपोज़र घटाता है, लेकिन मूल कारण समाप्त नहीं करता।	नियंत्रण, परीक्षण, पथता-जोखिम और सीमा।
स्वीकार किया गया।	उत्तरदायी व्यक्ति कारण और समाप्ति तिथि सहित अवशिष्ट जोखिम स्वीकार करता है।	निर्णय, दायरा और समीक्षा।
खुला।	स्थिति दोहराई जा सकती है या पर्याप्त प्रमाण उपलब्ध नहीं है।	मूल निष्कर्ष और लंबित कार्रवाइयाँ।

6.3 अंतिम रिपोर्ट और प्राप्त सीख

अंतिम रिपोर्ट प्रारंभिक निष्कर्ष, परिवर्तन, पुनःपरीक्षण और स्थिति को जोड़े, पिछले प्रमाण मिटाए बिना। इसमें अवशिष्ट जोखिम, सीमाएँ और अगली समीक्षा तिथि शामिल हों। कार्यकारी सारांश “सुरक्षित सिस्टम” का वादा न करे; बताए कि किन जोखिमों का मूल्यांकन हुआ और सुधार का क्या प्रमाण है। यदि परीक्षण संभव नहीं था, तो उसे सफल चिह्नित करने के बजाय यह घोषित करें।

इन सीखों के लिए फ़िशिंग-प्रतिरोधी प्रमाणीकरण, प्राधिकरण की समीक्षा, रिग्रेशन परीक्षण, तीसरे पक्षों की इन्वेंटरी या बेहतर लॉग आवश्यक हो सकते हैं। NIST SP 800-63B-4 प्रमाणीकरण मार्गदर्शन और आश्वासन स्तर देता है; यह पुनर्प्राप्ति प्रवाह के मूल्यांकन का स्थान नहीं लेता, जो अक्सर वास्तविक समझौते का मार्ग होता है।[2]

> **वास्तविक समापन**
> परीक्षण तब समाप्त होता है जब संगठन दिखा सके कि क्या मिला, क्या बदला, क्या सत्यापित किया और कौन-सा जोखिम शेष है—तब नहीं जब PDF का नाम “final” रख दिया जाए।

[2] NIST SP 800-63B-4 (जुलाई 2025). प्रमाणीकरण और प्रमाणीकरण-साधनों के प्रबंधन के दिशानिर्देश, जिनमें आश्वासन स्तर और फ़िशिंग-प्रतिरोधी प्रमाणीकरण शामिल हैं। खाता पुनर्प्राप्ति भी जोखिम का हिस्सा है और इसे केवल पासवर्ड तक सीमित नहीं करना चाहिए। आधिकारिक ऑनलाइन स्रोत



चित्र 3. पुनःपरीक्षण केवल पैच नहीं, जोखिम सत्यापित करता है। मूल प्रमाण सुरक्षित रखें और नए प्रमाण से तुलना करें। संपादकीय पुनर्चित्रण; वास्तविक प्रमाण नहीं।

परिशिष्ट A. परीक्षण-संचालन नियम और निष्कर्ष विवरण

A.1 परीक्षण-संचालन नियम

अनुमोदन के लिए काल्पनिक टेम्पलेट

परियोजना: DEMO-PENTEST-2026-009
उद्देश्य और व्यावसायिक जोखिम: [विशिष्ट प्रश्न]
शामिल एसेट: [डोमेन, रेंज, एप्लिकेशन, खाते]
बहिष्करण: [एसेट, तीसरे पक्ष, डेटा और तकनीकें]
परीक्षण-विंडो और समय क्षेत्र: [प्रारंभ, समाप्ति, संपर्क]
अनुमत डेटा: [काल्पनिक डेटा, मास्किंग, प्रबंधन]
अनुमत कार्रवाइयाँ: [समीक्षा, सत्यापन, शर्तें]
निषिद्ध कार्रवाइयाँ: [DoS, ब्रूट फ़ोर्स, सोशल इंजीनियरिंग, अन्य]
रोकने की सीमाएँ: [गिरावट, डेटा, दायरा, अलर्ट]
आपातकालीन और वैकल्पिक संपर्क: [सुरक्षित चैनल]
प्रमाण: [प्रारूप, न्यूनतमकरण और कस्टडी]
डिलीवरी: [प्राप्तकर्ता, एन्क्रिप्शन और तिथि]
विलोपन: [ऑब्जेक्ट, बैकअप और सीमाएँ]
पुनःपरीक्षण: [तिथि, दायरा और स्वीकृति]
प्राधिकरण: [मालिक, तीसरे पक्ष और संस्करण]

A.2 निष्कर्ष विवरण

फ़ील्ड	आवश्यक सामग्री	काल्पनिक उदाहरण
भेद्यता	कार्यवाही-लायक से शुरू। स्पष्ट भेद्यता।	DEMO-AUTH-003.
एसेट और संस्करण	एप्लिकेशन, वातावरण और कॉन्फ़िगरेशन।	DEMO पोर्टल v2.4, परीक्षण वातावरण।
रोत	कौन-सा नियंत्रण किस चूनकी में विफल होता है।	किसी अन्य काल्पनिक उपयोगकर्ता की संवेदनशील उपलब्ध है।
प्रक्रिया	अनुमत चरण, अनुरोध और परामीटर।	सामान्य चूनकी और नियंत्रण संवेदनशील।
परिणाम	प्रतिक्रिया और आर्टिफ़ैक्ट, बिना रहस्य के।	कोड 200 और आंशिक संरचना।

फ़ील्ड	आवश्यक सामग्री	काल्पनिक उदाहरण
प्रमाण	प्रदर्शित परिणाम और दावेदार।	काल्पनिक ऑब्जेक्ट तक पहुँच, बाहर सामान्यीकरण नहीं।
सीमाएँ	क्या नहीं सीखा हुआ और क्या।	वास्तविक दस्तावेज़ नहीं देखे गए।
पारेषण	परिवर्तन, मालिक और प्रावीनकता।	सपर-साइड प्राधिकरण सत्यापन।
पुनःपरीक्षण	पारंपरिकता, तिथि और परिणाम।	यहाँ पथ और भूमिका, साथ में रिग्रेशन परीक्षण।

A.3 पुनःपरीक्षण रिपोर्ट

पुनर्मा रिकॉर्ड

मूल निष्कर्ष: [ID, प्रमाण और तिथि]
लागू परिवर्तन: [कॉन्फ़िगरेशन, संस्करण, मालिक]
पुनःपरीक्षण की तिथि और समय क्षेत्र: [यथावत]
समकक्ष परिस्थितियाँ: [भूमिका, ऑब्जेक्ट, पैरामीटर]
मूल परीक्षण दोहराने का परिणाम: [देखा गया]
रिग्रेशन परीक्षण: [वैध फ़ंक्शन]
अतिरिक्त कवरेज: [पथ या एसेट]
स्थिति: [सही किया गया, आंशिक, शमन किया गया, स्वीकार किया गया, खुला]
अवशिष्ट जोखिम और सीमाएँ: [विवरण]
अगली समीक्षा: [तिथि और उत्तरदायी व्यक्ति]
परिशिष्ट: [आउटपुट, लॉग और मैनिफ़ेस्ट]

परिशिष्ट B. कानूनी ढाँचा और अंतिम जाँच

प्राधिकरण पहली आवश्यकता है; इलेक्ट्रॉनिक प्रमाण के लिए पद्धति, अट्रिब्यूशन, अखंडता और सुलभता आवश्यक है। मेक्सिको में लागू CNBV प्रावधानों के तहत क्रेडिट संस्थान सुरक्षा समीक्षाओं और विशिष्ट अभिलेख-पालन के अधीन हैं, जिनमें अपने दायरे में अनुच्छेद 316 Bis 17 के अंतर्गत कम से कम वार्षिक समीक्षा शामिल है। पेरू और अर्जेंटीना में क्षेत्र-विशिष्ट प्रबंधन और प्रतिक्रिया आवश्यकताएँ हैं; स्पेन भुगतान और जोखिम में अंतर करता है। इन दायित्वों को हर संगठन पर एक समान लागू नहीं करना चाहिए।[3][4][5][6][7][8]

[3] क्रेडिट संस्थानों पर लागू सामान्य प्रावधान, अनुच्छेद 316 Bis, 316 Bis 1 और 316 Bis 10 से 17: अभिलेख, एन्क्रिप्शन, पहुँच, घटनाएँ, समस्याएँ, कार्यवाही-लॉग और समीक्षाएँ। आधिकारिक ऑनलाइन स्रोत

[4] पेरू. SBS 504-2021, अनुच्छेद 12.6.g, 15 और 17.3–17.4: संरक्षण, रिपोर्टिंग और फोरेंसिक विश्लेषण; नामांकन, प्रमाणीकरण और लेनदेन के लॉग। आधिकारिक ऑनलाइन स्रोत

[5] अर्जेंटीना. BCRA Comunicación A 8280: साइबर घटनाओं से प्रतिक्रिया और पुनर्प्राप्ति; रोकथाम, पुनर्प्राप्ति और समाधान के बाद पांच कैलेंडर दिनों के भीतर अंतिम रिपोर्ट। आधिकारिक ऑनलाइन स्रोत

[6] स्पेन. रॉयल डिक्री-लॉ 19/2018, अनुच्छेद 45, 66 और 67: अनधिकृत लेनदेन की प्रतिपूर्ति, जोखिम प्रबंधन और गंभीर घटनाओं की तत्काल सूचना। आधिकारिक ऑनलाइन स्रोत

[7] मेक्सिको की वाणिज्य संहिता, अनुच्छेद 89–94 और 1205: तटस्थता, प्रेषक से संबद्धता, लिखित रूप, मूल, अखंडता, सुलभता और डेटा संदेशों की स्वीकार्यता। आधिकारिक संकलन। आधिकारिक ऑनलाइन स्रोत

[8] राष्ट्रीय नागरिक और पारिवारिक प्रक्रिया संहिता, अनुच्छेद 348–350। 15-01-2026 के संशोधन सहित संकलन। इसका लागू होना क्रमिक है और आधिकारिक घोषणाओं पर निर्भर करता है। आधिकारिक ऑनलाइन स्रोत

कोलंबिया, इक्वाडोर, चिली और स्पेन में इलेक्ट्रॉनिक दस्तावेज़, हस्ताक्षर और संरक्षण के नियम प्रमाण की संरचना में मदद करते हैं; ये अपने आप घुसपैठ परीक्षण का प्राधिकरण नहीं देते। डेटा संरक्षण यह सीमित करता है कि क्या कैप्चर और साझा किया जा सकता है, भले उद्देश्य कमज़ोरी दिखाना हो।[9][10][11][12][13][14]

निष्कर्ष	स्वीकृति का प्रश्न
प्राधिकरण	क्या एसेट, तकनीक, डेटा, परीक्षण-विंडो और रोकने की सीमाएँ स्वीकृत हैं?
सुरक्षा	क्या परीक्षण नुकसान और अनावश्यक एक्सपोज़र से बचता है?
पीवी	क्या उपकरणों, सत्यापनों और आउटपुट को सत्यापित किया गया था?
निष्कर्ष	क्या एसेट, प्रक्रिया, परिणाम और प्रमाण ट्रेस करने योग्य हैं?
सुधार	क्या परिवर्तन और फॉलो-अप दस्तावेज़ित हैं?
पुनःपरीक्षण	क्या समान परिस्थितियों और रिग्रेशन का जोखिम है?
निष्कर्ष	क्या अवशिष्ट जोखिम और सीमाएँ छिपाई नहीं गई हैं?

समापन

सबसे अच्छा परीक्षण वह नहीं जो सबसे अधिक पहुँच दिखाए, बल्कि वह जो पर्याप्त प्रमाण के साथ जोखिम घटाए और दूसरी घटना पैदा न करे।

[9] चिली. इलेक्ट्रॉनिक दस्तावेज़ों और इलेक्ट्रॉनिक हस्ताक्षर संबंधी कानून 19.799, अनुच्छेद 1–5: समकक्षता, लिखित रूप, साधारण/उन्नत हस्ताक्षर, तिथि और प्रमाणीय मूल्य। आधिकारिक ऑनलाइन स्रोत

[10] कोलंबिया. 1999 का कानून 527, अनुच्छेद 5–13, 16–25 और 28: डेटा संदेश, लिखित रूप, मूल, अखंडता, स्वीकार्यता, संरक्षण, भेजना, प्राप्ति और डिजिटल हस्ताक्षर। आधिकारिक ऑनलाइन स्रोत

[11] इक्वाडोर. इलेक्ट्रॉनिक वाणिज्य, इलेक्ट्रॉनिक हस्ताक्षर और डेटा संदेश कानून, कानून 67, अनुच्छेद 2, 6–8, 10–16: समकक्षता, लिखित रूप, मूल, संरक्षण, उद्गम, भेजना, प्राप्ति और इलेक्ट्रॉनिक हस्ताक्षर। आधिकारिक ऑनलाइन स्रोत

[12] विनियमन (UE) 910/2014 eIDAS, अनुच्छेद 25–26 और 46: प्रारूप के कारण इलेक्ट्रॉनिक हस्ताक्षरों और दस्तावेज़ों से भेदभाव न करना, उन्नत इलेक्ट्रॉनिक हस्ताक्षर और क्वालिफ़ाइड इलेक्ट्रॉनिक हस्ताक्षर के प्रभाव। आधिकारिक ऑनलाइन स्रोत

[13] मेक्सिको. निजी क्षेत्र के व्यक्तियों के पास मौजूद व्यक्तिगत डेटा के संरक्षण संबंधी संघीय कानून, 20-03-2025 को प्रकाशित पाठ और 14-11-2025 का संशोधन। अनुच्छेद 5–9, 18–20 और 31: सिद्धांत, सुरक्षा, गोपनीयता, उल्लंघन और अधिकारों का निपटान। वर्तमान संघीय प्राधिकरण Secretaría Anticorrupción y Buen Gobierno है। आधिकारिक ऑनलाइन स्रोत

[14] यूरोपीय संघ. विनियमन (UE) 2016/679, अनुच्छेद 5, 25, 28 और 32–34: सिद्धांत, डिज़ाइन से सुरक्षा, प्रोसेसर, सुरक्षा और सुरक्षा उल्लंघनों की अधिसूचना/संचार। स्पेन में लागू राष्ट्रीय और क्षेत्रगत कानून की भी समीक्षा आवश्यक है। आधिकारिक ऑनलाइन स्रोत