



RVU / PRACTICAL RESOURCES

THE FIELD KIT

بداية أوضح وشغل مرتب

ثلاثة أدلة عملية بالعربي والإنجليزي مع أوراق عمل ترتب بيها فهمك واختبارك وتقريرك

ARABIC / 01

قالب تقرير أمني

ARABIC / 02

قائمة لفهم ال Target

ARABIC / 03

تجهيزك قبل الكامب

ENGLISH / 01

Security report playbook

ENGLISH / 02

Target research fieldnotes

ENGLISH / 03

Camp readiness checklist



SECURITY REPORT PLAYBOOK

01

قالب تقرير أمني

اختبار واضح ودليل يقدر غيرك يعيده

قالب كتابة ومراجعة املأ الأقسام بأدلة اختبارك الفعلي واحذف أي قسم غير مناسب المثال أدناه تعليمي وليس تقريراً عن ثغرة في خدمة حقيقية

03

اكتب

خلي غيرك يقدر يعيد النتيجة

02

اثبت

اربط كل خطوة بدليل من الاختبار

01

افهم

حدد المتوقع والفرق اللي لاحظته



اكتب تقرير يقدر غيرك يراجعه

رتب السلوك والخطوات والأثر وراجع دليلك قبل الإرسال

01 عنوان يصف السلوك والأثر

اكتب نوع الخلل + الوظيفة المتأثرة + الأثر المثبت

مثال للصياغة غياب فحص ملكية الطلب يسمح لحساب اختباري بعرض طلب حساب اختباري آخر

02 ملخص

اذكر السلوك الطبيعي والسلوك الذي لاحظته والشروط اللازمة وضح هل يتطلب حساباً أو دوراً معيناً

03 النطاق وبيئة الاختبار

- حدد الأصل والمسار والطريقة HTTP method والدور الذي استخدمته
- سجل وقت الاختبار ونسخة التطبيق إن كانت معروفة
- استخدم أسماء مثل Account A و Account B للحسابات التي تملكها
- احذف Cookies و Tokens والبيانات الشخصية من النسخة المعدة للمشاركة

04 خطوات إعادة الاختبار

- 1 جهز الحسابات والموارد المطلوبة داخل النطاق المصرح به
- 2 نفذ العملية الطبيعية من صاحب المورد وسجل الطلب المرجعي Baseline
- 3 غير متغيراً واحداً من جلسة الحساب الآخر مع توضيح المورد المطلوب
- 4 قارن النتيجة المتوقعة بالنتيجة الفعلية
- 5 تحقق من البيانات أو الحالة المحفوظة على السيرفر HTTP 200 وحده لا يثبت الخلل



الدليل والأثر والمراجعة

رتب السلوك والخطوات والأثر وراجع دليلك قبل الإرسال

05 الأدلة

لكل خطوة الطلب المهم الجزء الدال من الاستجابة والحساب المستخدم وضح الربط بين معرف المورد وصاحبه استخدم صوراً واضحة ومقطعا قصيرا عند الحاجة ولا تجعل الفيديو بديلا للخطوات المكتوبة

06 الأثر وحدود الاستنتاج

اذكر ما أثبتته تحديدا قراءة تعديل تنفيذ إجراء أو تغيير حالة فرق بين الدليل والاحتمال لا تستنتج الوصول لكل المستخدمين من تجربة محدودة ولا تضع رقم خسائر بلا دليل

07 توصية معالجة

اربط التوصية بسبب الخلل في مثال ملكية الطلب تحقق على السيرفر من صلاحية المستخدم على المورد عند كل عملية حساسة مع اختبارات تمنع الرجوع للخلل

08 مراجعة قبل الإرسال

- الهدف والاختبار داخل النطاق
- الخطوات قابلة للتكرار من شخص آخر
- النتيجة المتوقعة والفعلية واضحتان
- الأسرار والبيانات الخاصة محذوفة من النسخة المشتركة
- الأثر مرتبط بالأدلة والتقييم لا يتجاوز ما أثبتته
- العنوان والملخص لا يكرران نصا عاما لا يصف الحالة



من الاختبار لمسودة قابلة للإرسال

رتب السلوك والخطوات والأثر وراجع دليلك قبل الإرسال

الحسابات والموارد

Account A / Account B / Owner

الأصل والمسار

العنوان والملخص

الخلل + الوظيفة + الأثر المثبت + الشروط

خطوات إعادة الاختبار

التجهيز ثم Baseline ثم التغيير ثم النتيجة

الأثر وحدود الدليل

المتوقع والفعلي

الأدلة وتوصية المعالجة

اربط المرفقات بالخطوات وحدد سبب الخلل

مراجعة أخيرة

شخص تاني يقدر يعيد الاختبار؟ الأسرار محذوفة؟ الأثر على قد الي أثبتته؟ HTTP 200 لوحده مش دليل على ثغرة



TARGET RESEARCH FIELDNOTES

02

قائمة لفهم ال Target

افهم التطبيق قبل ما تزود الأدوات

استخدم القائمة لبناء صورة واضحة عن التطبيق قبل زيادة الأدوات الناتج المطلوب خريطة صغيرة +
أسئلة مرتبة + دليل لكل اختبار

03

رتب الأسئلة

فرضية واضحة ونتيجة تقدر تتحقق
منها

02

ارسم الخريطة

وظائف وطلبات وأدوار وموارد

01

حدد الحدود

الأصول والحسابات وقواعد الاختبار



خمس خطوات لصورة أوضح

خريطة صغيرة وأسئلة مرتبة ودليل مطلوب لكل اختبار

01 حدود الشغل

- دون الأصول المسموحة والاستثناءات وقواعد الحسابات والطلبات
- تأكد أن أي نطاق أو رابط جديد داخل النطاق قبل التفاعل معه
- حدد حسابات الاختبار التي تملكها والأدوار المتاحة

02 الاستخدام الطبيعي

- جرب الوظائف الأساسية كما يفعل المستخدم إنشاء عرض تعديل إلغاء
- تابع الطلبات والاستجابات في Burp Suite
- حدد أين تخزين الجلسة وكيف تتغير أثناء الدخول والخروج
- ارسم خطوات ال Workflow والحالات المسموحة للانتقال بينها

03 خريطة التطبيق

- أنشئ جدولاً بالأعمدة الوظيفة | المسار | طريقة الطلب | الدور | المورد | الأثر المحتمل | ملاحظات
- اجمع المسارات المرتبطة بالوظائف المهمة من حركة التطبيق وال JavaScript والتوثيق المتاح
- اربط كل معرف بالموارد وصاحبه
- دون الوظائف الحساسة مثل استرجاع الحساب وتغيير البريد وإدارة الأدوار والدفع
- اكتب ما لا تفهمه بدل افتراضه



من الخريطة لفرضية اختبار

خريطة صغيرة وأسئلة مرتبة ودليل مطلوب لكل اختبار

04 فرضيات قابلة للاختبار

- ☐ هل يفحص الدور وملكية المورد في كل خطوة؟
- ☐ هل يؤكد السيرفر السعر والكمية والحالة بنفسه؟
- ☐ هل يتغير السلوك بين الواجهة ومسار API المقابل؟
- ☐ هل يمكن الانتقال لحالة قبل استكمال شروطها؟
- ☐ لكل فرضية Baseline تغيير واحد نتيجة متوقعة ودليل مطلوب

05 الأولوية والمراجعة

- ☐ ابدأ بالوظائف الحساسة والأسئلة التي تملك حسابات وموارد مناسبة للتحقق منها
 - ☐ سجل نتائج الاختبارات السلبية أيضا
 - ☐ ميز بين أثر حقيقي على السيرفر وتغيير محلي في الواجهة
 - ☐ احتفظ بخطوة تالية واضحة قبل التوقف
- وجود أدوات أكثر لا يعني خريطة أوضح قياس التقدم هل تعرف ماذا تختبر ولماذا وما الدليل الذي سيؤكد النتيجة؟



ورقة شغل لـ Target

خريطة صغيرة وأسئلة مرتبة ودليل مطلوب لكل اختبار

الحسابات والأدوار

الأصل وحدود الشغل

خريطة صغيرة للتطبيق

الوظيفة والمسار	الدور والموارد	السؤال أو الملاحظة

فرضية واحدة نبدأ بها

القاعدة المتوقعة + الافتراض الي محتاج اختبار

النتيجة والدليل المطلوب

Baseline والتغيير الواحد

الملاحظات والخطوة التالية

إيه الي اتأكد وإيه الي لسه محتاج دليل

قبل ما تزود أدوات

تقدر تشرح هتختبر إيه وليه وإيه النتيجة الي تثبت الفرضية أو ترفضها؟ لو لأ ارجع للخريطة



CAMP READY CHECKLIST

03

تجهيزك قبل الكامب

جهز وقتك وأدواتك وتعالى بمحاولة

قائمة للاستعداد وليست اختبار قبول لو نقطة ناقصة جهزها أو ناقشها معايا في الانترفيو

03

نظم التطبيق

وقت أسبوعي وملاحظات وأسئلة واضحة

02

جهز البيئة

جهاز واتصال وصوت وأدوات شغالة

01

راجع الأساسيات

ويب وحسابات وطلبات وتجربة بالبرب



ابدأ وانت مجهز الأساسيات

قائمة تساعدك تبدأ من نقطة واضحة وليست اختبار قبول

01 الأساسيات

- أقدر أشرح الفرق بين Request و Response
- أعرف وظيفة URL و Method و Headers و Body و Status code
- فاهم فكرة الحساب والجلسة والفرق بين الدخول والصلاحيات
- اشتغلت بالبرب داخل بيئة تدريب
- أعرف أتحرك بين الملفات والمجلدات وأشغل أمرا بسيطا في Terminal

02 الجهاز والاتصال

- كمبيوتر مناسب شاحن وإنترنت ثابت
- Burp Suite ومتصفح تجريبي جاهزان
- Discord يعمل والصوت واضح
- مساحة لحفظ الملاحظات والتسجيلات والملفات التدريبية عند الحاجة
- أختبر مشاركة الشاشة قبل أول جلسة
- أراجع تعليمات RVU Commerce في مستودعه قبل التثبيت وأتبع متطلبات النسخة المستخدمة في الكامب



نظم وقتك ومحاولاتك

قائمة تساعدك تبدأ من نقطة واضحة وليست اختبار قبول

03 الوقت

- راجع مواعيد الاثنين والخميس ٧:٣٠-١٠:٣٠ مساء بتوقيت مصر
- خصص 5 ل 7 ساعات تطبيق أسبوعيا بجانب السيشنز
- احتفظ بوقت لتجميع الأسئلة قبل المتابعة الفردية كل أسبوعين

04 طريقة توثيق المحاولة

اكتب لكل محاولة كنت متوقع إليه؟ غيرت إليه؟ حصل إليه فعلا؟ إليه الدليل؟ إليه الي مش واضح؟ إليه الخطوة التالية؟

05 قبل الانتريفيو

جهز وصفا مختصرا لمستواك مثلا لمحاولة توقفت فيها هدفك من الكامب والوقت المتاح مش محتاج تحفظ إجابات المطلوب نفهم نقطة البداية



خطتك لأول أسبوع

قائمة تساعدك تبدأ من نقطة واضحة وليست اختبار قبول

الحاجة الي هجتها

أداة أو أساس ناقص خطوة لتجهيزه

مستواي دلوقتي

إيه الي فاهمه وجربته بإيدي

وقت التطبيق الي محافظ عليه

اليوم	الوقت	التطبيق أو المراجعة

محاولة أقدر أناقشها

التوقع / التغيير / الي حصل / الدليل

الخطوة الجاية

السؤال الي محتاج مساعدة فيه

وثق كل محاولة

كنت متوقع إيه؟ غيرت إيه؟ حصل إيه فعلا؟ إيه الدليل؟ إيه الي مش واضح؟ وإيه الخطوة الي بعدها؟



01 / RVU PRACTICAL RESOURCES

SECURITY REPORT PLAYBOOK

Security report playbook

A clear test. Evidence others can reproduce.

Use your actual test evidence to complete each section and remove irrelevant sections. The example is educational, not a claim about a real service.

01

Understand

Identify expected and observed behavior

02

Verify

Connect each claim to test evidence

03

Write

Make the result reproducible



01 / METHOD / REFERENCE

Write a report others can review

Organize behavior, steps and impact, then review your evidence

01 Title

Describe the flaw, affected feature and demonstrated impact.

Example wording: Missing order ownership validation allows one test account to view another test account's order.

02 Summary

Describe expected behavior, observed behavior and prerequisites, including the account role required.

03 Scope and environment

Identify the asset, endpoint, HTTP method, role, test time and application version if known. Label accounts you own Account A and Account B. Remove cookies, tokens and personal information from shared evidence.

04 Reproduction steps

- 1 Prepare the required accounts and resources in the authorized environment.
- 2 Perform the normal action as the resource owner and capture a baseline.
- 3 Change one variable using the other account's session, identifying the requested resource.
- 4 Compare the expected and actual outcomes.
- 5 Verify returned data or stored server-side state; HTTP 200 alone proves nothing.



Evidence, impact and final review

Organize behavior, steps and impact, then review your evidence

05 Evidence

For each relevant step, include the request, meaningful response excerpt and acting account. Establish resource ownership. Add a readable screenshot or short video when useful; video should complement written reproduction steps.

06 Impact and limits

State the access or state change you demonstrated. Separate evidence from hypotheses. Do not generalize a limited test to all users or invent financial loss.

07 Remediation

Address the underlying cause. For the order ownership example: validate server-side permission for the resource on every sensitive action and add regression coverage.

08 Before submitting

- ☐ The asset and testing are in scope.
- ☐ Another person can reproduce the steps.
- ☐ Expected and actual outcomes are explicit.
- ☐ Secrets and private data are removed from shared evidence.
- ☐ Impact and severity follow the evidence.
- ☐ The title and summary describe this specific finding.



01 / PRACTICE / WORKSHEET

From a test to a reviewable draft

Organize behavior, steps and impact, then review your evidence

Asset and endpoint

Accounts and resources

Account A / Account B / Owner

Title and summary

Flaw + affected feature + demonstrated impact + prerequisites

Reproduction steps

Setup, baseline, controlled change, verified result

Expected / actual

Impact and evidence limits

Evidence and remediation

Connect evidence to steps and address the underlying cause

Final review

Can someone else reproduce it? Have you removed secrets? Does impact follow the evidence? HTTP 200 alone does not prove a flaw.



02 / RVU PRACTICAL RESOURCES

TARGET RESEARCH FIELDNOTES

Target research fieldnotes

Understand the application before adding tools.

Build a small map, prioritized questions and evidence for each test before expanding your toolchain.

01

Set boundaries

Assets, accounts and engagement rules

02

Map the app

Features, requests, roles and resources

03

Prioritize

A clear hypothesis and a verifiable outcome



Five steps to a clearer target

A small map, prioritized questions and evidence for each test

01 Boundaries

- ☐ Record allowed assets, exclusions, account rules and request limits.
- ☐ Verify newly discovered assets are in scope before interacting.
- ☐ Identify your test accounts and available roles.

02 Normal behavior

- ☐ Use core features: create, read, update and cancel.
- ☐ Follow requests and responses in Burp Suite.
- ☐ Identify session storage and changes during login and logout.
- ☐ Map workflow steps and allowed state transitions.

03 Application map

Create columns for: feature, path, method, role, resource, potential impact and notes.

- ☐ Map relevant paths from application traffic, JavaScript and available documentation.
- ☐ Link identifiers to resources and owners.
- ☐ Identify sensitive features such as recovery, email changes, roles and payments.
- ☐ Record uncertainties instead of assuming answers.



02 / REVIEW / NEXT STEPS

From a map to a testable hypothesis

A small map, prioritized questions and evidence for each test

04 Testable hypotheses

- ☐ Are roles and resource ownership checked at each step?
- ☐ Does the server validate prices, quantities and state?
- ☐ Do the UI and corresponding API enforce the same rules?
- ☐ Can a state transition happen before its prerequisites?
- ☐ Give each test a baseline, one controlled change, expected outcome and evidence requirement.

05 Prioritize and review

- ☐ Start with sensitive features you can verify using appropriate test accounts and resources.
- ☐ Record negative results too.
- ☐ Distinguish server-side impact from local interface changes.
- ☐ Leave yourself a clear next step before stopping.

Measure progress by whether you can explain what you are testing, why it matters and which evidence would confirm the result.



02 / PRACTICE / WORKSHEET

Your target research worksheet

A small map, prioritized questions and evidence for each test

Asset and boundaries

Accounts and roles

A small application map

Feature / endpoint	Role / resource	Question / observation

One hypothesis to start with

Expected rule + the assumption to test

Baseline and controlled change

Expected outcome and evidence

Notes and next step

What is confirmed and what still needs evidence?

Before adding tools

Can you explain what you will test, why it matters and which result would support or reject the hypothesis? If not, return to the map.



CAMP READY CHECKLIST

Camp readiness checklist

Prepare your time and tools. Bring an attempt.

A preparation checklist, not an admission test. Work on missing items or discuss them with me during the interview.

01

Review foundations

Web concepts and hands-on Burp use

02

Prepare your setup

Computer, connection, audio and tools

03

Plan your practice

Weekly time, useful notes and questions



03 / METHOD / REFERENCE

Arrive with the foundations ready

A checklist for a clearer starting point, not an admission test

01 Foundations

- ☐ Explain the difference between a request and a response.
- ☐ Understand URLs, methods, headers, bodies and status codes.
- ☐ Understand accounts, sessions, authentication and authorization.
- ☐ Intercept a request with Burp Suite in a training environment.
- ☐ Navigate files and folders and run a simple terminal command.

02 Setup

- ☐ Computer, charger and stable internet.
- ☐ Burp Suite and a testing browser ready.
- ☐ Working Discord access and clear audio.
- ☐ Space for notes, recordings and training files when needed.
- ☐ Screen sharing tested before the first session.
- ☐ Read RVU Commerce setup instructions in its repository and follow the version used in the camp.



Plan your time and document attempts

A checklist for a clearer starting point, not an admission test

03 Time

- ☐ Review the Monday and Thursday schedule: 7:30-10:30 PM, Cairo time.
- ☐ Set aside 5-7 practice hours weekly, in addition to live sessions.
- ☐ Collect questions for the private review every two weeks.

04 Document an attempt

Record: What did I expect? What did I change? What actually happened? What evidence supports it?
What remains unclear? What should I try next?

05 Before the interview

Prepare a short description of your level, one attempt where you got stuck, your goal and your available time. The purpose is to understand your starting point, not memorize answers.



03 / PRACTICE / WORKSHEET

Your first-week plan

A checklist for a clearer starting point, not an admission test

My starting point

What I understand and have tried myself

What I need to prepare

A missing tool or foundation and one practical step

Practice time I can protect

Day	Time	Practice / review

An attempt I can discuss

Expectation / controlled change / result / evidence

A question I need help with

My next step

Document each attempt

What did I expect? What did I change? What happened? What is the evidence? What remains unclear? What should I try next?