



TANNER TOBEY CONSULTING L.L.C.

Sample penetration test.

NOT A CLIENT · NOT A REAL TEST

This is the document. An owner can read the decision.
The person who fixes the system can read the evidence. I
write both.

Application test
Staging only
One high finding

Prepared by Tanner Tobey, CISSP
The person who would scope it
is the person who would test it
thtobey@tobeyconsulting.com

Read it in the order of the decision.

If you own the company, stop after the executive summary unless you want the detail. If you will make the change, the finding page is yours.

For the owner

You are paying for a judgment, not a pile of scanner rows. The summary says what is wrong, why it matters to the business, and what to do before anyone outside the company asks.

For the person who will fix it

You get the condition, the evidence, and the fix in that order. A real report names the real host. This one uses a made-up host so no one's system is in the sample.

Document control

Document	TTCL-SAMPLE-001
Status	Illustration. Published so a buyer can see the form.
Author	Tanner Tobey. I write the report. I do not hand it to a junior to sign.
Engagement shown	Application test. Staging only. Dates below are examples.
Distribution	In a real engagement, the named client and the people they invite to the readout. This file is public because it is a sample.

Harbor Supply is not a client. staging.example.test is not a real host. Nothing in these pages was found on a customer system.

One door was open. Close it before you brief anyone.

The staging admin page answered without asking who was calling. If that host can be reached, the admin page can be seen by someone who is not your employee.

Finding	Staging admin panel, no login. High.
This week	Put that page behind the same login as production. Confirm the host is not on the public internet.
Then	Decide if you want that one item retested. A retest is a separate, smaller quote. It is not inside this price.
Not this	Not a passing grade. Not an insurer's approval. Not a claim that the rest of the company is safe. Staging only. One window of time.

What high means

Critical means stop and fix before the next business day. High means fix before a customer, an insurer, or an auditor asks what you have done about access. Medium means schedule it. Low means write it down so it is not forgotten. This sample has one high finding and nothing critical.

The business sentence

You do not have a failed company. You have one staging door that does not ask for a name. Fix the door. Do not walk into a renewal meeting and discover it there.

I test what you name. Nothing else.

A real test does not start from a website form. It starts when a named person agrees, in writing, to the targets, the dates, what is out of bounds, and how to stop the work. The price is on that page before the first request is sent.

In scope	The staging application at staging.example.test, and the public marketing host named in the sample scope.
Out of scope	Production. The corporate network. Employee mail. Social engineering. Denial of service. Anything not named.
Window	Example only: three business days, dates agreed before testing. You know which days.
Authorization	A named owner. Written. Before testing. This sample has no signed page because there was no client.
Stop	If the client says stop, the test stops that day. Findings already confirmed stay in the report.

Rules I will not bend

I do not test a host because it looks interesting. I do not knock a system over to prove a point. I do not take the work outside the names on the scope, even if the next host would have been an easy finding. Easy and out of scope is still out of scope.

Manual. Aimed. Written down.

I do not hand you a scanner printout and call it a test. A scanner lists known issues. A test tries to use the ones that matter, then says which results change the business.

On a real engagement I look at the doors named in the scope and I try to open the ones that should have been locked. I record what answered. I stop at the proof. I do not wander into production because staging was quiet.

In this sample, the work was

1. Confirm the named staging host and the named marketing host, and ignore everything else.
2. Request the admin path on staging the way an outsider would, with no session.
3. Request the same path on the marketing host.
4. Confirm the customer login on staging still asked for a password.
5. Write the result in owner language and in operator language. Same finding. Two readers.

Denial of service was out of scope, so nothing was done to see if the service could be knocked down. Staff were not phished. Those are different jobs, and they were not this job.

A real method section names the build that was tested and the account, if any, the client provided. It does not include a recipe for breaking the next company.

The staging admin page did not ask who I was.

High.

I asked for the admin page on the staging host. It answered with the admin page. No login. No session. That is the whole finding.

If you own the company

Fix this before a customer, an insurer, or an auditor asks what you have done about access. Do not wait for the renewal meeting to be the moment you learn the staging door is open. Staging is still your system. "It is only staging" is not a control.

If you will make the change

Condition	GET of the admin path on staging.example.test returned the admin page. No session cookie was sent.
Evidence	In a real report this row is the request and the response, with secrets removed, and the real host name. This sample refuses to invent a customer's hostname.
Impact	Anyone who can reach that host can see the admin page. What they can do after that depends on what the page allows. The test stopped at proof of access.
Fix	Put the host behind the same login as production. Then confirm it is not reachable from the public internet. Do those in that order.
Retest	Not included. One check of this item, after you say it is fixed. Separate quote.

I will not pad this page with ten low items so the report looks thick. One high finding is the report.

Two checks held. Then we talk.

Customer login

The staging login that customers use still asked for a password. It was not the open door.

Marketing host

The public marketing host named in the sample scope did not serve the admin page.

The readout

Thirty minutes. The owner and the person who will make the change. I walk the finding once. We leave with the order of work. I do not stay on as your IT department.

Limits

Point in time. Named hosts only. No promise that an insurer, a customer, or an auditor will accept the report. That decision is theirs. The report is written so they can make it. This file is an illustration. Harbor Supply is a name I made up.

I scoped the shape of this sample and I wrote every page. On a real engagement that is also true. If a sentence is unclear, that is on me.

Tanner Tobey

Owner, Tanner Tobey Consulting L.L.C.

thtobey@tobeyconsulting.com

South Florida. Remote nationwide.