

Forum: [Hack Forums](#)

Thread: [Bug Bounty Find a WAP time capsule with active CGI & TRACE](#)

onlineuser | D3RFER - October 22, 2025, 4:56 pm

For the beginners: example.com is a placeholder for the actual domain.

Hello there - small recon story from today.

So I was running my usual subdomain sweep on example.com and one of the results made me super curious - wap.example.com.

WAP? Really?

Like, the Nokia-era mobile web? Hmm. That seems off.

I pointed at <http://wap.example.com> (no HTTPS - more on that later) and then page served raw WML.

The kind of stuff we used before smartphones even existed.

Response headers showing legacy Apache/OpenSSL stack and WML content-type.

Naturally, I wanted to see if anything else from the old days was still alive.

So I peaked at /cgi-bin/ and it did not disappoint.

I hit /cgi-bin/test-cgi and got a 200 OK.

The server returned the actual source code of the CGI test script.

The active test-cgi script literally warning you not to use it in production.

The best part?

Right here in the source, this line jumped out at me:

“WARNING: This script echoes the server environment variables and therefore leaks information — so NEVER use it in a live server environment!”

Someone clearly didn't read the manual. ?

Just to be sure, I tried /cgi-bin/printenv, and yep, same deal.

It spits out environment variables and server info in plain text.

printenv endpoint confirming environment variable leakage

Then I checked the allowed HTTP methods, and there it was TRACE.

I tried it and the host echoed my custom header back. Classic misconfiguration (enabler for XST) right next to the CGI leaks.

Could be serious, but exploitation usually needs outdated clients/proxies or an XSS..

TRACE request echoing the injected header, confirms method is enabled.

At this point, the picture was pretty clear to me..

This wasn't some live production service. It's a literal digital fossil still running Apache 2.4.56 with OpenSSL 1.1.1k - EOL version.

My thoughts? Probably a completely forgotten legacy host, long outside their main Azure setup.

You can't make this stuff up. This is what's so great about bug bounty hunting, it's always exciting, because you literally never know what to expect.

This program does not pay out money, however - They do have a hall of fame, which is super cool, as I can add it to my CV, and I already found a low severity vulnerability same place back in May month.