

Forum:[Hack Forums](#)

Thread: [Pentesting company reported ruby code injection, but the server doesn't have ruby ins](#)

Fishsticks - March 1, 2019, 2:21 pm

Long story short, we received the pen test report today, and one of the "high risk" things we need to fix is ruby code injection, but the server doesn't have ruby installed. How can that be possible? Is this maybe a false positive or a bad test?

valetta - March 1, 2019, 2:42 pm

Who ran your pentest? Kinda unrelated

Fishsticks - March 1, 2019, 2:52 pm

(Mar 1, 2019 03:42 PM)valetta Wrote: [\[CITE\]](#) Who ran your pentest? Kinda unrelated
A company. Not gonna name specifics. But a legit registered infosec company from around here.

valetta - March 1, 2019, 2:58 pm

(Mar 1, 2019 03:52 PM)Fishsticks Wrote: [\[CITE\]](#) A company. Not gonna name specifics. But a legit registered infosec company from around here.

Well did they do a pentest or did they just run a VA and just call it a "pentest" ? Because automated scans aren't pentest and a lot of "legit" orgs don't even validate findings and just slap them on the report.

Maybe it's calling something that involves ruby that doesn't directly affect the assets = FP, but they slapped it on the report because they did a VA instead of a pentest.

Fishsticks - March 1, 2019, 3:02 pm

What is FP?

It was more of a VA/vulnerability scan using Burp suite, they claim to have found 4 possible attack vectors but in the end, security wasn't compromised and no data was leaked.

valetta - March 1, 2019, 5:39 pm

(Mar 1, 2019 04:02 PM)Fishsticks Wrote: [\[CITE\]](#) What is FP?

It was more of a VA/vulnerability scan using Burp suite, they claim to have found 4 possible attack vectors but in the end, security wasn't compromised and no data was leaked.

FP = False Positives

Yeah, pick who does your pentest properly, Burp scanner just scans and has tons of FP, it's hard to tell if they don't validate the findings.

They don't pursue those things. Sometimes, something that's marked as "low" or "medium" threat can also be leveraged to compromise a machine, so point is, don't just do a VA, validate and ask them to do manual testing.

Fishsticks - March 2, 2019, 1:29 am

They describe doing manual testing, but they were unable to use any of the vulnerabilities from the burp scanner to access data or compromise security. The ruby one strikes me as an obvious FP, but there are two more that also seem to be FP.

Sitrep - March 2, 2019, 10:51 am

This sure sounds like a scanner that left a false positive to a person with low experience in the subject. Don't pay that guy if you hired him.

Fishsticks - March 2, 2019, 11:32 am

We paid them \$1500, but we do know the tester used was a Junior guy. The dumb thing is this pentest(that has to be done by an external company) is standing in the way of \$1,000,000 in VC funds, so I'm kinda pissed off.

Sitrep - March 2, 2019, 1:09 pm

(Mar 2, 2019 12:32 PM)Fishsticks Wrote: [\[CITE\]](#) We paid them \$1500, but we do know the tester used was a Junior guy. The dumb thing is this pentest(that has to be done by an external company) is standing in the way of \$1,000,000 in VC funds, so I'm kinda pissed off.

Oh damn! I feel ya man... That's bad news for you.

valetta - March 3, 2019, 8:21 am

(Mar 2, 2019 12:32 PM)Fishsticks Wrote: [\[CITE\]](#) We paid them \$1500, but we do know the tester used was a Junior guy. The dumb thing is this pentest(that has to be done by an external company) is standing in the way of \$1,000,000 in VC funds, so I'm kinda pissed off.

Ok 1,000,000 is a bit too expensive for a webapp. We don't even charge that much LOL, never cheap up on a pentest. It's protecting you from losing money rather than earning you money, which is important.

Burp suite pro is \$400 for a year, so you could've ran that yourself on the website instead of paying \$1500 for the exact same thing, without proper validation.

Fishsticks - March 3, 2019, 1:27 pm

(Mar 3, 2019 09:21 AM)valetta Wrote: [\[CITE\]](#) Ok 1,000,000 is a bit too expensive for a webapp. We don't even charge that much LOL, never cheap up on a pentest. It's protecting you from losing money rather than earning you money, which is important.

Burp suite pro is \$400 for a year, so you could've ran that yourself on the website instead of paying \$1500 for the exact same thing, without proper validation.

We had to use an external company otherwise we could spoof our results. The VCs required it.

valetta - March 3, 2019, 7:21 pm

(Mar 3, 2019 02:27 PM)Fishsticks Wrote: [\[CITE\]](#) We had to use an external company otherwise we could spoof our results. The VCs required it.

Ah gotcha, yeah just something to keep in mind next time I guess! Good luck