

Forum:[Hack Forums](#)

Thread: [Pentest help with termux](#)

aktarburak - May 25, 2025, 1:04 pm

Hello, I have just joined you. I do not know much English. I am writing from the translation.

I want to scan a target website with an android phone without root and exploit the vulnerability I found

I don't know where to start. Your ideas are important to me. I want to know where to start researching.

DramaKing - May 25, 2025, 1:22 pm

Let me do it, and I'll explain everything to you. Someone who has no prior knowledge and attacks a live website could end up in quite some trouble.

Hmmm, usually one scans a target in order to find a vulnerability. You're using the past tense here.

aktarburak - May 26, 2025, 4:24 am

(May 25, 2025 01:22 PM)DramaKing Wrote: [\[CITE\]](#) Let me do it, and I'll explain everything to you. Someone who has no prior knowledge and attacks a live website could end up in quite some trouble.

Hmmm, usually one scans a target in order to find a vulnerability. You're using the past tense here. My intention is not to damage a live site and get myself into trouble.

I am questioning how far I can reach on my own with just the phone. I want to learn and be informed about this issue.

As far as I know, basic vulnerabilities and exploits can be done with Termux, but I don't know which tool and tool should I use most tools on this subject are from 2016 and are not up to date.

Can you give me a map of what I should do from scratch with which vehicle?

DramaKing - May 26, 2025, 4:38 am

(May 26, 2025 04:24 AM)aktarburak Wrote: [\[CITE\]](#) My intention is not to damage a live site and get myself into trouble.

I am questioning how far I can reach on my own with just the phone. I want to learn and be informed about this issue.

As far as I know, basic vulnerabilities and exploits can be done with Termux, but I don't know which tool and tool should I use most tools on this subject are from 2016 and are not up to date.

Can you give me a map of what I should do from scratch with which vehicle?

Hard to say. You're unlikely to make any sense of the results even if you do.

I would recommend this repo for Termux pentesting.

```
Code yes|apt install wget gnupg && \
mkdir -p $PREFIX/etc/apt/sources.list.d && \
wget
```

```
https://raw.githubusercontent.com/ivam3/termux-packages/gh-pages/ivam3-termux-packages.list -O \
$PREFIX/etc/apt/sources.list.d/ivam3-termux-packages.list && \
curl -fsSL
"https://raw.githubusercontent.com/ivam3/termux-packages/gh-pages/dists/stable/public_key.gpg" \
|gpg --dearmor|tee "$PREFIX/etc/apt/trusted.gpg.d/ivam3.gpg" >/dev/null && \
apt update
```