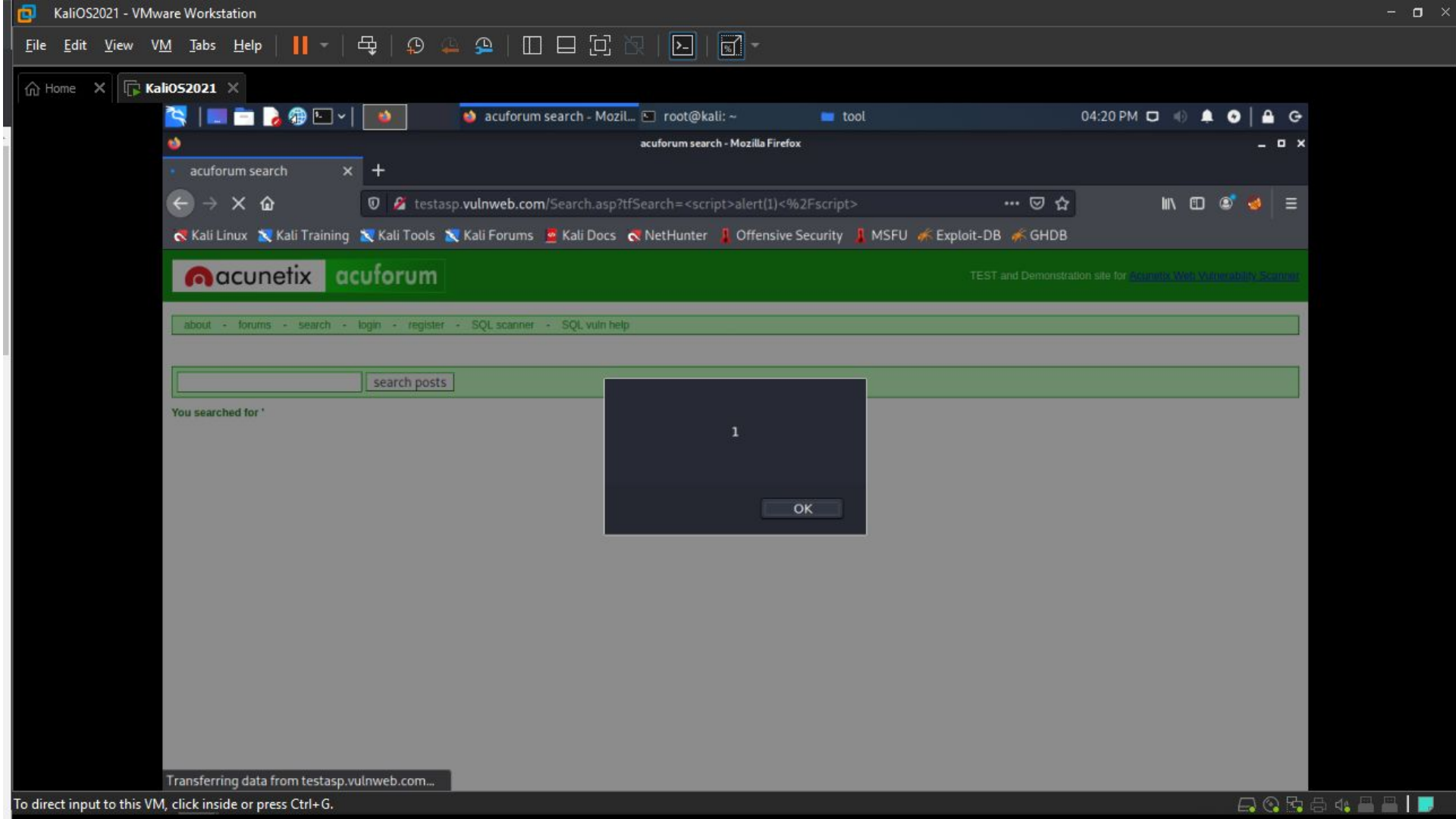
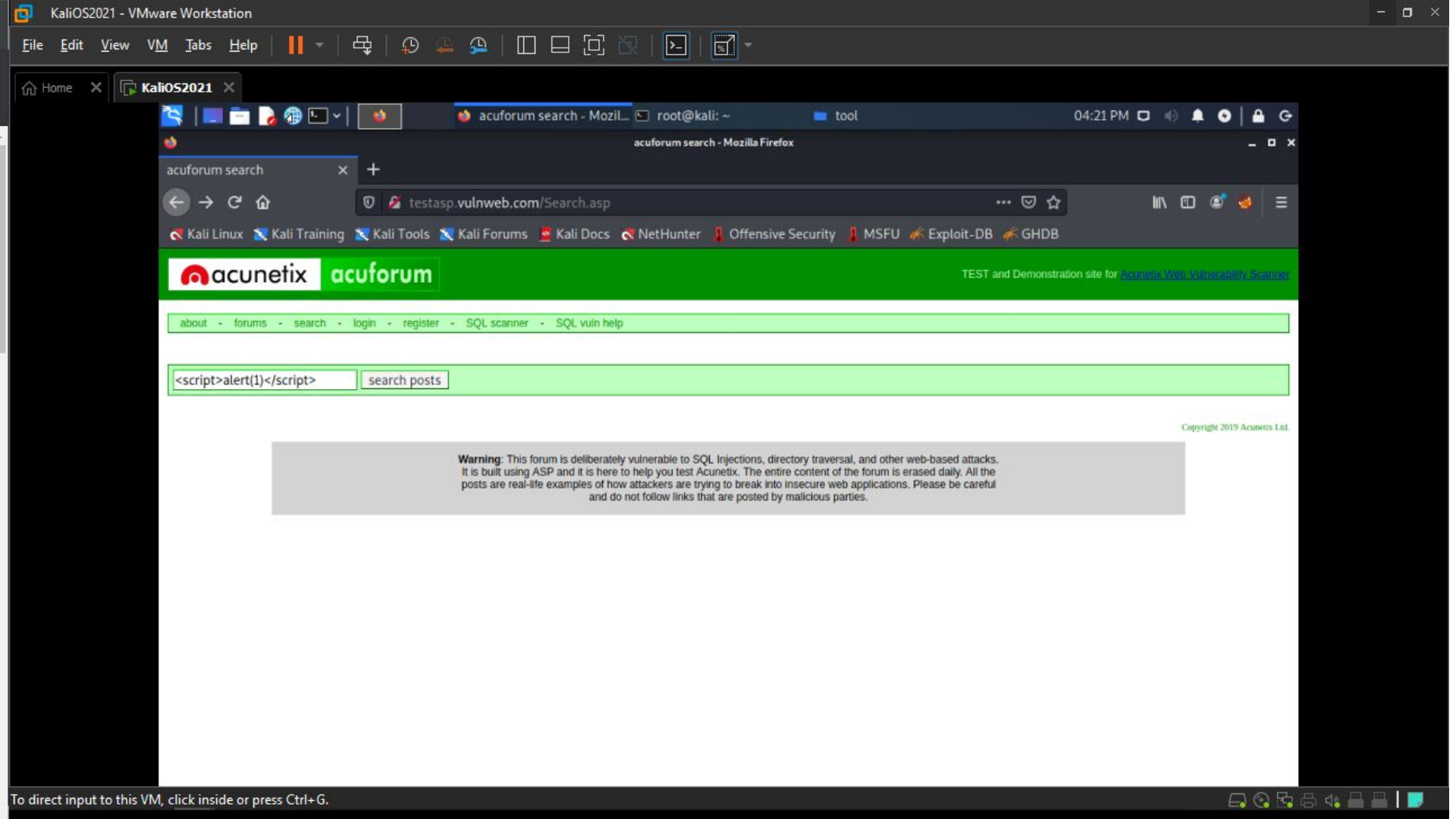
Task 3

Vulnweb


KaliOS2021 - VMware Workstation
File Edit View VM Tabs Help
Home
KaliOS2021
acuforum search - Mozil...
root@kali: ~
tool
04:20 PM
acuforum search - Mozilla Firefox
acuforum search
testasp.vulnweb.com/Search.asp?tfSearch=<script>alert(1)<%2Fscript>
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register - SQL scanner - SQL vuln help
search posts
You searched for '
1
OK
Transferring data from testasp.vulnweb.com...
To direct input to this VM, click inside or press Ctrl+G.


KaliOS2021 - VMware Workstation
File Edit View VM Tabs Help
Home
KaliOS2021
acuforum search - Mozil...
root@kali: ~
tool
04:21 PM
acuforum search - Mozilla Firefox
acuforum search
testasp.vulnweb.com/Search.asp
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register - SQL scanner - SQL vuln help
<script>alert(1)</script>
search posts
Copyright 2019 Acunetix Ltd.
Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.
To direct input to this VM, click inside or press Ctrl+G.

Report Title: Found Cross Site Scripting in http://testasp.vulnweb.com

Url>> http://testasp.vulnweb.com/Search.asp?tfSearch="><scRipt>alert(9)</scRipt>

Paraneter Type>>GET

Tools>>Linux 7.1, Wifi, Brup Suite

Description>> Cross Site Scripting in the url

Steps to reproduce>>
1)First of all visited http://testasp.vulnweb.com/
2)Burp Suite intruder detect some fault in http://testasp.vulnweb.com/Search.asp
3)Then we will use <script>alert(9)</script> in search bar or use the url directly to get the alert.

Impact>>1)Can steal User Data
2)Can steal money from User's Account
3) User will be prone to future phishing attack

PoC