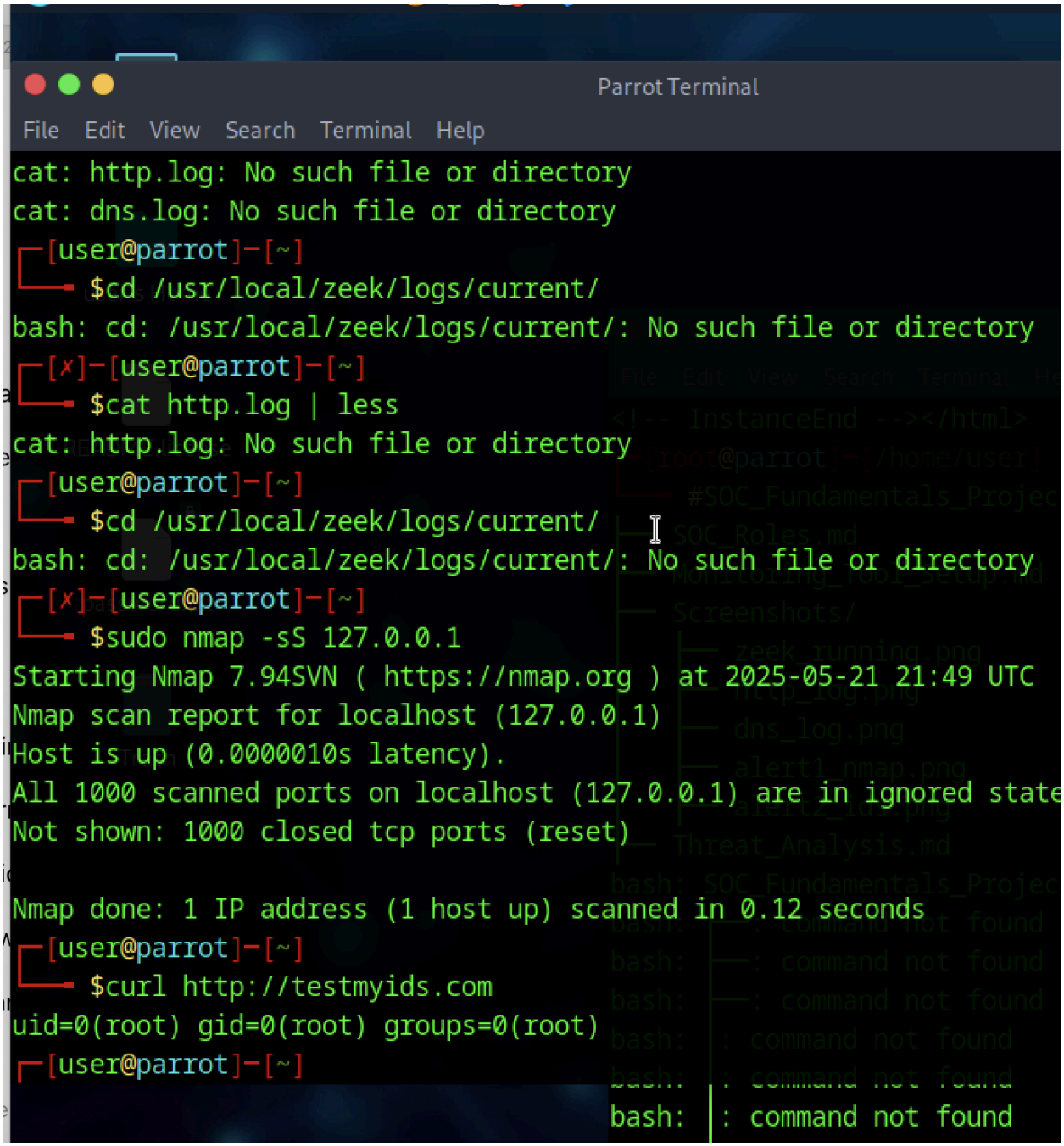
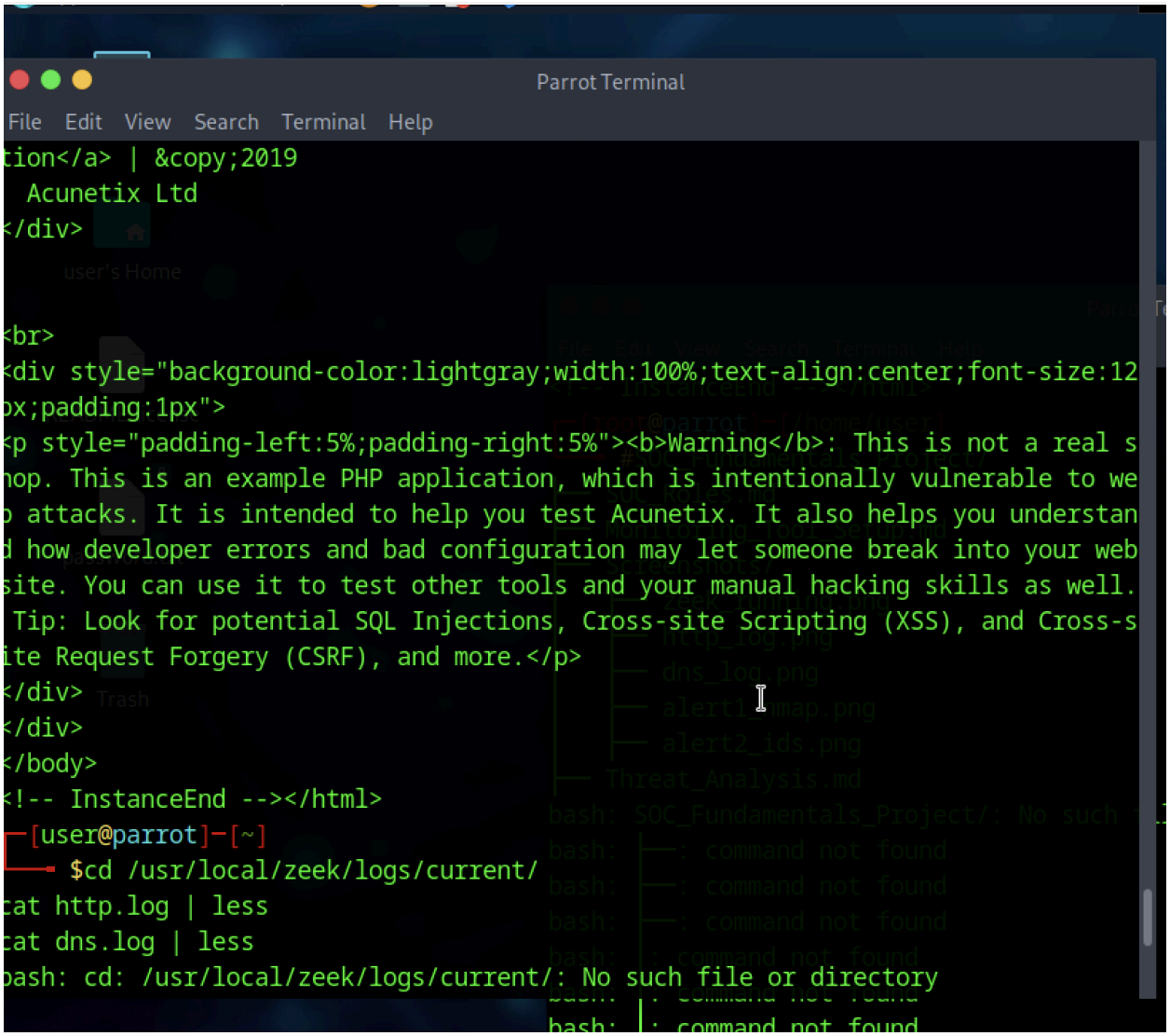
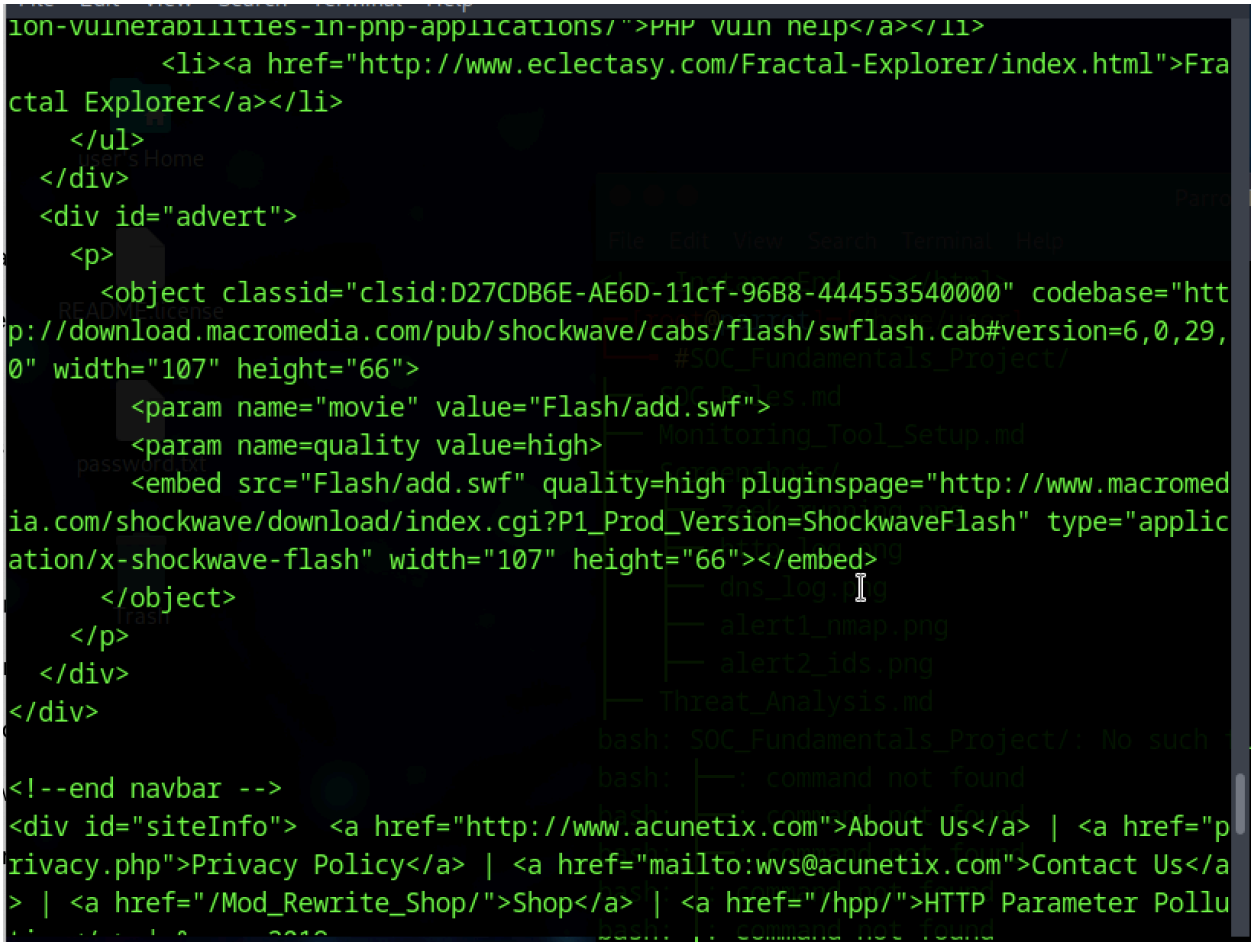

Parrot Terminal
File Edit View Search Terminal Help
cat: http.log: No such file or directory
cat: dns.log: No such file or directory
[user@parrot]-[~]
$cd /usr/local/zeek/logs/current/
bash: cd: /usr/local/zeek/logs/current/: No such file or directory
[✗]-[user@parrot]-[~]
$cat http.log | less
cat: http.log: No such file or directory
[user@parrot]-[~]
$cd /usr/local/zeek/logs/current/
bash: cd: /usr/local/zeek/logs/current/: No such file or directory
[✗]-[user@parrot]-[~]
$sudo nmap -sS 127.0.0.1
Starting Nmap 7.94SVN (https://nmap.org) at 2025-05-21 21:49 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored state
Not shown: 1000 closed tcp ports (reset)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
[user@parrot]-[~]
$curl http://testmyids.com
uid=0(root) gid=0(root) groups=0(root)
[user@parrot]-[~]
bash: : command not found


Parrot Terminal
File Edit View Search Terminal Help
tion | ©2019
Acunetix Ltd

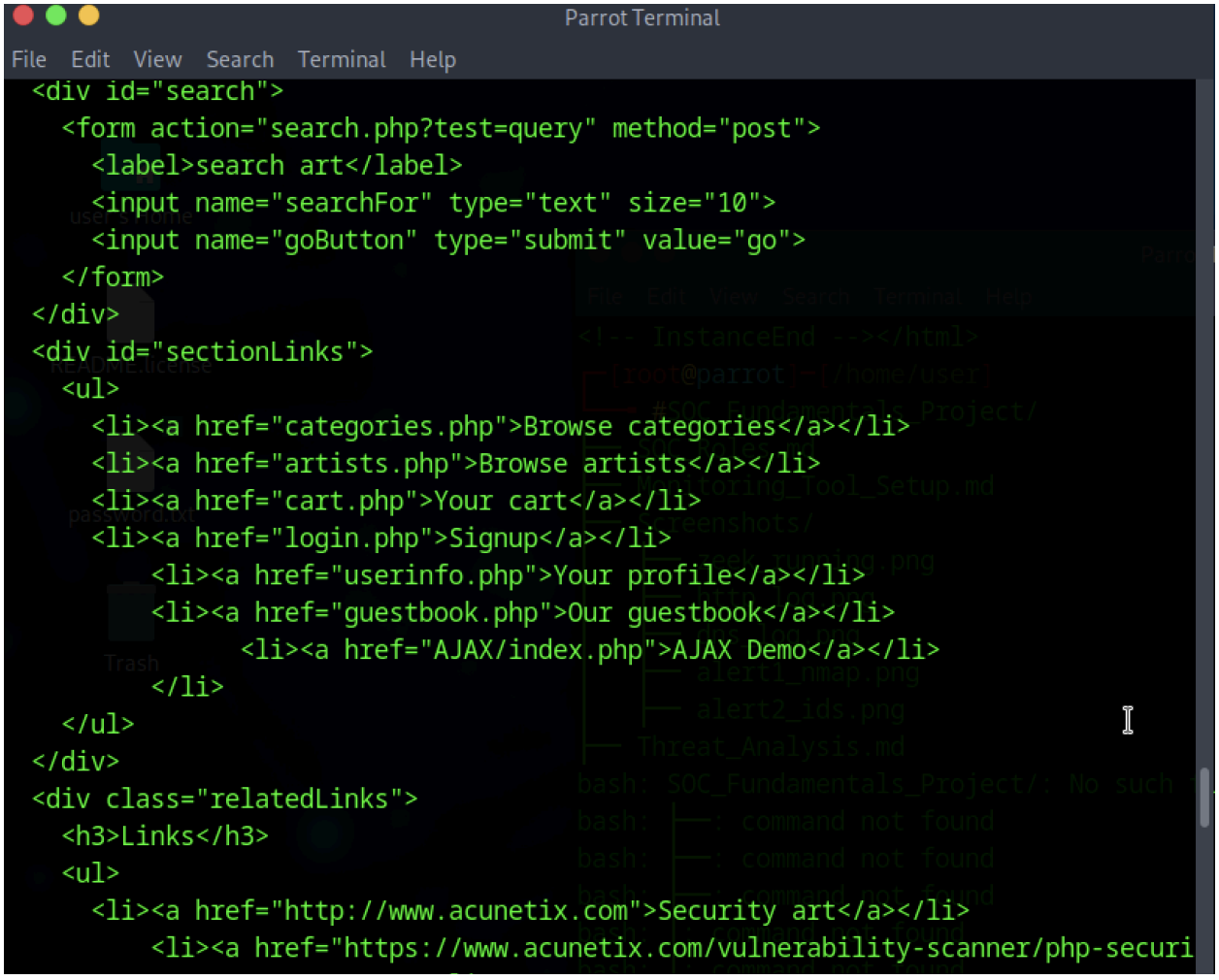
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12
px;padding:1px">
Warning: This is not a real s
hop. This is an example PHP application, which is intentionally vulnerable to we
b attacks. It is intended to help you test Acunetix. It also helps you understan
d how developer errors and bad configuration may let someone break into your web
site. You can use it to test other tools and your manual hacking skills as well.
Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-s
ite Request Forgery (CSRF), and more.

</body>
<!-- InstanceEnd --></html>
[user@parrot]-[~]
$cd /usr/local/zeek/logs/current/
cat http.log | less
cat dns.log | less
bash: cd: /usr/local/zeek/logs/current/: No such file or directory


ion-vulnerabilities-in-php-applications/">PHP Vuln help
Fra
ctal Explorer

<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="htt
p://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,
0" width="107" height="66">
<param name="movie" value="Flash/add.swf">
<param name=quality value=high>
<embed src="Flash/add.swf" quality=high pluginspage="http://www.macromed
ia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash" type="applic
ation/x-shockwave-flash" width="107" height="66"></embed>
</object>

<!--end navbar -->
 About Us | <a href="p
rivacy.php">Privacy Policy | Contact Us | Shop | HTTP Parameter Pollu

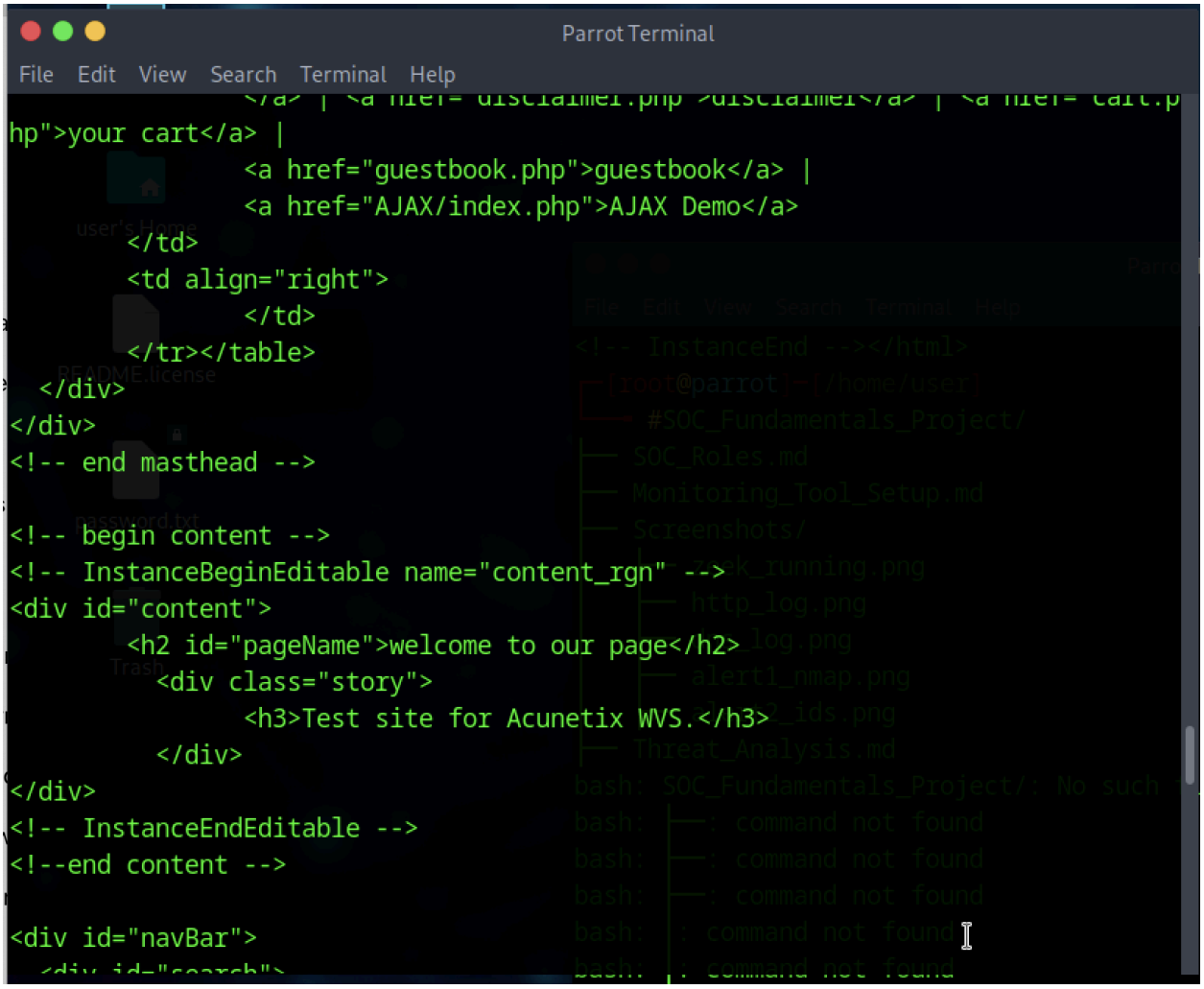

Parrot Terminal
File Edit View Search Terminal Help

<form action="search.php?test=query" method="post">
<label>search art</label>
<input name="searchFor" type="text" size="10">
<input name="goButton" type="submit" value="go">
</form>

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

<h3>Links</h3>

Security art
<a href="https://www.acunetix.com/vulnerability-scanner/php-securi


Parrot Terminal
File Edit View Search Terminal Help
hp">your cart |
guestbook |
AJAX Demo
</td>
<td align="right">
</td>
</tr></table>

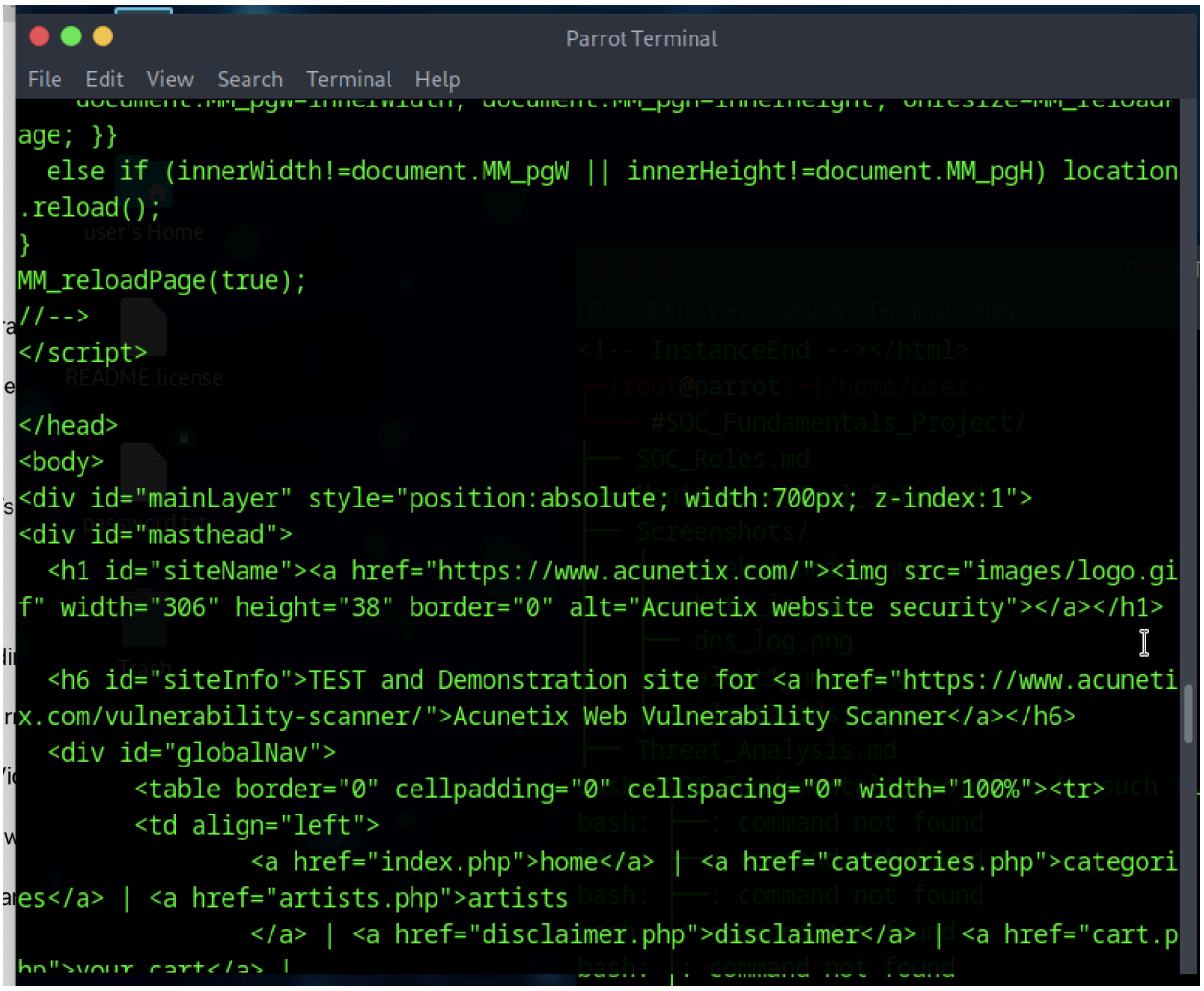
<!-- end masthead -->
<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->

<h2 id="pageName">welcome to our page</h2>

<h3>Test site for Acunetix WVS.</h3>

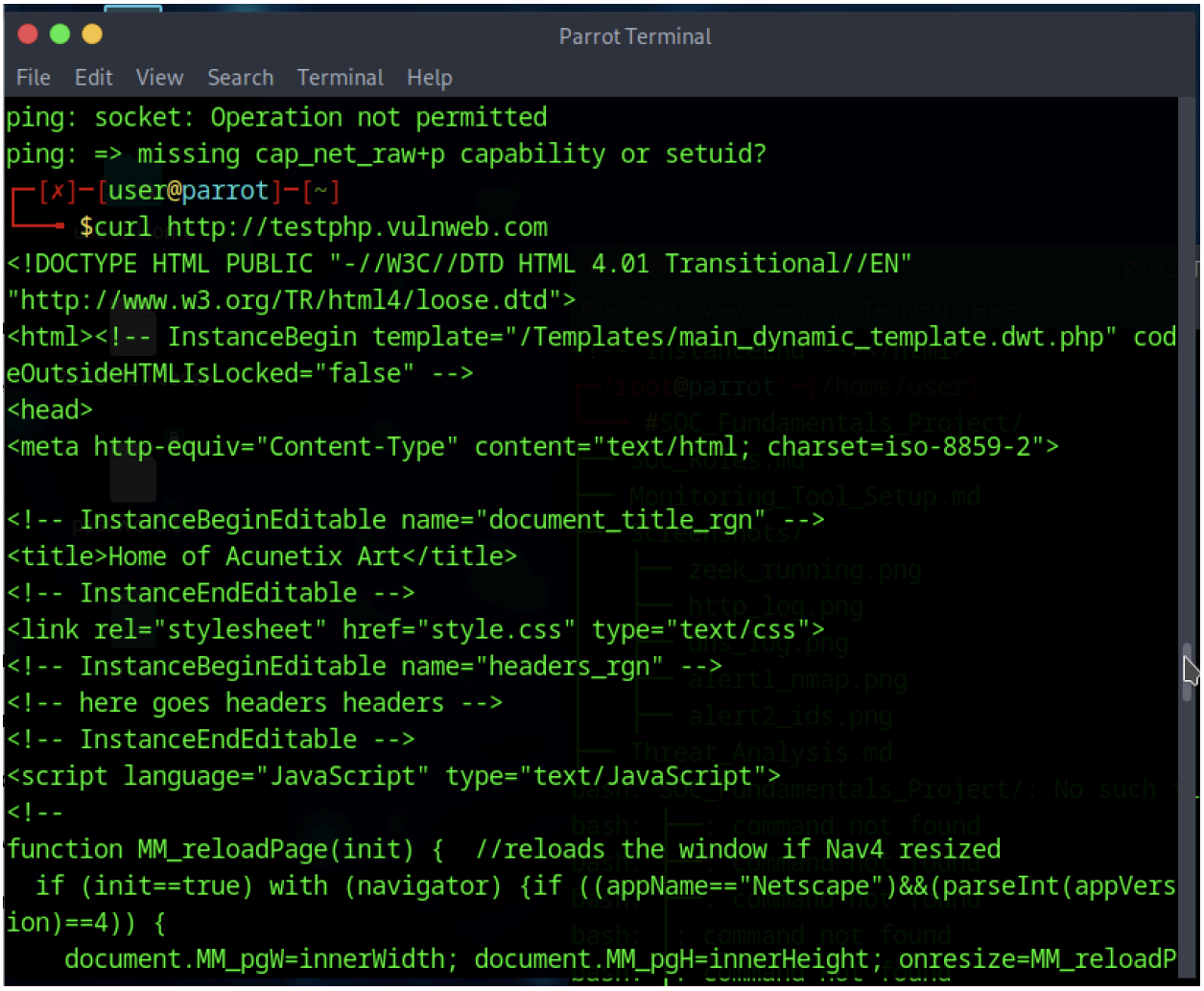
<!-- InstanceEndEditable -->
<!--end content -->

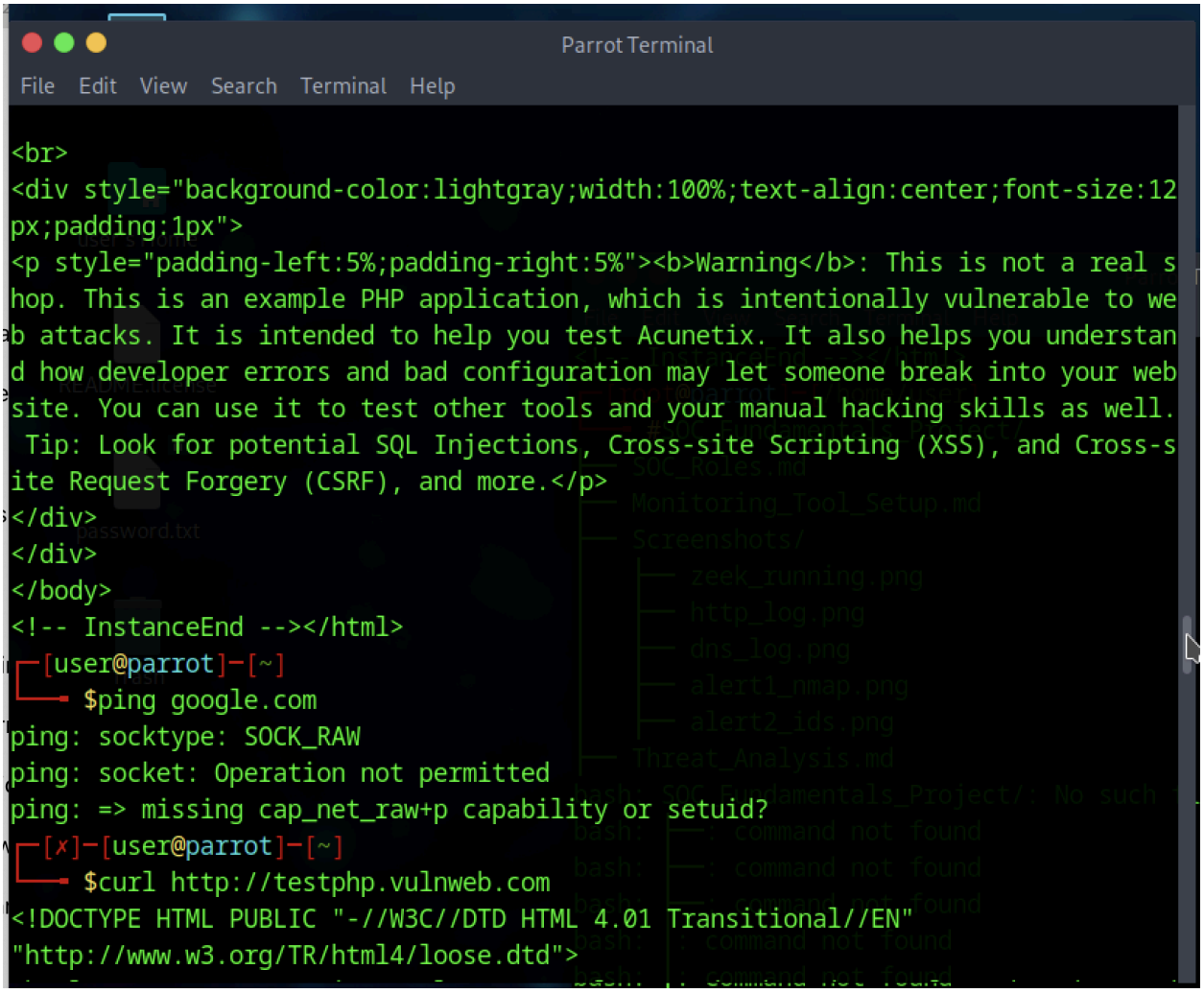
#SOC_Fundamentals_Project/
SOC_Roles.md
Monitoring_Tool_Setup.md
Screenshots/
Threat_Analysis.md
bash: SOC_Fundamentals_Project/: No such
command not found
command not found
command not found
command not found
command not found


Parrot Terminal
File Edit View Search Terminal Help
age; }}
else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location
.reload();
}
MM_reloadPage(true);
//-->
</script>
</head>
<body>

<h1 id="siteName"><img src="images/logo.gi
f" width="306" height="38" border="0" alt="Acunetix website security"></h1>
<h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acuneti
x.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</h6>

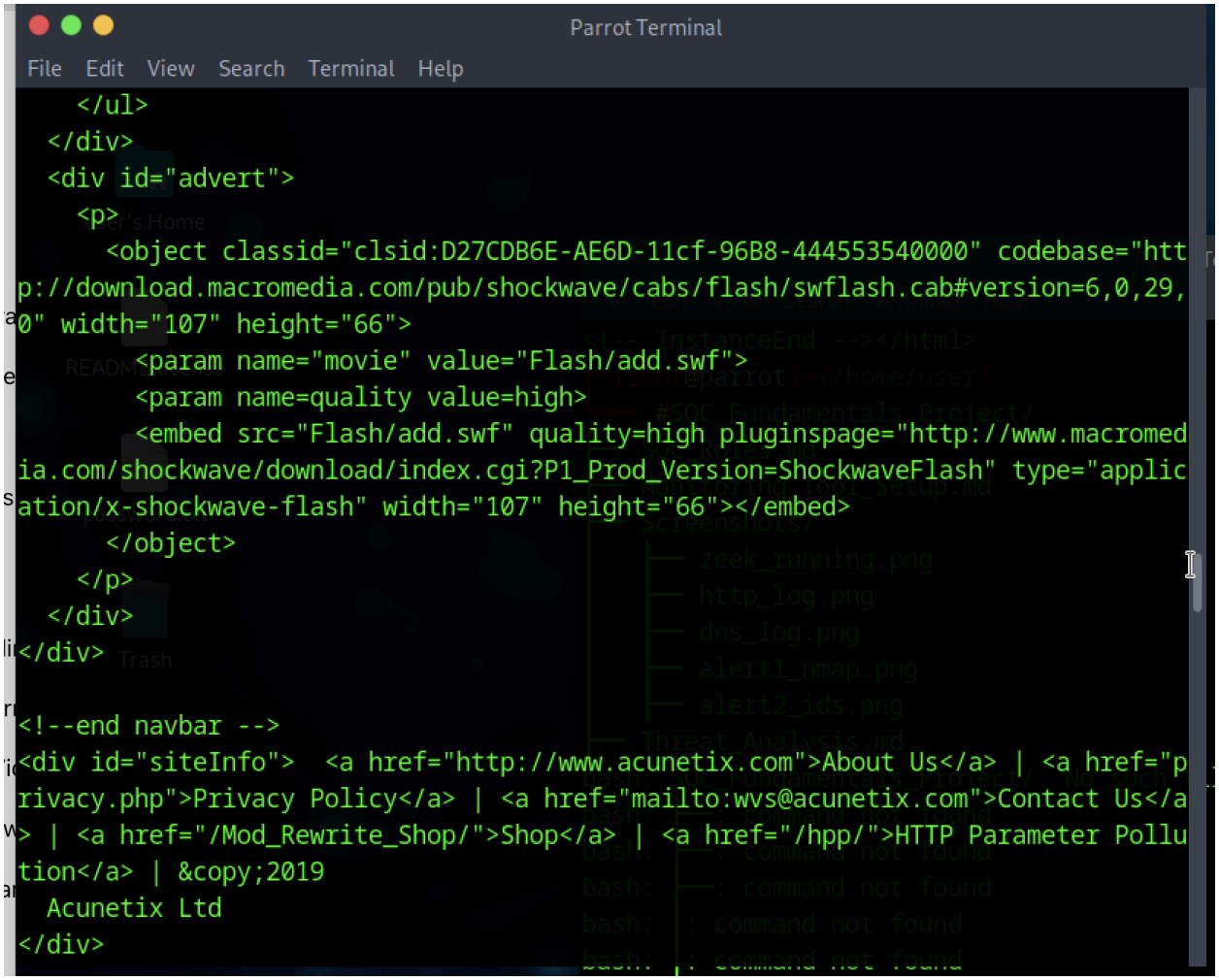
<table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
<td align="left">
home | categori
es | artists
 | disclaimer | <a href="cart.p


Parrot Terminal
File Edit View Search Terminal Help
ping: socket: Operation not permitted
ping: => missing cap_net_raw+p capability or setuid?
[✗]-[user@parrot]-[~]
$curl http://testphp.vulnweb.com
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" cod
eOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of Acunetix Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVers
ion)==4)) {
document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadP


Parrot Terminal
File Edit View Search Terminal Help

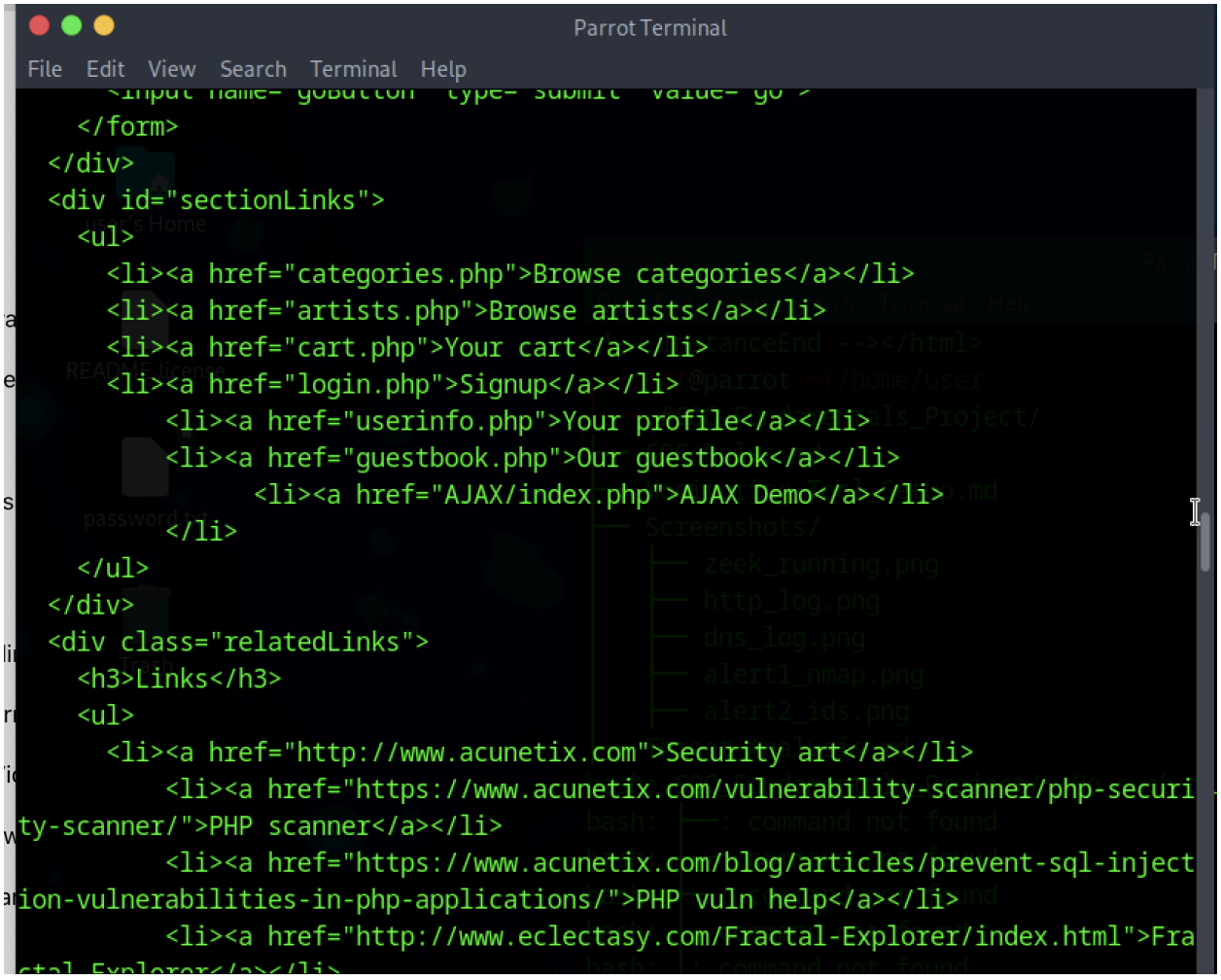
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12
px;padding:1px">
Warning: This is not a real s
hop. This is an example PHP application, which is intentionally vulnerable to we
b attacks. It is intended to help you test Acunetix. It also helps you understan
d how developer errors and bad configuration may let someone break into your web
site. You can use it to test other tools and your manual hacking skills as well.
Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-s
ite Request Forgery (CSRF), and more.

</body>
<!-- InstanceEnd --></html>
[user@parrot]-[~]
$ping google.com
ping: socktype: SOCK_RAW
ping: socket: Operation not permitted
ping: => missing cap_net_raw+p capability or setuid?
[x]-[user@parrot]-[~]
$curl http://testphp.vulnweb.com
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">


Parrot Terminal
File Edit View Search Terminal Help

<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0" width="107" height="66">
<param name="movie" value="Flash/add.swf">
<param name=quality value=high>
<embed src="Flash/add.swf" quality=high pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66"></embed>
</object>

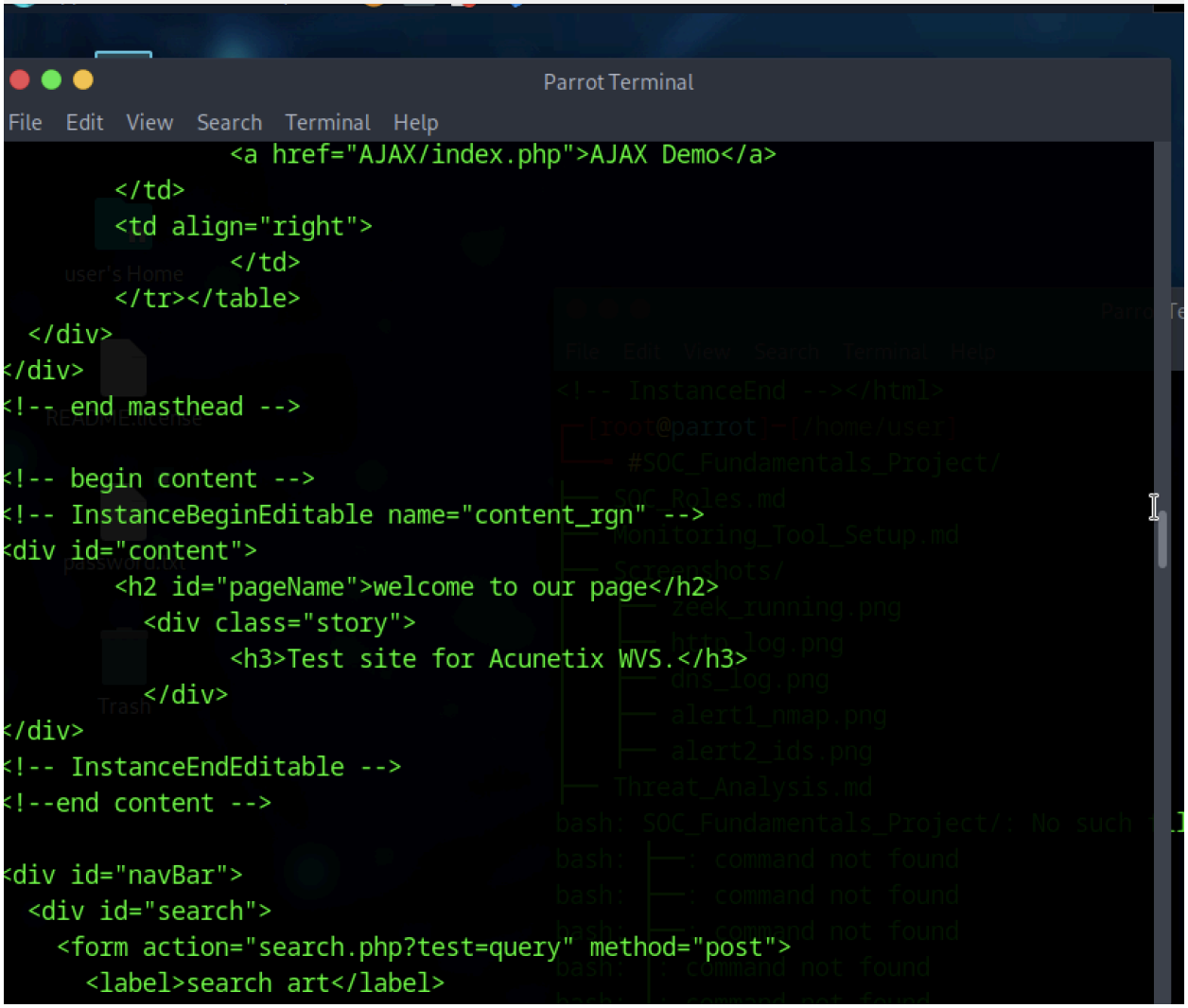
<!--end navbar -->
 About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019
Acunetix Ltd


Parrot Terminal
File Edit View Search Terminal Help
</form>

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

<h3>Links</h3>

Security art
<a href="https://www.acunetix.com/vulnerability-scanner/php-securi
ty-scanner/">PHP scanner
<a href="https://www.acunetix.com/blog/articles/prevent-sql-inject
ion-vulnerabilities-in-php-applications/">PHP vuln help
Fra


Parrot Terminal
File Edit View Search Terminal Help
AJAX Demo
</td>
<td align="right">
</td>
</tr></table>

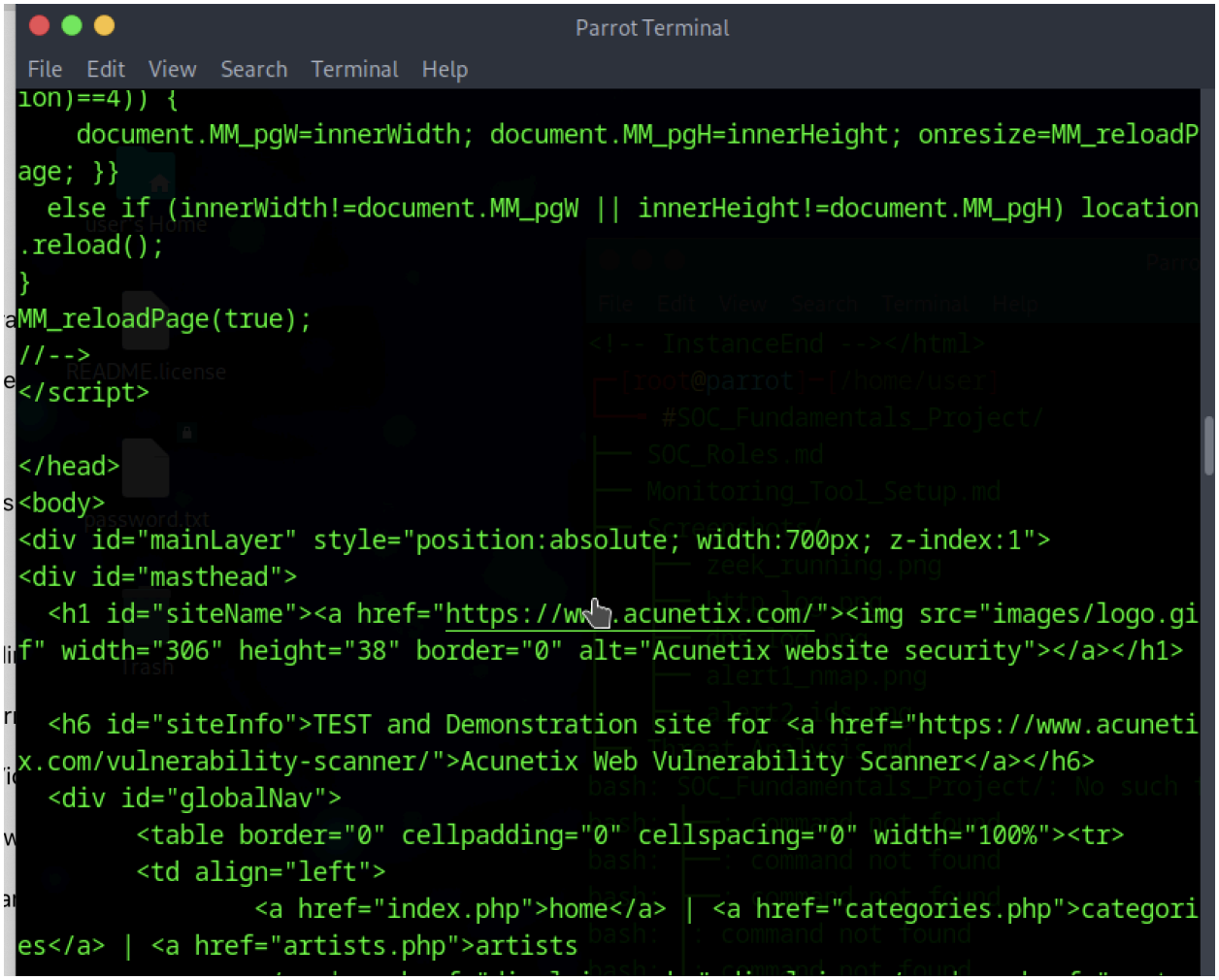
<!-- end masthead -->
<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->

<h2 id="pageName">welcome to our page</h2>

<h3>Test site for Acunetix WVS.</h3>

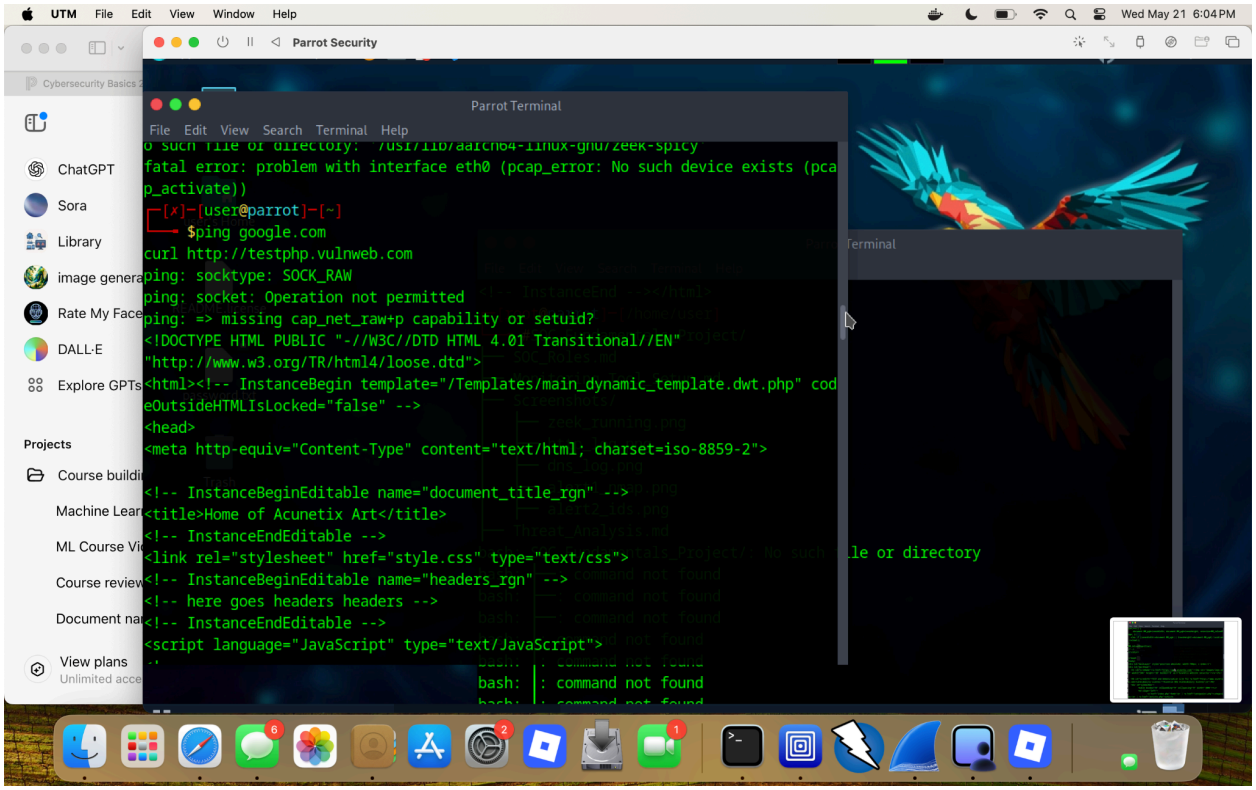
<!-- InstanceEndEditable -->
<!--end content -->

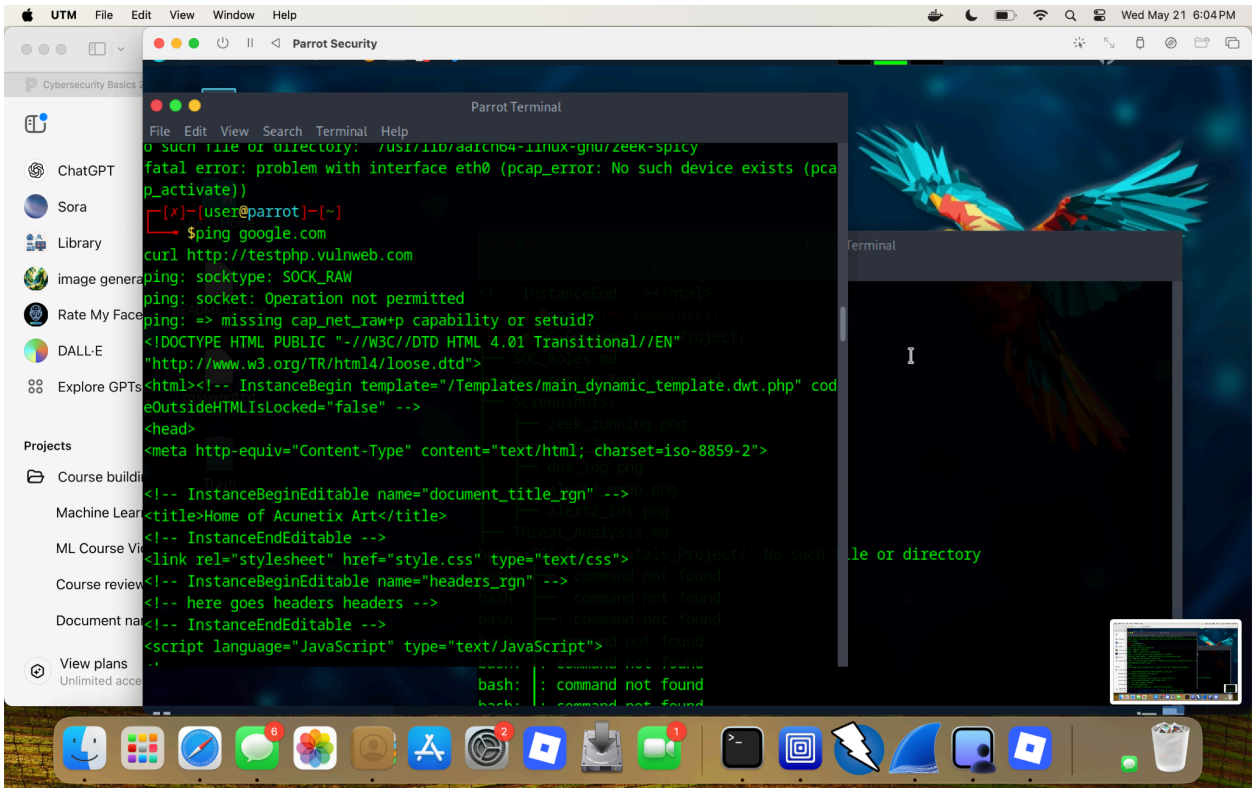
<form action="search.php?test=query" method="post">
<label>search art</label>

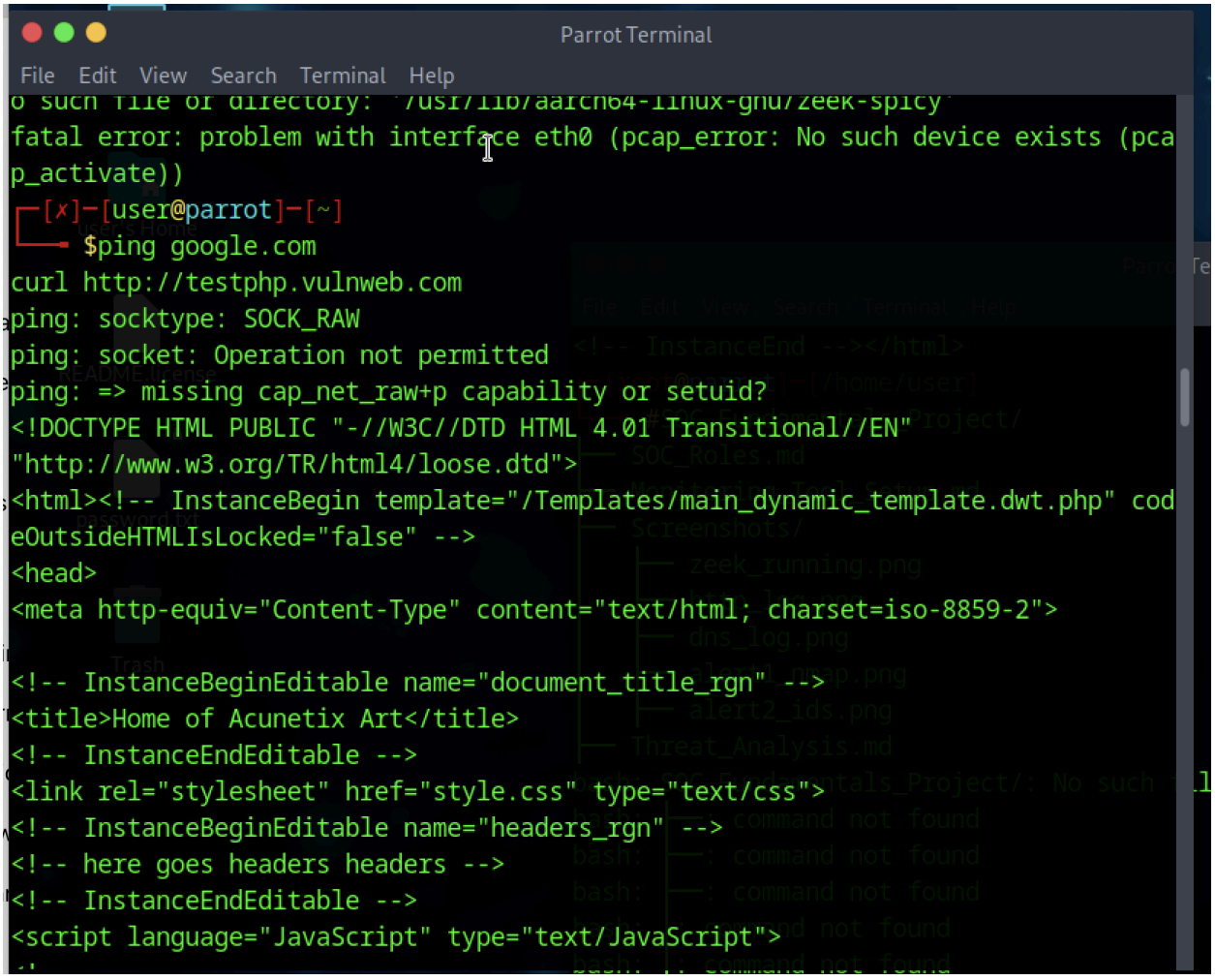

Parrot Terminal
File Edit View Search Terminal Help
ion)==4)) {
document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadP
age; }}
else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location
.reload();
}
MM_reloadPage(true);
//-->
</script>
</head>
<body>

<h1 id="siteName"><img src="images/logo.gi
f" width="306" height="38" border="0" alt="Acunetix website security"></h1>
<h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acuneti
x.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</h6>

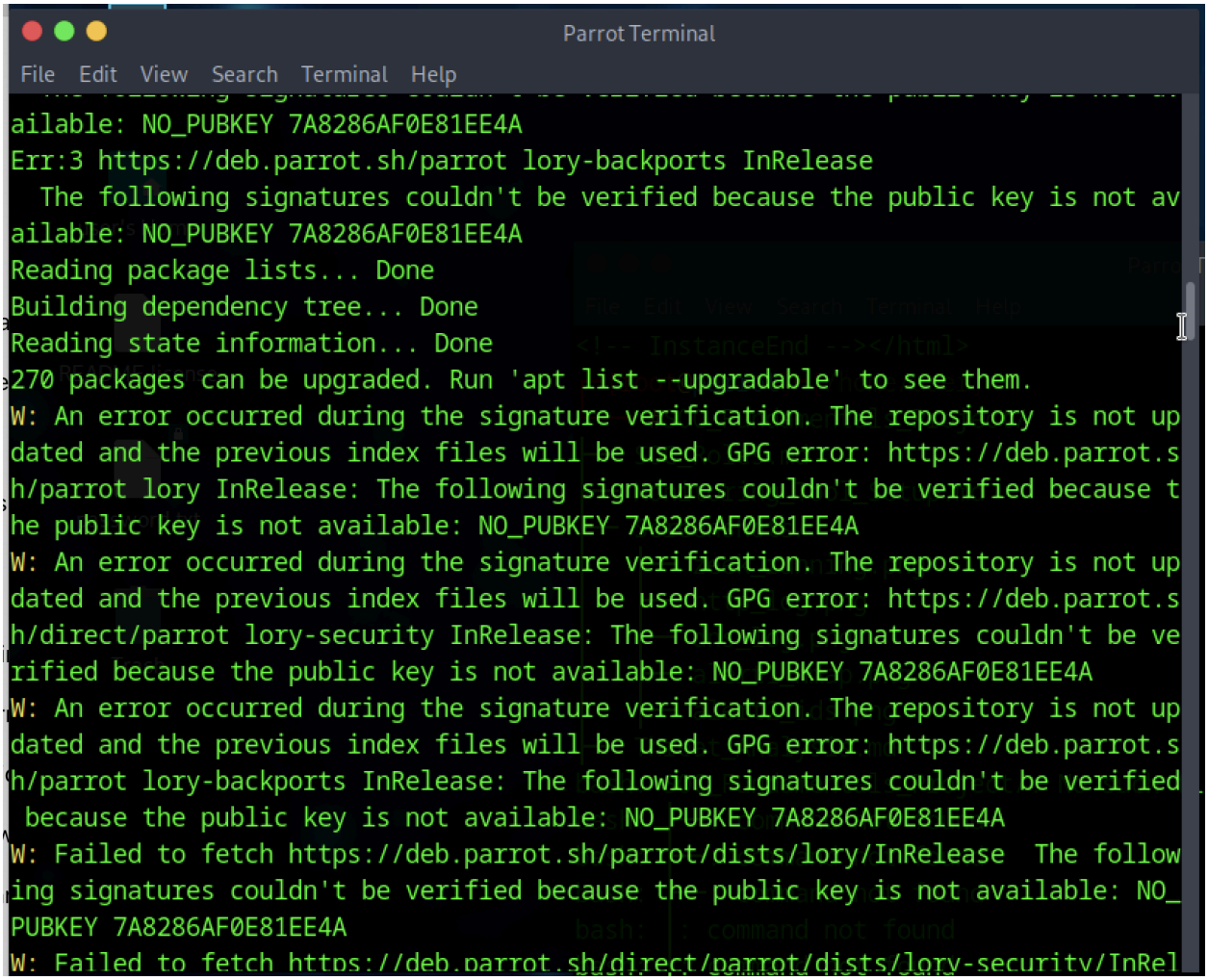
<table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
<td align="left">
home | categori
es | <a href="artists.php">artists

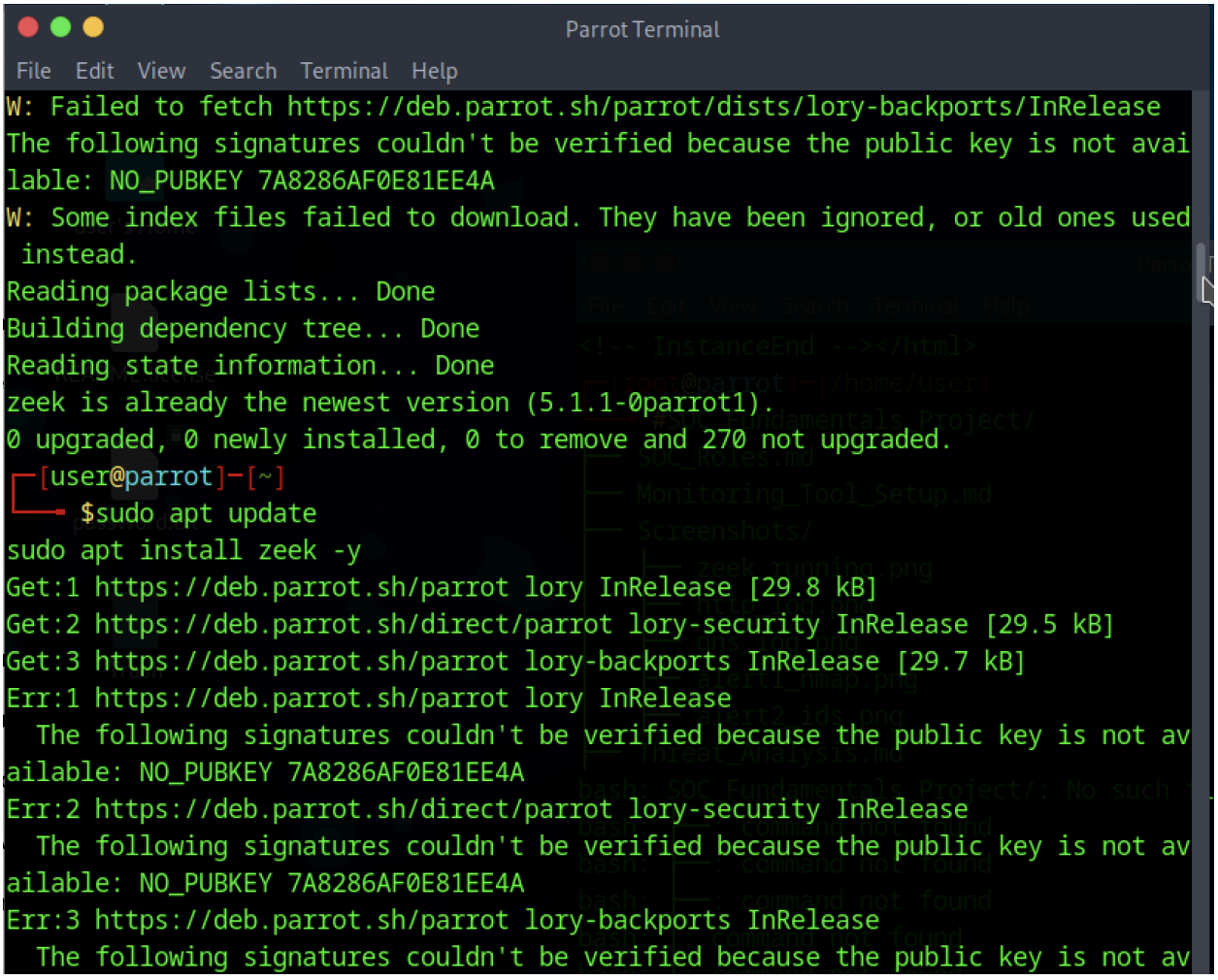

UTM File Edit View Window Help
Wed May 21 6:04 PM
Parrot Security
Parrot Terminal
File Edit View Search Terminal Help
fatal error: problem with interface eth0 (pcap_error: No such device exists (pca
p_activate))
[x]-[user@parrot]-[~]
$ping google.com
curl http://testphp.vulnweb.com
ping: socktype: SOCK_RAW
ping: socket: Operation not permitted
ping: => missing cap_net_raw+p capability or setuid?
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" cod
eOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of Acunetix Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
bash: : command not found
ChatGPT
Sora
Library
Rate My Face
DALL·E
Explore GPTs
Projects
Course buildi
Machine Learn
ML Course Vi
Course review
Document na
View plans

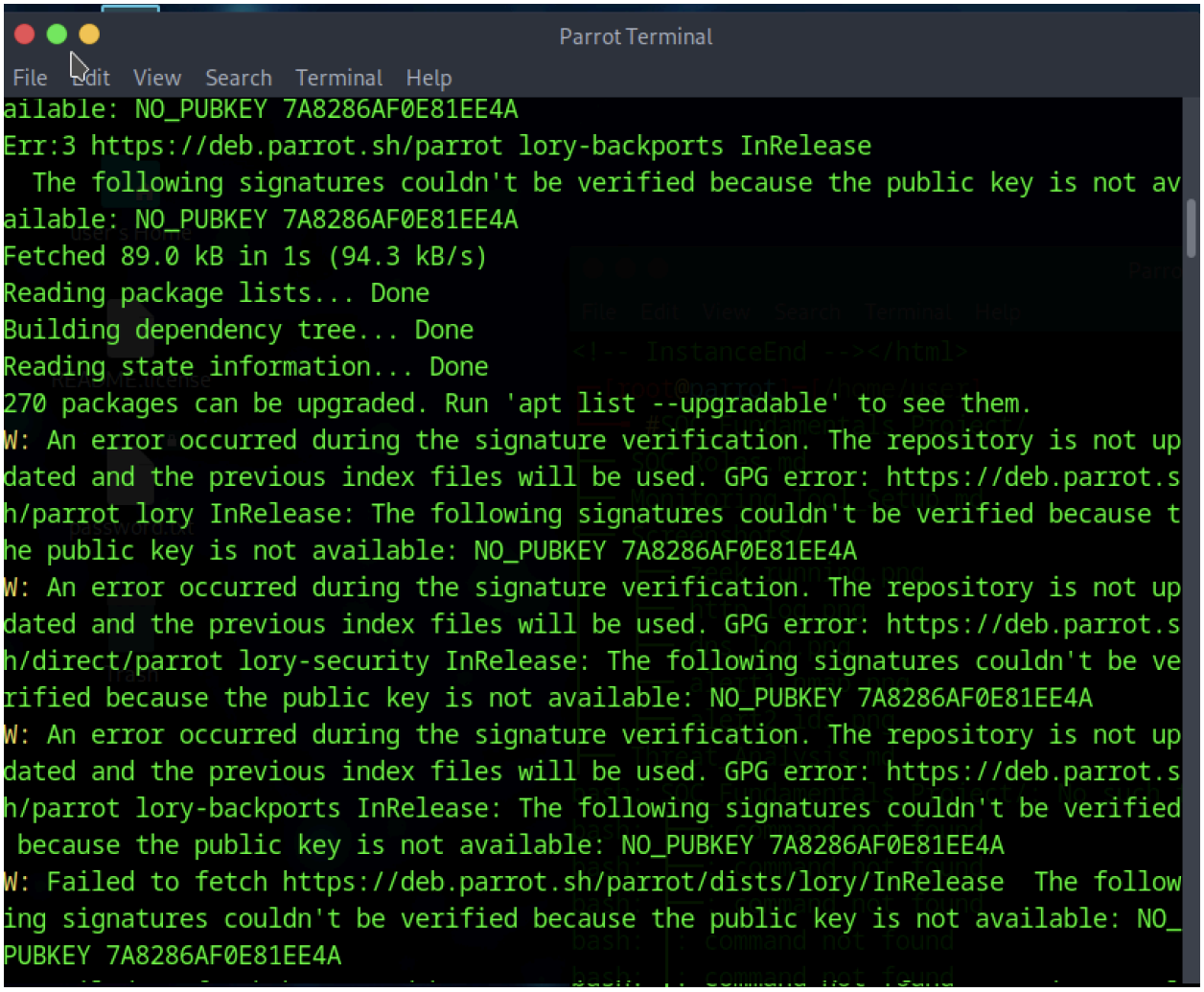

UTM File Edit View Window Help
Wed May 21 6:04 PM
Parrot Security
Parrot Terminal
File Edit View Search Terminal Help
fatal error: problem with interface eth0 (pcap_error: No such device exists (pca
p_activate))
[x]-[user@parrot]-[~]
$ping google.com
curl http://testphp.vulnweb.com
ping: socktype: SOCK_RAW
ping: socket: Operation not permitted
ping: => missing cap_net_raw+p capability or setuid?
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" cod
eOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of Acunetix Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
bash: : command not found
ChatGPT
Sora
Library
Rate My Face
DALL·E
Explore GPTs
Projects
Course buildi
Machine Learn
ML Course Vi
Course review
Document na
View plans

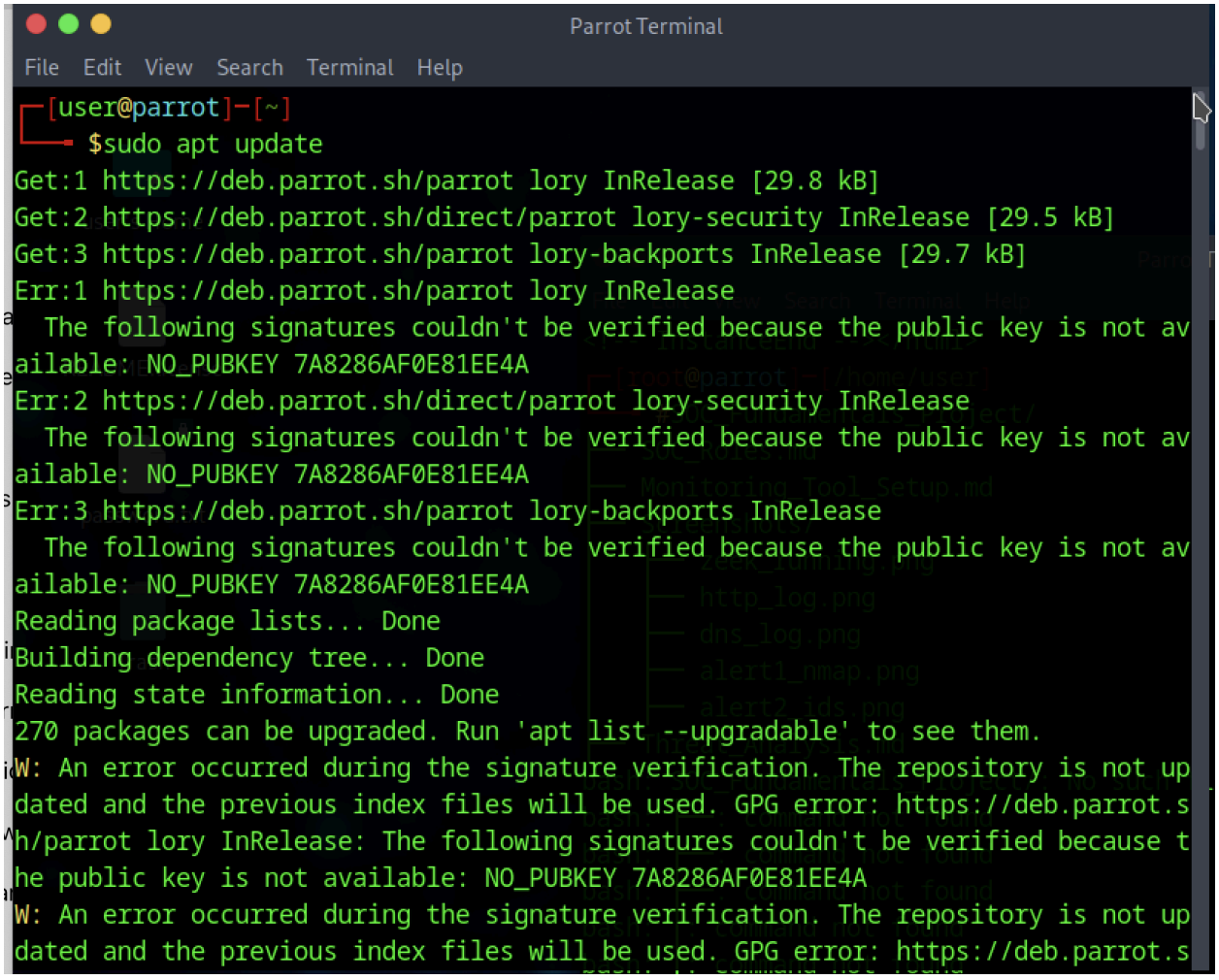

Parrot Terminal
File Edit View Search Terminal Help
o such file or directory: '/usr/lib/aarch64-linux-gnu/zeek-spicy'
fatal error: problem with interface eth0 (pcap_error: No such device exists (pca
p_activate))
[x]-[user@parrot]-[~]
$ping google.com
curl http://testphp.vulnweb.com
ping: socktype: SOCK_RAW
ping: socket: Operation not permitted
ping: => missing cap_net_raw+p capability or setuid?
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" cod
eOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of Acunetix Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">

```
File  Edit  View  Search  Terminal  Help
ease  The following signatures couldn't be verified because the public key is no
t available: NO_PUBKEY 7A8286AF0E81EE4A
W: Failed to fetch https://deb.parrot.sh/parrot/dists/lory-backports/InRelease
The following signatures couldn't be verified because the public key is not avai
lable: NO_PUBKEY 7A8286AF0E81EE4A
W: Some index files failed to download. They have been ignored, or old ones used
 instead.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
zeek is already the newest version (5.1.1-0parrot1).
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.
┌─[user@parrot]─[~]
└──╼ $sudo apt install zeek -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
zeek is already the newest version (5.1.1-0parrot1).
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.
┌─[user@parrot]─[~]
└──╼ $sudo zeek -i eth0
[warning] invalid plugin base directory /usr/lib/aarch64-linux-gnu/zeek-spicy: N
o such file or directory: '/usr/lib/aarch64-linux-gnu/zeek-spicy'
fatal error: problem with interface eth0 (pcap_error: No such device exists (pca
```


Parrot Terminal
File Edit View Search Terminal Help
ailable: NO_PUBKEY 7A8286AF0E81EE4A
Err:3 https://deb.parrot.sh/parrot lory-backports InRelease
The following signatures couldn't be verified because the public key is not av
ailable: NO_PUBKEY 7A8286AF0E81EE4A
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
270 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: An error occurred during the signature verification. The repository is not up
dated and the previous index files will be used. GPG error: https://deb.parrot.s
h/parrot lory InRelease: The following signatures couldn't be verified because t
he public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: An error occurred during the signature verification. The repository is not up
dated and the previous index files will be used. GPG error: https://deb.parrot.s
h/direct/parrot lory-security InRelease: The following signatures couldn't be ve
rified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: An error occurred during the signature verification. The repository is not up
dated and the previous index files will be used. GPG error: https://deb.parrot.s
h/parrot lory-backports InRelease: The following signatures couldn't be verified
because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: Failed to fetch https://deb.parrot.sh/parrot/dists/lory/InRelease The follow
ing signatures couldn't be verified because the public key is not available: NO_
PUBKEY 7A8286AF0E81EE4A
W: Failed to fetch https://deb.parrot.sh/direct/parrot/dists/lory-security/InRel


Parrot Terminal
File Edit View Search Terminal Help
W: Failed to fetch https://deb.parrot.sh/parrot/dists/lory-backports/InRelease
The following signatures couldn't be verified because the public key is not avai
lable: NO_PUBKEY 7A8286AF0E81EE4A
W: Some index files failed to download. They have been ignored, or old ones used
instead.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
zeek is already the newest version (5.1.1-0parrot1).
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.
[user@parrot]-[~]
$sudo apt update
sudo apt install zeek -y
Get:1 https://deb.parrot.sh/parrot lory InRelease [29.8 kB]
Get:2 https://deb.parrot.sh/direct/parrot lory-security InRelease [29.5 kB]
Get:3 https://deb.parrot.sh/parrot lory-backports InRelease [29.7 kB]
Err:1 https://deb.parrot.sh/parrot lory InRelease
The following signatures couldn't be verified because the public key is not av
ailable: NO_PUBKEY 7A8286AF0E81EE4A
Err:2 https://deb.parrot.sh/direct/parrot lory-security InRelease
The following signatures couldn't be verified because the public key is not av
ailable: NO_PUBKEY 7A8286AF0E81EE4A
Err:3 https://deb.parrot.sh/parrot lory-backports InRelease
The following signatures couldn't be verified because the public key is not av


Parrot Terminal
File Edit View Search Terminal Help
ailable: NO_PUBKEY 7A8286AF0E81EE4A
Err:3 https://deb.parrot.sh/parrot lory-backports InRelease
The following signatures couldn't be verified because the public key is not av
ailable: NO_PUBKEY 7A8286AF0E81EE4A
Fetched 89.0 kB in 1s (94.3 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
270 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: An error occurred during the signature verification. The repository is not up
dated and the previous index files will be used. GPG error: https://deb.parrot.s
h/parrot lory InRelease: The following signatures couldn't be verified because t
he public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: An error occurred during the signature verification. The repository is not up
dated and the previous index files will be used. GPG error: https://deb.parrot.s
h/direct/parrot lory-security InRelease: The following signatures couldn't be ve
rified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: An error occurred during the signature verification. The repository is not up
dated and the previous index files will be used. GPG error: https://deb.parrot.s
h/parrot lory-backports InRelease: The following signatures couldn't be verified
because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: Failed to fetch https://deb.parrot.sh/parrot/dists/lory/InRelease The follow
ing signatures couldn't be verified because the public key is not available: NO_
PUBKEY 7A8286AF0E81EE4A



1. SOC Functions and Operations

Primary SOC Roles and Responsibilities:

1. **Security Analyst:** Monitors network traffic and logs for suspicious activities, investigates alerts, and initiates incident response procedures.
2. **Incident Responder:** Handles confirmed incidents by containing threats, mitigating damage, and restoring systems.
3. **SOC Manager:** Oversees SOC operations, manages the team, ensures compliance with security policies, and reports to higher management.

---

2. Monitoring Fundamentals

Monitoring Tool Used: Zeek (formerly Bro)

Configuration Summary:

- Zeek was configured on the Parrot OS system to monitor network traffic.
- Attempted access to `/usr/local/zeek/logs/current/` for logs like `http.log` and `dns.log` to verify monitoring.
- Though directory was missing due to possible misconfiguration, the system executed traffic monitoring and scanning tests using Nmap and cURL.

Network Activities Monitored:

- **Nmap Scan:** `sudo nmap -sS 127.0.0.1` used to simulate and detect port scanning.
- **Web Requests:** `curl http://testphp.vulnweb.com` and `curl http://testmymids.com` were used to generate HTTP request logs (simulate potential external threats).

---

3. Alert Management

Alert Generation and Handling:

1. **Alert 1 - Port Scan Detection:**
    - Simulated using Nmap SYN scan.
    - Zeek/NIDS tools were intended to capture this as suspicious network behavior.
2. **Alert 2 - Suspicious Web Request:**
    - Used `curl` to access vulnerable test sites like `testphp.vulnweb.com`, which generate alerts due to possible exposure to XSS/SQLi.

Investigation and Resolution:

- Analysts would examine `http.log`, `dns.log`, and `conn.log` (if generated) to trace the source IP and accessed endpoints.
- Identified alerts would be marked and systems would be hardened to prevent repeated access.

---

4. Basic Threat Detection

Detected Threat: Test site visit to `testphp.vulnweb.com` revealed vulnerabilities like SQL injection, XSS, and CSRF exposed by the site.

Detection Technique:

- Manual HTTP request via `curl` triggered log entries.

- HTML response showed details of known web application vulnerabilities.

Conclusion:

- Zeek and network monitoring tools help simulate and detect common threats.
- Alert generation through basic tools (Nmap, cURL) confirms operational understanding.
- Manual investigation and interpretation of HTML responses and log data demonstrate foundational SOC skills.

Screenshots Attached:

- Terminal output of curl/nmap
- HTML from vulnerable sites
- Log access attempts

System Used: Parrot OS (primary); MacOS (for file handling and report compilation)