SECURITY ASSESSMENT REPORT

Target: hackthissite.org
Date: November 24, 2025
Scan ID: 4

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **hackthissite.org** on 2025-11-24. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

Severity	Count
Critical	0
High	2
Medium	2
Low	4
Info	6

2. Detailed Findings

1. Exposed Git Repository

Severity: HIGH **Tool:** Passive Recon

Description:

The subdomain 'git.hackthissite.org' suggests a publicly accessible Git repository. This could expose sensitive information such as source code, configuration files, and credentials.

Remediation:

Restrict access to the Git repository to authorized personnel only. Ensure proper access controls and authentication mechanisms are in place. Regularly audit the repository for sensitive information and remove any exposed credentials.

---

2. Administrative Interface Exposure

Severity: HIGH **Tool:** Passive Recon

Description:

The subdomain 'admin.hackthissite.org' suggests a publicly accessible administrative interface. This could allow unauthorized access to sensitive system settings and data.

Remediation:

Restrict access to the administrative interface to authorized personnel only. Implement strong authentication mechanisms, such as multi-factor authentication. Regularly audit the interface for vulnerabilities and apply necessary patches. Consider using a non-standard URL for the admin interface.

---

3. Staging/Development Environment Exposure

Severity: MEDIUM **Tool:** Passive Recon

Description:

The subdomains 'v3stage.hackthissite.org', 'v3dev.hackthissite.org', '*-v3stage-cdn.hackthissite.org', and '*-v3dev-cdn.hackthissite.org' indicate the presence of staging or development environments. These environments may contain outdated or vulnerable code, debugging tools, or sensitive data that could be exploited.

Remediation:

Implement strict access controls for staging and development environments. Ensure that these environments are isolated from the production environment. Regularly update and patch the software running in these environments. Remove any unnecessary debugging tools or sensitive data.

---

4. Internal Infrastructure Exposure

Severity: MEDIUM **Tool:** Passive Recon

Description:

The subdomains 'vm-*.outbound.firewall.hackthissite.org' suggest the exposure of internal virtual machines and firewall configurations. This could provide attackers with valuable information about the network architecture and potential attack vectors.

Remediation:

Ensure that internal infrastructure is not directly exposed to the internet. Implement strict firewall rules to restrict access to internal resources. Regularly audit firewall configurations for vulnerabilities. Consider using a VPN or other secure access methods for remote access to internal resources.

---

5. IRC Server Exposure

Severity: LOW **Tool:** Passive Recon

Description:

The subdomains related to IRC ('irc.hackthissite.org', 'new-irc.hackthissite.org', 'irc-v6.hackthissite.org', etc.) might indicate an outdated or vulnerable IRC server. While IRC is less common now, misconfigurations or vulnerabilities in the server software could be exploited.

Remediation:

If the IRC server is still in use, ensure it is running the latest version with all security patches applied. Review the server configuration for any potential vulnerabilities. If the IRC server is no longer needed,

consider decommissioning it.

6. Potential Information Disclosure via h5ai

Severity: LOW **Tool:** Passive Recon

Description:

The subdomain 'h5ai.hackthissite.org' suggests the use of h5ai, an HTTP web server index. If misconfigured, it could lead to unintended directory listing and information disclosure.

Remediation:

Review the h5ai configuration to ensure that sensitive files and directories are not publicly accessible. Implement proper access controls and authentication mechanisms.

7. Open HTTP Port (80)

Severity: LOW **Tool:** Active Recon

Description:

The presence of an open HTTP port (80) without redirection to HTTPS (443) could allow for man-in-the-middle attacks where traffic is intercepted and potentially modified. While HTTPS is also open, users might initially connect via HTTP.

Remediation:

Implement a permanent redirect from HTTP (port 80) to HTTPS (port 443) at the web server level. This ensures all traffic is encrypted.

8. DMARC Policy with pct=25

Severity: LOW **Tool:** Active Recon

Description:

The DMARC policy is set to quarantine 25% of emails that fail DMARC checks. While DMARC is implemented, the 'pct' value is not set to 100%. This means that some potentially spoofed emails will still be delivered to recipients' inboxes.

Remediation:

Gradually increase the 'pct' value to 100% to ensure that all emails failing DMARC checks are quarantined or rejected. Monitor DMARC reports to identify and address any legitimate emails that are being incorrectly flagged.

---

9. MTA-STS Policy Exposure

Severity: INFO **Tool:** Passive Recon

Description:

The subdomain 'mta-sts.hackthissite.org' indicates the presence of an MTA-STS policy. While not directly a vulnerability, misconfiguration of the policy could weaken email security.

Remediation:

Review the MTA-STS policy to ensure it is correctly configured and enforced. Monitor for any potential misconfigurations or weaknesses.

---

10. WhatWeb Failure

Severity: INFO **Tool:** Active Recon

Description:

The WhatWeb tool failed to execute due to a missing dependency. This prevents the identification of technologies used on the web server, hindering vulnerability assessment.

Remediation:

Investigate and resolve the WhatWeb error by installing the missing dependency (`/usr/bin/lib/messages`). Ensure the tool is properly configured and updated.

---

11. DNSSEC Query Failure

Severity: INFO **Tool:** Active Recon

Description:

The DNSRecon tool reported 'No answer for DNSSEC query'. This could indicate that DNSSEC is not properly configured for the domain, making it potentially vulnerable to DNS spoofing attacks.

Remediation:

Verify DNSSEC configuration for the domain. If not enabled, consider implementing DNSSEC to enhance DNS security and prevent tampering.

---

12. Multiple A Records

Severity: INFO **Tool:** Active Recon

Description:

The domain has multiple A records pointing to different IP addresses. This could be for load balancing or redundancy. While not inherently a vulnerability, it increases the attack surface and requires careful management of each server.

Remediation:

Ensure all servers associated with the A records are properly secured and patched. Regularly review and update the server configurations.

---

13. Closed SSH Port (22)

Severity: INFO **Tool:** Active Recon

Description:

The SSH port (22) is closed. While this is generally good for reducing the attack surface, it's important to verify that SSH access is available through other means if required for administration, and that those means are properly secured.

Remediation:

Verify that SSH access is available through alternative ports or methods if required. If not required, ensure the service is disabled at the firewall level to prevent future exposure.

14. SPF Record Includes Multiple IP Addresses

Severity: INFO **Tool:** Active Recon

Description:

The SPF record includes multiple IP addresses and domains. While this is not inherently a vulnerability, it's important to ensure that all listed IP addresses and domains are legitimate and authorized to send email on behalf of the domain. Incorrectly configured SPF records can lead to email spoofing.

Remediation:

Regularly review and update the SPF record to ensure that all listed IP addresses and domains are authorized to send email on behalf of the domain. Remove any outdated or unauthorized entries.

3. Appendix: Raw Tool Output

The following section contains raw output from the security tools used during the assessment.

Tool: Passive Recon


```
{"unique_subdomains_count": 48, "subdomains": ["git.hackthissite.org",
"vm-150.outbound.firewall.hackthissite.org", "1-v3stage-cdn.hackthissite.org",
"staff.hackthissite.org", "legal.hackthissite.org", "ns2.hackthissite.org",
"v3stage.hackthissite.org", "new-irc.hackthissite.org",
"2-v3stage-cdn.hackthissite.org", "lille.irc-v6.hackthissite.org",
"status.hackthissite.org", "lille.irc.hackthissite.org",
"vm-099.outbound.firewall.hackthissite.org", "jupiter.hackthissite.org",
"v3stage-cdn.hackthissite.org", "irc-v6.hackthissite.org",
"vm-005.outbound.firewall.hackthissite.org", "admin.hackthissite.org",
"irc-hub.hackthissite.org", "shadow.hackthissite.org", "1-v3dev-cdn.hackthissite.org",
"mta-sts.hackthissite.org", "kage.hackthissite.org", "pi.hackthissite.org",
"mail.hackthissite.org", "4-v3dev-cdn.hackthissite.org", "mirror.hackthissite.org",
"vm-200.outbound.firewall.hackthissite.org", "hackthissite.org",
"irc.hackthissite.org", "htsv4.hackthissite.org", "forums.hackthissite.org",
"3-v3stage-cdn.hackthissite.org", "ns1.hackthissite.org", "wolf.irc.hackthissite.org",
"vm-050.outbound.firewall.hackthissite.org", "www.irc.hackthissite.org",
"daemon.hackthissite.org", "v3dev.hackthissite.org", "www.hackthissite.org",
"stats.hackthissite.org", "wolf.irc-v6.hackthissite.org", "irc-wolf.hackthissite.org",
"irc-ipv6.hackthissite.org", "h5ai.hackthissite.org", "ctf.hackthissite.org",
"status-new.hackthissite.org", "api.hackthissite.org"], "resolved_hosts": [],
"live_services": [], "_raw_logs": "[02:47:11 AM] [+] Starting passive enumeration for:
hackthissite.org\n[02:47:11 AM] [+] Using temporary output directory:
/tmp/tmp6_ipm55v\n[02:47:11 AM] [+] Running Subfinder...\n[02:47:42 AM] [+] Running
Findomain...\n[02:47:44 AM] [+] Running Assetfinder...\n[02:47:45 AM] [+] Running Amass
Passive...\n[02:57:45 AM] [+] Merging results...\n[02:57:45 AM] [+] Found 48 unique
subdomains.\n[02:57:45 AM] [+] Checking DNS resolution with dnsx...\n[03:07:46 AM] [+]
DNSX resolved 0 hosts.\n[03:07:46 AM] [+] Checking HTTP/HTTPS services with
httpx...\n[03:07:46 AM] [!] HTTPX Error Output: Usage: httpx [OPTIONS] URL\n\nError: No
such option: -s\n[03:07:46 AM] [+] HTTPX found 0 live services.\n[03:07:46 AM] [+] Recon
complete.\n{\"unique_subdomains_count\": 48, \"subdomains\": [\"git.hackthissite.org\",
\"vm-150.outbound.firewall.hackthissite.org\", \"1-v3stage-cdn.hackthissite.org\",
\"staff.hackthissite.org\", \"legal.hackthissite.org\", \"ns2.hackthissite.org\",
\"v3stage.hackthissite.org\", \"new-irc.hackthissite.org\",
\"2-v3stage-cdn.hackthissite.org\", \"lille.irc-v6.hackthissite.org\",
\"status.hackthissite.org\", \"lille.irc.hackthissite.org\",
\"vm-099.outbound.firewall.hackthissite.org\", \"jupiter.hackthissite.org\",
\"v3stage-cdn.hackthissite.org\", \"irc-v6.hackthissite.org\",
\"vm-005.outbound.firewall.hackthissite.org\", \"admin.hackthissite.org\",
\"irc-hub.hackthissite.org\", \"shadow.hackthissite.org\",
\"1-v3dev-cdn.hackthissite.org\", \"mta-sts.hackthissite.org\",
\"kage.hackthissite.org\", \"pi.hackthissite.org\", \"mail.hackthissite.org\",
\"4-v3dev-cdn.hackthissite.org\", \"mirror.hackthissite.org\",
\"vm-200.outbound.firewall.hackthissite.org\", \"hackthissite.org\",
\"irc.hackthissite.org\", \"htsv4.hackthissite.org\", \"forums.hackthissite.org\",
\"3-v3stage-cdn.hackthissite.org\", \"ns1.hackthissite.org\",
\"wolf.irc.hackthissite.org\", \"vm-050.outbound.firewall.hackthissite.org\",
\"www.irc.hackthissite.org\", \"daemon.hackthissite.org\", \"v3dev.hackthissite.org\",
\"www.hackthissite.org\", \"stats.hackthissite.org\", \"wolf.irc-v6.hackthissite.org\",
\"irc-wolf.hackthissite.org\", \"irc-ipv6.hackthissite.org\",
\"h5ai.hackthissite.org\", \"ctf.hackthissite.org\", \"status-new.hackthissite.org\",
\"api.hackthissite.org\"], \"resolved_hosts\": [], \"live_services\": []}\n"}
```

Tool: Active Recon


```
{"nmap_fast": "Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 03:07 EST\nNmap
scan report for hackthissite.org (137.74.187.102)\nHost is up (0.35s latency).\nOther
addresses for hackthissite.org (not scanned): 137.74.187.101 137.74.187.100
137.74.187.104 137.74.187.103\nNot shown: 97 filtered tcp ports (no-response)\nPORT
STATE SERVICE\n22/tcp closed ssh\n80/tcp open http\n443/tcp open https\n\nNmap done: 1
IP address (1 host up) scanned in 10.16 seconds", "whatweb": "/usr/bin/whatweb:257:in
`require_relative': cannot load such file -- /usr/bin/lib/messages (LoadError)\n\tfrom
/usr/bin/whatweb:257:in `'", "dnsrecon": "2025-11-24T03:08:05.739017-0500 INFO Starting
enumeration for domain: hackthissite.org\n2025-11-24T03:08:05.740190-0500 INFO std:
Performing General Enumeration against:
hackthissite.org...\n2025-11-24T03:08:06.631770-0500 ERROR No answer for DNSSEC query
for hackthissite.org\n2025-11-24T03:08:07.013487-0500 INFO \t SOA c.ns.buddyns.com
116.203.6.3\n2025-11-24T03:08:07.013723-0500 INFO \t SOA c.ns.buddyns.com
2a01:4f8:1c0c:8115::3\n2025-11-24T03:08:10.835096-0500 INFO \t NS f.ns.buddyns.com
5.223.55.119\n2025-11-24T03:08:11.022349-0500 INFO \t NS f.ns.buddyns.com
2a01:4ff:2f0:3661::3\n2025-11-24T03:08:11.264338-0500 INFO \t NS h.ns.buddyns.com
103.25.56.55\n2025-11-24T03:08:11.911795-0500 INFO \t NS h.ns.buddyns.com
2406:d500:7:2::ca\n2025-11-24T03:08:13.027385-0500 INFO \t NS h.ns.buddyns.com
2406:d500:2::de4f:f105\n2025-11-24T03:08:19.033548-0500 INFO \t NS j.ns.buddyns.com
37.143.61.179\n2025-11-24T03:08:19.576027-0500 INFO \t NS j.ns.buddyns.com
2a01:a500:2766::5c3f:d10b\n2025-11-24T03:08:20.063917-0500 INFO \t NS c.ns.buddyns.com
116.203.6.3\n2025-11-24T03:08:20.705680-0500 INFO \t NS c.ns.buddyns.com
2a01:4f8:1c0c:8115::3\n2025-11-24T03:08:21.344101-0500 INFO \t NS g.ns.buddyns.com
192.184.93.99\n2025-11-24T03:08:21.983637-0500 INFO \t NS g.ns.buddyns.com
2604:180:1:92a::3\n2025-11-24T03:08:28.865000-0500 INFO \t MX aspmx.l.google.com
64.233.170.26\n2025-11-24T03:08:28.865230-0500 INFO \t MX alt2.aspmx.l.google.com
172.217.78.26\n2025-11-24T03:08:28.865284-0500 INFO \t MX alt1.aspmx.l.google.com
192.178.163.27\n2025-11-24T03:08:28.865320-0500 INFO \t MX aspmx5.googlemail.com
192.178.164.26\n2025-11-24T03:08:28.865396-0500 INFO \t MX aspmx4.googlemail.com
142.250.101.26\n2025-11-24T03:08:28.865432-0500 INFO \t MX aspmx2.googlemail.com
192.178.163.26\n2025-11-24T03:08:28.865478-0500 INFO \t MX aspmx3.googlemail.com
172.217.78.26\n2025-11-24T03:08:28.865512-0500 INFO \t MX aspmx.l.google.com
2404:6800:4003:c03::1a\n2025-11-24T03:08:28.865677-0500 INFO \t MX
alt2.aspmx.l.google.com 2607:f8b0:4023:1c05::1b\n2025-11-24T03:08:28.865727-0500 INFO
\t MX alt1.aspmx.l.google.com 2607:f8b0:400e:c17::1b\n2025-11-24T03:08:28.865758-0500
INFO \t MX aspmx5.googlemail.com
2607:f8b0:4023:2009::1a\n2025-11-24T03:08:28.865785-0500 INFO \t MX
aspmx4.googlemail.com 2607:f8b0:4023:c06::1a\n2025-11-24T03:08:28.865809-0500 INFO \t
MX aspmx2.googlemail.com 2607:f8b0:400e:c17::1a\n2025-11-24T03:08:28.881383-0500 INFO
\t A hackthissite.org 137.74.187.103\n2025-11-24T03:08:28.881512-0500 INFO \t A
hackthissite.org 137.74.187.104\n2025-11-24T03:08:28.881546-0500 INFO \t A
hackthissite.org 137.74.187.100\n2025-11-24T03:08:28.881571-0500 INFO \t A
hackthissite.org 137.74.187.101\n2025-11-24T03:08:28.881597-0500 INFO \t A
hackthissite.org 137.74.187.102\n2025-11-24T03:08:29.686980-0500 INFO \t SPF v=spf1 a
mx ip4:137.74.187.96 ip4:137.74.187.97 ip4:137.74.187.98 a:mail.hackthissite.org
include:aspmx.googlemail.com include:spf.hackmail.org
-all\n2025-11-24T03:08:29.871711-0500 INFO \t TXT hackthissite.org
Harica-PM9RrLqWMFZXTJCoEoK\n2025-11-24T03:08:29.871881-0500 INFO \t TXT
hackthissite.org
t-verify=e3f12c9c23e2e475563590326df31a12\n2025-11-24T03:08:29.871982-0500 INFO \t TXT
hackthissite.org v=spf1 a mx ip4:137.74.187.96 ip4:137.74.187.97 ip4:137.74.187.98
a:mail.hackthissite.org include:aspmx.googlemail.com include:spf.hackmail.org
-all\n2025-11-24T03:08:29.872030-0500 INFO \t TXT _dmarc.hackthissite.org v=DMARC1;p=qu
arantine;sp=quarantine;fo=0:1:d:s;aspf=r;adkim=r;ri=86400;pct=25;rua=mailto:8rbjyycl@ag
.dmarcian.eu;ruf=mailto:8rbjyycl@fr.dmarcian.eu;\n2025-11-24T03:08:30.620718-0500 INFO
Enumerating SRV Records\n2025-11-24T03:08:33.019061-0500 ERROR No SRV Records Found for
hackthissite.org\n2025-11-24T03:08:33.019358-0500 INFO Completed enumeration for
domain: hackthissite.org", "_raw_logs": "[03:07:54 AM] [+] Starting Active Recon on
hackthissite.org...\n[03:07:54 AM] [+] Nmap: Scanning top 1000 ports...\n[03:08:04 AM]
[+] Nmap scan completed.\n[03:08:04 AM] [+] WhatWeb: Identifying
technologies...\n[03:08:05 AM] [+] WhatWeb completed.\n[03:08:05 AM] [+] DNSRecon:
```

```
Enumerating DNS records...\n[03:08:33 AM] [+] DNSRecon completed.\n[03:08:33 AM] [+]
Active Recon phase finished.\n{\"nmap_fast\": \"Starting Nmap 7.95 ( https://nmap.org )
at 2025-11-24 03:07 EST\\nNmap scan report for hackthissite ...[Truncated]
```