

# NexusPenTest Security Report

Target: <https://hackthissite.org/>

Methodology: OWASP

Date: 2026-02-12 08:22 UTC

## Severity Summary

Critical: 4

High: 3

Medium: 10

Low: 5

Info: 14

## Findings

### nmap [low]

Command: nmap -F -T4 -sV <https://hackthissite.org/>

Starting Nmap 7.98 ( <https://nmap.org> ) at 2026-02-12 02:50 -0500

Nmap done: 0 IP addresses (0 hosts up) scanned in 0.19 seconds

### theharvester [low]

Command: theharvester <https://hackthissite.org/>

??( [1;31mMessage from Kali developers [00m]

?

? The command theharvester is deprecated. Please use theHarvester instead.

?

??

### whois [info]

Command: whois <https://hackthissite.org/>

No whois server is known for this kind of object.

### whatweb [info]

Command: whatweb <https://hackthissite.org/>

[1m [34m<https://hackthissite.org/> [0m [200 OK] [1mContent-Language [0m[ [0m [22men [0m],  
[1mCookies [0m[ [0m [22mHackThisSite [0m], [1mCountry [0m[ [0m [22mCANADA [0m][ [1m [31mCA [0m],  
[1mHTTPServer [0m[ [1m [36mHackThisSite [0m], [1mIP [0m[ [0m [22m137.74.187.102 [0m], [1mjQuery [0m[ [1m [32m1.8.1 [0m],  
[1mMeta-Author [0m[ [0m [22mHackThisSite.org Staff [0m], [1mOpen-Graph-Protocol [0m[ [1m [32mwebsite [0m],  
[1mPasswordField [0m[ [0m [22mpassword [0m], [1mScript [0m[ [0m [22mtext/javascript [0m],  
[1mStrict-Transport-Security [0m[ [0m [22mmax-age=31536000; includeSubDomains; preload [0m], [1mTitle [0m[ [1m [33mHack  
This Site [0m],  
[1mUncommonHeaders [0m[ [0m [22mupgrade,union-location,access-control-allow-origin,content-security-policy,referrer-policy,featu  
re-policy,public-key-pins-report-only,report-to,nel [0m], [1mX-XSS-Protection [0m[ [0m [22m0 [0m]

### curl [medium]

Command: curl <https://hackthissite.org/>

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>
  <title>Hack This Site</title>
  <meta name="verify-v1" content="s/YXn7eQrMBoF9PL5jLJDjWpAxEXpJzE9JLg/zM4C2Y=" />
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <meta name="author" content="HackThisSite.org Staff" />
  <meta name="keywords" content="challenge, computer, culture, deface, digital, ethics, games, guide, hack, hack forums, hacker,
hackers, hacking, hacking challenges, hacking forums, mission, net, programming, radical, revolution, root, rooting, security, site,
society, tutorial, tutorials, war, wargame, wargames, web, website" />
  <meta name="title" content="HackThisSite" />
  <meta name="description" content="HackThisSite.org is a free, safe and legal training ground for hackers to test and expand their
ethical hacking skills with challenges, CTFs, and more." />
  <meta itemprop="name" content="HackThisSite" />
  <meta itemprop="description" content="HackThisSite.org is a free, safe and legal training ground for hackers to test and expand
their ethical hacking skills with challenges, CTFs, and more." />
  <meta itemprop="image" content="https://data.htscdn.org/images/hackthissite-meta-card.png" />
  <meta property="og:type" content="website" />
  <meta property="og:url" content="https://www.hackthissite.org/" />
  <meta property="og:title" content="HackThisSite" />
  <meta property="og:description" content="HackThisSite.org is a free, safe and legal training ground for hackers to test and expand
their ethical hacking skills with challenges, CTFs, and more." />
  <meta property="og:image" content="https://data.htscdn.org/images/hackthissite-meta-card.png" />
  <meta property="twitter:card" content="summary_large_image" />
  <meta property="twitter:url" content="https://www.hackthissite.org/" />
  <meta property="twitter:titl
```

masscan [info]

Command: masscan --top-ports 100 --rate 1000 https://hackthissite.org/

whatweb [info]

Command: whatweb https://hackthissite.org/

[1m [34mhttps://hackthissite.org/ [0m	[200	OK]	[1mContent-Language [0m[ [0m [22men [0m],
[1mCookies [0m[ [0m [22mHackThisSite [0m],			[1mCountry [0m[ [0m [22mCANADA [0m][ [1m [31mCA [0m],
[1mHTTPServer [0m[ [1m [36mHackThisSite [0m],	[1mIP [0m[ [0m [22m137.74.187.101 [0m],	[1mjQuery [0m[ [1m [32m1.8.1 [0m],	
[1mMeta-Author [0m[ [0m [22mHackThisSite.org	Staff [0m],	[1mOpen-Graph-Protocol [0m[ [1m [32mwebsite [0m],	
[1mPasswordField [0m[ [0m [22mpassword [0m],		[1mScript [0m[ [0m [22mtext/javascript [0m],	
[1mStrict-Transport-Security [0m[ [0m [22mmax-age=31536000; includeSubDomains; preload [0m],	[1mTitle [0m[ [1m [33mHack		
This		Site [0m],	
[1mUncommonHeaders [0m[ [0m [22mupgrade, onion-location, access-control-allow-origin, content-security-policy, referrer-policy, featu			
re-policy, public-key-pins-report-only, report-to, nel [0m],	[1mX-XSS-Protection [0m[ [0m [22m0 [0m]		

nmap [low]

Command: nmap -F -T4 -sV https://hackthissite.org/

Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-12 02:50 -0500

Nmap done: 0 IP addresses (0 hosts up) scanned in 0.17 seconds

dirb [medium]

Command: dirb https://hackthissite.org/

-----

DIRB v2.22  
By The Dark Raver

-----  
START\_TIME: Thu Feb 12 02:50:42 2026  
URL\_BASE: https://hackthissite.org/  
WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt  
-----

\*\*\* Generating Wordlist...

GENERATED WORDS: 4612

---- Scanning URL: https://hackthissite.org/ ----

\*\*\* Calculating NOT\_FOUND code...

--> Testing: https://hackthissite.org/.bash\_history  
https://hackthissite.org/.bashrc  
(CODE:301|SIZE:243)

--> Testing:

+ https://hackthissite.org/.bashrc

--> Testing: https://hackthissite.org/.cache

--> Testing: https://hackthissite.org/.config  
(CODE:301|SIZE:243)

+ https://hackthissite.org/.config

--> Testing: https://hackthissite.org/.cvs

--> Testing: https://hackthissite.org/.cvsignore  
https://hackthissite.org/.forward  
(CODE:301|SIZE:244)

--> Testing:

+ https://hackthissite.org/.forward

--> Testing: https://hackthissite.org/.git/HEAD

## nikto [medium]

Command: nikto -h https://hackthissite.org/

- Nikto v2.5.0

-----  
+ Multiple IPs found: 137.74.187.102, 137.74.187.104, 137.74.187.103, 137.74.187.101, 137.74.187.100

+ Target IP: 137.74.187.102

+ Target Hostname: hackthissite.org

+ Target Port: 443  
-----

+ SSL Info: Subject: /CN=hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion

Ciphers: ECDHE-RSA-AES256-GCM-SHA384

Issuer: /C=GR/O=Hellenic Academic and Research Institutions CA/CN=HARICA DV TLS RSA

+ Start Time: 2026-02-12 02:50:46 (GMT-5)  
-----

+ Server: HackThisSite

+ /: Retrieved access-control-allow-origin header: \*.

+ /: The anti-clickjacking X-Frame-Options header is not present. See:  
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

+ /: Uncommon header 'public-key-pins-report-only' found, with contents:  
pin-sha256="YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=";  
pin-sha256="Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys="; max-age=2592000; includeSubDomains;  
report-uri="https://hackthissite.report-uri.com/r/d/hpkip/reportOnly".

+ /: Uncommon header 'onion-location' found, with contents:  
<http://hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion/>.

+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>

+ /: Cookie HackThisSite created without the secure flag. See: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>

+ /: Cookie HackThisSite created without the httponly flag. See: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>

## hydra [info]

Command: hydra <https://hackthissite.org/>

## curl [critical]

Command: curl <https://hackthissite.org/>

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>
  <title>Hack This Site</title>
  <meta name="verify-v1" content="s/YXn7eQrMBoF9PL5jLJDjWpAxEXpJzE9JLg/zM4C2Y=" />
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <meta name="author" content="HackThisSite.org Staff" />
  <meta name="keywords" content="challenge, computer, culture, deface, digital, ethics, games, guide, hack, hack forums, hacker,
hackers, hacking, hacking challenges, hacking forums, mission, net, programming, radical, revolution, root, rooting, security, site,
society, tutorial, tutorials, war, wargame, wargames, web, website" />
  <meta name="title" content="HackThisSite" />
  <meta name="description" content="HackThisSite.org is a free, safe and legal training ground for hackers to test and expand their
ethical hacking skills with challenges, CTFs, and more." />
  <meta itemprop="name" content="HackThisSite" />
  <meta itemprop="description" content="HackThisSite.org is a free, safe and legal training ground for hackers to test and expand
their ethical hacking skills with challenges, CTFs, and more." />
  <meta itemprop="image" content="https://data.htscdn.org/images/hackthissite-meta-card.png" />
  <meta property="og:type" content="website" />
  <meta property="og:url" content="https://www.hackthissite.org/" />
  <meta property="og:title" content="HackThisSite" />
  <meta property="og:description" content="HackThisSite.org is a free, safe and legal training ground for hackers to test and expand
their ethical hacking skills with challenges, CTFs, and more." />
  <meta property="og:image" content="https://data.htscdn.org/images/hackthissite-meta-card.png" />
  <meta property="twitter:card" content="summary_large_image" />
  <meta property="twitter:url" content="https://www.hackthissite.org/" />
  <meta property="twitter:titl
```

## hydra [info]

Command: hydra <https://hackthissite.org/>

## sqlmap [info]

Command: sqlmap --batch --dbs --level 1 --risk 1 <https://hackthissite.org/>

## curl [critical]

Command: curl <https://hackthissite.org/>

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>
  <title>Hack This Site</title>
  <meta name="verify-v1" content="s/YXn7eQrMBoF9PL5jLJDjWpAxEXpJzE9JLg/zM4C2Y=" />
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <meta name="author" content="HackThisSite.org Staff" />
  <meta name="keywords" content="challenge, computer, culture, deface, digital, ethics, games, guide, hack, hack forums, hacker,
```

hackers, hacking, hacking challenges, hacking forums, mission, net, programming, radical, revolution, root, rooting, security, site, society, tutorial, tutorials, war, wargame, wargames, web, website" />

```
<meta name="title" content="HackThisSite" />
<meta name="description" content="HackThisSite.org is a free, safe and legal training ground for hackers to test and expand their ethical hacking skills with challenges, CTFs, and more." />
<meta itemprop="name" content="HackThisSite" />
<meta itemprop="description" content="HackThisSite.org is a free, safe and legal training ground for hackers to test and expand their ethical hacking skills with challenges, CTFs, and more." />
<meta itemprop="image" content="https://data.htscdn.org/images/hackthissite-meta-card.png" />
<meta property="og:type" content="website" />
<meta property="og:url" content="https://www.hackthissite.org/" />
<meta property="og:title" content="HackThisSite" />
<meta property="og:description" content="HackThisSite.org is a free, safe and legal training ground for hackers to test and expand their ethical hacking skills with challenges, CTFs, and more." />
<meta property="og:image" content="https://data.htscdn.org/images/hackthissite-meta-card.png" />
<meta property="twitter:card" content="summary_large_image" />
<meta property="twitter:url" content="https://www.hackthissite.org/" />
<meta property="twitter:titl
```

## ssllscan [medium]

Command: ssllscan https://hackthissite.org/

Version: [32m2.1.5 [0m

OpenSSL 3.5.4 30 Sep 2025

[0m

[32mConnected to 137.74.187.103 [0m

Testing SSL server [32mhackthissite.org [0m on port [32m443 [0m using SNI name [32mhackthissite.org [0m

[1;34mSSL/TLS Protocols: [0m

SSLv2 [32mdisabled [0m

SSLv3 [32mdisabled [0m

TLSv1.0 [32mdisabled [0m

TLSv1.1 [32mdisabled [0m

TLSv1.2 enabled

TLSv1.3 [33mdisabled [0m

[1;34mTLS Fallback SCSV: [0m

Server [32msupports [0m TLS Fallback SCSV

[1;34mTLS renegotiation: [0m

Session renegotiation [32mnot supported [0m

[1;34mTLS Compression: [0m

Compression [32mdisabled [0m

[1;34mHeartbleed: [0m

TLSv1.2 [32mnot vulnerable [0m to heartbleed

[1;34mSupported Server Cipher(s): [0m

[32mPreferred [0m TLSv1.2 [32m256 [0m bits [32mECDHE-RSA-AES256-GCM-SHA384 [0m Curve P-256 DHE 256

Accepted TLSv1.2 [32m128 [0m bits [32mECDHE-RSA-AES128-GCM-SHA256 [0m Curve P-256 DHE 256

Accepted TLSv1.2 [32m256 [0m bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256

Accepted TLSv1.2 [32m128 [0m bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256

Accepted TLSv1.2 [32m256 [0m bits AES256-GCM-SHA384

Accepted TLSv1.2 [32m128 [0m bits AES128-GCM-SHA256  
Accepted TLSv1.2 [32m256 [0m bits AES256-SHA256  
Accepted TLSv1.2 [32m128 [0m bits AES128-SHA256

[1;34mServer Key Exchange Group(s): [0m  
TLSv1.2 [32m128 [0m bits secp256r1 (NIST P-256) [0m

[1;34mSSL Certificate: [0m  
Signature Algorithm: [32msha256WithRSAEncryption [0m  
RSA Key Strength: [32m4096 [0m

Subject: hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion  
Altnames: DNS:hackthissite.org, DNS:www.hackthissite.org,  
DNS:hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion  
Issuer: HARICA DV TLS RSA

Not valid before: [32mMar 25 04:43:22 2025 GMT [0m  
Not valid after: [32mMar 25 04:43:22 2026 GMT [0m

nikto [high]

Command: nikto -h https://hackthissite.org/  
- Nikto v2.5.0

+ Multiple IPs found: 137.74.187.102, 137.74.187.103, 137.74.187.100, 137.74.187.101, 137.74.187.104  
+ Target IP: 137.74.187.102  
+ Target Hostname: hackthissite.org  
+ Target Port: 443

+ SSL Info: Subject: /CN=hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion  
Ciphers: ECDHE-RSA-AES256-GCM-SHA384  
Issuer: /C=GR/O=Hellenic Academic and Research Institutions CA/CN=HARICA DV TLS RSA  
+ Start Time: 2026-02-12 02:56:04 (GMT-5)

+ Server: HackThisSite  
+ /: Retrieved access-control-allow-origin header: \*.  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>  
+ /: Uncommon header 'public-key-pins-report-only' found, with contents:   
pin-sha256="YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=";  
pin-sha256="Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys="; max-age=2592000; includeSubDomains;  
report-uri="https://hackthissite.report-uri.com/r/d/hpkip/reportOnly".  
+ /: Uncommon header 'onion-location' found, with contents:   
<http://hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion/>.  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>  
+ /: Cookie HackThisSite created without the secure flag. See: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>  
+ /: Cookie HackThisSite created without the httponly flag. See: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>

curl [high]

Command: curl https://hackthissite.org/  
<!DOCTYPE html>  
<html lang="en">  
<head>

```

<meta charset="UTF-8">
<title>HackThisSite.org | Offline for Maintenance</title>
<style>
body { background: #eee; text-align: center; padding: 20px; }
h1 { font-size: 50px; }
body { font: 20px Helvetica, sans-serif; color: #333; }
article { display: block; text-align: left; width: 700px; margin: 0 auto; }
img { max-width: 650px; height: auto; }
a { color: #dc8100; text-decoration: none; }
a:hover { color: #000; text-decoration: none; }
</style>
</head>
<body>
<article>
<h1>Offline for Maintenance</h1>
<div></div>
<div>
<p>Our apologies for the inconvenience, but this site is temporarily offline for maintenance (usually nightly backups at 8:00 AM UTC).
If this lasts longer than 60 minutes, please feel free to <a href="mailto:admin AT hack this site DOT org">email us</a> or <a
href="https://hacked.chat">contact us on Discord</a>.</p>
<p>&mdash; HackThisSite.org</p>
</div>
</article>
</body>
</html>

```

## dirb [medium]

Command: dirb https://hackthissite.org/

```

-----
DIRB v2.22
By The Dark Raver
-----

```

```

START_TIME: Thu Feb 12 03:01:14 2026
URL_BASE: https://hackthissite.org/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

```

\*\*\* Generating Wordlist...

GENERATED WORDS: 4612

---- Scanning URL: https://hackthissite.org/ ----

\*\*\* Calculating NOT\_FOUND code...

```

--> Testing: https://hackthissite.org/.bash_history
https://hackthissite.org/.bashrc
(CODE:301|SIZE:243)

```

--> Testing:

+ https://hackthissite.org/.bashrc

--> Testing: https://hackthissite.org/.cache

```

--> Testing: https://hackthissite.org/.config
(CODE:301|SIZE:243)

```

+ https://hackthissite.org/.config

--> Testing: https://hackthissite.org/.cvs

```

--> Testing: https://hackthissite.org/.cvsignore
https://hackthissite.org/.forward
(CODE:301|SIZE:244)

```

--> Testing:

+ https://hackthissite.org/.forward

\_\_\_\_\_ ^ \ \_\_\_\_\_  
/\_\ / \_\ ' \_\ ' \_\ '\ \ \ \ [1m [4m [37mv4.1 [0m  
^ \ /\ \ \ \ \ \ \ \ \ \ \ \ \ \ > </



```
\\____\\____^\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\  [90m [4mhttps://commixproject.com [0m
V____N____/ V_N_N_N_N_N_N_N_N_N_N/ ( [91m@commixproject [0m
```

+--

[1mAutomated All-in-One OS Command Injection Exploitation Tool [0m  
Copyright © 2014-2025 Anastasios Stasinopoulos [0m ( [91m@ancst [0m)

+--

( [1m [31m! [0m) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[0m

[ [94m03:08:22 [0m] [ [41mcritical [0m] Missing a mandatory option (-u, -l, -m, -r, -x, --wizard, --list-tampers or --purge). Use -h for help. [0m

## curl [medium]

Command: curl https://hackthissite.org/

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>HackThisSite.org | Offline for Maintenance</title>
<style>
body { background: #eee; text-align: center; padding: 20px; }
h1 { font-size: 50px; }
body { font: 20px Helvetica, sans-serif; color: #333; }
article { display: block; text-align: left; width: 700px; margin: 0 auto; }
img { max-width: 650px; height: auto; }
a { color: #dc8100; text-decoration: none; }
a:hover { color: #000; text-decoration: none; }
</style>
</head>
<body>
<article>
<h1>Offline for Maintenance</h1>
<div></div>
<div>
<p>Our apologies for the inconvenience, but this site is temporarily offline for maintenance (usually nightly backups at 8:00 AM UTC). If this lasts longer than 60 minutes, please feel free to <a href="mailto:admin AT hack this site DOT org">email us</a> or <a href="https://hacked.chat">contact us on Discord</a>.</p>
<p>&mdash; HackThisSite.org</p>
</div>
</article>
</body>
</html>
```

## curl [medium]

Command: curl https://hackthissite.org/

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>HackThisSite.org | Offline for Maintenance</title>
```

```

<style>
body { background: #eee; text-align: center; padding: 20px; }
h1 { font-size: 50px; }
body { font: 20px Helvetica, sans-serif; color: #333; }
article { display: block; text-align: left; width: 700px; margin: 0 auto; }
img { max-width: 650px; height: auto; }
a { color: #dc8100; text-decoration: none; }
a:hover { color: #000; text-decoration: none; }
</style>
</head>
<body>
<article>
<h1>Offline for Maintenance</h1>
<div></div>
<div>
<p>Our apologies for the inconvenience, but this site is temporarily offline for maintenance (usually nightly backups at 8:00 AM UTC).
If this lasts longer than 60 minutes, please feel free to <a href="mailto:admin AT hack this site DOT org">email us</a> or <a
href="https://hacked.chat">contact us on Discord</a>.</p>
<p>&mdash; HackThisSite.org</p>
</div>
</article>
</body>
</html>

```

## nikto [critical]

Command: nikto -h https://hackthissite.org/

- Nikto v2.5.0

```

-----
+ Multiple IPs found: 137.74.187.104, 137.74.187.103, 137.74.187.102, 137.74.187.101, 137.74.187.100
+ Target IP:      137.74.187.104
+ Target Hostname:  hackthissite.org
+ Target Port:    443

```

```

-----
+ SSL Info:      Subject: /CN=hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion
                  Ciphers: ECDHE-RSA-AES256-GCM-SHA384
                  Issuer:  /C=GR/O=Hellenic Academic and Research Institutions CA/CN=HARICA DV TLS RSA
+ Start Time:    2026-02-12 03:08:32 (GMT-5)

```

```

-----
+ Server: HackThisSite
+ /: Retrieved access-control-allow-origin header: *.
+ /: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'onion-location' found, with contents:
http://hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion/.
+ /: Uncommon header 'public-key-pins-report-only' found, with contents:
pin-sha256="YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=";
pin-sha256="Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys="; max-age=2592000; includeSubDomains;
report-uri="https://hackthissite.report-uri.com/r/d/hpkp/reportOnly".
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different
fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie HackThisSite created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie HackThisSite created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

```

## tcpdump [info]

Command: tcpdump https://hackthissite.org/

## nmap [low]

Command: nmap -F -T4 -sV https://hackthissite.org/

Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-12 03:13 -0500

Nmap done: 0 IP addresses (0 hosts up) scanned in 0.16 seconds

## curl [critical]

Command: curl https://hackthissite.org/

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>HackThisSite.org | Offline for Maintenance</title>
<style>
body { background: #eee; text-align: center; padding: 20px; }
h1 { font-size: 50px; }
body { font: 20px Helvetica, sans-serif; color: #333; }
article { display: block; text-align: left; width: 700px; margin: 0 auto; }
img { max-width: 650px; height: auto; }
a { color: #dc8100; text-decoration: none; }
a:hover { color: #000; text-decoration: none; }
</style>
</head>
<body>
<article>
<h1>Offline for Maintenance</h1>
<div></div>
<div>
<p>Our apologies for the inconvenience, but this site is temporarily offline for maintenance (usually nightly backups at 8:00 AM UTC).
If this lasts longer than 60 minutes, please feel free to <a href="mailto:admin AT hack this site DOT org">email us</a> or <a
href="https://hacked.chat">contact us on Discord</a>.</p>
<p>&mdash; HackThisSite.org</p>
</div>
</article>
</body>
</html>
```

## ssllscan [medium]

Command: ssllscan https://hackthissite.org/

Version: [32m2.1.5 [0m

OpenSSL 3.5.4 30 Sep 2025

[0m

[32mConnected to 137.74.187.103 [0m

Testing SSL server [32mhackthissite.org [0m on port [32m443 [0m using SNI name [32mhackthissite.org [0m

[1;34mSSL/TLS Protocols: [0m

SSLv2 [32mdisabled [0m

SSLv3 [32mdisabled [0m

TLSv1.0 [32mdisabled [0m

TLSv1.1 [32mdisabled [0m

TLSv1.2 enabled

TLSv1.3 [33mdisabled [0m

[1;34mTLS Fallback SCSV: [0m

Server [32msupports [0m TLS Fallback SCSV

[1;34mTLS renegotiation: [0m

Session renegotiation [32mnot supported [0m

[1;34mTLS Compression: [0m

Compression [32mdisabled [0m

[1;34mHeartbleed: [0m

TLSv1.2 [32mnot vulnerable [0m to heartbleed

[1;34mSupported Server Cipher(s): [0m

[32mPreferred [0m TLSv1.2 [32m256 [0m bits [32mECDHE-RSA-AES256-GCM-SHA384 [0m Curve P-256 DHE 256

Accepted TLSv1.2 [32m128 [0m bits [32mECDHE-RSA-AES128-GCM-SHA256 [0m Curve P-256 DHE 256

Accepted TLSv1.2 [32m256 [0m bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256

Accepted TLSv1.2 [32m128 [0m bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256

Accepted TLSv1.2 [32m256 [0m bits AES256-GCM-SHA384

Accepted TLSv1.2 [32m128 [0m bits AES128-GCM-SHA256

Accepted TLSv1.2 [32m256 [0m bits AES256-SHA256

Accepted TLSv1.2 [32m128 [0m bits AES128-SHA256

[1;34mServer Key Exchange Group(s): [0m

TLSv1.2 [32m128 [0m bits secp256r1 (NIST P-256) [0m

[1;34mSSL Certificate: [0m

Signature Algorithm: [32msha256WithRSAEncryption [0m

RSA Key Strength: [32m4096 [0m

Subject: hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion

AltNames: DNS:hackthissite.org,

DNS:www.hackthissite.org,

DNS:hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion

Issuer: HARICA DV TLS RSA

Not valid before: [32mMar 25 04:43:22 2025 GMT [0m

Not valid after: [32mMar 25 04:43:22 2026 GMT [0m

## wireshark [info]

Command: wireshark https://hackthissite.org/

## hydra [info]

Command: hydra https://hackthissite.org/

## curl [medium]

Command: curl https://hackthissite.org/

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

```
<title>HackThisSite.org | Offline for Maintenance</title>
<style>
body { background: #eee; text-align: center; padding: 20px; }
h1 { font-size: 50px; }
body { font: 20px Helvetica, sans-serif; color: #333; }
article { display: block; text-align: left; width: 700px; margin: 0 auto; }
img { max-width: 650px; height: auto; }
a { color: #dc8100; text-decoration: none; }
a:hover { color: #000; text-decoration: none; }
</style>
</head>
<body>
<article>
<h1>Offline for Maintenance</h1>
<div></div>
<div>
<p>Our apologies for the inconvenience, but this site is temporarily offline for maintenance (usually nightly backups at 8:00 AM UTC).
If this lasts longer than 60 minutes, please feel free to <a href="mailto:admin AT hack this site DOT org">email us</a> or <a
href="https://hacked.chat">contact us on Discord</a>.</p>
<p>&mdash; HackThisSite.org</p>
</div>
</article>
</body>
</html>
```

## curl [high]

Command: curl https://hackthissite.org/

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>HackThisSite.org | Offline for Maintenance</title>
<style>
body { background: #eee; text-align: center; padding: 20px; }
h1 { font-size: 50px; }
body { font: 20px Helvetica, sans-serif; color: #333; }
article { display: block; text-align: left; width: 700px; margin: 0 auto; }
img { max-width: 650px; height: auto; }
a { color: #dc8100; text-decoration: none; }
a:hover { color: #000; text-decoration: none; }
</style>
</head>
<body>
<article>
<h1>Offline for Maintenance</h1>
<div></div>
<div>
<p>Our apologies for the inconvenience, but this site is temporarily offline for maintenance (usually nightly backups at 8:00 AM UTC).
If this lasts longer than 60 minutes, please feel free to <a href="mailto:admin AT hack this site DOT org">email us</a> or <a
href="https://hacked.chat">contact us on Discord</a>.</p>
<p>&mdash; HackThisSite.org</p>
</div>
</article>
</body>
```

