

Forum:[Hack Forums](#)

Thread: [Help With Pentesting a Server. Nginx, Pterodactyl](#)

Varoax - October 20, 2019, 9:49 am

Hey guys, I am trying to pen test my friends server. (He asked me to do this since he knew I am trying to get into pen testing.)

I found shellshock vulnerability and I think one other but I don't know what to do. I ran a shellshock Python exploit on Kali Linux but it have me a HTTP. No response 404 error.

This is all the info I have found on it, could someone guide me in the right direction to finding it and trying to fix it.

I do think there are some outdated server programs that are outdated.

(I have taken out the IP's for safety of the server.)

Heres the file download to all of the scans. (All the text was to big to put here.)

mega(.)nz/#!Afojmk4!oQCEYPj1Caqf Oi9MU9q9n_JfbheCePgdwZSCSrv18Ks

- Nikto v2.1.6

+ Target IP:

+ Target Hostname:

+ Target Port: 443

+ SSL Info: Subject: /CN=

Ciphers: ECDHE-RSA-AES256-GCM-SHA384

Issuer: /C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3

+ Start Time: 2019-10-19 23:16:30 (GMT-4)

+ Server: nginx

+ Cookie pterodactyl_session created without the secure flag

+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.

+ The site uses SSL and Expect-CT header is not present.

+ Root page / redirects to:

+ No CGI Directories found (use '-C all' to force check all possible dirs)

-C all

- STATUS: Completed 370 requests (~5% complete, 22.9 minutes left): currently in plugin 'Site Files'

- STATUS: Running average: 100 requests: 0.22311 sec, 10 requests: 0.2296 sec.

+ OSVDB-112004: /admin.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /administrator.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /authLogin.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /bb-hist.sh: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /banner.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /book.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /cgiinfo.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /cgittest.py: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /cgi_wrapper: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /contact.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /count.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /defaultwebpage.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /download.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /entropysearch.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /env.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /environment.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /ezmlm-browse: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /formmail.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /FormMail-clone.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /guestbook.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /helpdesk.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /index.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /index.pl: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /info.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /info.sh: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /loadpage.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /login.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /login.pl: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /pathtest.pl: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /php: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /php4: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /php5: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /php-cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

+ OSVDB-112004: /php.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).
+ OSVDB-112004: /php.fcgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).
+ OSVDB-112004: /printenv: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).
+ OSVDB-112004: /restore_config.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).
+ OSVDB-112004: /ruby.rb: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).
+ OSVDB-112004: /search: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).
+ OSVDB-112004: /search.cgi: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6278).

nOrr - *October 21, 2019, 1:46 pm*

Read up on how shellshock works and then do it. Its relatively simple.