

Forum:[Hack Forums](#)

Thread: [Website hacked, but didnt find the Vuln?](#)

PingByte1337 - November 20, 2021, 11:29 am

Hey Guys, i found a hacked Website.

I would like to see, how the hacker find the vuln.

w w w. sterngold.digitalbrandz.net/

Nmap say

```
21/tcp open  ftp
22/tcp open  ssh
25/tcp filtered smtp
26/tcp open  rsftp
42/tcp filtered nameserver
53/tcp open  domain
80/tcp open  http
110/tcp open  pop3
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
143/tcp open  imap
443/tcp open  https
445/tcp filtered microsoft-ds
465/tcp open  smtps
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s
2222/tcp open  EtherNetIP-1
3306/tcp open  mysql
```

i scanned with gobuster a lot of dirs, but all access denied. Now my question, how hacked the guy this site?

Beladonis - November 20, 2021, 11:53 am

Imagine you were the attacker, and you didn't care about remaining undetected, what would you do to prevent others to compromise your hacked webserver? Well, you would probably remove or patch the vulnerability by sanitizing the scripts, removing page(s), etc. That's probably what they did, hence you can't find an entry way... or you didn't dig deep enough.

PingByte1337 - November 20, 2021, 12:01 pm

(Nov 20, 2021 12:53 PM)Beladonis Wrote: [\[CITE\]](#) Imagine you were the attacker, and you didn't care about remaining undetected, what would you do to prevent others to compromise your hacked webserver? Well, you would probably remove or patch the vulnerability by sanitizing the scripts, removing page(s), etc.

a deface page? common... at a company where i am on a server, i agree with you

Payload™ - November 20, 2021, 12:12 pm

Basically there is no magic tool to get this done within few clicks. You should re-search every protocol you have posted, do the according tests on them, and after that start looking for a CVE's or another exploits. Kali Linux / ParrotOS is a good place to start, but it will require learning it aswell.

Beladonis - November 20, 2021, 4:47 pm

Okay so apparently the files are still there, it's just that the web server replies 500 Internal Server Error when you try to access PHP files, the hacker threw a wrench into the works by messing with the htaccess or the server configuration.

I found [this](#) but I don't think you can do anything useful with that.

So how did the hacker do that? It's hard to tell. Was most likely an SQL injection in my opinion, when things were still accessible.

PingByte1337 - November 20, 2021, 11:43 pm

(Nov 20, 2021 05:47 PM)Beladonis Wrote: [CITE](#) Okay so apparently the files are still there, it's just that the web server replies 500 Internal Server Error when you try to access PHP files, the hacker threw a wrench into the works by messing with the htaccess or the server configuration.

I found [this](#) but I don't think you can do anything useful with that.

So how did the hacker do that? It's hard to tell. Was most likely an SQL injection in my opinion, when things were still accessible.

Ah Ok, thanks ?

3thicalnoob - November 23, 2021, 11:56 pm

Try Reverse IP Hack Any website then try to hack there server

Code <https://viewdns.info/reverseip/?host=173.254.51.208&t=1>
or you can try bruteforcing

This website using wordpress

dbran.net/?author=1 USERNAME:admin

Or you can scan there plugin via wpscan

or try Domain Dossier

Here is the details

sterngold.digitalbran.net

Email: surojitbis***@gmail.com

find there pass in leaked db.. and try to login there domain and cp

webking - December 11, 2021, 2:48 pm

You need do a scan for this website on all of ports. Should get something

lorrrra - December 11, 2021, 3:04 pm

Yo bro check your private message please i messaged you

wyvn - December 13, 2021, 5:58 am

(Nov 24, 2021 12:56 AM)3thicalnoob Wrote: [\[CITE\]](#) Try Reverse IP Hack Any website then try to hack there server

Code <https://viewdns.info/reverseip/?host=173.254.51.208&t=1>
or you can try bruteforcing

This website using wordpress

dbran.net/?author=1 USERNAME:admin

Or you can scan there plugin via wpscan

or try Domain Dossier

Here is the details

sterngold.digitalbran.net

Email: surojitbis***@gmail.com

find there pass in leaked db.. and try to login there domain and cp
this guy fucks.. "Reverse IP Hack"? crazy

618C - December 13, 2021, 6:04 am

man all these trolls here. OP its not related to any open ports, ports doesn't matter for this.

its most likeliy found by using an web app scanner searching for vulnerabilities within the software that runs on the server.

Apache maybe?

Or just another word-press website with obsolete and out of date plugins. ?

looks like they uploaded a shell that give em access to your environment. happens a lot.
there for always make backups.

Vypez. - December 15, 2021, 11:04 pm

Its bu**sh*t, idk why would you do something like this. Better do ransomware lol