

Forum:[Hack Forums](#)

Thread: [Accessing backend of one webpage by exploiting a different website on the same server](#)

41phafr34k - February 3, 2017, 1:32 am

Forgive my ignorance here but this is the first time I have taken the knowledge I have, the tools I've learnt and the scripts I have made and put them all together for the purpose of doing a pen-test.

Anyways, last night I set a vague but pretty obvious goal and this morning I began my recon. I had no direct focus. I just wanted to access a system within a certain organization, whether it be someone in charges phone or email or pc. the website database or the office vcomputer/wifi/file system. Anyways, not wanting to leave my house I focused that days recon on the website they have created and some also easy to obtain public information. Anyways, while search, digging and probing it turns out there are 2 other websites on the same server as the site I want to exploit but so far have come up short (trying to find a way that doesn't raise any flags so I can open a back door then step away for a very very extended period of time. Its running APACHE which as far as I know is easily exploitable especially using metasploit but its risky situation so I'd rather not attempt something I haven't done.

ANYWAYS!!! another site on the server (completely unrelated to the one i want) is very exploitable using SQL and much much more (PHP and SQL)

To the point of this thread:

If I exploit the second site with the SQL vulnerabilities and manage to access the backend will I be able to easily access the other webpage on said server??

Like I said I just want to know I can get in, take a look around so I can add any info needed to complete my recon information folder and make a back door available so at any time I can access it and I was thinking if access from a different site on the server maybe I can avoid raising alarms on my target.

Hopefully you guys understand what I was asking.

Viktory - February 3, 2017, 2:03 am

like yani said there's many ways this can go. you must enum further

one approach is to see if you can gain shell on that domain and try symlink to where you want access. apart from access to db creds you may also find some test code being eval'd which you can use to code exec...

41phafr34k - February 3, 2017, 2:19 pm

(Feb 3, 2017 02:33 AM)Anubis™ Wrote: [\[CITE\]](#) I just came to say that you seem like troll and I don't want to bother reading this.

So because I am not an expert pen-tester/programmer/server admin I'm a troll??

Thanks to you other guys for the help.

Servers essentially act just like a regular computer then but with public access (like file-sharing through http port) to certain documents? i.e html?

So if I get in maybe I could bruteforce the administrator pass? Does that normal sound any alarms or could someone just keep going until they are in? (bruteforcing I mean)

ASLR - February 3, 2017, 2:28 pm

(Feb 3, 2017 03:19 PM)41phafr34k Wrote: [\[CITE\]](#) So because I am not an expert pen-tester/programmer/server admin I'm a troll??

Thanks to you other guys for the help.

Servers essentially act just like a regular computer then but with public access (like file-sharing through http port) to certain documents? i.e html?

So if I get in maybe I could bruteforce the administrator pass? Does that normal sound any alarms or could someone just keep going until they are in? (bruteforcing I mean)

The better option would be to collect system information then look for a public local privilege escalation vulnerability that they haven't patched yet.

41phafr34k - February 3, 2017, 2:39 pm

(Feb 3, 2017 03:28 PM)Packy Wrote: [\[CITE\]](#) The better option would be to collect system information then look for a public local privilege escalation vulnerability that they haven't patched yet.

Thats a good idea. Thank you.