

Forum:[Hack Forums](#)

Thread: [exploiting a website](#)

ichung - February 15, 2025, 8:36 am

Hi guys anyone can suggest me any exploit i can use for an https site? I would like to get an admin access, I've done a quick analysis of the site and noticed that it doesn't have CSP and HSTS, it doesn't even have X-Frame-Options and X-Content-Type-Options. The version of the server is Apache/2.4.6 that is pretty old. Any advice??

Tyr - February 15, 2025, 8:55 am

sqlmap is my go to and is great for beginners but best way to learn in manual injection by playing with parameters

ichung - February 15, 2025, 9:32 am

(Feb 15, 2025 09:55 AM)Tyr Wrote: [\[CITE\]](#) sqlmap is my go to and is great for beginners but best way to learn in manual injection by playing with parameters

oh thanks dude, can you give me some good sources for that? Another thing, what about logs? I've noticed that logs are not always easy to hide. Thanks for your kindness

Tyr - February 15, 2025, 9:47 am

(Feb 15, 2025 10:32 AM)ichung Wrote: [\[CITE\]](#) oh thanks dude, can you give me some good sources for that? Another thing, what about logs? I've noticed that logs are not always easy to hide. Thanks for your kindness

sure: <https://github.com/sqlmapproject/sqlmap/wiki/usage> - if you prefer videos just search on YT; there's many. as far as logs do you mean obfuscated your attempts at cracking the site? i.e. getting blocked?

DramaKing - February 15, 2025, 12:06 pm

(Feb 15, 2025 10:32 AM)ichung Wrote: [\[CITE\]](#) oh thanks dude, can you give me some good sources for that? Another thing, what about logs? I've noticed that logs are not always easy to hide. Thanks for your kindness

Your attacks will be logged. There is nothing that you can do to get around that.

Some vulnerabilities to look at:

<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=apache+2.4>

https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=apache+2.4&search_type=all&isCpeNameSearch=false

I haven't even been able to hack apache2 on vulnerable lab machines, so I won't be much more help.

Money- - February 15, 2025, 10:14 pm

These things you mentioned aren't going to get you admin access though , they are just information for you to further find out more severe vulnerabilities to exploit further.

ichung - February 16, 2025, 5:44 am

(Feb 15, 2025 10:47 AM)Tyr Wrote: [\[CITE\]](#) - if you prefer videos just search on YT; there's many. as far as logs do you mean obfuscated your attempts at cracking the site? i.e. getting blocked? yeah exactly cause sometimes the sites register everything, even small changes.

(Feb 15, 2025 11:14 PM)Money- Wrote: [\[CITE\]](#) These things you mentioned aren't going to get you admin access though, they are just information for you to further find out more severe vulnerabilities to exploit further.
yeah, but with an SQL injection i should be able to get admin access, isn't it?

(Feb 15, 2025 01:06 PM)DramaKing Wrote: [\[CITE\]](#) Your attacks will be logged. There is nothing that you can do to get around that.

Some vulnerabilities to look at:

I haven't even been able to hack apache2 on vulnerable lab machines, so I won't be much more help.
really? No way to hide that?

vetbesim - February 16, 2025, 8:24 am

Maybe you could find an admin login or something you could use to get admin access. Check out robots.txt and also run a directory brute forcer like dirsearch

ichung - February 16, 2025, 10:12 am

(Feb 16, 2025 09:24 AM)vetbesim Wrote: [\[CITE\]](#) Maybe you could find an admin login or something you could use to get admin access. Check out robots.txt and also run a directory brute forcer like dirsearch

oh i didn't know about that brute forcer, i checked it out and seems great. Yeah probably brute force is a great way to obtain the admin credentials. Thanks for all the advices dude

Tyr - February 17, 2025, 8:41 am

(Feb 16, 2025 06:44 AM)ichung Wrote: [\[CITE\]](#) yeah exactly cause sometimes the sites register everything, even small changes.

yeah, but with an SQL injection i should be able to get admin access, isn't it?

really? No way to hide that?
i gotcha. yeah sql is a very good ttp to get into many web servers especially phpmyadmin stacks without proper hardening applied

vetbesim - February 17, 2025, 8:34 pm

Here, this will help you learn about some ways to break in <https://www.hacksplaining.com/lessons> and <https://www.hacksplaining.com/owasp>

everynight - February 18, 2025, 12:20 am

I need help because I want to learn hacking, and I am a beginner. In addition, I also need to send a character, don't blame (?) translation

Skorp - February 18, 2025, 2:21 pm

Website sounds like a easy target and vuln to mime if it doesn't have the xcontent header. You definitely don't need sqlmap for this, what's the url? Easy shell for me.

Money- - February 18, 2025, 5:21 pm

(Feb 18, 2025 03:21 PM)Skorp Wrote: [\[CITE\]](#) Website sounds like a easy target and vuln to mime if it doesn't have the xcontent header. You definitely don't need sqlmap for this, what's the url? Easy shell for me.

What methodology you plan to use? Bypass MIME via file upload? Since xcontent aren't specified.

ichung - February 20, 2025, 7:22 am

(Feb 18, 2025 06:21 PM)Money- Wrote: [\[CITE\]](#) What methodology you plan to use? Bypass MIME via file upload? Since xcontent aren't specified.

ehy dude, I don't know if MIME (image/jpeg, application/pdf) could work, I was going through sqlmap but the only problem is that it's hard to get an admin access with that, you know.

ichung - February 24, 2025, 11:03 am

(Feb 18, 2025 03:21 PM)Skorp Wrote: [\[CITE\]](#) Website sounds like a easy target and vuln to mime if it doesn't have the xcontent header. You definitely don't need sqlmap for this, what's the url? Easy shell for me.

do you think without xcontent header i would be easy with mime? can you contact me in DM? (I can't cause i need to write 25 quality post to unlock DMs) Imma give you the url so you can give a quick check to the site if you want, cause to me it seems very vurnerable but as i said I'm not a pro.

id0rr - February 25, 2025, 2:22 pm

if you can't find the vulnerability, you can't exploit it

i saw the replies, com'n, you kids need to shut down that computer and learn.

sam_sepiol - February 26, 2025, 5:59 am

Guys I want to hack a porn website, hack in the sense of killing the website or shutting it down or enlisting it off the internet ? can anyone teach me ?