

Forum:[Hack Forums](#)

Thread: [Need advice cracking into a site](#)

ElHombre - June 13, 2015, 3:51 pm

Hey guys!

Please bear with me here as I do not know much about web penetration.

The site is basically a database. It has a simple user and password access page that redirects you to individual databases for each user. There are plenty of admins and plenty of normal users from what I know.

The connection uses TLS 1.0 and it's encrypted using AES_256_CBC with SHA1 signatures for message authentication and RSA for key exchange (it's got a pretty outdated security).

I ran a quick scan with Acunetix and, among others, it only found the following weaknesses:

- HTML form without CSRF protection
- SSL weak ciphers
- TLS1/SSLv3 Renegotiation Vulnerability
- Login page password-guessing attack
- OPTIONS and TRACE methods are enabled

The idea is to be able to break in the database, being able to twitch some values and whatnot on the site, it's mostly a learning project. I already have several normal users' passwords and names to login into the database too. The perfect outcome would be to obtain some actual admin accounts' access information.

I just want to hear some suggestions. Literally anything you think I could try that may work.

Thanks in advance for your time and help.

21redallday12 - June 13, 2015, 9:27 pm

I don't mind people not knowing much about a subject as long as their willing to learn. However in your case, you pretend to know what you're talking about when you do not.

I wouldn't describe thoose as major weaknesses.

Google Sql Injection, RCE, LFI, BruteForce etc

ElHombre - June 14, 2015, 2:17 am

(Jun 13, 2015 09:27 PM)21redallday12 Wrote: [\[CITE\]](#) I don't mind people not knowing much about a subject as long as their willing to learn. However in your case, you pretend to know what you're talking about when you do not.

I wouldn't describe thoose as major weaknesses.

Google Sql Injection, RCE, LFI, BruteForce etc

I apologize, I infact admit I do not know much at all about this topic. That's why I wanted to try this

as a 'learning project' as I specified on the message.

However those are the biggest weaknesses the scan could find on the page, that's why I thought they were 'major'. If you could guide me as in how to find the real major weaknesses it would be very helpful.

I will now check those methods out too and see what I can do.

Thanks for the help ?

Mr. Robot - June 14, 2015, 2:19 am

Scan the website with OWASP Zap and report back - TIA

ElHombre - June 14, 2015, 3:38 am

(Jun 14, 2015 02:19 AM)Mr. Robot Wrote: [\[CITE\]](#) Scan the website with OWASP Zap and report back - TIA

Ok so I've never used OWASP Zap before but I just performed the scan.

These are the only high and medium priority alerts it found;

- Remote OS Command Injection (1)
- X-Frame Options Header Not Set (19)

And these are the low priority ones;

- Cookie set without HttpOnly flag (8)
- Incomplete or No Cache-control and Pragma HTTP header set (14)
- Password autocomplete in browser (2)
- Web Browser XSS Protection Not Enabled (19)
- X-Content-Type-Options Header Missing (19)

What should I be looking for? I see this tool has a lot to offer. You can just give me a general idea and I'll try to find more information and tutorials myself.

Thanks for your time. ?

Mr. Robot - June 14, 2015, 3:42 am

Try look into each of the areas and go through one at a time. You aren't looking at trying to exploit this with an easy one type/click method. Try each and see where it fails - learn from it and next time you will be able to go smack back woop ting billa bolla ting tong.

ElHombre - June 14, 2015, 3:54 am

(Jun 14, 2015 03:42 AM)Mr. Robot Wrote: [\[CITE\]](#) Try look into each of the areas and go through one at a time. You aren't looking at trying to exploit this with an easy one type/click method. Try each and see where it fails - learn from it and next time you will be able to go smack back woop ting billa bolla ting tong.

Haha will do ?

Thanks again!

WubCannon - June 14, 2015, 7:29 am

You have remote command injection. Concentrate on the params of that vulnerability and try and exploit it

N0c7urn - June 15, 2015, 4:37 am

(Jun 14, 2015 03:42 AM)Mr. Robot Wrote: [\[CITE\]](#) Try look into each of the areas and go through one at a time. You aren't looking at trying to exploit this with an easy one type/click method. Try each and see where it fails - learn from it and next time you will be able to go smack back woop ting bolla bolla ting tong.

That was beautifully put!