

Forum:[Hack Forums](#)

Thread: [methods that hackers may use to breach website](#)

mohamed111 - April 17, 2023, 7:04 pm

1- Brute Force Attacks: This method involves trying every possible combination of passwords until the correct one is found. Hackers often use software tools that can automate the process, making it faster and more efficient.

2- Cross-Site Scripting (XSS): XSS involves injecting malicious code into a website, allowing the hacker to steal sensitive information, such as login credentials, from unsuspecting users.

3- SQL Injection: This type of attack involves inserting malicious SQL statements into a website's database, allowing the hacker to access or modify sensitive data.

4- Social Engineering: This technique involves tricking people into revealing sensitive information, such as login credentials or personal data. Phishing emails and social media scams are common examples of social engineering.

5- Session Hijacking: This type of attack involves taking over a user's active session on a website, allowing the hacker to access the user's account and perform actions on their behalf.

6- DNS Spoofing: This technique involves redirecting a user's web traffic to a fake website that looks like the real one, allowing the hacker to steal sensitive information.

Ducky - April 17, 2023, 7:29 pm

Please stop spamming LQ ChatGPT posts.

Infomus - April 18, 2023, 3:21 am

(Apr 17, 2023 07:04 PM)mohamed111 Wrote: [CITE](#) 1- Brute Force Attacks: This method involves trying every possible combination of passwords until the correct one is found. Hackers often use software tools that can automate the process, making it faster and more efficient.

2- Cross-Site Scripting (XSS): XSS involves injecting malicious code into a website, allowing the hacker to steal sensitive information, such as login credentials, from unsuspecting users.

3- SQL Injection: This type of attack involves inserting malicious SQL statements into a website's database, allowing the hacker to access or modify sensitive data.

4- Social Engineering: This technique involves tricking people into revealing sensitive information, such as login credentials or personal data. Phishing emails and social media scams are common examples of social engineering.

5- Session Hijacking: This type of attack involves taking over a user's active session on a website, allowing the hacker to access the user's account and perform actions on their behalf.

6- DNS Spoofing: This technique involves redirecting a user's web traffic to a fake website that looks like the real one, allowing the hacker to steal sensitive information.

Some Good Info / techniques For Beginners To Learn And Research!

DramaKing - April 18, 2023, 10:15 am

Command injection is another one.

PurpleMoss - April 18, 2023, 12:20 pm

(Apr 17, 2023 07:04 PM)mohamed111 Wrote: [CITE](#) 1- Brute Force Attacks: This method involves trying every possible combination of passwords until the correct one is found. Hackers often use software tools that can automate the process, making it faster and more efficient.

2- Cross-Site Scripting (XSS): XSS involves injecting malicious code into a website, allowing the hacker to steal sensitive information, such as login credentials, from unsuspecting users.

3- SQL Injection: This type of attack involves inserting malicious SQL statements into a website's database, allowing the hacker to access or modify sensitive data.

4- Social Engineering: This technique involves tricking people into revealing sensitive information, such as login credentials or personal data. Phishing emails and social media scams are common examples of social engineering.

5- Session Hijacking: This type of attack involves taking over a user's active session on a website, allowing the hacker to access the user's account and perform actions on their behalf.

6- DNS Spoofing: This technique involves redirecting a user's web traffic to a fake website that looks like the real one, allowing the hacker to steal sensitive information.

Worth considering the following:

1 and 3 aren't very common anymore, maybe 10 years ago but most frameworks that websites are built on have protection in place against brute forcing and SQLi.

2 is still seen but becoming rarer as the fix is a rather easy one.

4 is your best bet.

5 how would you go about getting a user's active session?

6 not really hacking the website, more along the lines of SE.

CSRF is a good one and still an issue I see a lot.

doom3 - April 26, 2023, 1:59 pm

For me, it's the following.

1. Unpatched CVEs.

2. Leaked credentials (Source code CTRL + U, js files, GITHUB REPO, etc.)

3. Leaked .git, .env, and other configuration files (there's a high chance of getting the source code of the web app through this and being able to see the source code and configs of the application.)

4. Prod server on DEBUG MODE ON (Dev tends to forget to disable this making the application leak sensitive information such as DB Creds, etc.)

5. SQLi (SQLi is still a thing; you must know where to test them and try for time-based SQLi payloads).

