

Hack the Box: Next Steps



Workshop 5 - 17/11/2022

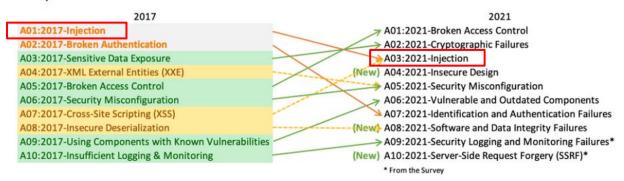
Common Web vulnerabilities



OWASP Top 10 list shows all the most common threats currently. This shows that injection is still a very useful technique to know

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



Source: https://owasp.org/www-project-top-ten/

Structured Query Language



SQL is very useful when used properly and it's a good language to know

Can be used for SQL injections

Useful for navigating a database. Using SHOW tables; to show the tables SELECT * FROM table; to select data from a table

Brute Forcing



When trying to find subdomains or directories it can be useful to try brute force

This is trying every combination of

```
word.domain for subdomains #e.g. docs.google.com
domain/word for directories #e.g. youtube.com/feed
```

and listening for a response

Gobuster



There are lots of tools that uses brute force for network discovery such as gobuster, wfuzz and dirbuster

However gobuster is the tool we will be using as it is easy to use and has all the functionality we need

Gobuster and Wordlists



Any wordlist can be used in Gobuster and there are a few on kali by default in /usr/share/wordlists/ such as dnsmap.txt

However we recommend you download SecLists by running sudo apt install seclists

This is a much more exhaustive list than the default but it may take a while to download so do it in a separate terminal

Gobuster Commands



```
gobuster dir -u url -w wordlist
gobuster dns -d domain -t 50 -w wordlist
gobuster vhost -u url -w wordlist
Url - The site url, can be an IP
Domain - The site domain, cannot be an IP
Wordlist - List of words to iterate through
Threads - Number of threads to use at once
```

Setting a host



IPs can be connected to domains by editing your hosts file at /etc/hosts

This allows your browser to easily connect to them

It is also used when discovering subdomains as IPs are not allowed for this

An easy command to add a domain to an IP is

echo "{ip} {domain}" | sudo tee -a /etc/hosts

Useful commands



```
sudo openvpn /Downloads/{vpn file}
gobuster dir/dns/vhost -u {url}/-d {domain} -w wordlist
nmap \{ip\} -p 80/-p mysql -sV -sC
echo "{ip} {domain}" | sudo tee -a /etc/hosts
Adding --help to the end of any command will give you a list
of options
Default wordlists are in /usr/share/wordlists/
```



EXCITING OPPORTUNITIES

from





NETWORK SUMMER INTERNSHIP



CYBER SECURITY
LEADERSHIP
GRADUATE

Crackchester



Here's a link to our link tree where you can find all our socials and our discord!



