

Forum:[Hack Forums](#)

Thread: ([Beginner's Tutorial](#)) Using Subfinder And XSS Tools For Web Exploits

Chorozon - February 22, 2025, 2:57 pm

(Beginner's Tutorial) Using Subfinder , Nuclei And XSSStrike For Cross Site Scripting Detection

Bounty Hunt Tutorial

These 2 tools are imperative to your success at starting to learn bounty hunting

Lets start with the tool Subfinder [Subfinder Github](#) <https://github.com/projectdiscovery/subfinder>

Use Subfinder to find all valid sub-domains attached to your target

Subfinder is coded in GO so make sure you have go1.21 installed

[Full Install Docs](#)

Run

Code go install -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest

Run subfinder with -h flag for options

Code subfinder -h

To run Subfinder on a specific target use the -d flag to specify the domain

Code subfinder -d hackforums.net

Use the -o flag to save to a file

Code subfinder -d hackforums.net -o output.txt

Now you should have a list of all your targets valid sub domains :)

Now armed with our full list of domains its time to start our recon and attack

Lets use Nuclei to scan our Url list for vulnerabilities

Nuclei is a powerful tool and also supports scanning multiple urls from list

lets download it the same as the last tool

Code go install -v github.com/projectdiscovery/nuclei/v3/cmd/nuclei@latest

We can pull up the Help information the same as well using the -h flag

Code nuclei -h
Lets scan our whole list

Code nuclei -targets urls.txt
We can also use XSSStrike to scan and test payload lists on vulnerable urls

Github - <https://github.com/s0md3v/XSSStrike>

Run to download
Code git clone https://github.com/s0md3v/XSSStrike.git
Test a single webpage which uses GET method.
Code python3 xsstrike.py -u "http://<URL>/faq.php?lang=q"
If you want to skip DOM testing use the -skip-dom flag
Code python3 xsstrike.py -u "http://<URL>/faq.php?lang=q" -skip-dom
Again we can pull up the help details for the tool using
Code python3 xsstrike.py -h
Happy hacking guys ?

If you want me to go into detail on any section of the guide or you have a topic you would like one written on drop a comment below

Also want to mention [Katana Git](https://github.com/projectdiscovery/katana)
<https://github.com/projectdiscovery/katana>

Nuclei Templates - <https://github.com/projectdiscovery/nuclei-templates>
<https://github.com/projectdiscovery>

s0lo - February 22, 2025, 3:27 pm

(Feb 22, 2025 03:57 PM)Chorozon Wrote: [\[CITE\]](#) (Beginner's Tutorial) Using Subfinder , Nuclei And XSSStrike For Cross Site Scripting Detection

Bounty Hunt Tutorial

These 2 tools are imperative to your success at starting to learn bounty hunting

Lets start with the tool Subfinder [Subfinder Github https://github.com/projectdiscovery/subfinder](https://github.com/projectdiscovery/subfinder)

Use Subfinder to find all valid sub-domains attached to your target

Subfinder is coded in GO so make sure you have go1.21 installed
[Full Install Docs](#)

Run
Code go install -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest
Run subfinder with -h flag for options
Code subfinder -h
To run Subfinder on a specific target use the -d flag to specify the domain

Code subfinder -d hackforums.net
Use the -o flag to save to a file

Code subfinder -d hackforums.net -o output.txt
Now you should have a list of all your targets valid sub domains :)

Now armed with our full list of domains its time to start our recon and attack

Lets use Nuclei to scan our Url list for vulnerabilities

Nuclei is a powerful tool and also supports scanning multiple urls from list

lets download it the same as the last tool

Code go install -v github.com/projectdiscovery/nuclei/v3/cmd/nuclei@latest
We can pull up the Help information the same as well using the -h flag

Code nuclei -h
Lets scan our whole list

Code nuclei -targets urls.txt
We can also use XSSStrike to scan and test payload lists on vulnerable urls

Github - <https://github.com/s0md3v/XSSStrike>

Run to download
Code git clone https://github.com/s0md3v/XSSStrike.git
Test a single webpage which uses GET method.
python3 xsstrike.py -u "http://<URL>/faq.php?lang=q"

If you want to skip DOM testing use the -skip-dom flag
python3 xsstrike.py -u "http://<URL>/faq.php?lang=q" --skip-dom

Again we can pull up the help details for the tool using
Code python3 xsstrike.py -h
Happy hacking guys ?

If you want me to go into detail on any section of the guide or you have a topic you would like one written on drop a comment below

Also want to mention [Katana Git](https://github.com/projectdiscovery/katana)
<https://github.com/projectdiscovery/katana>

Nuclei Templates - <https://github.com/projectdiscovery/nuclei-templates>

<https://github.com/projectdiscovery>

maybe you can elaborate on using templates for nuclei, to run something stronger then "nuclei -targets urls.txt", is there is a reason. ive stubled uppon some nuclei templates on github, but I have not got around of using them

Chorozon - February 22, 2025, 3:42 pm

(Feb 22, 2025 04:27 PM)s0lo Wrote: [\[CITE\]](#) maybe you can elaborate on using templates for nuclei, to run something stronger then "nuclei -targets urls.txt", is there is a reason. ive stubled uppon some nuclei templates on github, but I have not got around of using them

Projectdiscovery has alot of documentation on Templates

Check out - <https://docs.projectdiscovery.io/templates/introduction> Template library - <https://github.com/projectdiscovery/nuclei-templates>

Here is a diagram of Nuclei Templates and the use cases

Use case	Nuclei template
Detect known CVEs	CVE-2021-44228 (Log4Shell)
Identify Out-of-Band vulnerabilities	Blind SQL Injection via OOB
SQL Injection detection	Generic SQL Injection
Cross-Site Scripting (XSS)	Reflected XSS Detection
Default or weak passwords	Default Credentials Check
Secret files or data exposure	Sensitive File Disclosure
Identify open redirects	Open Redirect Detection
Detect subdomain takeovers	Subdomain Takeover Templates
Security misconfigurations	Unprotected Jenkins Console
Weak SSL/TLS configurations	SSL Certificate Expiry
Misconfigured cloud services	Open S3 Bucket Detection
Remote code execution vulnerabilities	RCE Detection Templates
Directory traversal attacks	Path Traversal Detection
File inclusion vulnerabilities	Local/Remote File Inclusion

Quote: to run something stronger then "nuclei -targets urls.txt", is there is a reason

In short yes ! depending on your use case and what you are looking for Nuclei has many use cases

s0lo - February 22, 2025, 3:46 pm

(Feb 22, 2025 04:42 PM)Chorozon Wrote: [\[CITE\]](#) Projectdiscovery has alot of documentation on Templates

Check out - <https://docs.projectdiscovery.io/templates/introduction> Template library - <https://github.com/projectdiscovery/nuclei-templates>

Here is a diagram of Nuclei Templates and the use cases

Use case	Nuclei template
Detect known CVEs	CVE-2021-44228 (Log4Shell)
Identify Out-of-Band vulnerabilities	Blind SQL Injection via OOB
SQL Injection detection	Generic SQL Injection
Cross-Site Scripting (XSS)	Reflected XSS Detection
Default or weak passwords	Default Credentials Check
Secret files or data exposure	Sensitive File Disclosure
Identify open redirects	Open Redirect Detection

Detect subdomain takeovers Subdomain Takeover Templates
Security misconfigurations Unprotected Jenkins Console
Weak SSL/TLS configurations SSL Certificate Expiry
Misconfigured cloud services Open S3 Bucket Detection
Remote code execution vulnerabilities RCE Detection Templates
Directory traversal attacks Path Traversal Detection
File inclusion vulnerabilities Local/Remote File Inclusion

In short yes ! depending on your use case and what you are looking for Nuclei has many use cases decent, thanks

Chorozon - February 22, 2025, 3:57 pm

(Feb 22, 2025 04:46 PM)s0lo Wrote: [\[CITE\]](#) decent, thanks

Its a slow grind sometimes but keep building recon on your target instead of focusing on directly triggering a exploit

Go through a checklist of strategies and methods you have utilized on the target so you can plan your attack better

The learning curve from watching people exploiting POC controlled sites compared to the Bug bounty "Pros" that you see post on youtube can be steep

I would recommend familiarizing yourself with these tools and similar tools on live sites , depending on your hat color you could host your own or some simple dorks should expose some less then optimal configured sites and trying to find exploits in those before moving on to something like <https://hackerone.com/bug-bounty-programs>

s0lo - February 23, 2025, 12:53 am

(Feb 22, 2025 04:57 PM)Chorozon Wrote: [\[CITE\]](#) Its a slow grind sometimes but keep building recon on your target instead of focusing on directly triggering a exploit

Go through a checklist of strategies and methods you have utilized on the target so you can plan your attack better

The learning curve from watching people exploiting POC controlled sites compared to the Bug bounty "Pros" that you see post on youtube can be steep

I would recommend familiarizing yourself with these tools and similar tools on live sites , depending on your hat color you could host your own or some simple dorks should expose some less then optimal configured sites and trying to find exploits in those before moving on to something like <https://hackerone.com/bug-bounty-programs>

about recon, a few month ago I had rengine running on my VPS, that was interesting, so much info that can be found

samasugeti - March 6, 2025, 6:59 am

thanks man, very nice this one