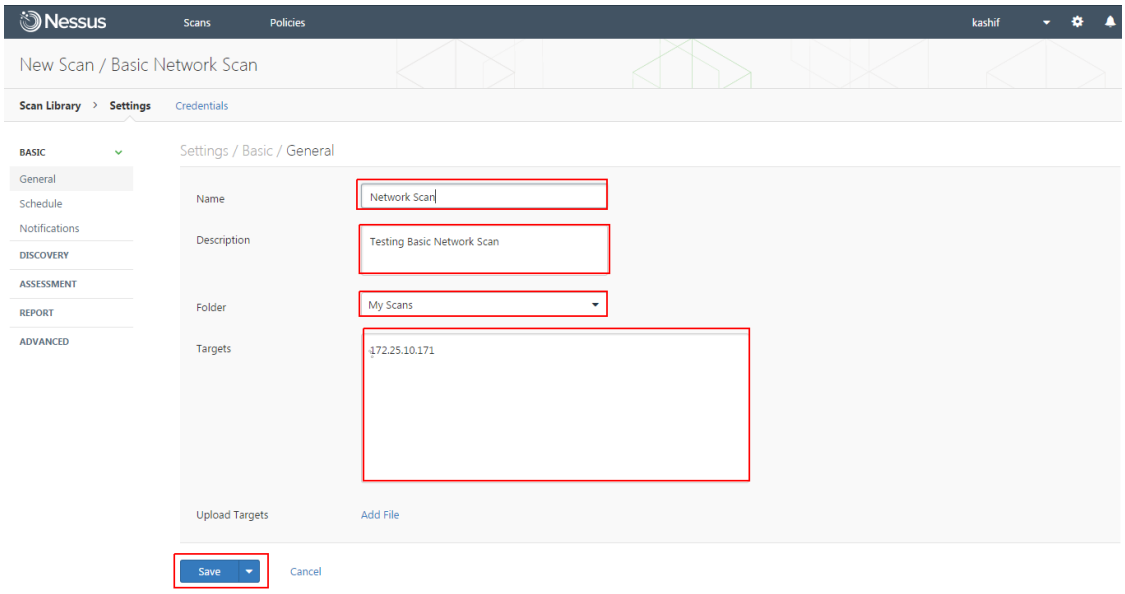
Phase 3: Identify Vulnerabilities

Nessus

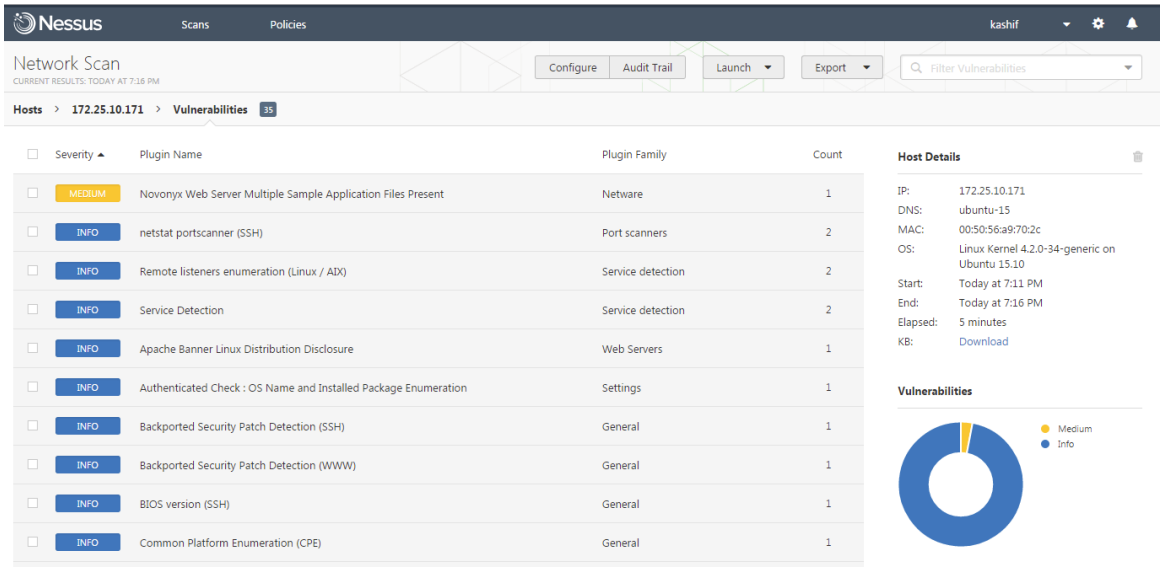
Usage: Nessus is a cross-platform vulnerability scanner from Tenable, Inc. that is able to scan many types of systems, including web applications, Internet-facing attack surfaces, and more.

Config & Settings:

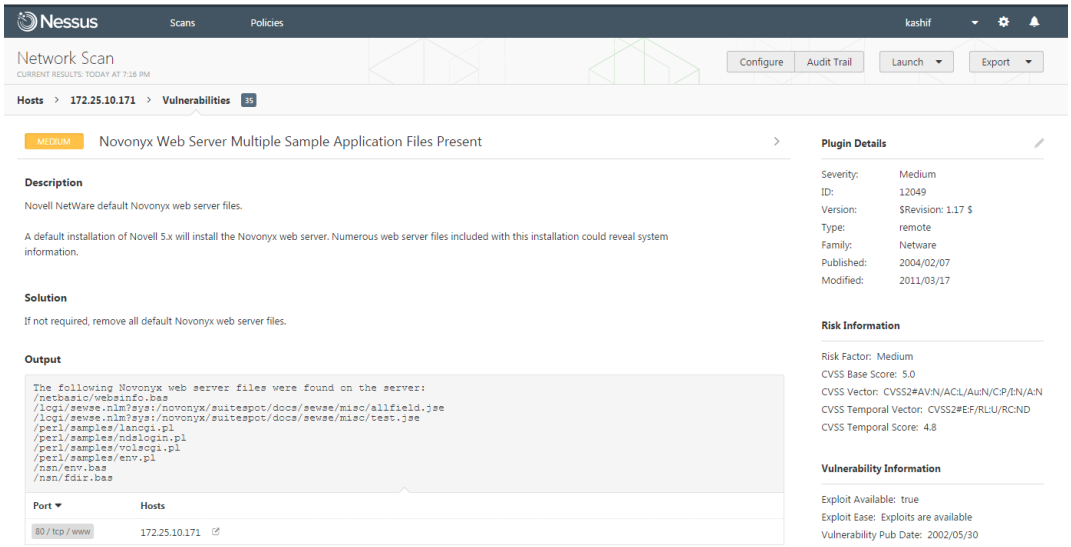
Setting up a new scan:



Example of vulnerabilities found:



Click on one vulnerability to see more details:



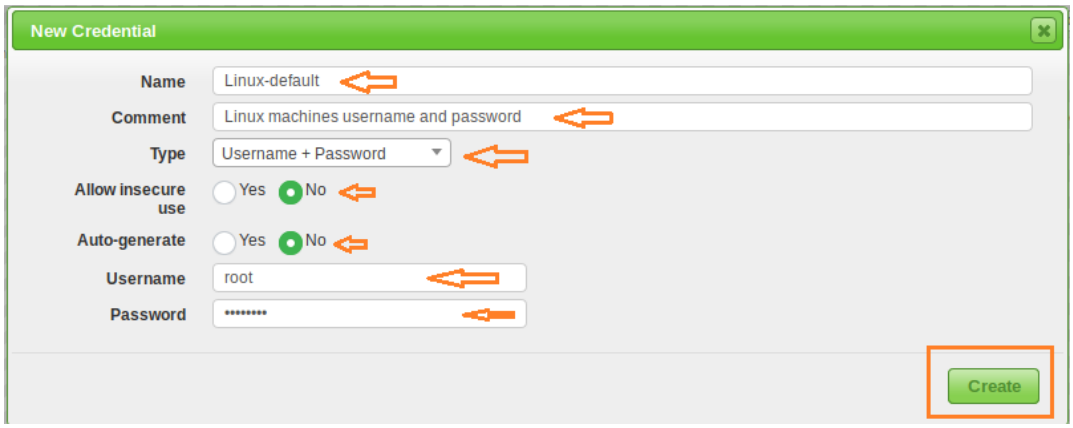
Pros	Cons
cross-platform	expensive license
live results	proprietary software
easy to use and understand results	free version is very limited and slow

OpenVAS

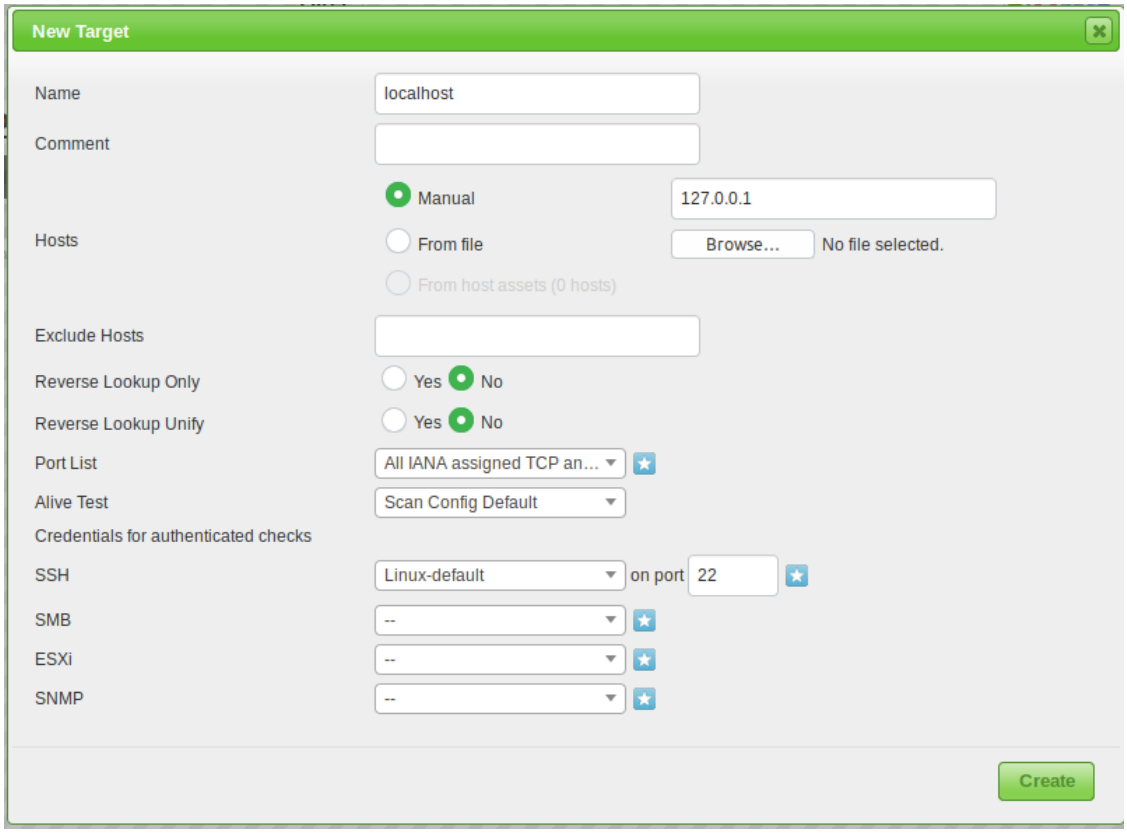
Usage: OpenVAS is a software framework containing multiple services and tools for vulnerability scanning and management.

Config & Settings:

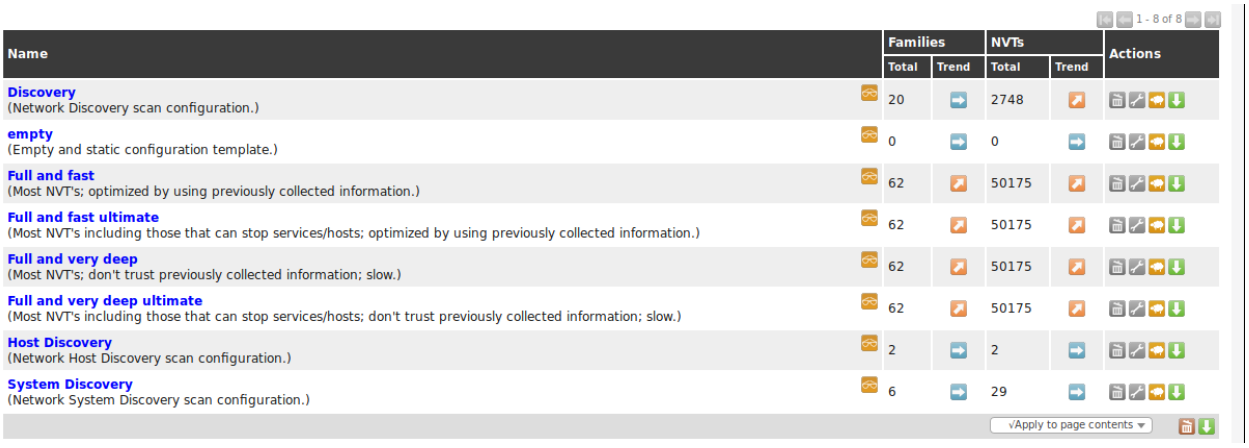
Add credentials:



Configure target:



Configure scan:

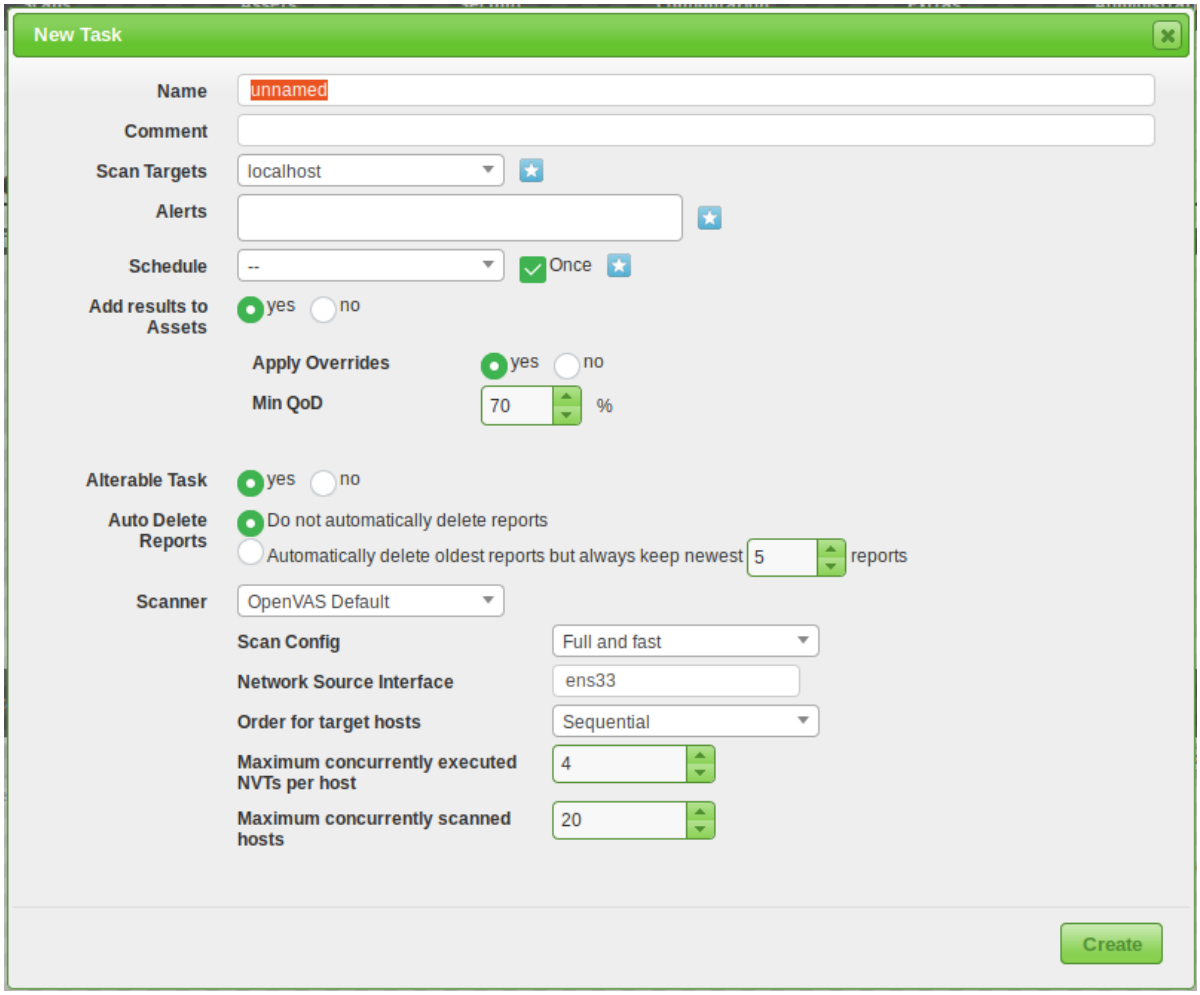


Name	Families		NVTs		Actions
	Total	Trend	Total	Trend	
Discovery (Network Discovery scan configuration.)	20		2748		
empty (Empty and static configuration template.)	0		0		
Full and fast (Most NVT's; optimized by using previously collected information.)	62		50175		
Full and fast ultimate (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	62		50175		
Full and very deep (Most NVT's; don't trust previously collected information; slow.)	62		50175		
Full and very deep ultimate (Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	62		50175		
Host Discovery (Network Host Discovery scan configuration.)	2		2		
System Discovery (Network System Discovery scan configuration.)	6		29		

1 - 8 of 8

√Apply to page contents

Configure task:



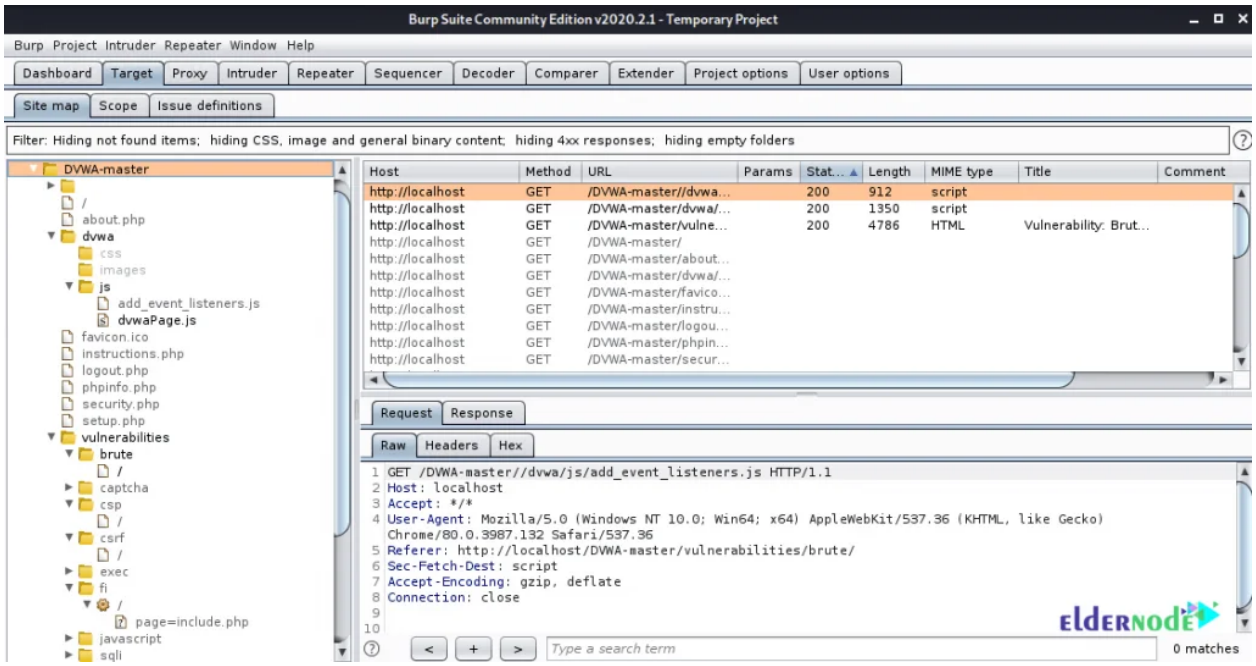
Pros	Cons
FOSS	GUI can be difficult to use/navigate
cross-platform	can be misconfigured
GUI available	sometimes results in false negatives

Burp Suite

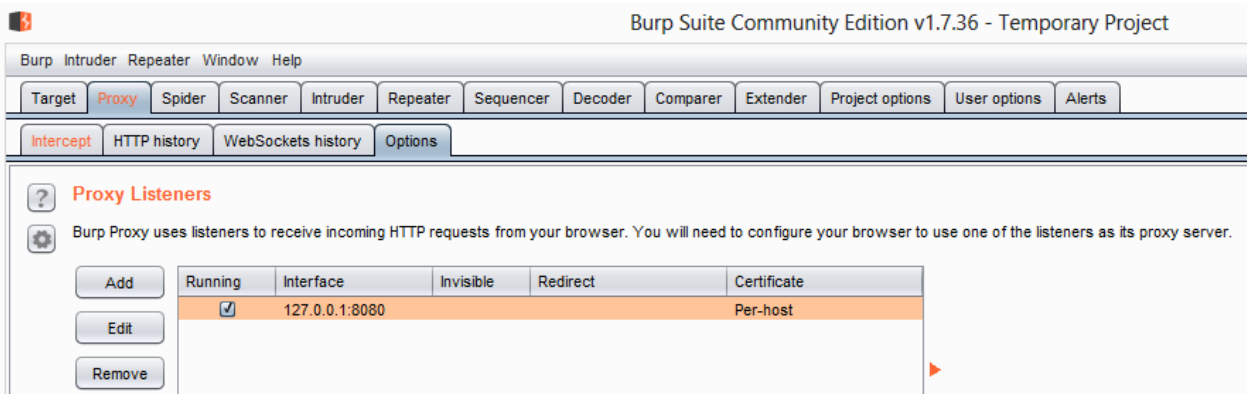
Usage: Burp Suite is a software security tool suite for pentesting web applications.

Config & Settings:

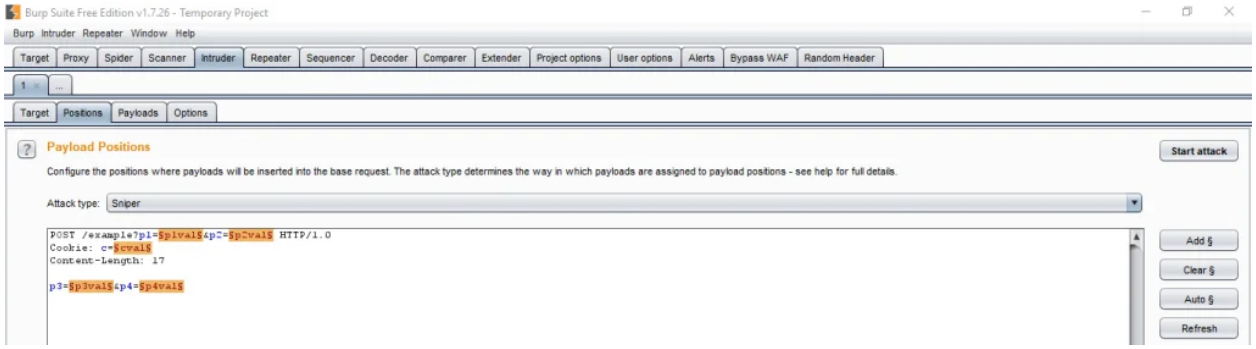
Target view:



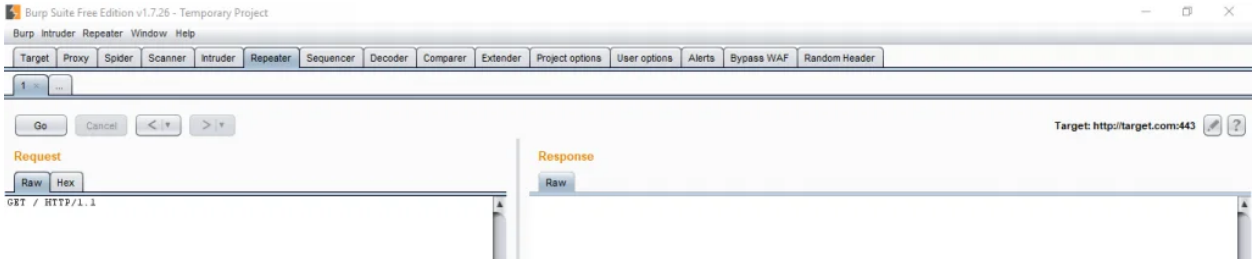
Proxy:



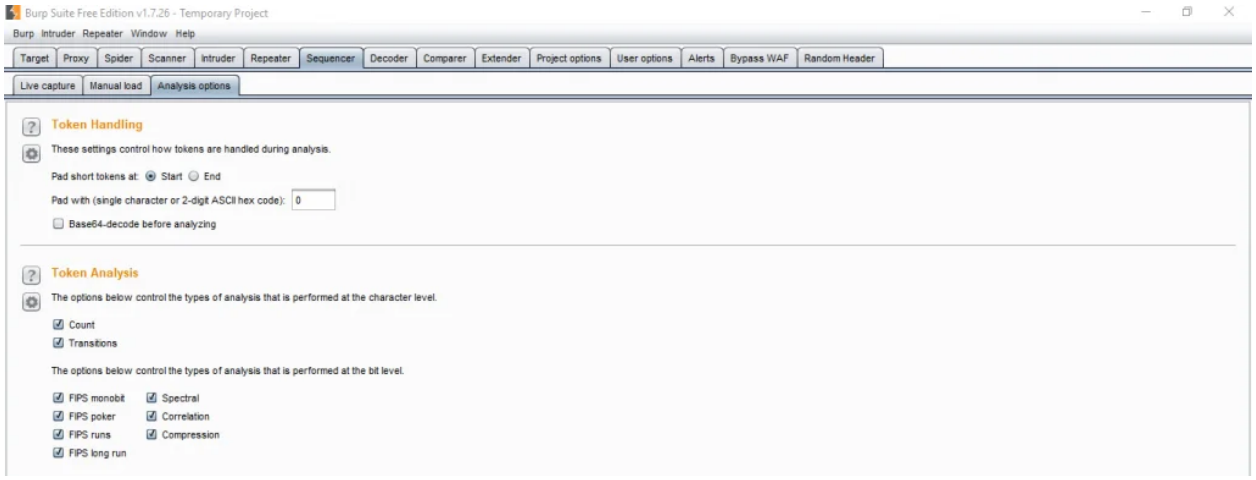
Intruder:



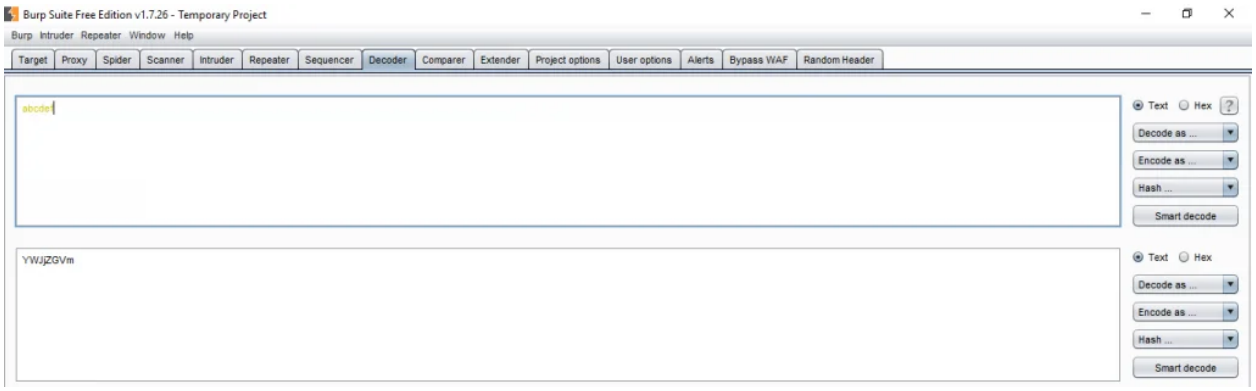
Repeater:



Sequencer:



Decoder:



Pros	Cons
cross-platform	can be overwhelming
GUI	free version has limited features
comprehensive toolkit	can be overwhelming to use

Nikto

Usage: Nikto is a command-line vulnerability scanner for scanning web servers.

Config & Settings:

Scan scanme.nmap.org on port 80:

```
nikto -h scanme.nmap.org
```

(append -ssl or -p 80 if site uses https)

Scan scanme.nmap.org and output results to text file:

```
nikto -h scanme.nmap.org -o output.txt
```

Pros	Cons
FOSS	uses some non-FOSS resources
CLI	no GUI
many plugins available	by default, very noisy

Wapiti

Usage: Wapiti performs black-box security scans of web applications by crawling the sites to find injection points.

Config & Settings:

```
root@kali:~# wapiti -h

      __  __                  _ _   _ _____
     / / /\ \ \__ _ _ __ (_) |_(_)___ /
     \ \/  \/ / _` | '_ \| | __| | |_ \
      \  /\  / (_| | |_) | | |_| |___) |
       \/  \/ \__,_| .__/|_|\__|_|____/
                   |_|
Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Be careful! New moon tonight.
usage: wapiti [-h] [-u URL] [--scope {page,folder,domain,url,punk}]
              [-m MODULES_LIST] [--list-modules] [--update] [-l LEVEL]
              [-p PROXY_URL] [--tor] [-a CREDENTIALS]
              [--auth-type {basic,digest,kerberos,ntlm,post}] [-c COOKIE_FILE]
              [--skip-crawl] [--resume-crawl] [--flush-attacks]
              [--flush-session] [--store-session PATH] [--store-config PATH]
              [-s URL] [-x URL] [-r PARAMETER] [--skip PARAMETER] [-d DEPTH]
              [--max-links-per-page MAX] [--max-files-per-dir MAX]
              [--max-scan-time SECONDS] [--max-attack-time SECONDS]
              [--max-parameters MAX] [-S FORCE] [-t SECONDS] [-H HEADER]
              [-A AGENT] [--verify-ssl {0,1}] [--color] [-v LEVEL] [-f FORMAT]
              [-o OUPUT_PATH] [--external-endpoint EXTERNAL_ENDPOINT_URL]
              [--internal-endpoint INTERNAL_ENDPOINT_URL]
              [--endpoint ENDPOINT_URL] [--no-bugreport] [--version]

Wapiti-3.0.4: Web application vulnerability scanner
```

Basic usage form:

```
wapiti -u <target> <options>
```

Pros	Cons
CLI	no GUI
FOSS	running on Windows requires WSL
tests for many different injection attacks	ongoing project that may have bugs