Sri Lanka Institute of Information Technology

Web Audit Report

(Individual Assignment)

IE2062 – Web Security

Submitted by:

Student Registration Number	Student Name
IT20076498	Dias L.R. S

Purpose

The primary goal of this online audit is to search for and find security flaws in a well-known website, and students must apply their academic knowledge to a real-world security audit. For this security web audit, we were instructed to utilize both automated and manual testing. Dotdotpwn, nikto, sublist3r, wafw00f, and Nessus, Nmap were used to check the vulnerabilities using the automated technique.

Abstract

Cybercrime, misrepresentation, and information breach are all risks that pose significant risks to organizations. A great deal of money has been lost, and organizations must devise ways to prevent the threats from becoming actual and to deflect additional losses. This investigation looked into the systems related to online audits for IT security and how they might help companies enhance their IT security. The examination assessed IT administrators' and employees' awareness of cybercrime risks; estimated their understanding of IT security audit norms and regulations; and calculated the impact of IT security audit on the growth of the association. This research used an organization as a setting, analyzed the organization's flow IT security audit state, and determined the adaptability for the creation of an IT security audit strategy and system. To get more detailed information on cybercrime, a quantitative investigation was conducted. This research unequivocally demonstrated that IT security auditing is critical for the advancement of any organization that employs IT.

Contents

1. Introduction

In today's environment, it wouldn't be inaccurate to claim that you can follow all standard protocols to the letter, apply all best practices you can think of, and tie up loose ends. However, it will not be sufficient to deter hackers. Simply because there is a lot that can be done to secure a website, and hackers are continuously developing new ways to penetrate online systems.

A Website Security Audit is a procedure that examines your online system for vulnerabilities and loopholes, including the core, extensions, themes, and other infrastructure. Static and dynamic code analysis, business logic error testing, configuration tests, and other procedures are generally included in a comprehensive online security audit. The audit identifies any hidden vulnerabilities in your website and security architecture and is often followed/accompanied by a penetration test. While the goal of a security audit is to identify and assess weak areas, the goal of a penetration test is to attack such vulnerabilities. Pen tests are nothing more than simulating a hacker and a real-life attack environment, then exploiting the vulnerabilities to determine the risk associated with each one. Both automatic tools and human expertise are used in the most trustworthy security audits.

There are two stages to a website security audit:

- Examining Vulnerabilities
- Vulnerability Exploitation

Prime goal of website security audits is to find and fix flaws in your website's architecture before hackers with harmful intent detect them. There are web tools for doing security audits. For security scanning, there are several free and paid tools and services accessible online.

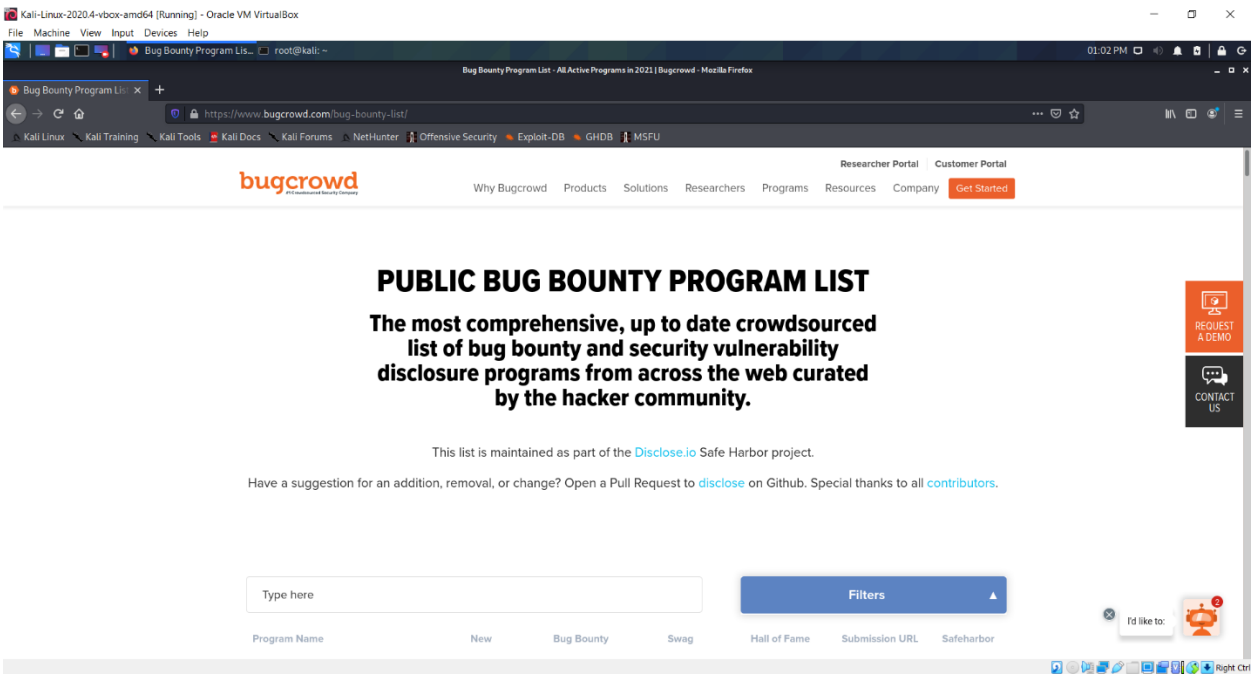
A website security audit is a wonderful method to remain on top of your website's security status and make sure you're doing everything you can to keep intruders out. The greatest thing is that there are many free scanning tools available online, allowing website owners to execute audits autonomously with minimum assistance from other entities.

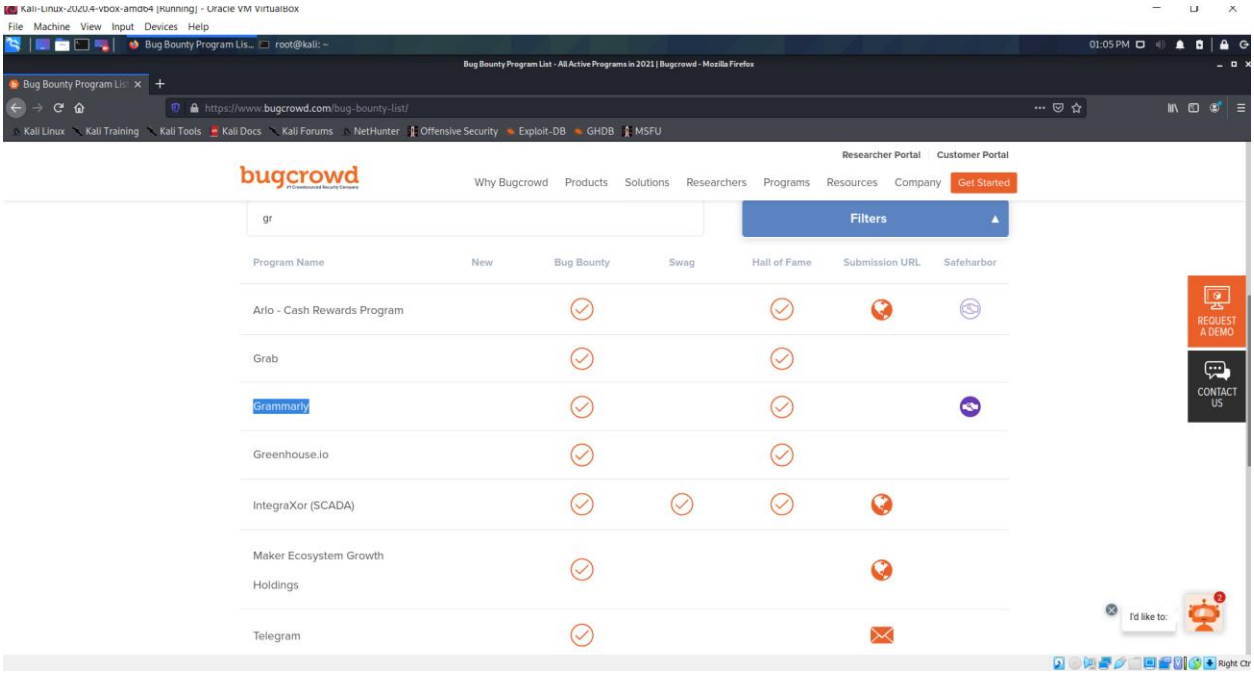
2. Choosing the Domain

I chose **Grammarly** as the domain for this web audit. The AI-powered tools from Grammarly help individuals communicate more effectively. Every day, millions of people rely on Grammarly to make their communications, papers, and social media postings clear, error-free, and powerful. Grammarly is a San Francisco, New York, Kyiv, and Vancouver-based Inc. 500 business.

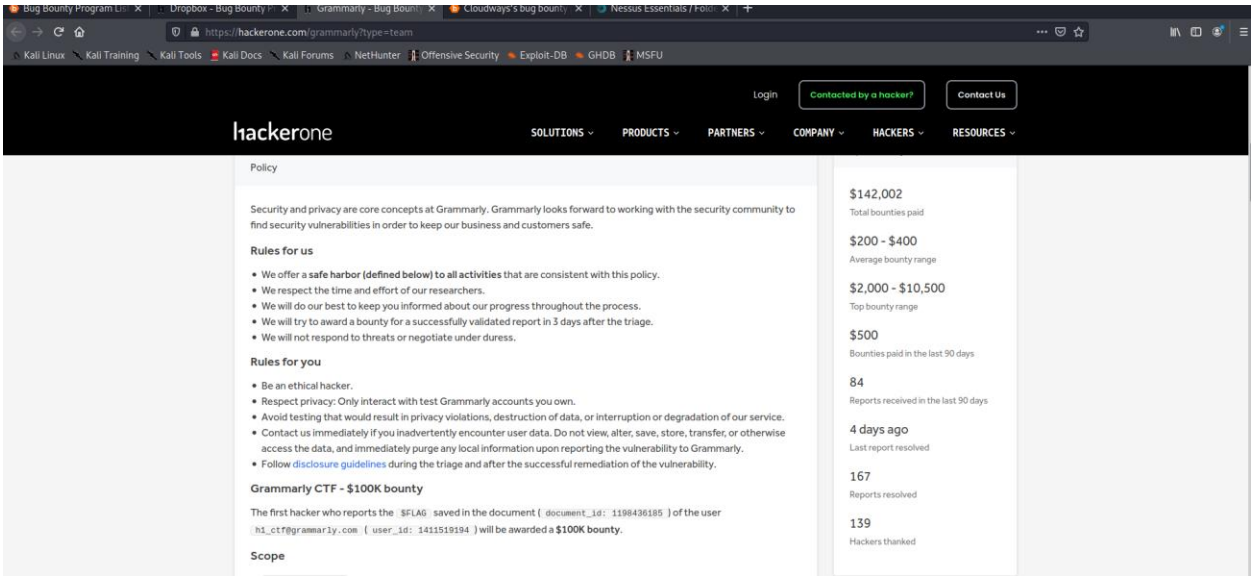
Grammarly's advanced AI not just to corrects your grammar errors, but also makes your writing more comprehensible and assists us in making the best impression on the reader depending on our audience and goals. Grammarly can also analyze the tone of our conversation, propose synonyms to make our content more accessible and precise, and even verify our papers for plagiarism. They are available on a variety of platforms and devices.

The primary goal of this web audit is to determine whether the domain has any of the "OWASP top 10 vulnerabilities for the year 2020."

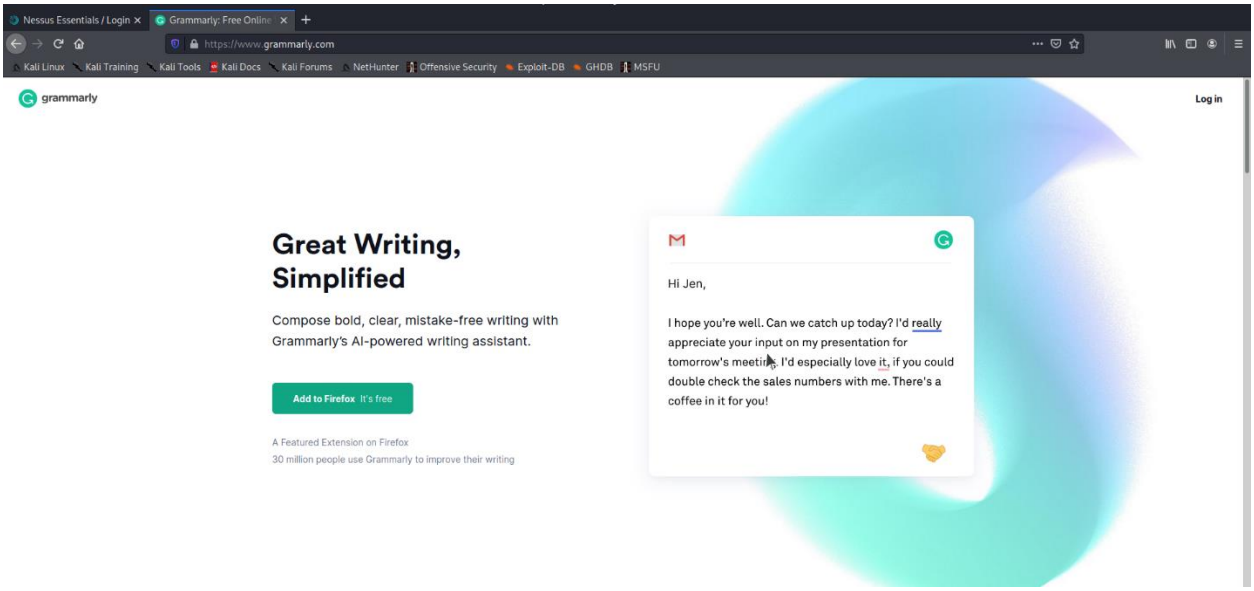




They've launched a bug bounty program on Hackerone. Grammarly has given some conditions for us.



Interface of my selected domain as shown in the figure 03



Conditions of the domain

Rules for us

- ✓ We offer a safe harbor (defined below) to all activities that are consistent with this policy.
- ✓ We respect the time and effort of our researchers.
- ✓ We will do our best to keep you informed about our progress throughout the process.
- ✓ We will try to award a bounty for a successfully validated report in 3 days after the triage.
- ✓ We will not respond to threats or negotiate under duress.

Rules for you

- ✓ Be an ethical hacker.
- ✓ Respect privacy: Only interact with test Grammarly accounts you own.
- ✓ Avoid testing that would result in privacy violations, destruction of data, or interruption or degradation of our service.
- ✓ Contact us immediately if you inadvertently encounter user data. Do not view, alter, save, store, transfer, or otherwise access the data, and immediately purge any local information upon reporting the vulnerability to Grammarly.
- ✓ Follow disclosure guidelines during the triage and after the successful remediation of the vulnerability.

Vulnerability Disclosure Guidelines

https://www.hackerone.com/disclosure-guidelines

3. Web Reconnaissance

The phrase reconnaissance is derived from military use, where it refers to a mission to gather intelligence in hostile territory. In the realm of computer security, recognition is usually the first step in a more serious assault aimed at compromising the target device. The attacker, for example, may employ port scanning to find some susceptible ports. An intruder usually takes advantage of known vulnerabilities in services connected to open ports discovered by a port scan. In cybersecurity, reconnaissance refers to the initial stage of a cyberattack, when a hacker ‘scouts' the target system. This action is classified as a 'passive attack' since it occurs before any actual harm is done.

Because there are two types of reconnaissance: active and passive. Active and passive reconnaissance are frequently referred to as passive attacks, which is a bit misleading because they are just looking for information rather than actively targeting targets, as active assaults do. Both active and passive reconnaissance are commonly employed in ethical hacking, in which white hat hackers utilize attack tactics to identify device weaknesses so that concerns may be addressed before an actual attack occurs.

Hackers, users believe, are looking for one big break, one major flaw they can attack to get access to a company's whole network. Through fact, hackers collect data from a variety of sources in order to compile an information "dossier" about a target organization. This dossier might include network addresses, enabled services, open ports, proxy relays, VPN concentrators, SAS programs used by the firm, and important usernames and passwords for the company's domain and users stolen from the dark web. Before launching an assault, the hacker is studying everything there is to know about the firm.

During reconnaissance activity, common sources of information include:

- ✓ Subdomains and domains
- ✓ Whose Data Is It?
- ✓ information on the directory
- ✓ Accounts on social media (individuals and the company itself.
- ✓ Accounts for the sites in question were hacked on the dark web.

Tools used to perform this web audit

- ✓ Sublist3r
- ✓ Nmap
- ✓ Nikto
- ✓ Amass
- ✓ PwnXss
- ✓ DotDotpwn
- ✓ Walw00f
- ✓ Nessus
- ✓ Netsparker
- ✓ Burp Suite

3.1 Sublist3r

Sublister is a python-based program that leverages OSINT to enumerate subdomains of websites. Pen-testers can use it to collect and aggregate subdomains for a target domain. Sublilster use a variety of search engines, such as Google, Yahoo, and others, as well as programs such as Netcraft, Virustotal, and others, to obtain reliable results.

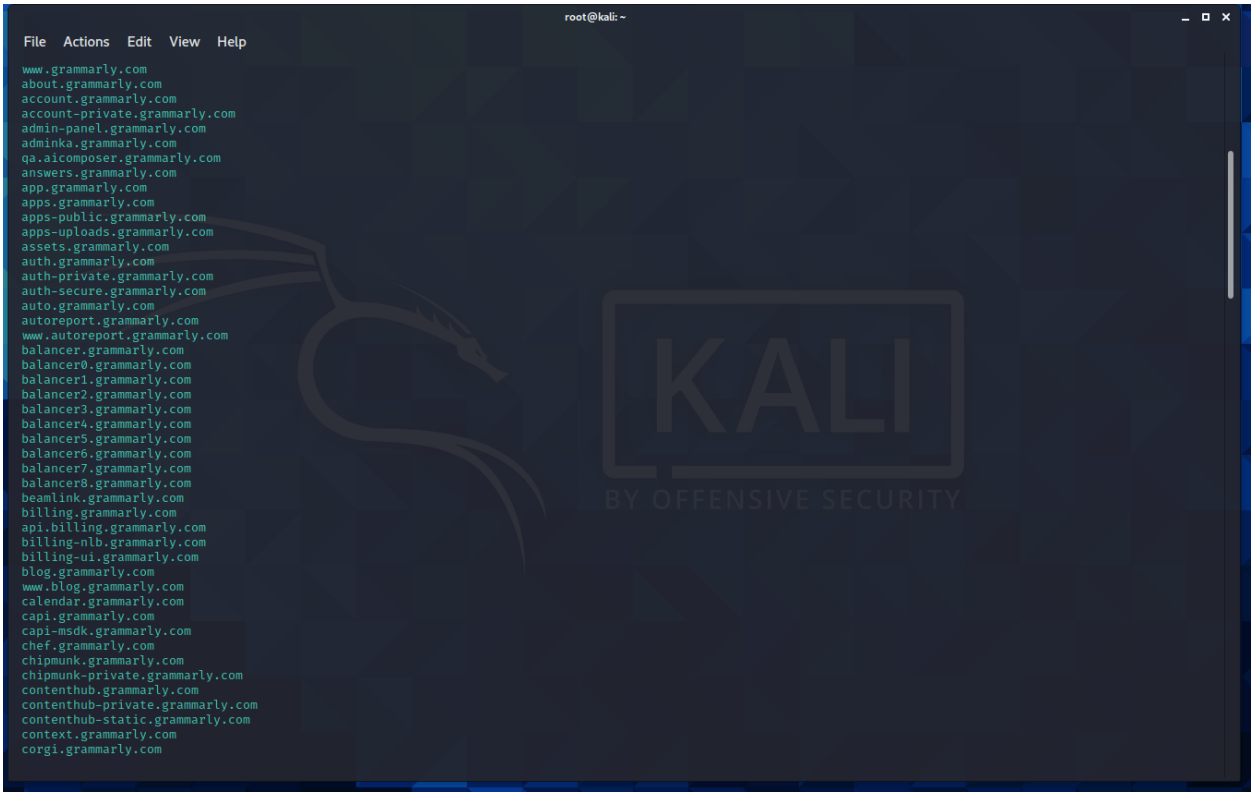
You may clone the Github repository and use it to install sublister. You may do so by following the command.

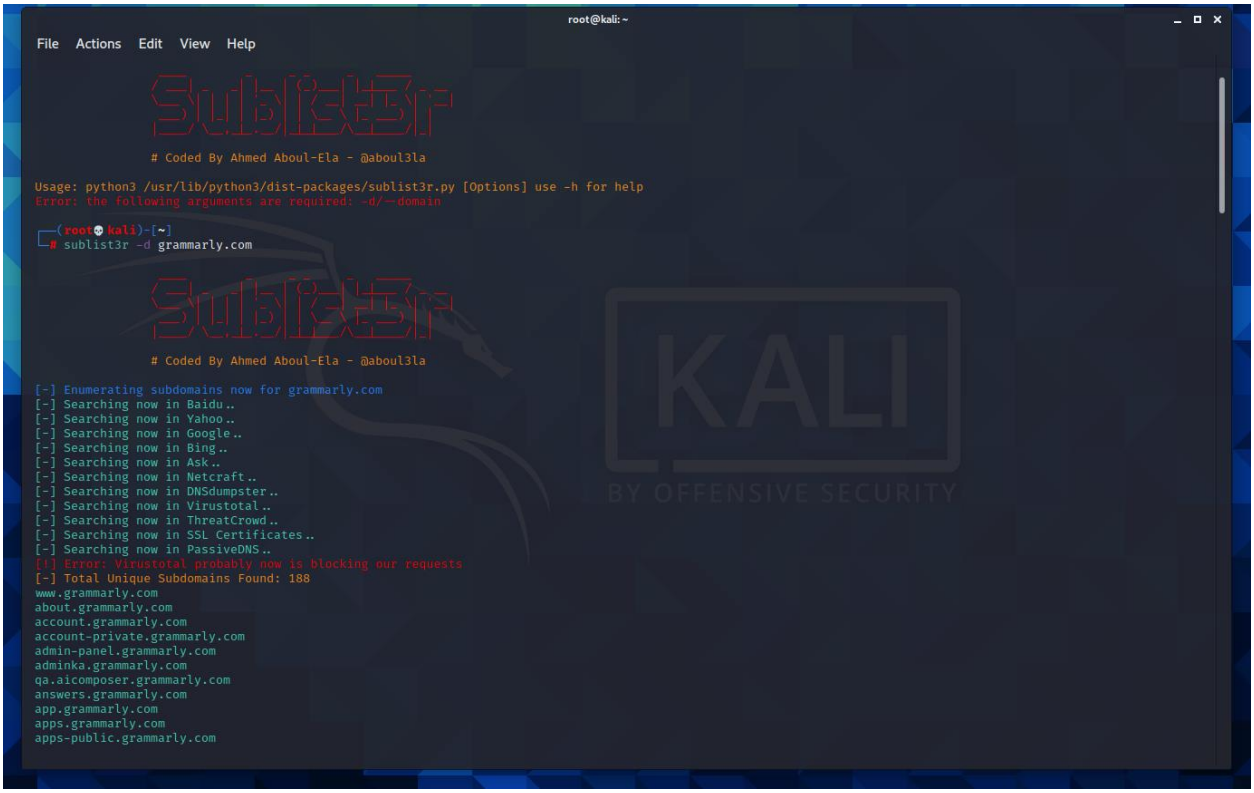
git clone https://github.com/aboul3la/Sublist3r.git

- I used Sublist3r to collect the subdomains of my main domain "grammarly.com," as well as I discovered 188 of them.
- Sublist3r's execute command:

sublist3r -d grammarly.com

After downloading the tool using the git clone command, we execute the sublist3r python code to identify the subdomains and their total number. In my case, I have already downloaded sublister, So I did not execute the git clone command. [This revealed the targeted site's subdomains, which are classified as P5 (informational) on the vulnerability scale.]


root@kali: ~
File Actions Edit View Help
www.grammarly.com
about.grammarly.com
account.grammarly.com
account-private.grammarly.com
admin-panel.grammarly.com
adminka.grammarly.com
qa.aicomposer.grammarly.com
answers.grammarly.com
app.grammarly.com
apps.grammarly.com
apps-public.grammarly.com
apps-uploads.grammarly.com
assets.grammarly.com
auth.grammarly.com
auth-private.grammarly.com
auth-secure.grammarly.com
auto.grammarly.com
autoreport.grammarly.com
www.autoreport.grammarly.com
balancer.grammarly.com
balancer0.grammarly.com
balancer1.grammarly.com
balancer2.grammarly.com
balancer3.grammarly.com
balancer4.grammarly.com
balancer5.grammarly.com
balancer6.grammarly.com
balancer7.grammarly.com
balancer8.grammarly.com
beamlink.grammarly.com
billing.grammarly.com
api.billing.grammarly.com
billing-nlb.grammarly.com
billing-ui.grammarly.com
blog.grammarly.com
www.blog.grammarly.com
calendar.grammarly.com
capi.grammarly.com
capi-msdk.grammarly.com
chef.grammarly.com
chipmunk.grammarly.com
chipmunk-private.grammarly.com
contenthub.grammarly.com
contenthub-private.grammarly.com
contenthub-static.grammarly.com
context.grammarly.com
corgi.grammarly.com


root@kali: ~
File Actions Edit View Help
Coded By Ahmed Aboul-Ela - @aboul3la
Usage: python3 /usr/lib/python3/dist-packages/sublist3r.py [Options] use -h for help
Error: the following arguments are required: -d/--domain
(root kali)-[~]
sublist3r -d grammarly.com
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for grammarly.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 188
www.grammarly.com
about.grammarly.com
account.grammarly.com
account-private.grammarly.com
admin-panel.grammarly.com
adminka.grammarly.com
qa.aicomposer.grammarly.com
answers.grammarly.com
app.grammarly.com
apps.grammarly.com
apps-public.grammarly.com

3.2 Nmap (Network Mapper)

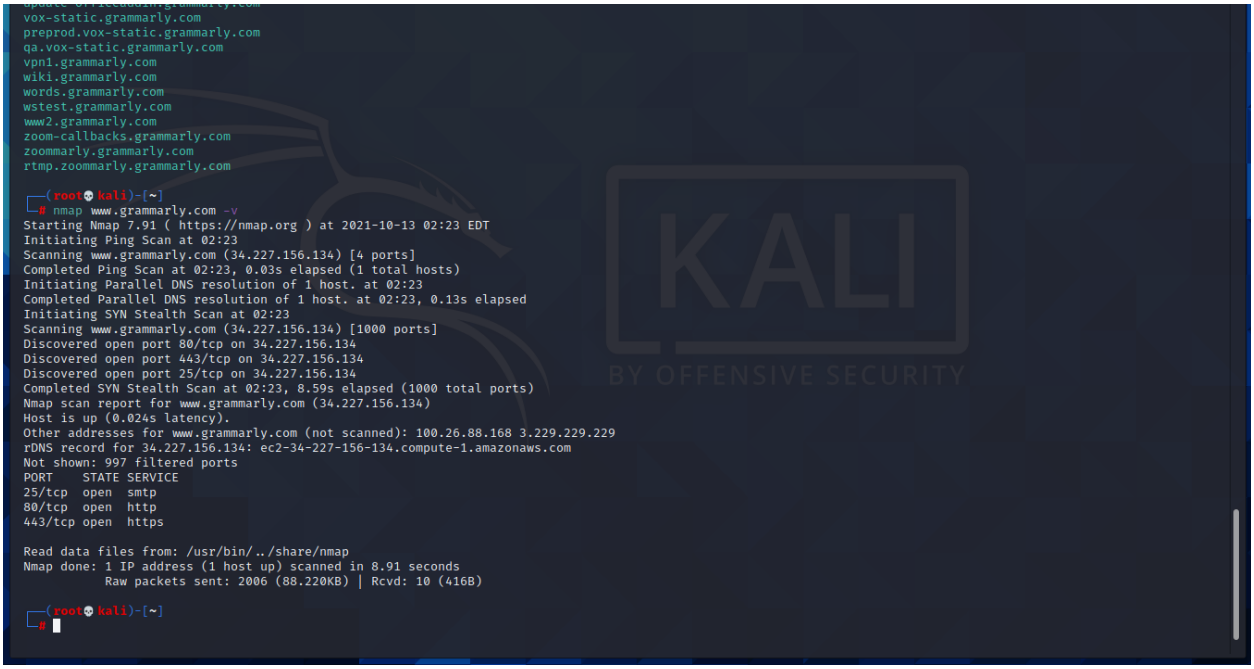
The acronym Nmap stands for Network Mapper. It's a network exploration, security scanning, and auditing tool that's open source. It was created to quickly scan big networks, although it also works well with single hosts. Nmap utilizes raw IP packets in unique ways to figure out what hosts are on the network, what services they offer, what OS systems they're running, what kind of packet filters/firewalls they're using, and a slew of other details.

Although this has been most commonly used for security audits, it's also useful for day-to-day tasks like network inventory, service upgrade schedule management, and host monitoring for many systems and network managers. It listens for responses and determines if ports are open, closed, or filtered in some way, such as by a firewall. Other terms for port scanning include port discovery and enumeration.

- I used Nmap to obtain the domain's IP address as well as the domain's open ports.
- Nmap execution command:

  nmap www.grammarly.com -v

  We discovered a lot of open ports, which is common yet interesting.



IP address of the domain: **34.227.156.134**

To find out what OS (and version) the domain was running, I ran an OS scan.

This site is informational on a P5 level, plus it contains a low P4 level vulnerability. Tunneling and clickjacking assaults, for example, may be carried out using it. **(LOW P4 and informational P5)**

3.3 Nikto

Nikto is an Open-Source web server scanner that performs thorough testing on web servers, including over 6700 potentially dangerous files/programs, over 1250 servers for obsolete versions, and over 270 servers for version-specific problems. Fast-paced project that is constantly updated with the most recent known vulnerabilities also stated as nikto. To detect any potential problems, this enables you to scan your web servers with confidence. It also looks for server configuration items like multiple index files, HTTP server settings, and attempts to detect installed web servers and applications. Scanning items and plugins are updated on a regular basis and can be updated automatically. Nikto was not designed to be sneaky. As a result, firewalls are able to identify it.

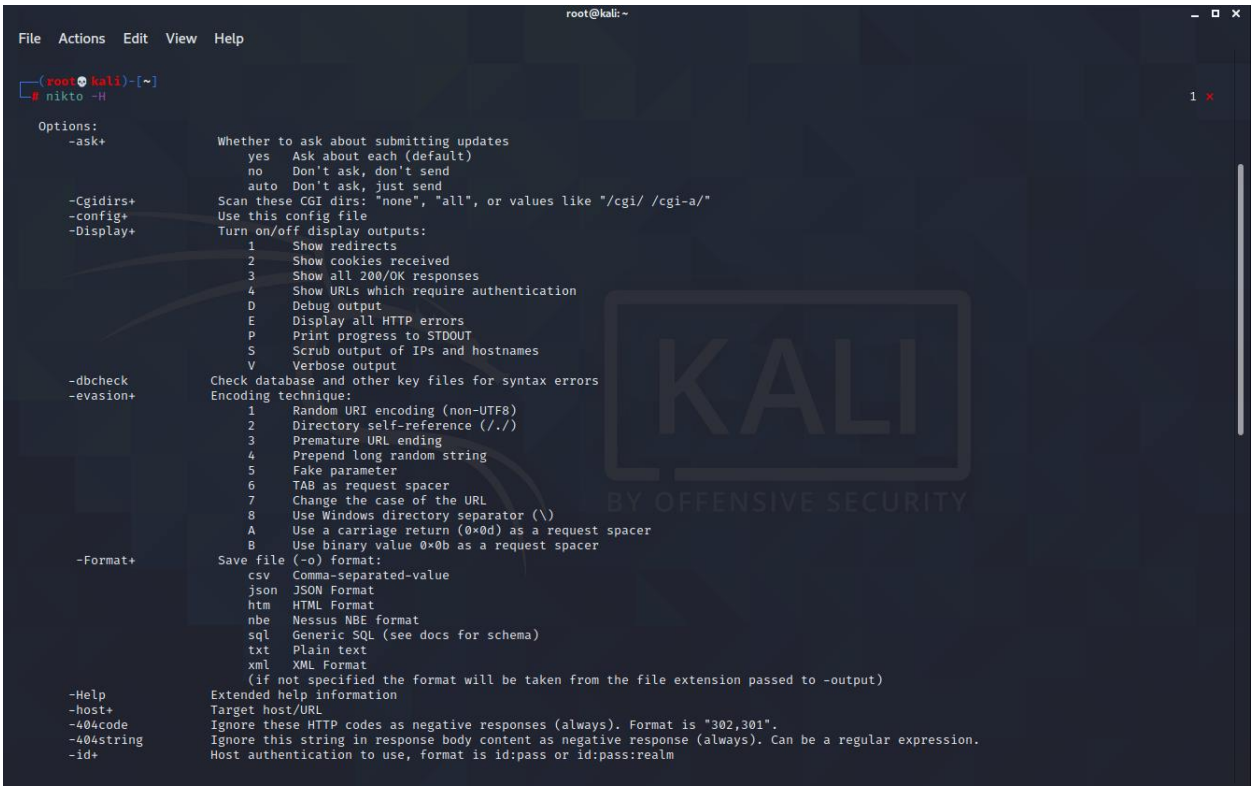
Features:

- ✓ Database of easily updatable CSV-format checks
- ✓ Reports can be written in plain text or HTML.
- ✓ Automatic switching between HTTP versions that are available
- ✓ Checks for both generic and specialized server software
- ✓ Support for proxy servers (with authentication)

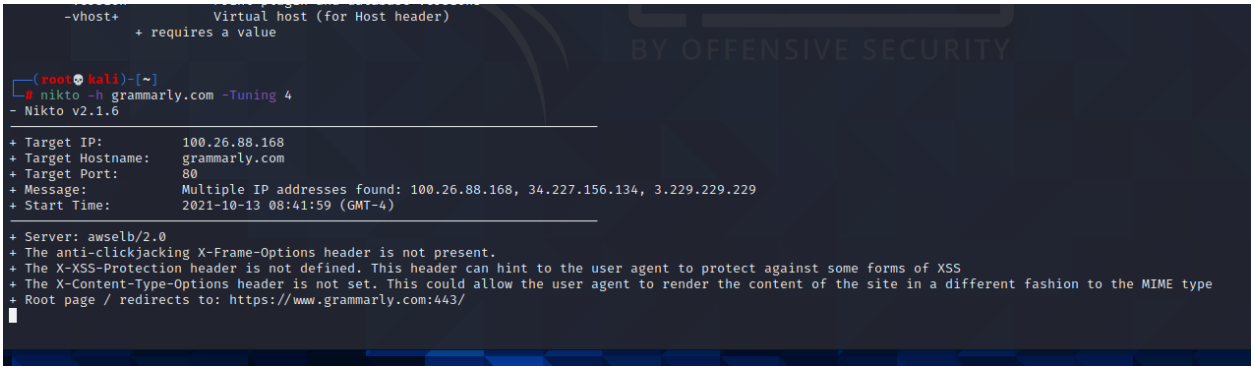
- Nikto was utilized to identify weak areas of my domain.
- Command to run Nikto:

  nikto -h 104.18.215.67

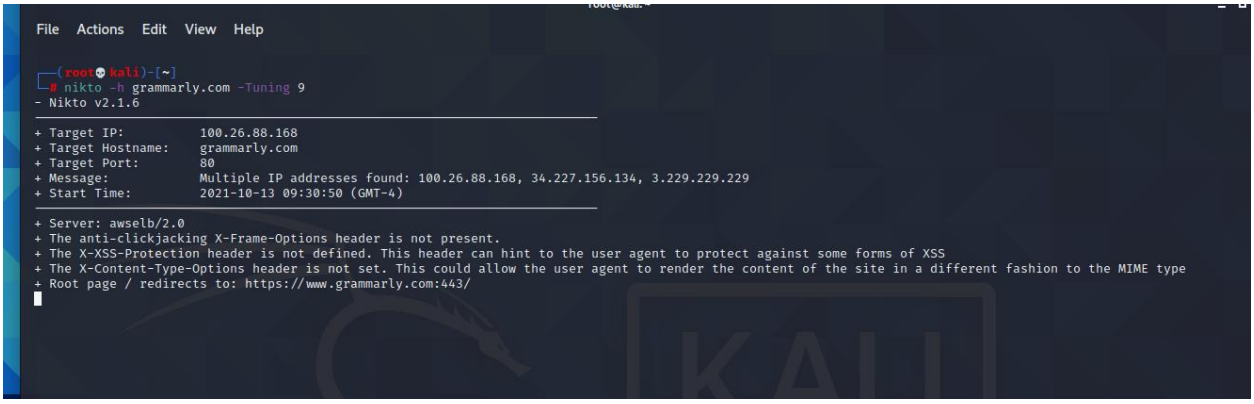
We may view additional advanced choices when we use the –H command.



Then we look for the injection command in the number 4 option.



The number 9 option, which is a SQL injection option, will then be used to scan the targeted host.



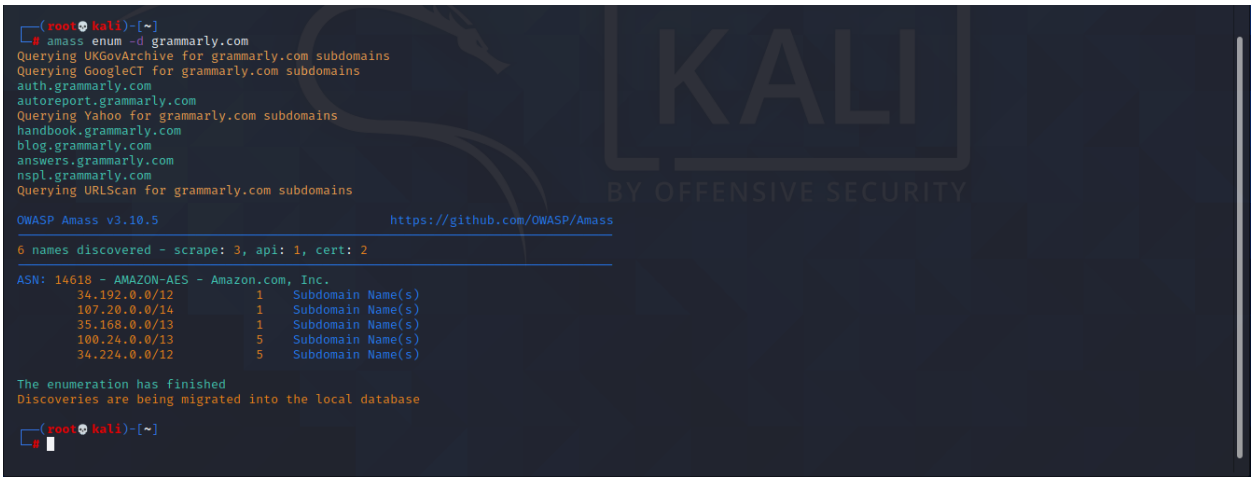
- The anti-clickjacking X-Frame-Options header is not present.
- The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
- The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

3.4 Amass

Amass is an open-source network mapping and attack surface identification tool that scrapes all accessible data using information gathering and other approaches such as active reconnaissance and external asset detection. To do so, it employs its own internal machinery and seamlessly connects with a variety of other services in order to improve its results, efficiency, and power. This tool focuses on DNS, HTTP, and SSL/TLS data discovery and scraping. It uses its own ways to accomplish this, and it integrates with a variety of API services, including (spoiler warning!) the Security Trails API. It also employs several online archiving algorithms to sift through the internet's forgotten data dumps.

Command to run Amass:

amass enum -d grammarly.com



3.5 DotDotpwn

DotDotPwn is a sharp fluffing gadget that enables an assailant to discover possible flaws that may be recognized using a navigation index inside a provided assist. The gadget is appealing and can assist in the detection of flaws in web server protocols such as TFTP, HTTP, and FTP. When dealing with infiltration testing on web applications, the equipment might be very useful. DotDotPwn is pre-installed as part of the Kali Linux package. This apparatus is the major Mexican tool in Back Track Linux, which is a precursor of Kali. The Perl programming language is used to create and program this gadget.

DotDotPwn, as a fluffing gadget, is completely adjustable and is also prepared to provide some elevated level understanding while doing fluffing activities. It's possible that programmers will use it on online platforms such as ERPs, CMSs, and so on. It features a remarkable feature that allows it to execute a convention-free module. We may easily send a payload to a host using a specific port of our choice using this method.

This instrument is quite good at computerizing fluffing operations due to its amazing features. You may use it to identify some of the escape clauses that can be utilized during an attack. DotDotPwn can be used to detect errors that may have occurred as a result of unsuitable information approval, incorrect boundaries, or incorrect information. This type of information might help the attacker

figure out what kind of assault payload to deliver to the target. Due to the device's several applications, it can provide a few assault vectors that can be used during an attack.

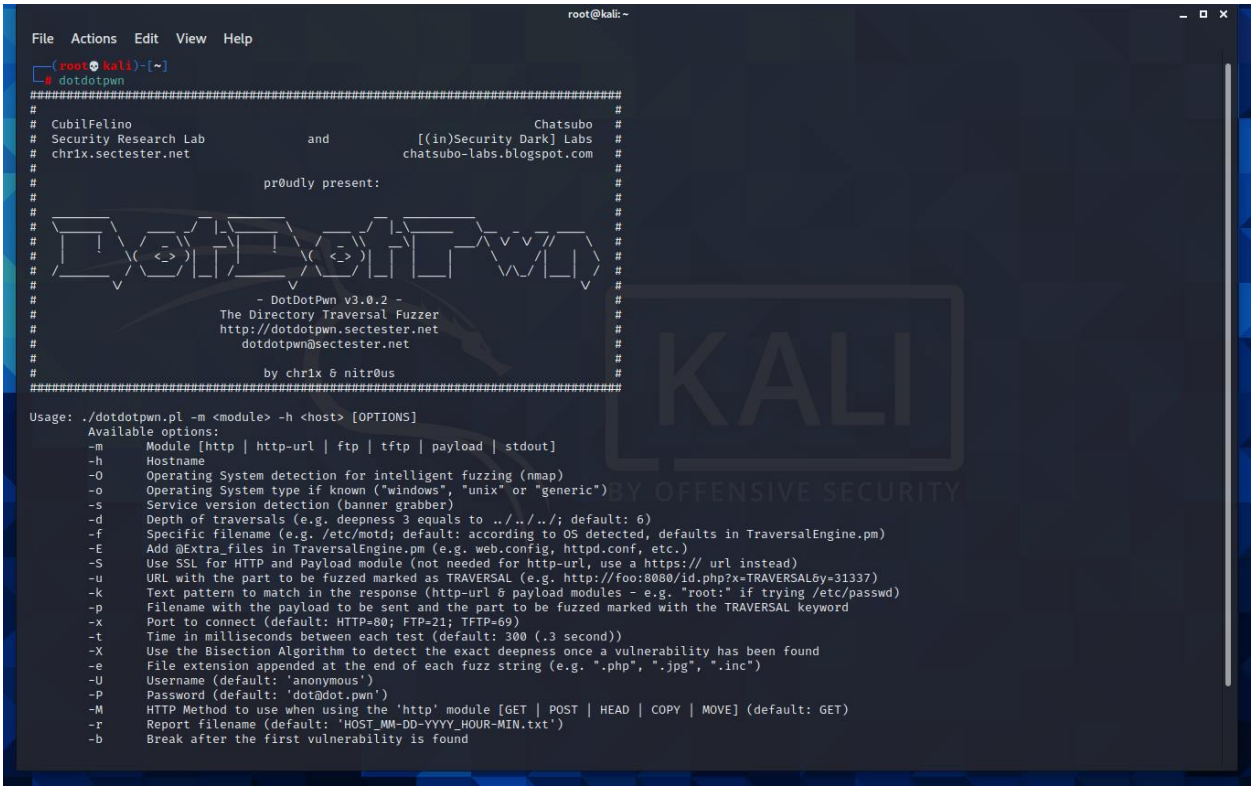
How does it work?

DotDotPwn, like other fluffing instruments, operates by piling a lot of information stages into the targeted administration. Following the submission of the information, the equipment will monitor how the software being attacked responds. DotDotPwn might view the data as vulnerable based on the input provided by the application. When the information piled into the program causes it to crash or gives yields that appear to be unnecessary, vulnerabilities are discovered. When placed on a website, the device may show the attacker the status of the HTTP request for each payload being tested. The attacker can learn whether the site being attempted is helpless by using the status input.

Start of DotDotpwn

Code:

DotDotpwn



- Because we already found the Grammarly.com's IP address through nmap, I'm not going to find it again.
- When I start the scan, it is rejected because the website uses a https webserver.
- Command to run the scan in DotDotpwn:

dotdotpwn -m https -h 34.227.156.134

This is a fantastic success by the web security team in preventing an attack and preventing information about the site from being displayed. It is mostly accomplished through the usage of the HTTPS protocol. There are no vulnerabilities or information given, therefore it's safe.

3.6 Nessus

Nessus is indeed a remote security scanning tool, which scans a computer and raises an alarm if it discovers any weaknesses that hostile hackers may exploit to obtain access to any machine you have joined to a network. It achieves this by running over 1200 tests on a given machine, trying to discover if any of these attacks may be used to break into the computer or otherwise harm it. Nessus isn't a full-fledged security solution; rather, it's an important component of a well-rounded security approach. Nessus is a program that scans your systems for vulnerabilities that hackers may exploit. It does not actively prevent assaults.

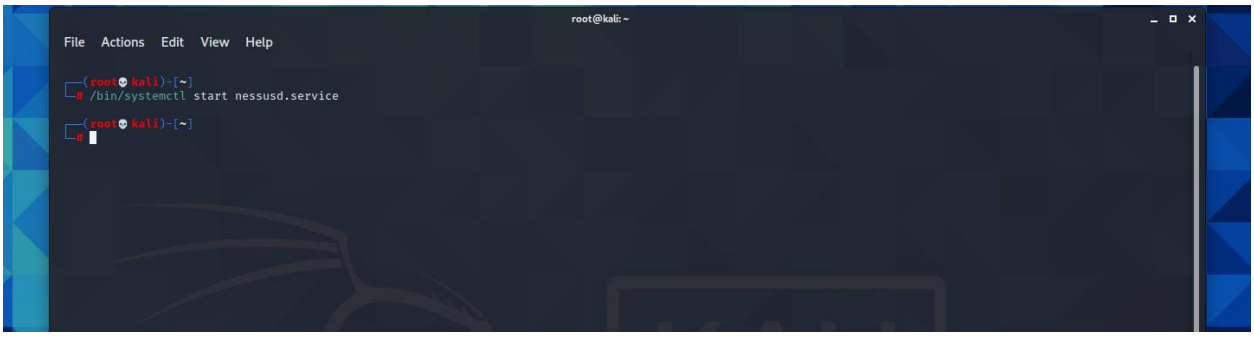
Information about new vulnerabilities and exploits that are currently being exploited. The Nessus team refreshes the list of vulnerabilities to search for on a regular basis in order to reduce the time

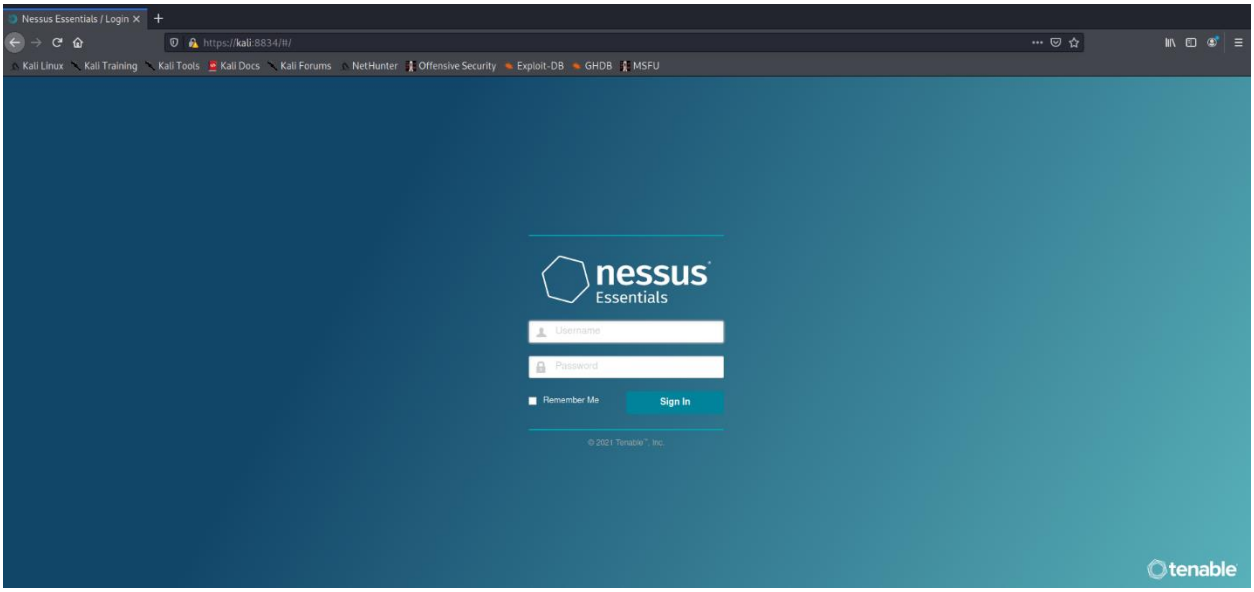
between an exploit being discovered in the wild and you being able to detect it using Nessus. Nessus is open source, which means it is free to use and modify.

- I ran Nessus and discovered vulnerabilities on my domain.
- Command to run Nessus:

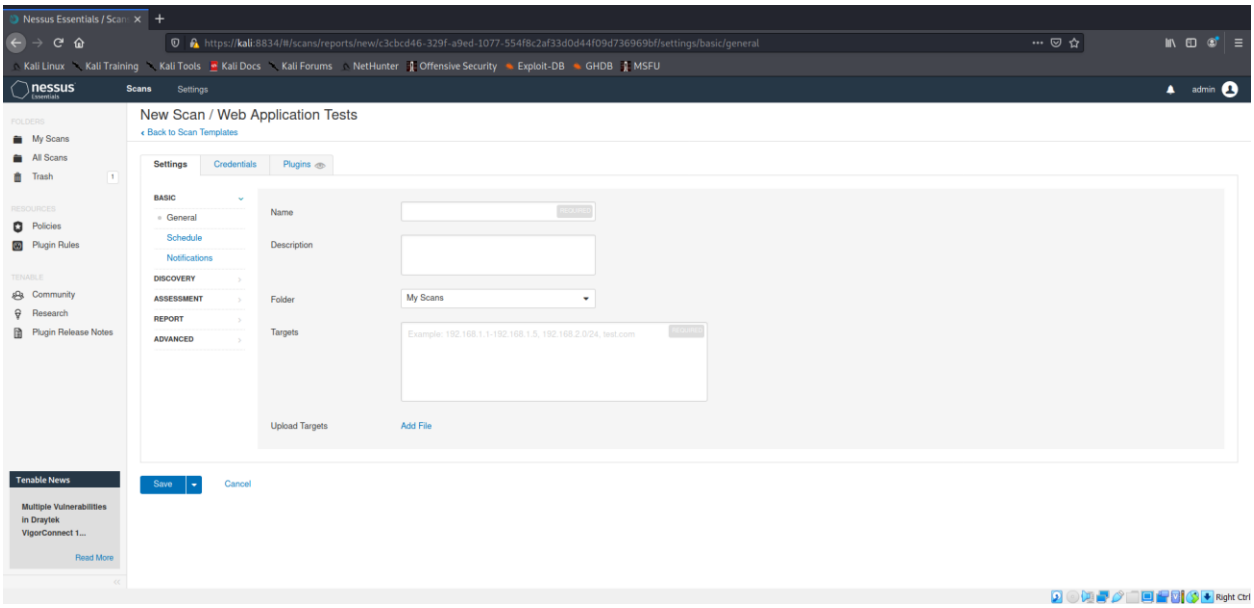
  In terminal - **/bin/systemctl start nessusd.service**

  In browser - **https://kali:8834/**

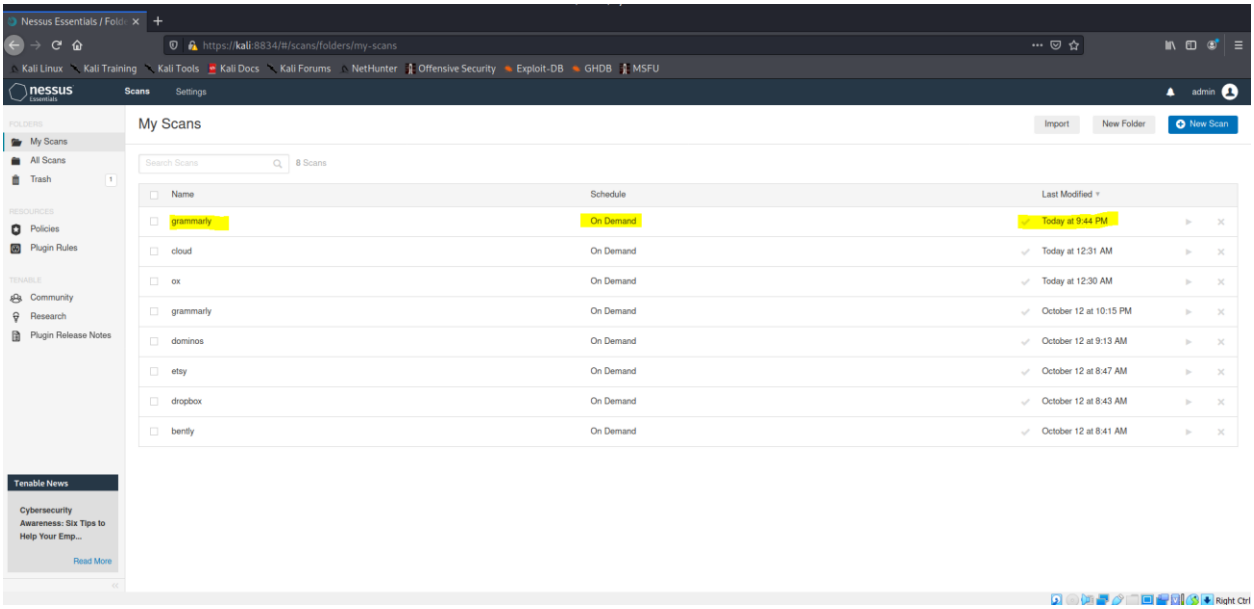




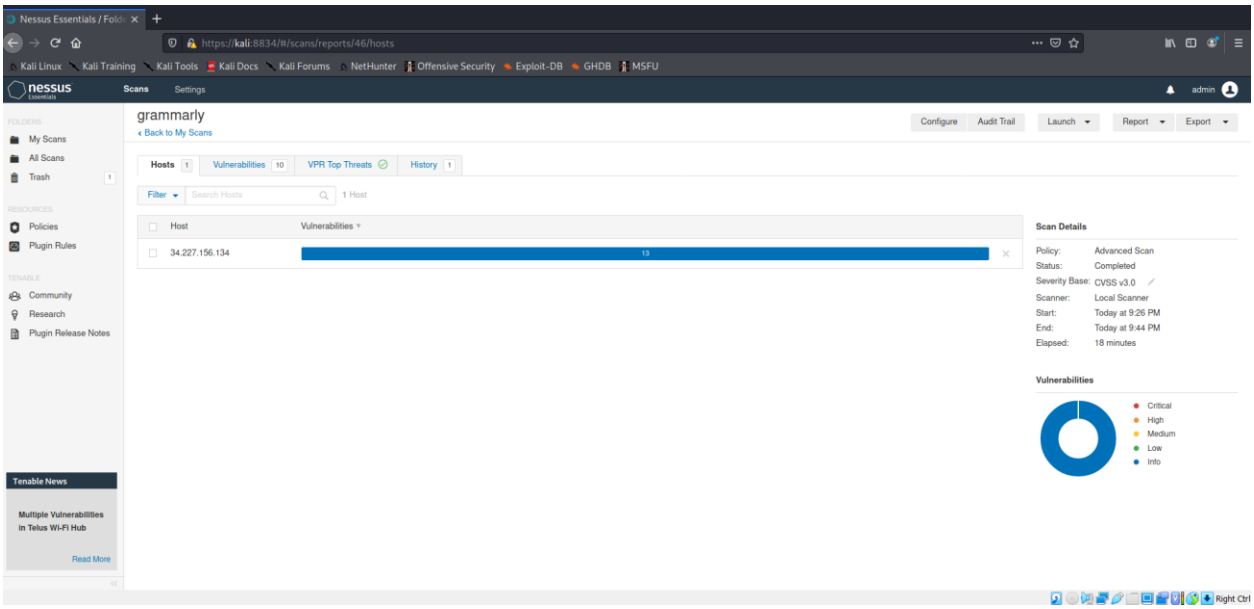
Starting a new scan in Nessus by giving the domain IP



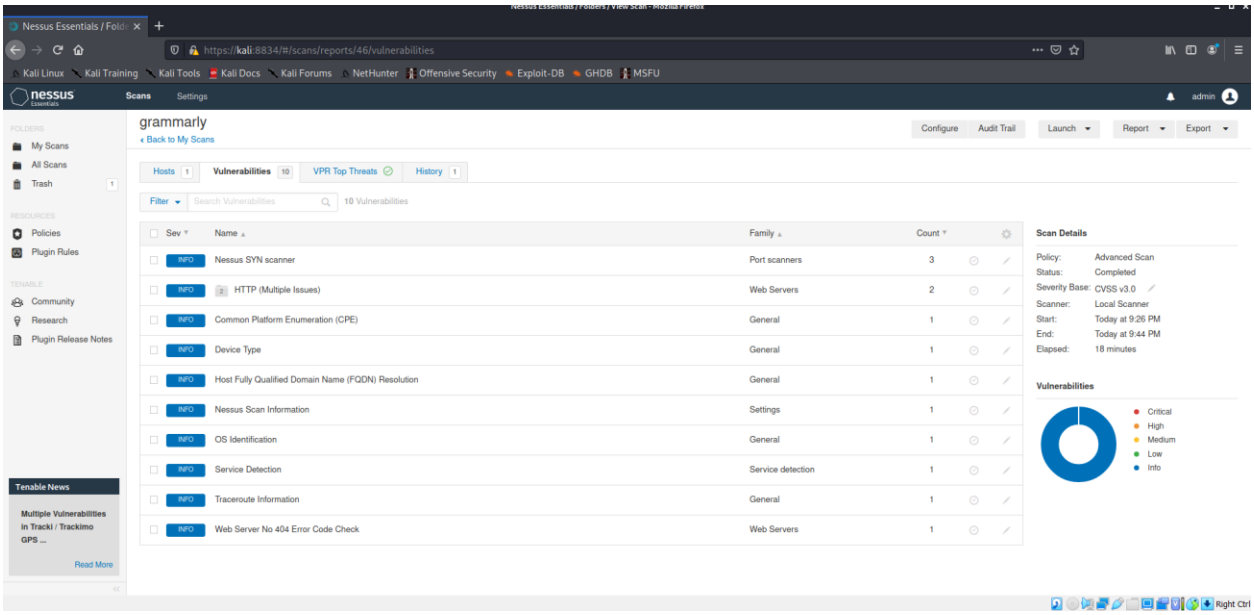
Nessus scan report

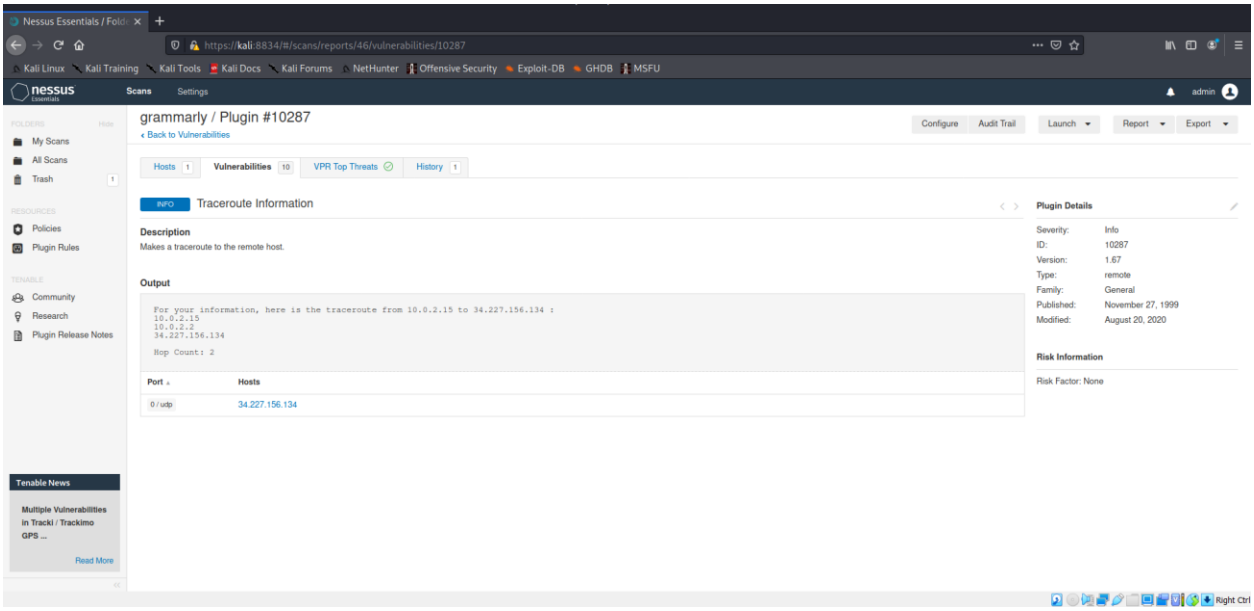


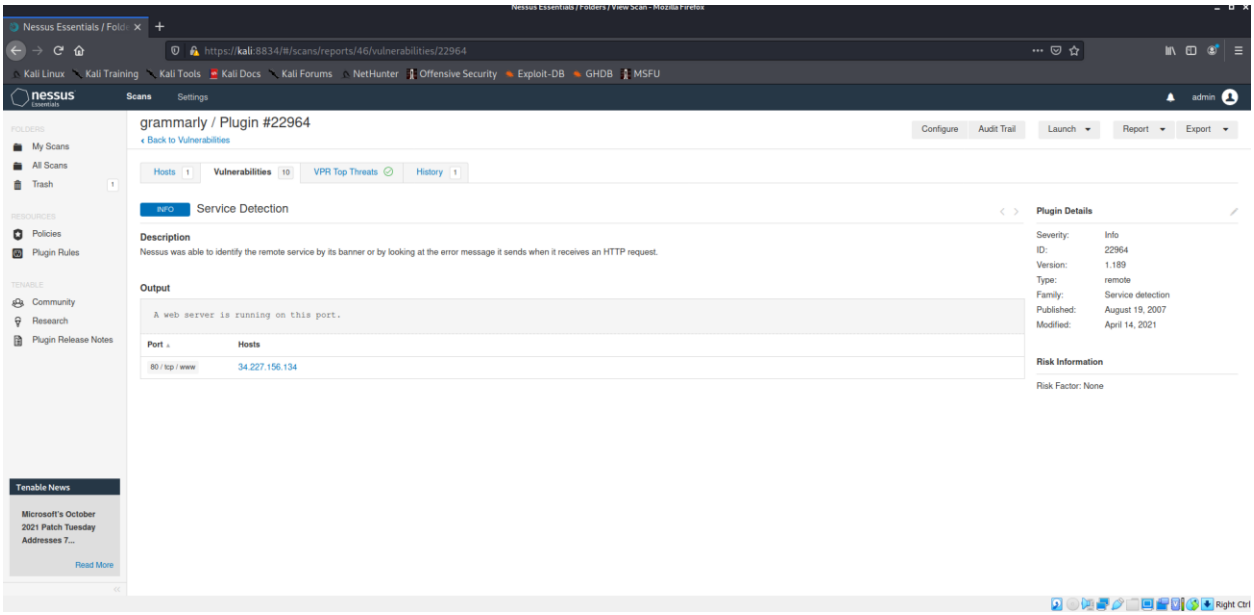
Information found on the website

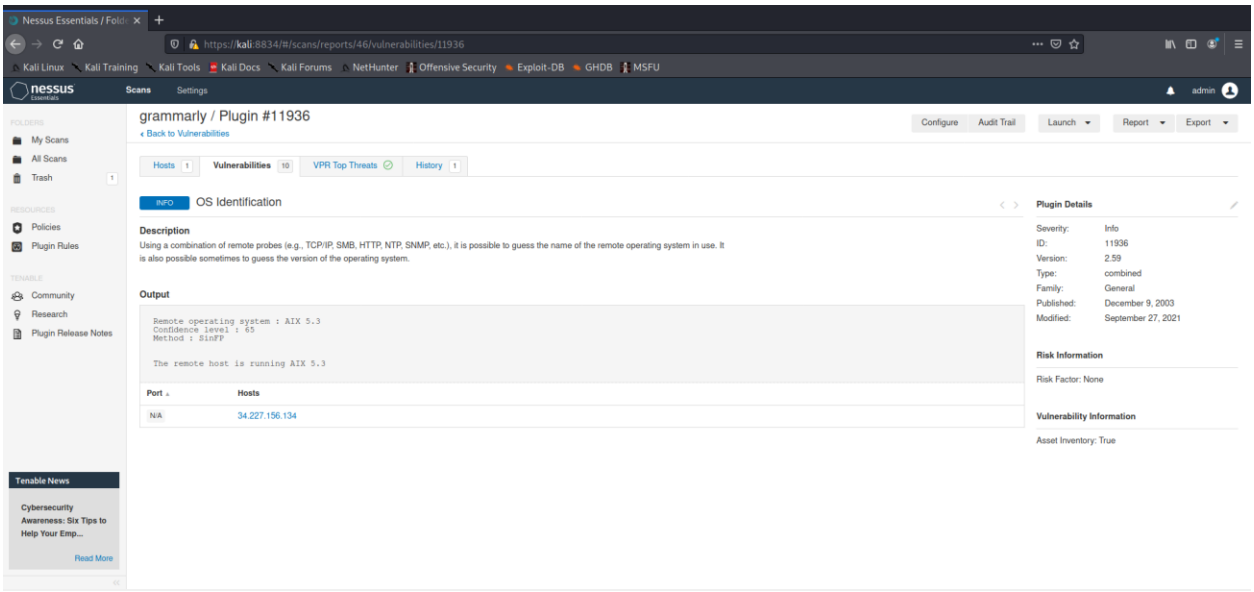


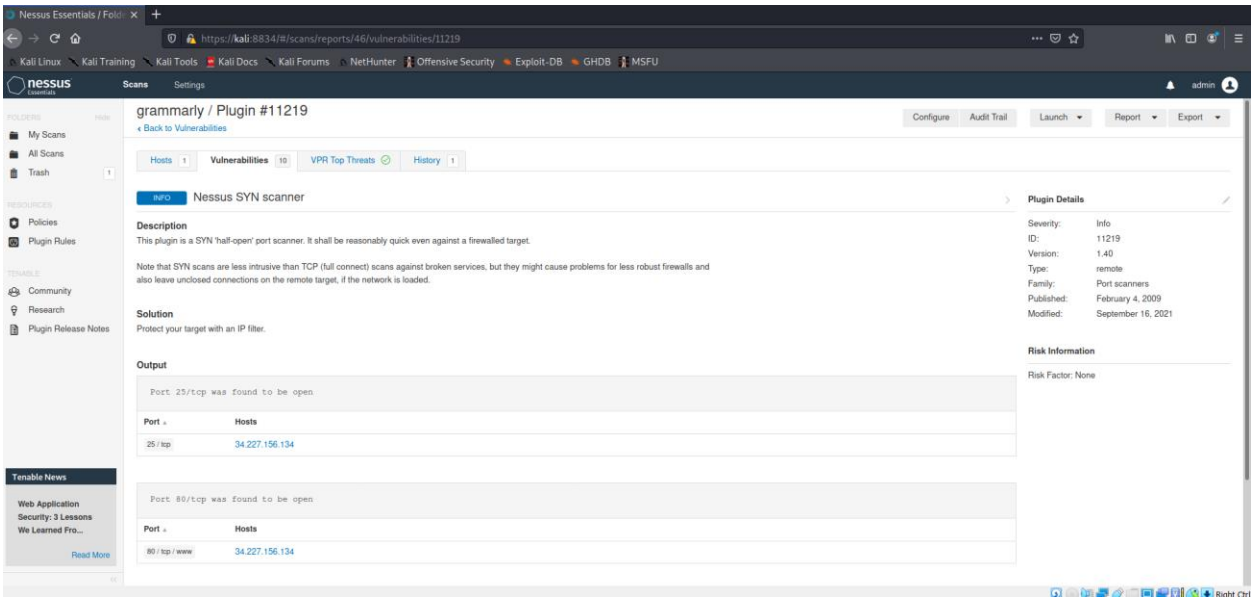
In the vulnerabilities tab we can see the ports and webs servers' information one by one which falls under the informative category.




Nessus Essentials / Folde
https://kali:8834/#/scans/reports/46/vulnerabilities/10287
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
nessus Essentials
Scans Settings
admin
My Scans
All Scans
Trash
Policies
Plugin Rules
Community
Research
Plugin Release Notes
grammarly / Plugin #10287
Back to Vulnerabilities
Configure Audit Trail Launch Report Export
Hosts 1 Vulnerabilities 10 VPR Top Threats History 1
INFO Traceroute Information
Description
Makes a traceroute to the remote host.
Output
For your information, here is the traceroute from 10.0.2.15 to 34.227.156.134 :
10.0.2.15
10.0.2.2
34.227.156.134
Hop Count: 2
Port Hosts
0 / udp 34.227.156.134
Plugin Details
Severity: Info
ID: 10287
Version: 1.67
Type: remote
Family: General
Published: November 27, 1999
Modified: August 20, 2020
Risk Information
Risk Factor: None
Tenable News
Multiple Vulnerabilities in Tracki / Trackimo GPS ...
Read More
Right Ctrl


Nessus Essentials / Folders / View Scan - Mozilla Firefox
Nessus Essentials / Folde
https://kali:8834/#/scans/reports/46/vulnerabilities/22964
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
nessus Essentials
Scans Settings
admin
My Scans
All Scans
Trash
Policies
Plugin Rules
Community
Research
Plugin Release Notes
grammarly / Plugin #22964
Back to Vulnerabilities
Configure Audit Trail Launch Report Export
Hosts 1 Vulnerabilities 10 VPR Top Threats History 1
INFO Service Detection
Description
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.
Output
A web server is running on this port.
Port Hosts
80 / tcp / www 34.227.156.134
Plugin Details
Severity: Info
ID: 22964
Version: 1.189
Type: remote
Family: Service detection
Published: August 19, 2007
Modified: April 14, 2021
Risk Information
Risk Factor: None
Tenable News
Microsoft's October 2021 Patch Tuesday Addresses 7...
Read More
Right Ctrl



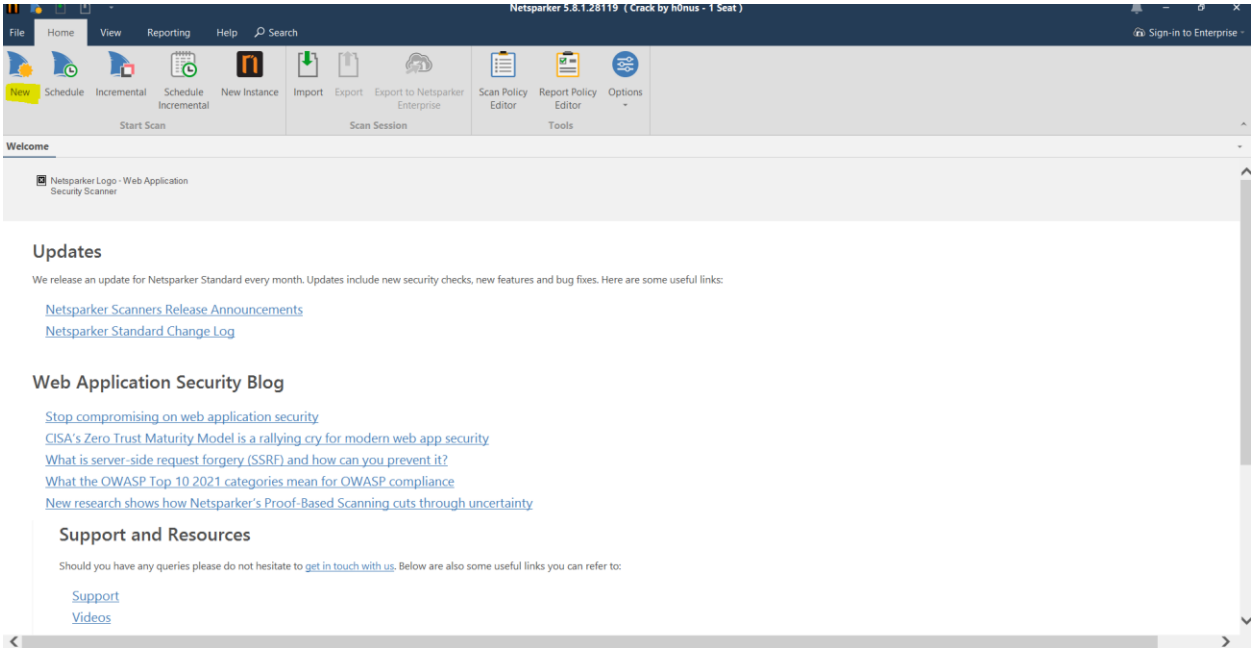


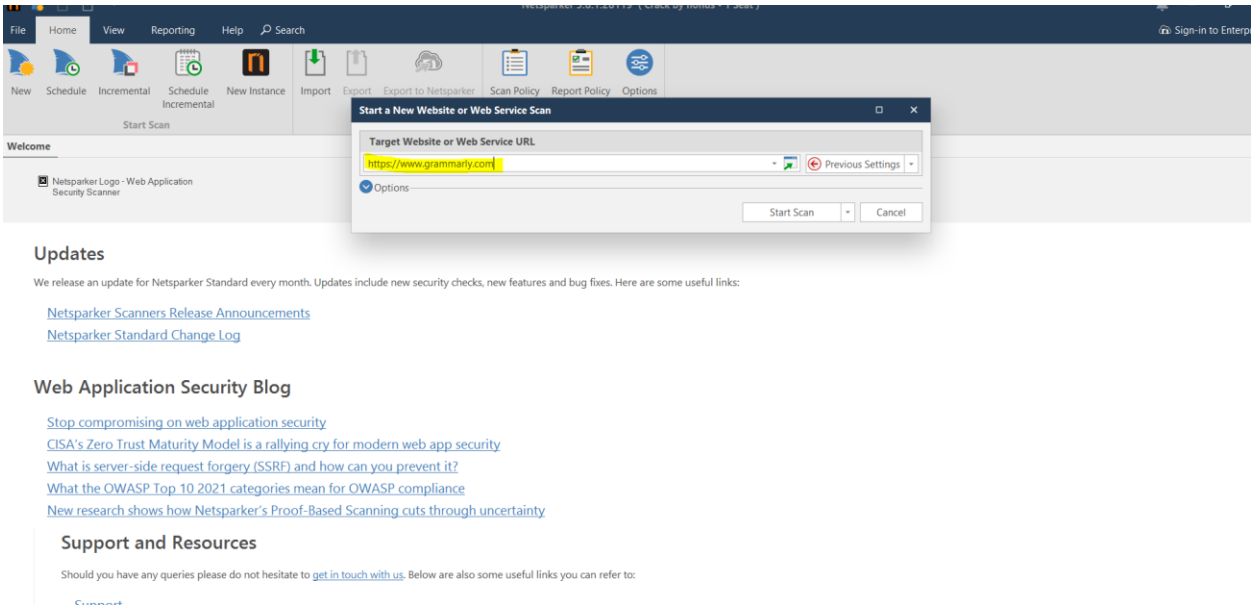
This scan only revealed open ports, cookies, and other information, making it a useful P5 on the vulnerability scale.

3.7 Netsparker

Netsparker is a web application security scanner that searches websites, web applications, and online services for security flaws. Netsparker can scan all types of online applications, independent of the platform or language in which they are written. Netsparker is the first online web application security scanner that automatically exploits reported vulnerabilities in a read-only and safe manner to validate known issues. It also provides proof of the flaw, so you don't have to waste time manually examining it. For example, if a SQL injection vulnerability is discovered, the database name will be presented as the exploit evidence.

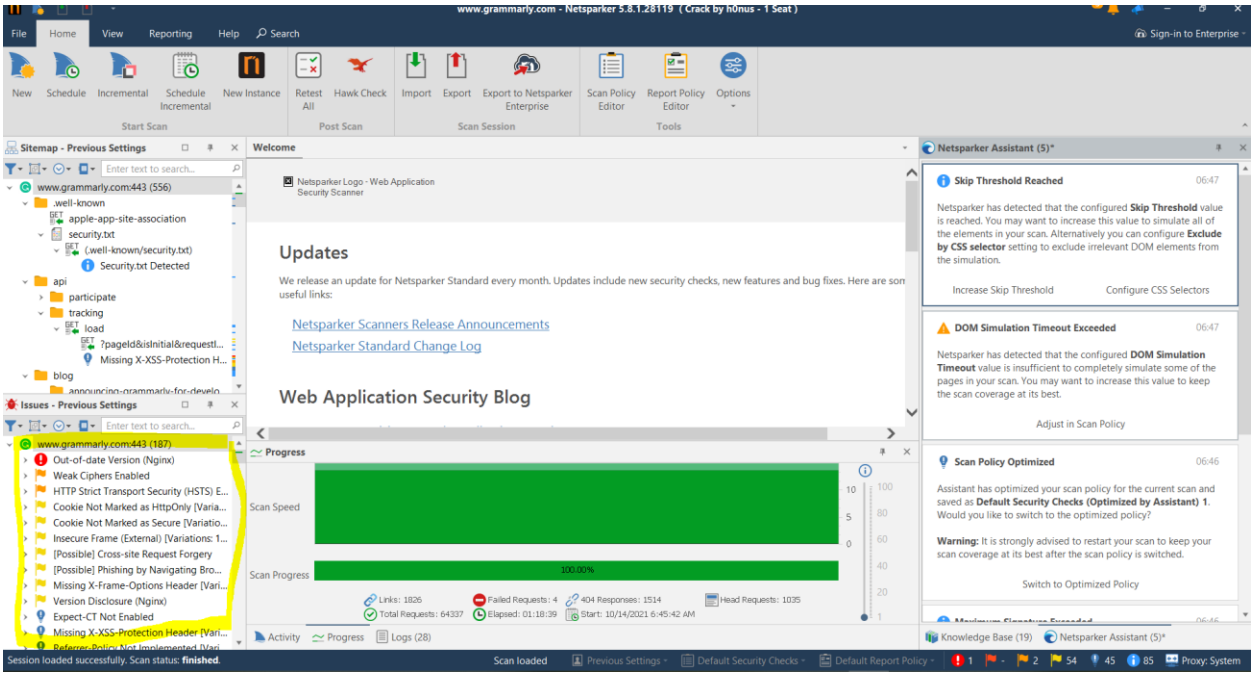
- The findings are obtained by running this program as a Windows application.
- First, we have to click new and enter the domain URL





When the session finished, we can see several vulnerabilities of our targeted domain. From the flags in the right side indicates the count of critical, high, medium, low vulnerabilities.

In the left side we can see the list of vulnerabilities we found from the scan. In my selected domain I have found one critical, two medium, seven low vulnerabilities and all other 45 are information.



The critical vulnerability I found is **Out-of-date Version (Nginx).** Grammarly is using an out-of-date version of Nginx, according to Netsparker. Because this is an older version of the program, it might be exposed to assaults. As a remedy, they claimed that they will upgrade their Nginx installation to the most recent stable version.

This Version's Vulnerabilities.

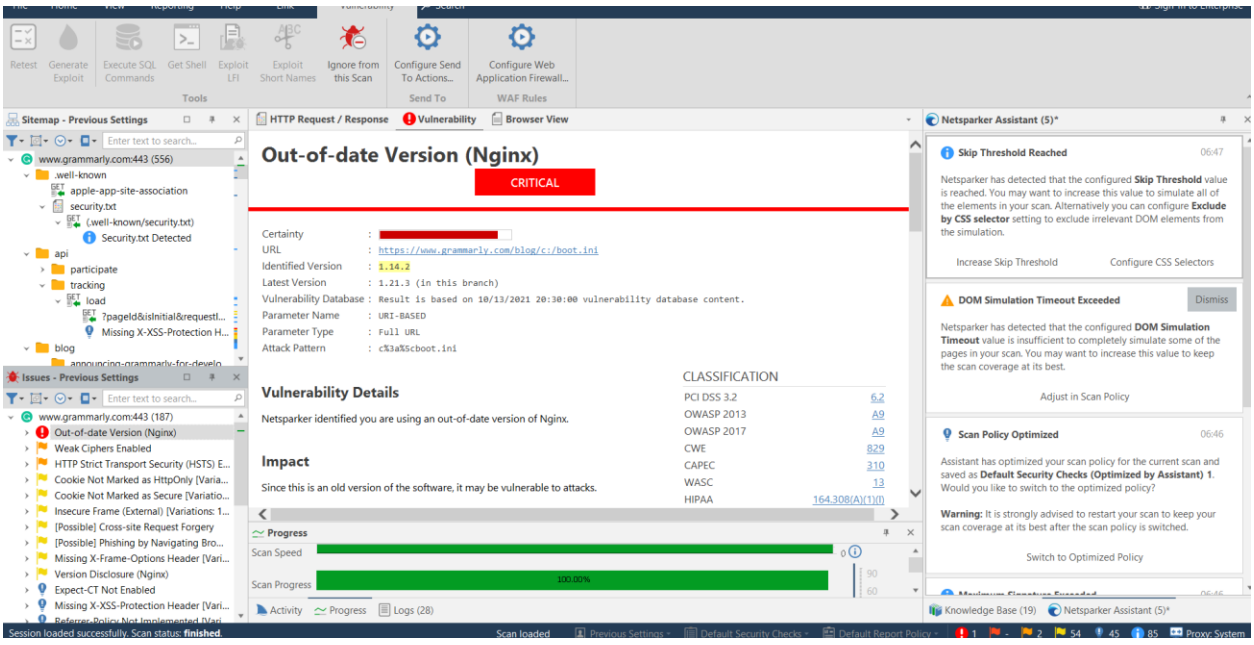
Nginx Resource Allocation Vulnerability without Limits or Throttling

A header leak vulnerability exists in some HTTP/2 implementations, which might result in a denial of service. The attacker delivers a stream of headers with a 0-length header name and 0-length header value, Huffman encoded into 1-byte or larger headers if desired. Some implementations allocate memory for these headers and maintain it alive until the session terminates. This has the potential to use up a lot of memory. Versions 1.9.5 to 1.16.0 are affected.

Latest Version :1.21.3 (in this branch)

Identified Version :1.14.2

For references they have mentioned a CVE - **CVE-2019-9516**



Netsparker has identified Weak Ciphers Enabled as a medium level vulnerability.

List of Supported Weak Ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)

During secure connection, Netsparker discovered that weak ciphers are enabled (SSL). To ensure safe communication with its visitors, Grammarly should only enable powerful ciphers on their web server. SSL traffic between Grammarly's server and its visitors might be decrypted by attackers. They should configure your web server to prevent the use of weak ciphers. Grammarly should edit the SSLCipherSuite directive in httpd.conf for Apache.

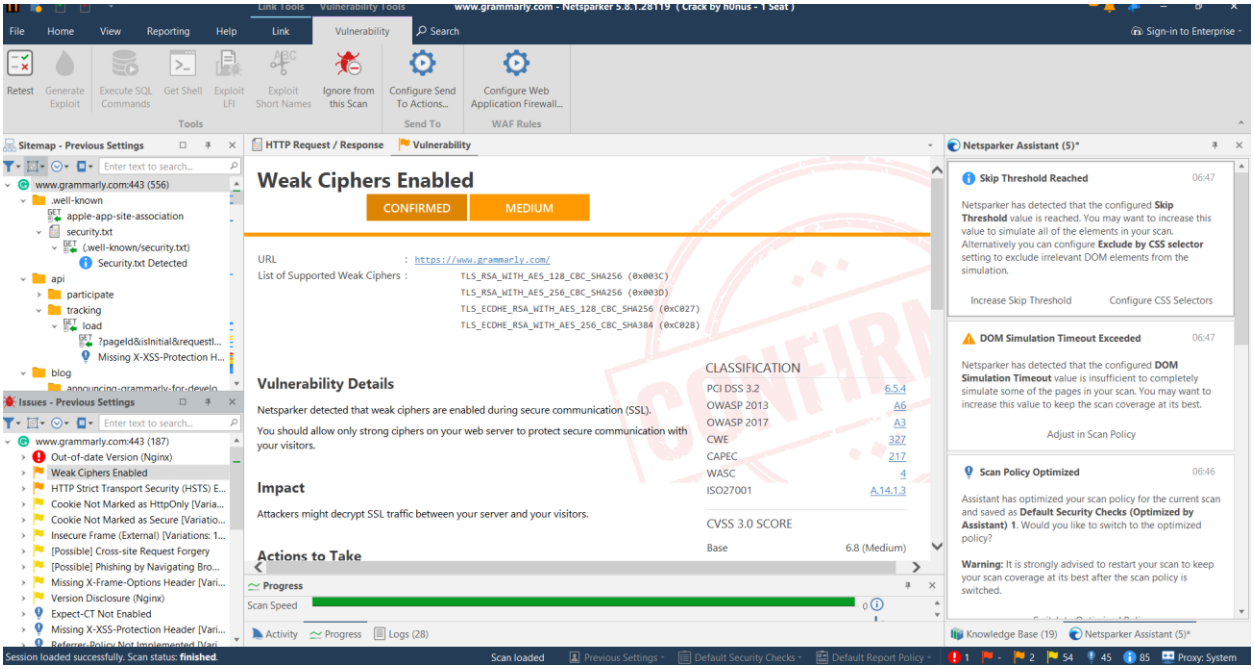
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4

Lighttpd:

ssl.honor-cipher-order = "enable"

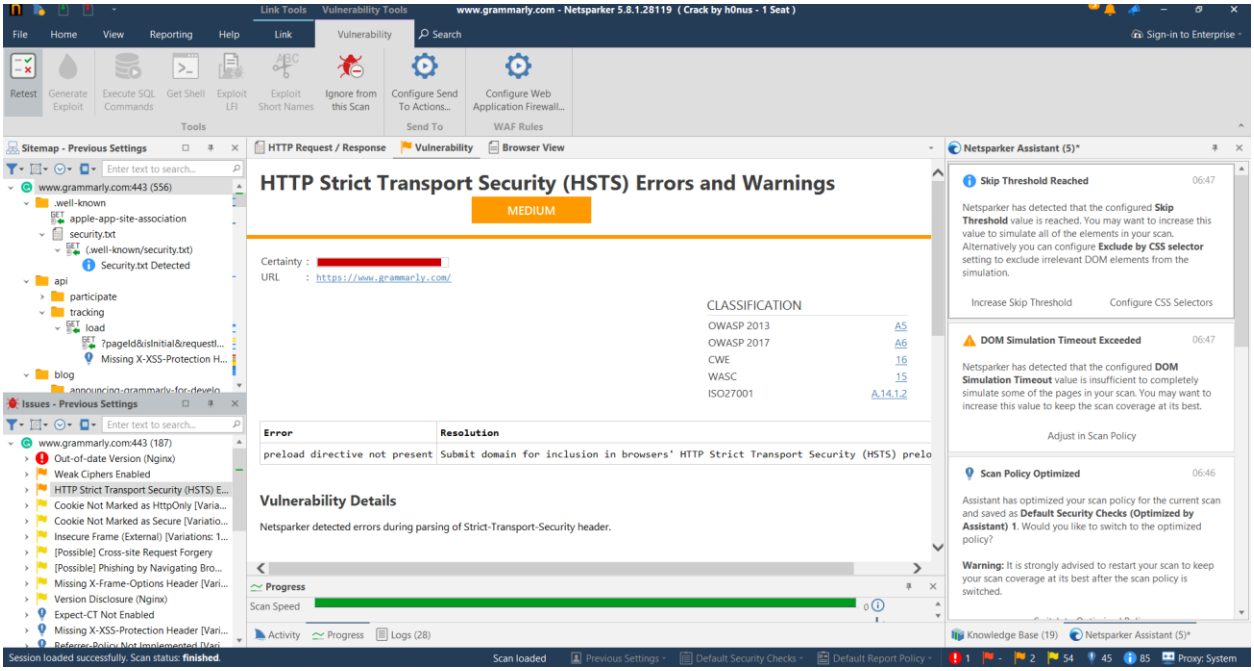
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"

Grammarly should modify the system registry for Microsoft IIS. Incorrectly changing the registry may do significant damage to their machine. They should back up any important data on their computer before making changes to the registry.



Medium level vulnerability - HTTP Strict Transport Security (HSTS) Errors and Warnings. During the processing of the Strict-Transport-Security header, Netsparker discovered problems.

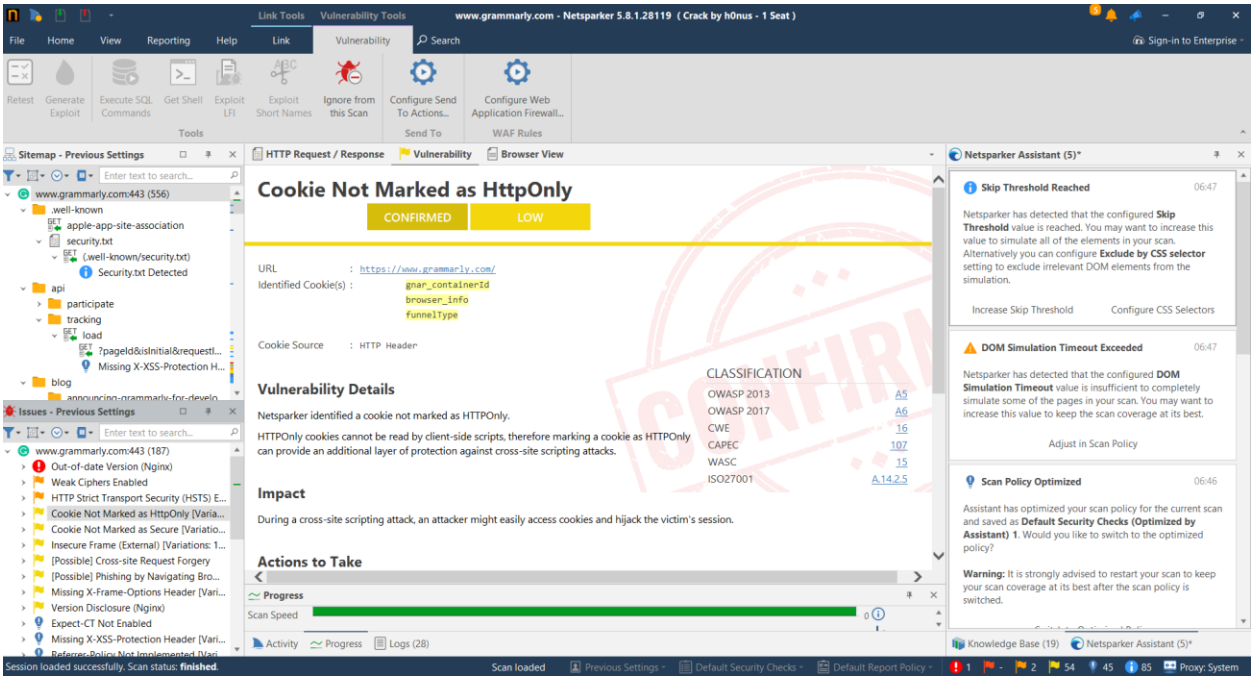
The HSTS Warning and Error may let attackers to circumvent HSTS, allowing them to view and change grammarly's interactions with the website.



Solution

After you've fixed the problems and warnings, you should think about adding your domain to the HSTS preload list. This will force browsers to connect to your website using HTTPS, thus prohibiting people from accessing it via HTTP. Because this list is hardcoded in users' browsers, it enables HSTS even before they visit your website for the first time, removing the requirement for Trust on First Use (TOFU) and its accompanying risks and drawbacks. Your website will not fulfill the requirements necessary to enter the browser's preload list until you address the issues and warnings.

Low level vulnerability - Cookie Not Marked as HttpOnly. A cookie that was not designated as HTTPOnly was discovered by Netsparker. Because HTTPOnly cookies cannot be read by client-side scripts, setting a cookie as HTTPOnly can offer an extra layer of security against cross-site scripting assaults. An attacker may simply access cookies and hijack the victim's session via a cross-site scripting attack.



Solution

Set the cookie to HTTPOnly. This will provide an additional layer of protection against XSS. This, however, is not a panacea and will not defend the system from cross-site scripting assaults. An attacker can circumvent HTTPOnly security by using a tool like XSS Tunnel.

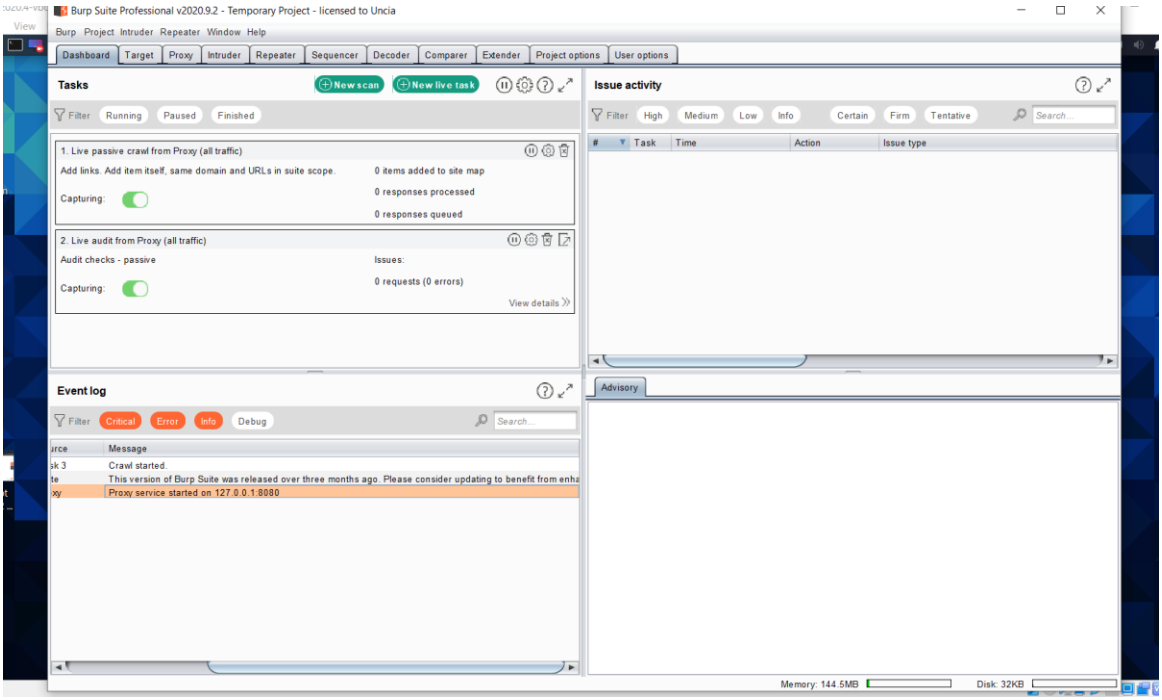
Other low-level vulnerabilities.

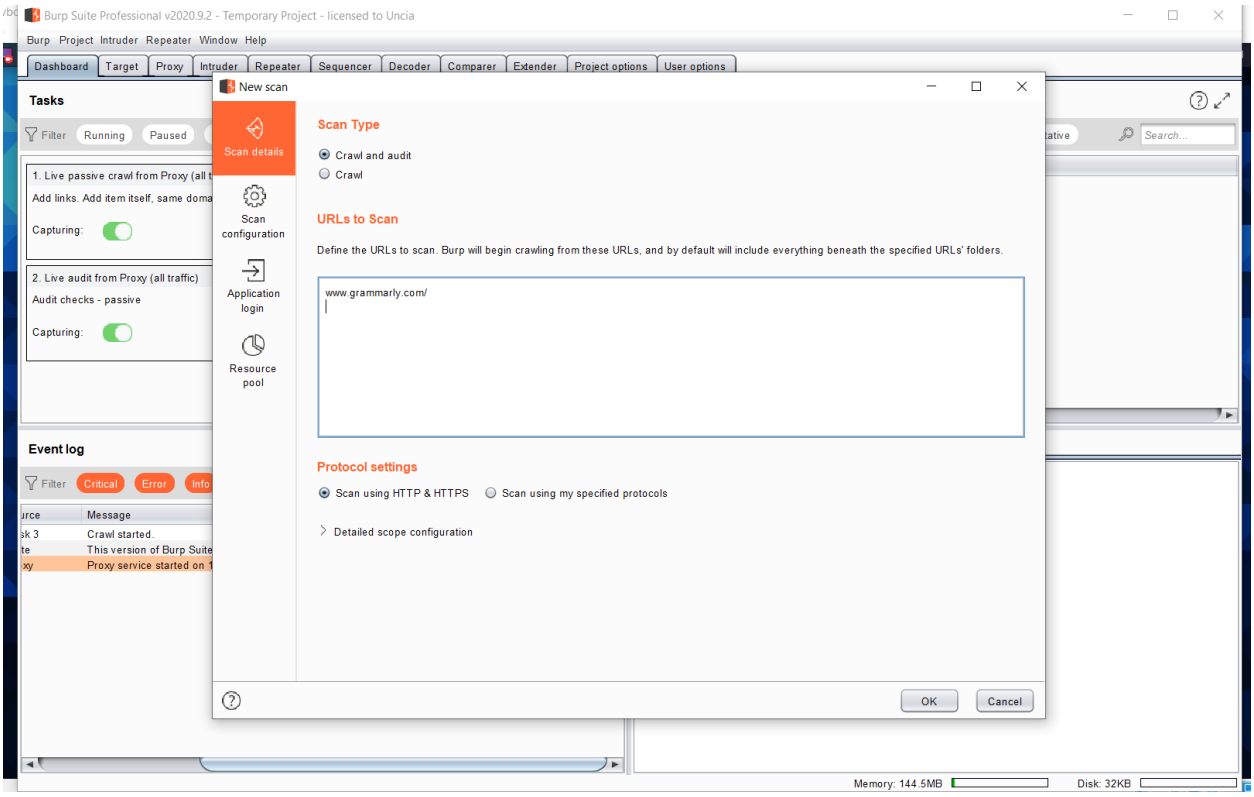
- Insecure Frame (External)
- Cookie Not Marked as Secure
- [Possible] Cross-site Request Forgery
- [Possible] Phishing by Navigating Browser Tabs
- Missing X-Frame-Options Header
- Version Disclosure (Nginx)

3.8 Burp Suite

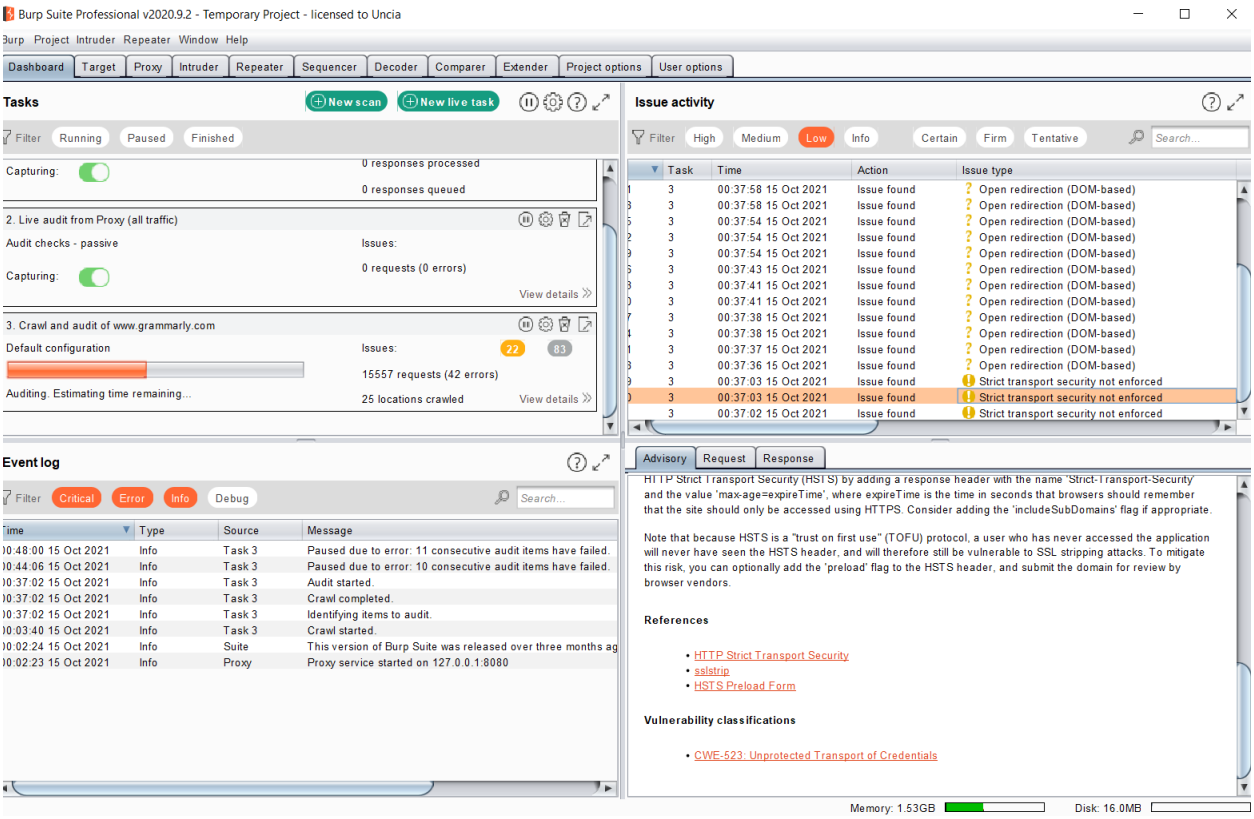
Burp Suite is a Java-based Web Penetration Testing tool. These have evolved into an industry standard collection of tools used by information security experts. Burp Suite helps you to identify online application vulnerabilities and attack vectors. Because of the popularity, extent, and depth of features of Burp Suite, we created this handy website as a compilation of Burp Suite knowledge and facts. In its most basic form, the Burp Suite is an Interception Proxy.

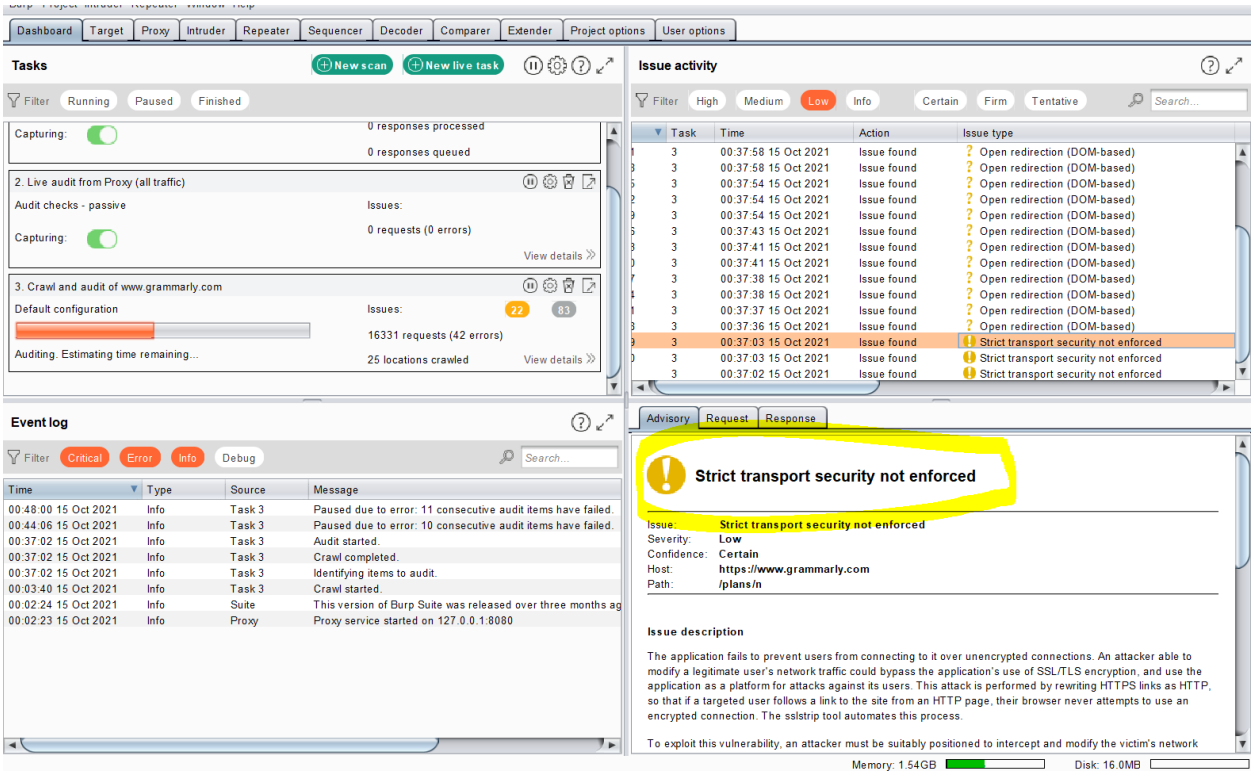
When accessing their target software, a penetration tester can setup their internet browser to redirect traffic through the Burp Suite proxy server. Burp Suite then serves as a Man in The Middle by capturing and analyzing requests to and from the target web application so that they may be analyzed. Penetration testers can pause, modify, and replay individual HTTP requests to analyze possible parameters or injection sites. Injection points can be set for both human and automated fuzzing attacks to uncover possibly unexpected application behaviors, crashes, and error messages.


Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished
1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing:
0 items added to site map
0 responses processed
0 responses queued
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing:
Issues:
0 requests (0 errors)
View details
Issue activity
Filter High Medium Low Info Certain Firm Tentative
Search...
Task Time Action Issue type
Advisory
Event log
Filter Critical Error Info Debug
Search...
Message
Crawl started.
This version of Burp Suite was released over three months ago. Please consider updating to benefit from enha
Proxy service started on 127.0.0.1:8080
Memory: 144.5MB
Disk: 32KB


Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
Filter Running Paused
1. Live passive crawl from Proxy (all t
Add links. Add item itself, same doma
Capturing:
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing:
Event log
Filter Critical Error Info
Message
Crawl started.
This version of Burp Suite
Proxy service started on 1
New scan
Scan details
Scan configuration
Application login
Resource pool
Scan Type
Crawl and audit
Crawl
URLs to Scan
Define the URLs to scan. Burp will begin crawling from these URLs, and by default will include everything beneath the specified URLs' folders.
www.grammarly.com/
Protocol settings
Scan using HTTP & HTTPS
Scan using my specified protocols
Detailed scope configuration
OK
Cancel
Memory: 144.5MB
Disk: 32KB


4. Crawl and audit of www.grammarly.com
Details
Audit items
Issue activity
Event log
Task details
Scan type: Crawl and audit
Scope: www.grammarly.com
Configuration: Default configuration
Issues: 0 0 0 0
Requests: 105
Errors: 0
Unique locations: 1
Unauthenticated crawl. Estimating time remaining...


Burp Suite Professional v2020.9.2 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Tasks
New scan
New live task
Filter Running Paused Finished
Capturing:
0 responses processed
0 responses queued
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing:
Issues:
0 requests (0 errors)
View details
3. Crawl and audit of www.grammarly.com
Default configuration
Issues: 22 83
15557 requests (42 errors)
Auditing. Estimating time remaining...
25 locations crawled
View details
Issue activity
Filter High Medium Low Info Certain Firm Tentative
Search...
Task Time Action Issue type
3 00:37:58 15 Oct 2021 Issue found Open redirection (DOM-based)
3 00:37:58 15 Oct 2021 Issue found Open redirection (DOM-based)
3 00:37:54 15 Oct 2021 Issue found Open redirection (DOM-based)
3 00:37:54 15 Oct 2021 Issue found Open redirection (DOM-based)
3 00:37:54 15 Oct 2021 Issue found Open redirection (DOM-based)
3 00:37:43 15 Oct 2021 Issue found Open redirection (DOM-based)
3 00:37:41 15 Oct 2021 Issue found Open redirection (DOM-based)
3 00:37:41 15 Oct 2021 Issue found Open redirection (DOM-based)
3 00:37:38 15 Oct 2021 Issue found Open redirection (DOM-based)
3 00:37:38 15 Oct 2021 Issue found Open redirection (DOM-based)
3 00:37:37 15 Oct 2021 Issue found Open redirection (DOM-based)
3 00:37:36 15 Oct 2021 Issue found Open redirection (DOM-based)
3 00:37:03 15 Oct 2021 Issue found Strict transport security not enforced
3 00:37:03 15 Oct 2021 Issue found Strict transport security not enforced
3 00:37:02 15 Oct 2021 Issue found Strict transport security not enforced
Event log
Filter Critical Error Info Debug
Search...
Time Type Source Message
00:48:00 15 Oct 2021 Info Task 3 Paused due to error: 11 consecutive audit items have failed.
00:44:06 15 Oct 2021 Info Task 3 Paused due to error: 10 consecutive audit items have failed.
00:37:02 15 Oct 2021 Info Task 3 Audit started.
00:37:02 15 Oct 2021 Info Task 3 Crawl completed.
00:37:02 15 Oct 2021 Info Task 3 Identifying items to audit.
00:03:40 15 Oct 2021 Info Task 3 Crawl started.
00:02:24 15 Oct 2021 Info Suite This version of Burp Suite was released over three months ag
00:02:23 15 Oct 2021 Info Proxy Proxy service started on 127.0.0.1:8080
Advisory
Request
Response
HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.
Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.
References
HTTP Strict Transport Security
sslstrip
HSTS Preload Form
Vulnerability classifications
CWE-523: Unprotected Transport of Credentials
Memory: 1.53GB
Disk: 16.0MB



By running the burpsuit scan, I have found some low-level vulnerabilities which are not very serious.

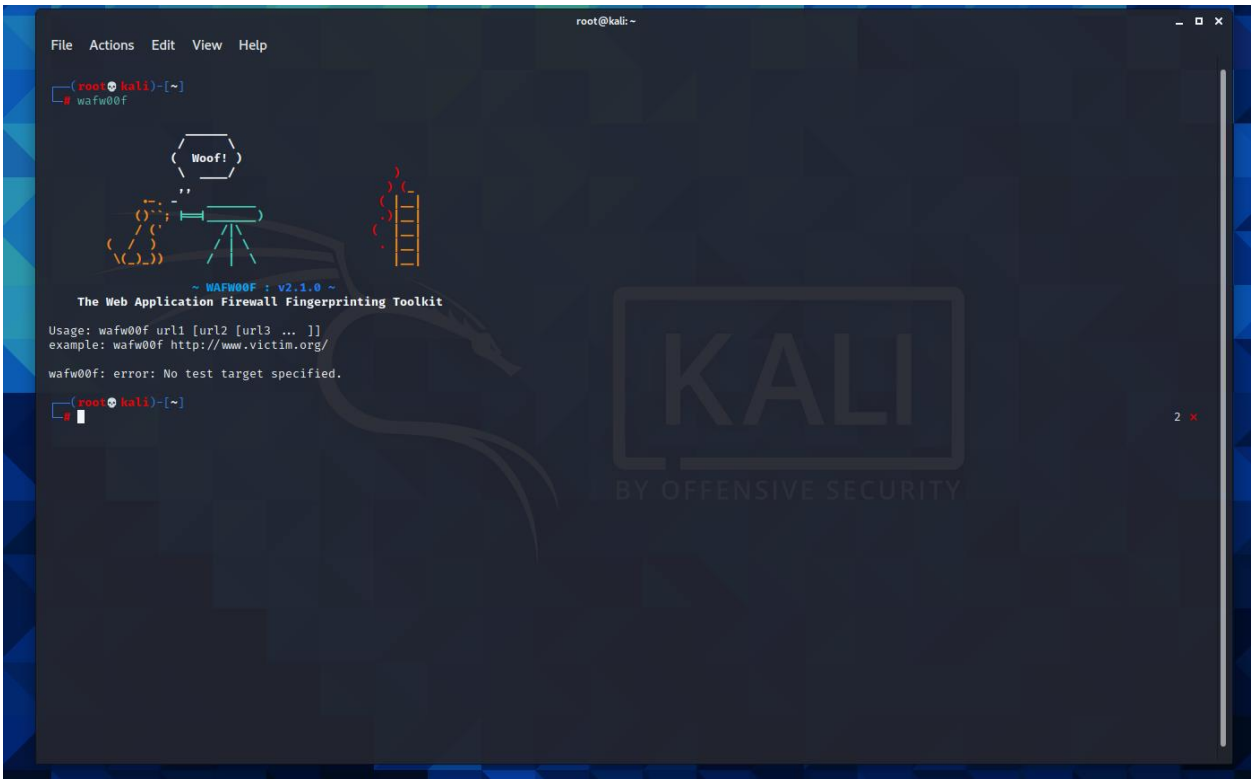
- Issue: Strict transport security not enforced
- Severity: Low
- Confidence: Certain
- Host:
- https://www.grammarly.com

3.9 Wafw00f

Web application firewalls are typically application-layer firewalls that filter and modify HTTP requests. The fundamental distinction is that WAFs attack the OSI Model's Layer 7 Application Layer. All WAFs, in essence, protect against different HTTP attacks and queries such as SQLi and XSS. Because the firewall can differentiate HTTP methods, SQL queries, and other contents contributed to various structures on a site, it can sift through the requests just like any other firewall. Through a site, one may realize an arrangement on what should be permitted and what should not be permitted as donation.

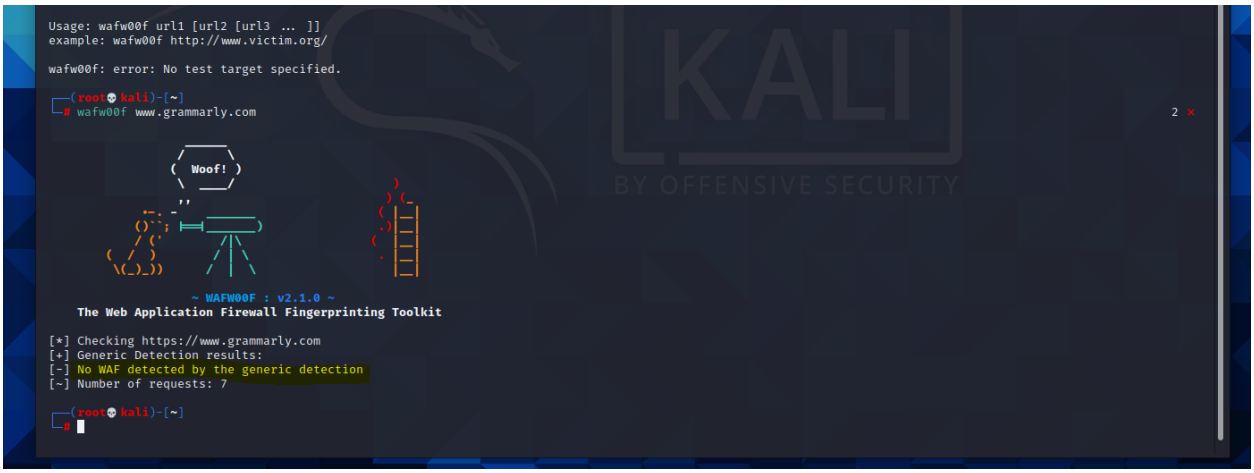
In a web application with Strict Transport Security enabled, such as a banking or internet business site, a WAF will be present on a regular basis. Identifying the waf goes under recon and planning the web application design while leading a pentest. It is necessary to recognize the presence of a WAF and evaluate it if Black Box testing occurs. This has a considerable influence on the tactics used during a Web-Application Penetration Test. Wafw00f is a Python program that automates a number of WAF-finding techniques. Wafw00f simply interrogates a web worker with a slew of HTTP requests and techniques. It investigates their reactions and identifies the firewall configuration.

When we execute the wafw00f without a URL, we get the message below.



We can observe that the web application has no WAF when we run the wafw00f with the targeted URL. This is a serious weakness. Because WAF decreases the number of assaults by 20%.

Command – wafw00f www.grammarly.com



We discovered that there is no WAF (web application firewall) for this targeted site, which has a high vulnerability P2.

Solutions

An Online Application Firewall, or WAF, protects web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It frequently protects online applications from attacks like as cross-website forgery, cross-webpage scripting (XSS), record consideration, and SQL infusion, among others. A WAF is a standard layer 7 protection (in the OSI model) that isn't meant to protect against a wide variety of attacks. This approach for attack alleviation is typically required for the installation of equipment that, when combined, provide an all-encompassing defense against a variety of assault vectors. As a result, employing cloudfare or AWS firewall will protect against these assaults.

3.10 dtect

D-TECT is a command-line based web application penetration testing tool that was created with Penetration Testers and Security Researchers in mind. It has the potential to make their work much simpler. One such tool may be used to gather data and identify web application vulnerabilities. Subdomain enumeration, port scanning, WordPress scanning, same site scripting detection, and vulnerability assessment are among the activities that may be accomplished using the D-TECT program. Cross Site Scripting (XSS), SQL injection, Click Jacking, header misconfigurations, and identification of sensitive files are examples of vulnerabilities that may be discovered with the D-TECT tool. D-TECT is a Python utility that only works with Python 2.7.

Features of the scanner:

- Sub-area Scanning
- Port Scanning
- WordPress Scanning
- WordPress Username Enumeration
- WordPress Backup Grabbing
- Delicate File Detection
- Same-Site Scripting Scanning
- Snap Jacking Detection
- Incredible XSS weakness checking
- SQL Injection weakness checking
- Easy to understand UI

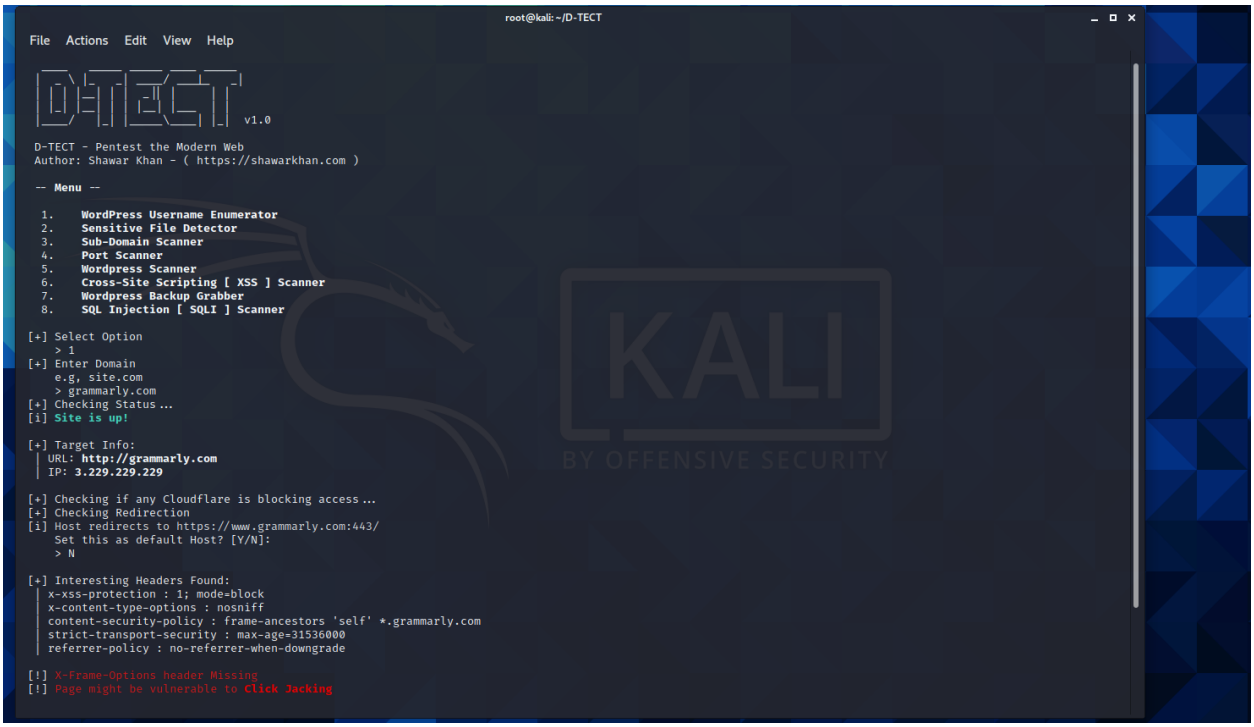
The following command may be used to clone the utility from Github:

git clone https://github.com/shawarkhanethicalhacker/D-TECT-1

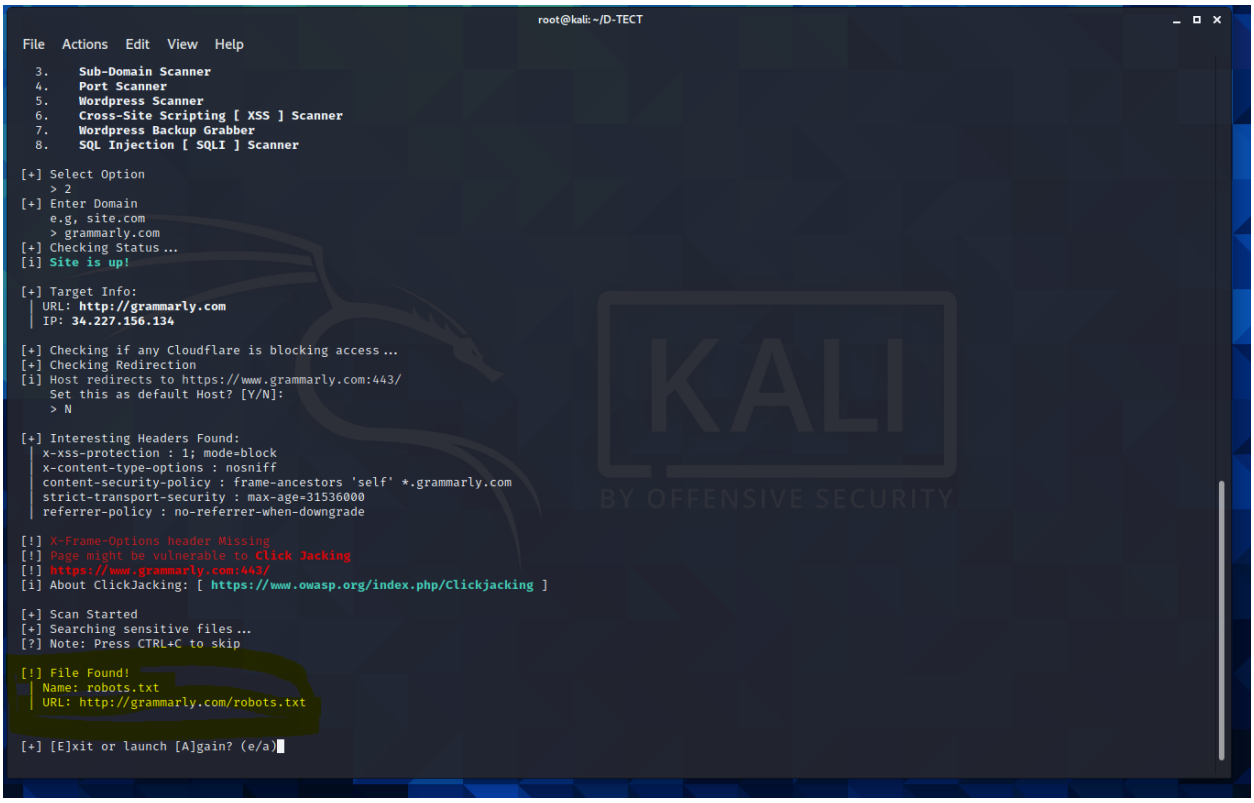
pip install colorama beautifulsoup

python d-tect.py

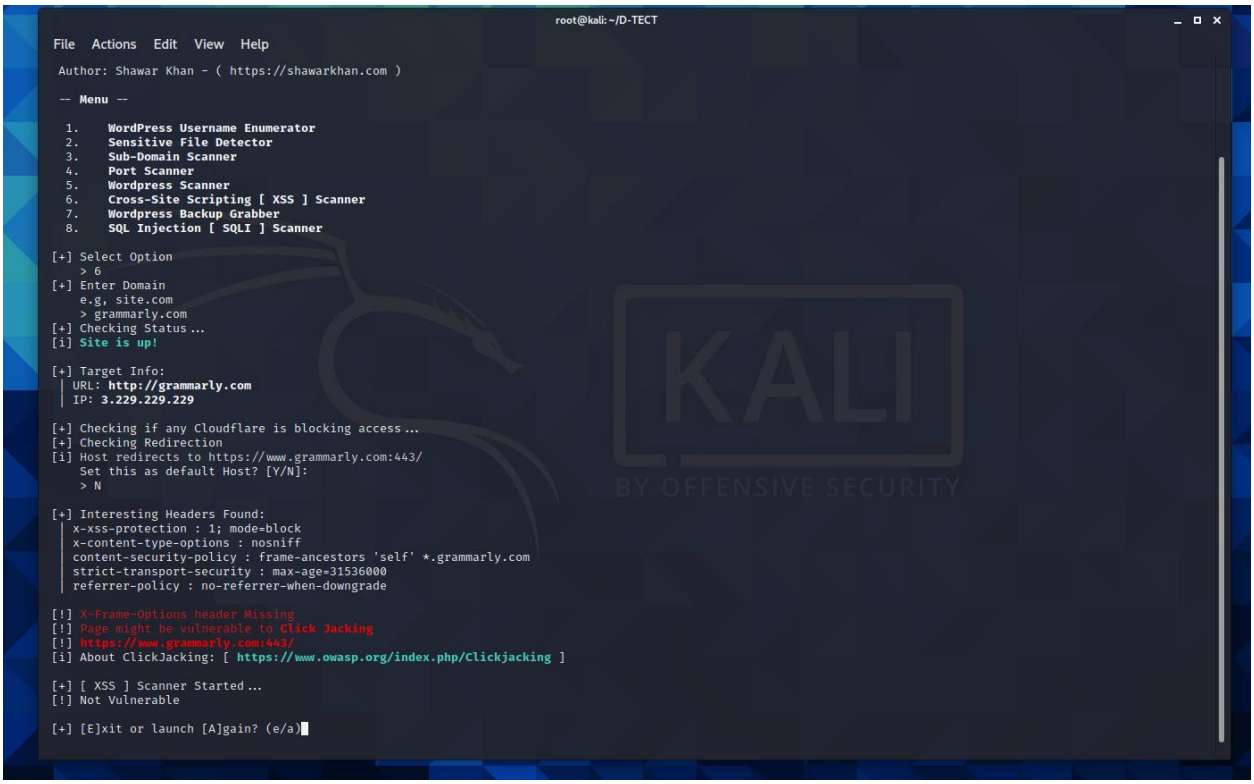
The git clone command is used to get the scanner, and then we run it using the command python./d-tect.py to access the right folder.



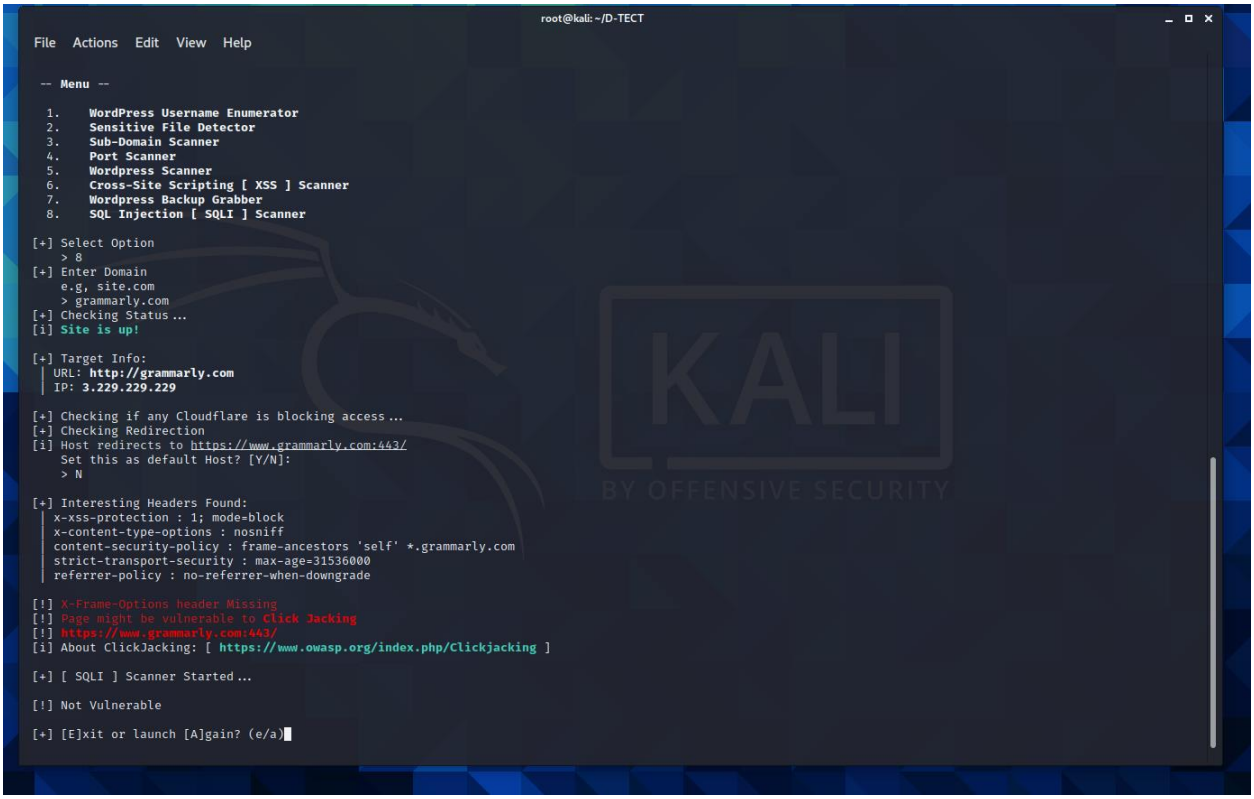
Then we select an option and enter the domain



In this case we can see it shows that the page is vulnerable to Click Jacking.



Now I ran the 8th option which is the SQL injection. Which gave a result of not vulnerable but highlighting the vulnerability of click jacking.



By using the D-TECT scanner we can see that this site is vulnerable for a click jacking attack which is a Medium (P3) in a vulnerable scale.

What is click Jacking?

Clickjacking is an assault that fools a client into clicking a page component which is undetectable or masked as another component. This can make clients accidentally download malware, visit noxious website pages, give qualifications or delicate data, move cash, or buy items on the web.

Commonly, clickjacking is performed by showing an undetectable page or HTML component, inside an iframe, on head of the page the client sees. The client accepts they are tapping the noticeable page, yet truth be told they are clicking an imperceptible component in the extra page translated on head of it. The imperceptible page could be a malevolent page, or an authentic page the client didn't expect to visit – for instance, a page on the client's financial site that approves the exchange of cash.

There are a few varieties of the clickjacking assault, for example,

- Likejacking – a procedure where the Facebook "Like" button is controlled, making clients "like" a page they really didn't expect to like.
- Cursorjacking – a UI reviewing method that changes the cursor for the position the client sees to another position.

Solutions to prevent this attack

Client-side strategies – the most well-known is called Frame Busting. Customer side techniques can be powerful at times, however, are considered not to be a best practice, since they can be handily circumvented.

Server-side strategies – the most widely recognized is X-Frame-Options. Worker side techniques are suggested by security specialists as a powerful method to safeguard against clickjacking.

The X-Frame-Options reaction header is passed as a feature of the HTTP reaction of a website page, showing whether a program ought to be permitted to deliver a page inside a or tag. There are **three qualities** took into consideration the X-Frame-Options header:

1. DENY – doesn't permit any domain to show this page inside a casing.
2. SAMEORIGIN – permits the current page to be shown in a frame on another page, yet just inside the current domain 1.
3. Permit FROM URI – permits the current page to be shown in a casing, yet just in a particular URI – for instance www.gitlab.com/frame-page.

3.11 SSLyze

SSLyze is a Python utility for analyzing a server's SSL settings. It's quick and thorough, and it should aid businesses and testers in identifying SSL server misconfigurations.

The following are some key features:

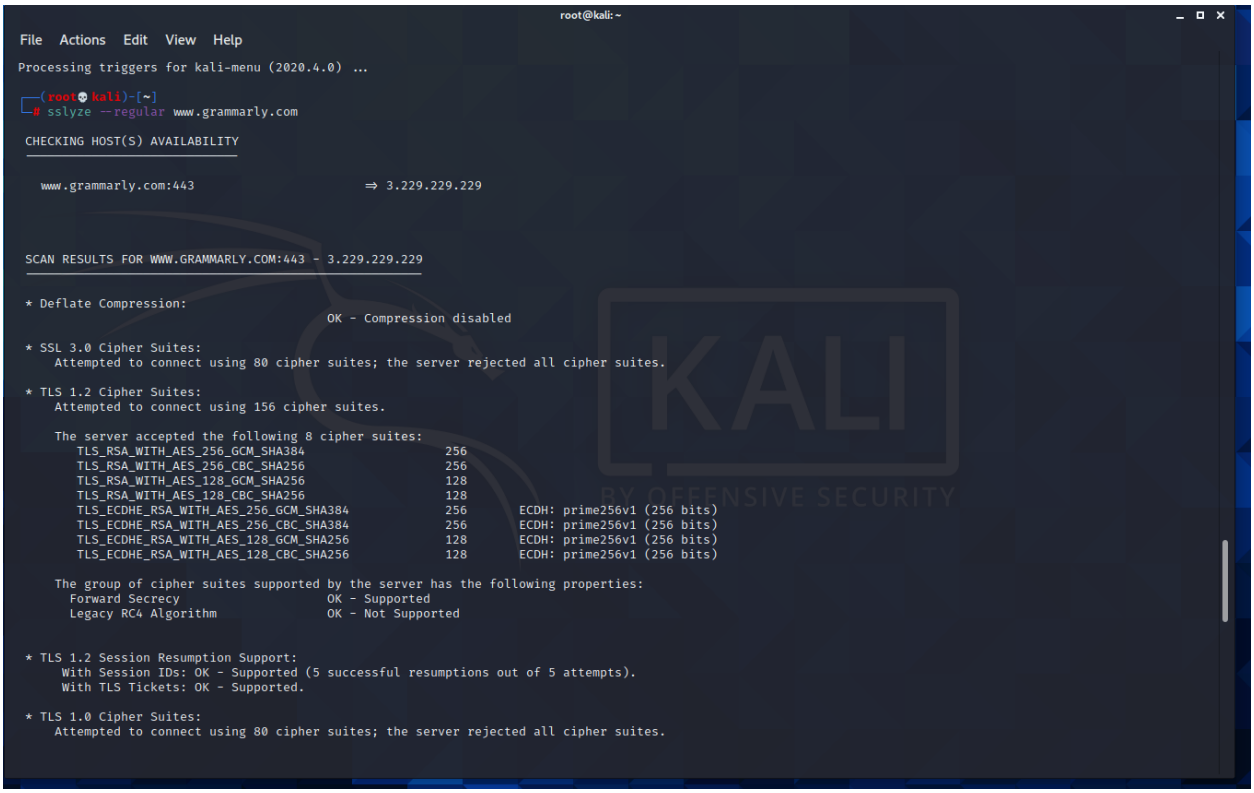
- Scanning that is multi-processed and multi-threaded (fast)
- Compatibility with SSL 2.0/3.0 and TLS 1.0/1.1/1.2
- Support for session resumption and TLS tickets in performance testing
- Weak cipher suites, unsafe renegotiation, CRIME, Heartbleed, and other security flaws

- Through OCSP stapling, server certificates are validated, and revocation checks are performed.
- SMTP, XMPP, LDAP, POP, IMAP, RDP, and FTP handshakes are all supported.
- When scanning servers that use mutual authentication, support for client certificates is provided.
- The XML output will be used to further process the scan findings.

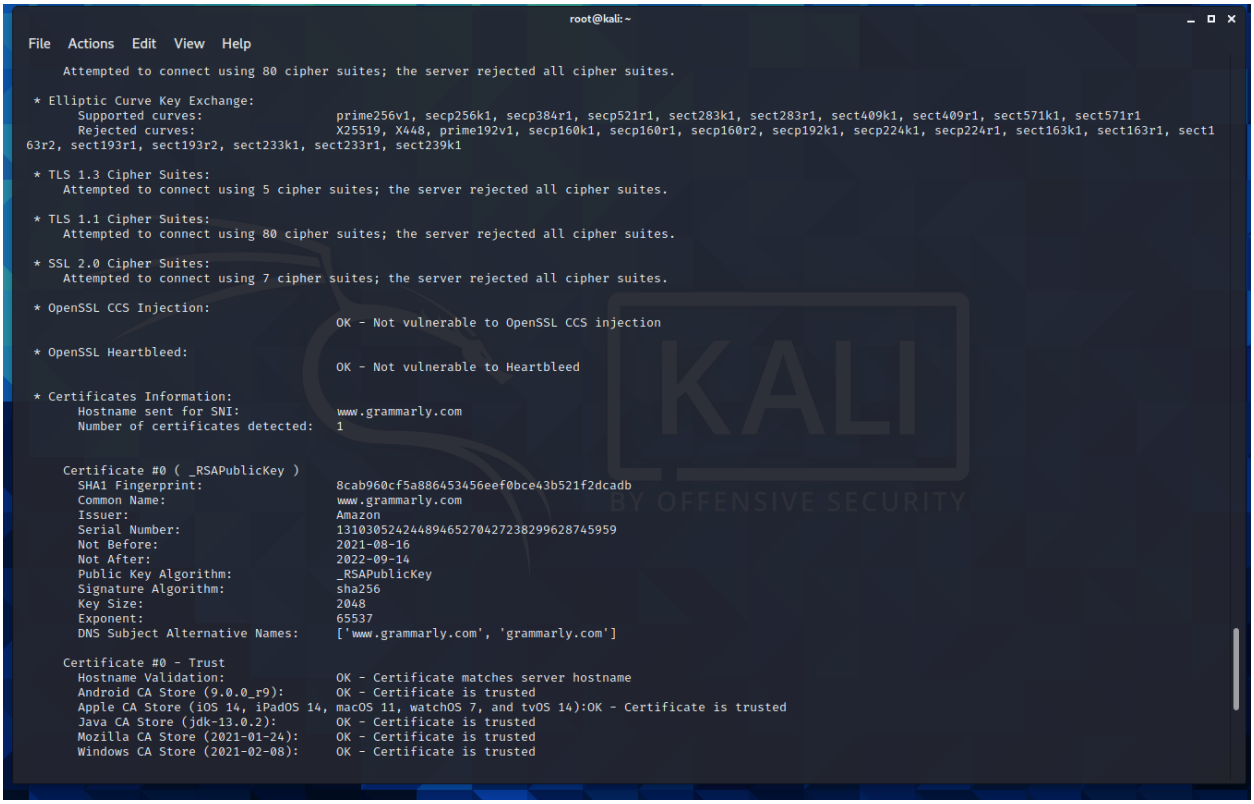
How to install:

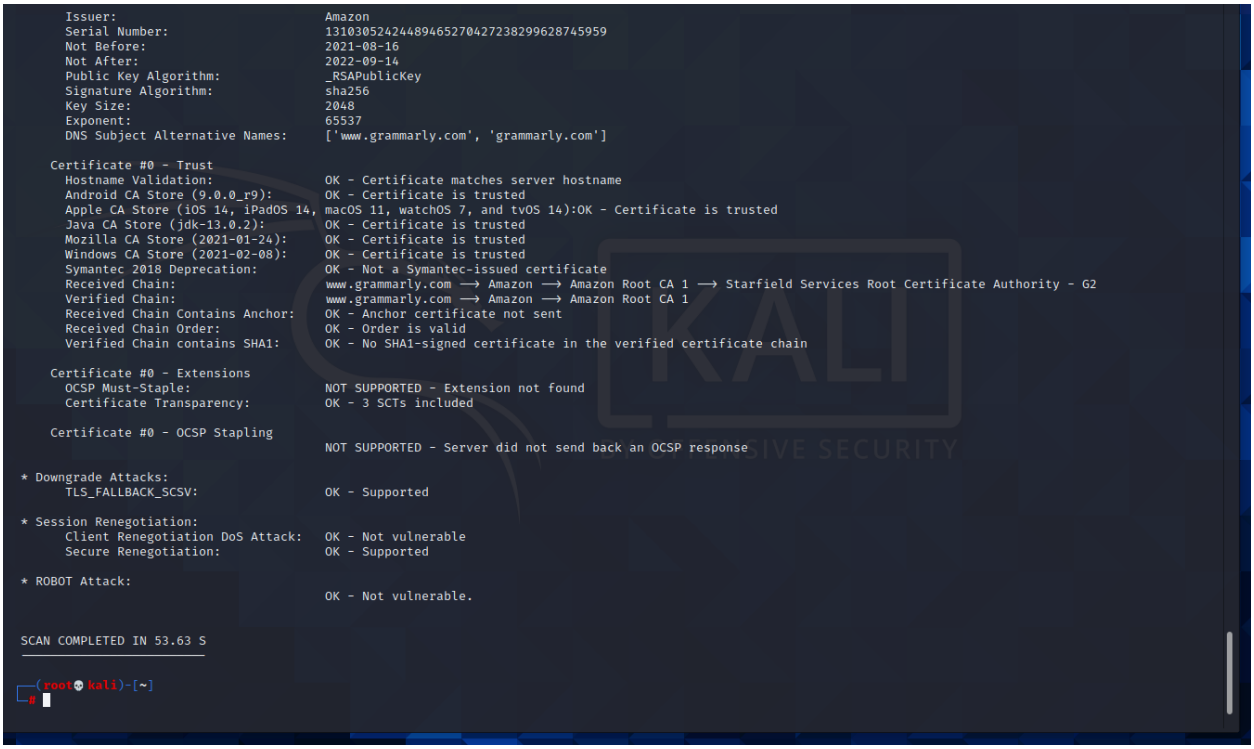
sudo apt install sslyze

Command: sslyze --regular www.grammarly.com



SSL Certificates, Session Renegotiation, Compression, Fingerprints, SAN Domain Entries, and Cipher Suites will all be checked for the Common name.


root@kali: ~
File Actions Edit View Help
Attempted to connect using 80 cipher suites; the server rejected all cipher suites.
* Elliptic Curve Key Exchange:
Supported curves: prime256v1, secp256k1, secp384r1, secp521r1, sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1
Rejected curves: X25519, X448, prime192v1, secp160k1, secp160r1, secp160r2, secp192k1, secp224k1, secp224r1, sect163k1, sect163r1, sect163r2, sect193r1, sect193r2, sect233k1, sect233r1, sect239k1
* TLS 1.3 Cipher Suites:
Attempted to connect using 5 cipher suites; the server rejected all cipher suites.
* TLS 1.1 Cipher Suites:
Attempted to connect using 80 cipher suites; the server rejected all cipher suites.
* SSL 2.0 Cipher Suites:
Attempted to connect using 7 cipher suites; the server rejected all cipher suites.
* OpenSSL CCS Injection:
OK - Not vulnerable to OpenSSL CCS injection
* OpenSSL Heartbleed:
OK - Not vulnerable to Heartbleed
* Certificates Information:
Hostname sent for SNI: www.grammarly.com
Number of certificates detected: 1
Certificate #0 (_RSAPublicKey)
SHA1 Fingerprint: 8cab960cf5a886453456eef0bce43b521f2dcadb
Common Name: www.grammarly.com
Issuer: Amazon
Serial Number: 131030524244894652704272382996287459 59
Not Before: 2021-08-16
Not After: 2022-09-14
Public Key Algorithm: _RSAPublicKey
Signature Algorithm: sha256
Key Size: 2048
Exponent: 65537
DNS Subject Alternative Names: ['www.grammarly.com', 'grammarly.com']
Certificate #0 - Trust
Hostname Validation: OK - Certificate matches server hostname
Android CA Store (9.0.0_r9): OK - Certificate is trusted
Apple CA Store (iOS 14, iPadOS 14, macOS 11, watchOS 7, and tvOS 14):OK - Certificate is trusted
Java CA Store (jdk-13.0.2): OK - Certificate is trusted
Mozilla CA Store (2021-01-24): OK - Certificate is trusted
Windows CA Store (2021-02-08): OK - Certificate is trusted

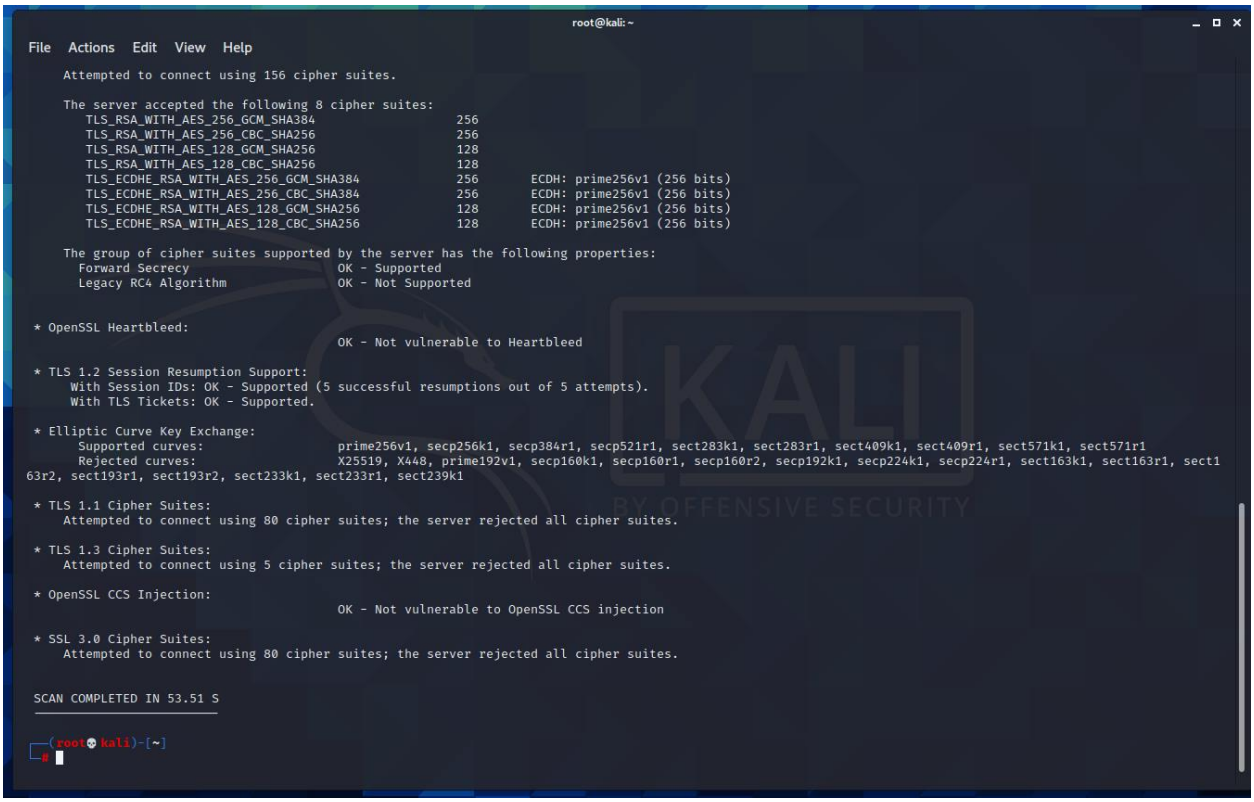

Issuer: Amazon
Serial Number: 131030524244894652704272382996287459 59
Not Before: 2021-08-16
Not After: 2022-09-14
Public Key Algorithm: _RSAPublicKey
Signature Algorithm: sha256
Key Size: 2048
Exponent: 65537
DNS Subject Alternative Names: ['www.grammarly.com', 'grammarly.com']
Certificate #0 - Trust
Hostname Validation: OK - Certificate matches server hostname
Android CA Store (9.0.0_r9): OK - Certificate is trusted
Apple CA Store (iOS 14, iPadOS 14, macOS 11, watchOS 7, and tvOS 14):OK - Certificate is trusted
Java CA Store (jdk-13.0.2): OK - Certificate is trusted
Mozilla CA Store (2021-01-24): OK - Certificate is trusted
Windows CA Store (2021-02-08): OK - Certificate is trusted
Symantec 2018 Deprecation: OK - Not a Symantec-issued certificate
Received Chain: www.grammarly.com ⟶ Amazon ⟶ Amazon Root CA 1 ⟶ Starfield Services Root Certificate Authority - G2
Verified Chain: www.grammarly.com ⟶ Amazon ⟶ Amazon Root CA 1
Received Chain Contains Anchor: OK - Anchor certificate not sent
Received Chain Order: OK - Order is valid
Verified Chain contains SHA1: OK - No SHA1-signed certificate in the verified certificate chain
Certificate #0 - Extensions
OCSP Must-Staple: NOT SUPPORTED - Extension not found
Certificate Transparency: OK - 3 SCTs included
Certificate #0 - OCSP Stapling
NOT SUPPORTED - Server did not send back an OCSP response
* Downgrade Attacks:
TLS_FALLBACK_SCSV: OK - Supported
* Session Renegotiation:
Client Renegotiation DoS Attack: OK - Not vulnerable
Secure Renegotiation: OK - Supported
* ROBOT Attack:
OK - Not vulnerable.
SCAN COMPLETED IN 53.63 S
(root kali)-[~]
#

This tool didn’t display any vulnerabilities. Not vulnerable to Open SSL CCS injection open SSL Heartbleed.

To test the Vulnerability with SSLyze, use the Heartbleed vulnerability using the OpenSSL cryptographic software package.

sslyze –heartbleed www.grammarly.com

SSLyze is a very handy tool for identifying all server misconfigurations.



3.12 XSStrike

XSStrike is a sophisticated cross-site scripting detection tool. It combines the tasks of a payload generator, crawler, and fuzzy engine in one package. XSStrike examines the answer through several parsers and then ensures the payload by context analysis combined with a fuzzy engine, as opposed to injecting payload and validating its functioning, like other tools do. Furthermore, xstrike includes crawling, fuzzy testing, parameter discovery, and WAF detection services. It also

searches for DOM XSS flaws. With millions of websites and webapps on the Internet, the question of whether your website is safe arises. Our websites' security is extremely essential. Cross-site scripting, or XSS, is a website vulnerability that can be exploited. This program makes it simple to identify such flaws.

XSStrike has the following features and uses:

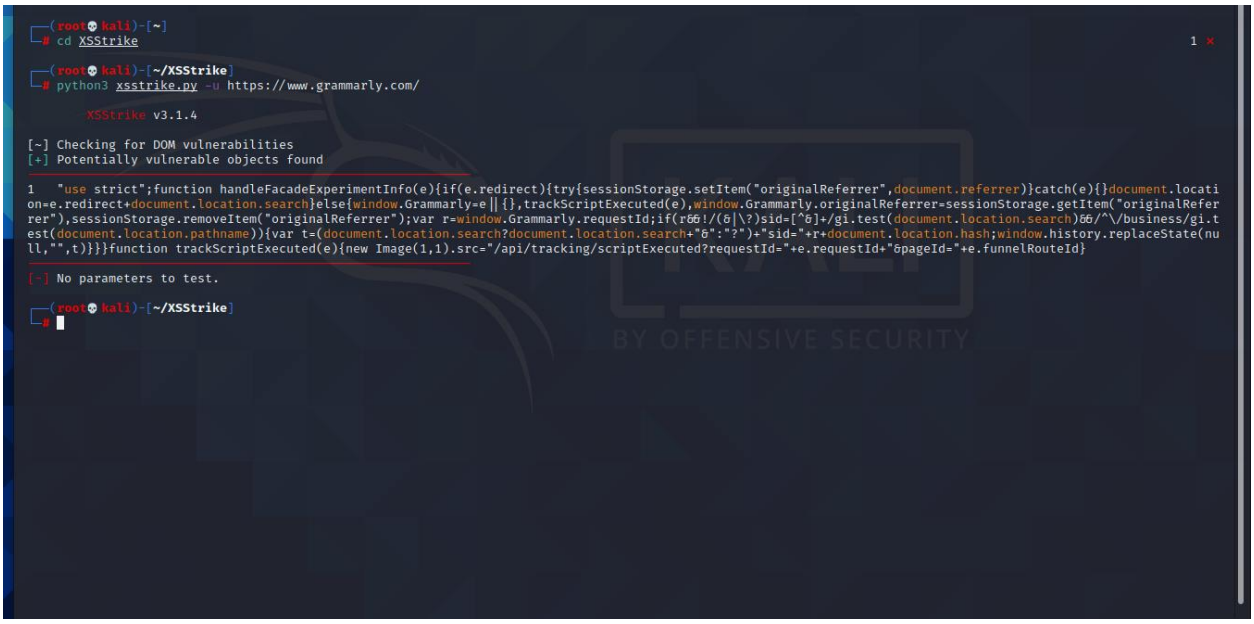
- It's a free and open-source tool for detecting cross-site scripting vulnerabilities. Simply download and run it.
- Install and start scanning webpages using this program, which is accessible on GitHub.
- It features an error handling function. It can quickly manage any errors that arise while scanning.
- It's a completely free and open-source program.
- It is written in the Python programming language.
- It makes scanning websites for xss much easier.
- This gadget functions similarly to a scanner. XSStrike is a tool for multiprocessing support.
- It is a tool that may be customized.
- It accepts all POST and GET requests.

Command to install:

git clone https://github.com/s0md3v/XSStrike.git

Command to run the tool:

python3 xsstrike.py -u https://www.grammarly.com/



This only displays that there are potential vulnerable objects found but not in depth.

3.13 Skipfish

Skipfish is a web application security reconnaissance tool that is in use. It creates an interactive sitemap for the selected site using a recursive crawl and dictionary-based probes. The output of numerous active security checks is then marked on the resultant map. The final report of the tool is meant to be used as a starting point for professional web application security reviews. On GitHub, Skipfish is a free and open-source Automated Penetration Testing tool for security researchers. Skipfish is a tool for obtaining information and assessing the security of websites and web servers. One of the most user-friendly and successful penetration testing tools available is Skipfish.

It includes a number of integrated tools for penetration testing the target system. An active web application security reconnaissance tool is another name for this technology. Using recursive crawls and dictionary-based queries, this program maps the console of the target site. This tool displays all of the domain's active security checks. Finally, this program generates a report that may be used for security audits.

We can use this command to install the Skipfish tool.

git clone https://gitlab.com/kalilinux/packages/skipfish.git

command to scan the website:

skipfish -o 202 https://www.grammarly.com/wordpress

As we can see, the tool has supplied all essential data, such as scan duration, HTTP requests to the host, compression size, HTTP faults, TCP handshakes, TCP faults, External links, and so on. This is also how we may conduct an operation on a specified target.

3.14 SQLmap

sqlmap is an open-source penetration testing tool that automates the detection and exploitation of SQL injection problems as well as database server takeover. It includes a robust detection engine, several specialists features for the ultimate penetration tester, and a wide variety of switches that include database fingerprinting, data retrieval from databases, access to the underlying file system, and out-of-band command execution on the operating system.

Features:

- MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, and HSQLDB database management systems are all fully supported.
- Enumeration of users, password hashes, rights, roles, databases, tables, and columns are supported.

- Password hash formats are automatically recognized, and a dictionary-based attack may be used to crack them.

- Allows the user to dump whole database tables, a range of entries, or select fields.
- The user may optionally select only a subset of the characters from each column's entry to dump.

How to install:

Most penetration testers choose kali Linux, which comes pre-installed with SQLMAP. The command sqlmap may be used to install sqlmap on different Debian-based Linux systems.

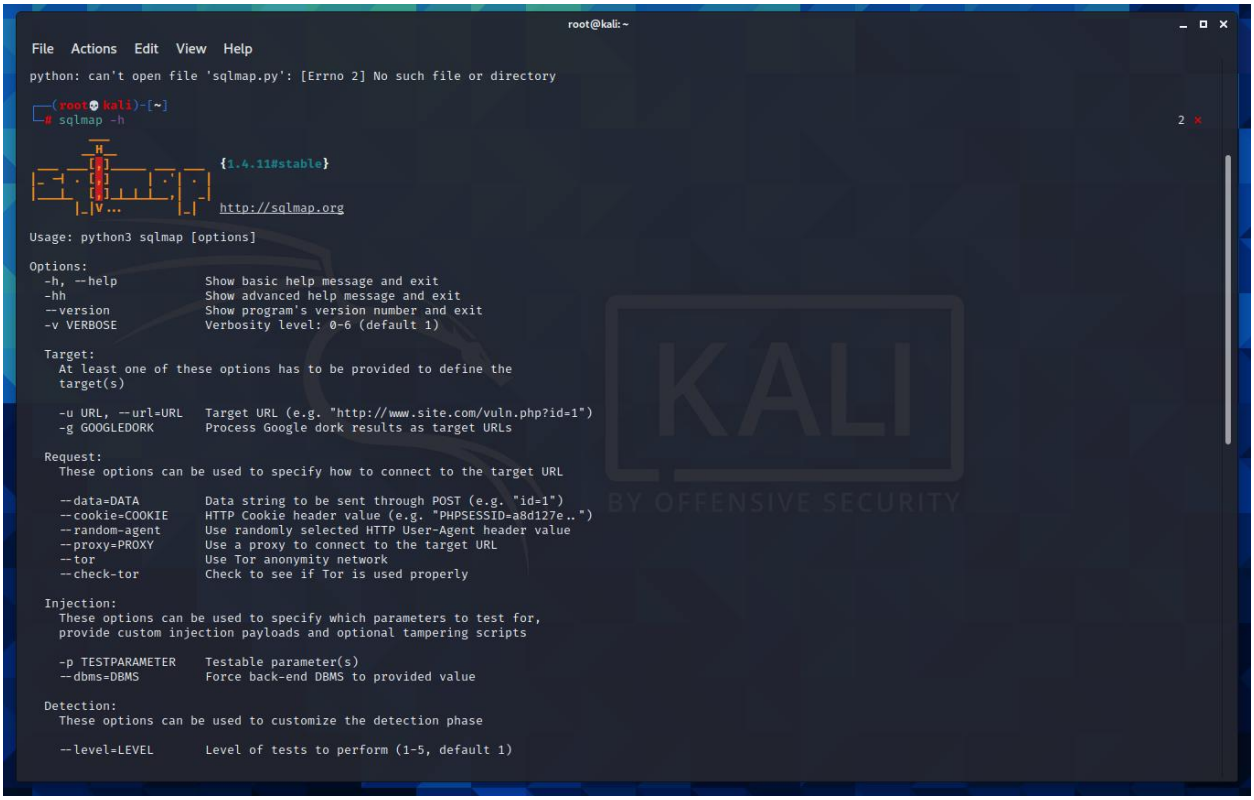
sudo apt install sqlmap

Or else, the best way to get sqlmap is to clone the Git repository:

git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev

In the terminal, type to see the list of arguments that can be supplied.

sqlmap -h



The parameters we'll utilize for simple SQL Injection are depicted in the diagram above. We will additionally utilize the –dbs and –u parameters in addition to these. So, using the -u argument, we must first specify the site url we wish to inspect.

If we want to test the website using proxies, we may use the –tor argument. Normally, we'd want to see if access to a database is possible. As a result, we employ the –dbs option. –dbs displays a list of all databases that are currently accessible.

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 –dbs

We occasionally see the following output, indicating that there are two databases accessible. The application may occasionally notify you that it has detected the database and ask whether you wish to try different database types. You may proceed to type 'Y'. It could also ask whether you wish to check for vulnerabilities in additional settings. There were no accessible databases to be discovered from my domain. So, I came to a conclusion that the site is protected towards SQL injection attack.

What is SQL Injection?

An attacker uses SQL Injection to manipulate a web application's database by executing malicious SQL queries. A user can acquire access to information contained in databases by using the proper set of queries. SQLMAP determines if a GET parameter is susceptible to SQL Injection.

Out of all the 188 subdomains that I found through using sublist3r tool, I selected 5 subdomains from the main domain Grammarly.com. They are as follows,

- nexus.grammarly.com – 10.0.30.134
- zoomarly.grammarly.com – 35.168.94.32
- mercury.grammarly.com – 54.243.38.36
- knots.grammarly.com – 44.196.169.175
- status.grammarly.com - 13.236.8.151
- support.grammarly.com - 104.16.53.111
- calendar.grammarly.com - 142.251.10.121

4. Conclusion

A thorough cyber security audit necessitates the evaluation of security procedures, security measures, and potential hazards connected with all information technology properties. While certain elements of the audit must be performed manually, technologies can help to automate the web risk assessment process. It evaluates the security of your online properties by performing vulnerability scans to discover known web vulnerabilities. It also assists you in identifying additional issues with information security, such as access control vulnerabilities, misconfigurations, or a lack of specific security procedures.

In my online security audit, I picked grammarly.com from the Bugcrowd bug bounty program as my main domain and scanned it with numerous automated tools such as Nmap, Nikto, Nessus, Amass, DotDotpwn, Netsparker, wafw00f, Burp Suite, and Sublist3r. I After examining all of this information, I found one critical vulnerability which has to be prevented to their website safety (from Netsparker) and two other medium vulnerabilities and other low risk vulnerabilities. From all of these I got to the conclusion that the domain grammarly.com has a solid cyber-attack protection system but need more safety controls to avoid some vulnerabilities to avoid dangerous attacks like Dos.

5. References

- 2021. [online] Available at: <https://www.kali.org/tools/sslyze/> [Accessed 4 November 2021].
- Fatalerrors.org. 2021. *Installation and use of XSStrike tool*. [online] Available at: <https://www.fatalerrors.org/a/installation-and-use-of-xsstrike-tool.html> [Accessed 4 November 2021].
- GBHackers On Security. 2021. *SSLyze - Fast and Complete SSL Scanner to find Misconfiguration*. [online] Available at: <https://gbhackers.com/fast-and-complete-ssl-scanner-to-find-mis-configurations-affecting-tlsssl-severs-a-detailed-analysis/> [Accessed 4 November 2021].
- Bugcrowd. 2021. *#1 Crowdsourced Cybersecurity Platform | Bugcrowd*. [online] Available at: <https://www.bugcrowd.com/> [Accessed 4 November 2021].
- Infosec Resources. 2021. *Top 19 Kali Linux tools for vulnerability assessments - Infosec Resources*. [online] Available at: <https://resources.infosecinstitute.com/topic/top-19-kali-linux-tools-for-vulnerability-assessments/> [Accessed 4 November 2021].