Sri Lanka Institute of Information Technology

Web Security Audit

IE2062 – Web Security

Domain

Verizon media – yahoo.com

Student Registration Number	Student Name
[redacted]	**Ekanayake E.M.I.R**

Table of Contents

Abstract

A web security audit is a popular topic these days in the world. These days, web applications, online platforms and also work through the internet are rapidly increasing. Most of the people who are in the IT industry engage with these activities. Because nowadays, people are considering their security and privacy. Therefore, most of the web applications are consider their security.

According to the web security module assigned to students who are studying this module, to perform a web security audit as a module assignment. Then create documentation for it. In this report describe how I perform the web security audit based on yahoo.com.

At the beginning of the report, give a brief introduction to the web security audit. Then discussed how to perform a web security audit and what resources have to get information for the audit. After that part, describe the domain that I selected to perform the web security audit. Then consider the information gathering phase in the audit. in this part discussed what tools are have for information gathering and facts about the domain that I selected. The next part of the report about a web audit considers about vulnerability scan which is a special phase in the audit. In that part discussed what tools can use to do a vulnerability scan and the result of a vulnerability scan of my audit. The latter part of the report contains a vulnerability analysis of I selected domain. Finally, the conclusion of the web security audit is including.

Introduction

Nowadays, the uses of the web application are rapidly increasing. Most of the people in this era doing their day to day life works and also their jobs are doing through these web application. While rapidly increasing these web applications at the same time web application security also take a major part in the world. Because users' privacy can be accessed through this web application, which can lead to anonymous illegal activity. So web application security is a very important topic as well as a issue that needs to be addressed around the world. If we not consider about this web security, hackers can access these web applications for some malicious activities and also they can do any illegal things in the world using web applications. We have to do various things to avoid these types of activities. Web auditing is one of the most important and most needed solutions for this matter.

What is a Web Audit?

A website security audit is an audit that looks at the infrastructure, core, extensions, and themes for vulnerabilities and shortcomings of the selected web application. In general, through this web security audit review the codes that include in the web application. So through this web audit can identify vulnerabilities in the selected web site. While a security audit purpose is to evaluate and pinpoint the vulnerable area. If it is found that there has any vulnerability in the website through this audit, the pentester can emulate hackers and attack situations and then exploit this vulnerability which is found through the audit. So it helps to find solutions and fix these vulnerabilities. This is the main advantage of doing a web security audit. Web security has several types,

- Automated security audit
- Manual security audit
- Professional security audit

Also, vulnerability scanners are the most used tools to test web security. [1]

How to start a web audit …

First, we want to select the domain to launch this web security audit. Here we can't access all domains in the world to doing this web security because they do not give any permission to scan their website. Only some of the domains are permitted to do this security audit. So first we want to select one of the domains from these permitted domains.

We have some platform to do these bug bounty programs. Through these platforms, we can select one of the domain and start our web security auditing. Listed below some of the platforms which we can use to select the domain.

- Hackerone
- Bug crowd
- Google

Also, some web security related organizations like,

- OWSAP
- PCI checks
- SANS

are given to the checklist to do a proper web security audit. When we are following one of these guidelines and we can do a proper web application security audit. According to the OWSAP given 10 main steps to do an audit. If we follow these guidelines, we can do a good web security audit.

OWASP

OWASP is the Open Web Application Security Project which found on 2001. It's a well-known community among information technology for supply articles, tools, technologies, and also methodologies of web application security. It provides a checklist for continue to web security audit properly. [2]

OWASP Checklist

1. Information Gathering
2. Configuration and deploy management testing
3. Identity management testing
4. Authentication testing
5. Authorization testing
6. Session management testing
7. Data validating testing
8. Error handling
9. Cryptography
10. Business logic testing
11. Client-side testing

OWASP Top 10

• Injection

• Broken Authentication

• Sensitive Data Exposure

• XML External Entities (XXE)

• Broken Access control

• Security misconfigurations

• Cross-Site Scripting (XSS)

• Insecure Deserialization

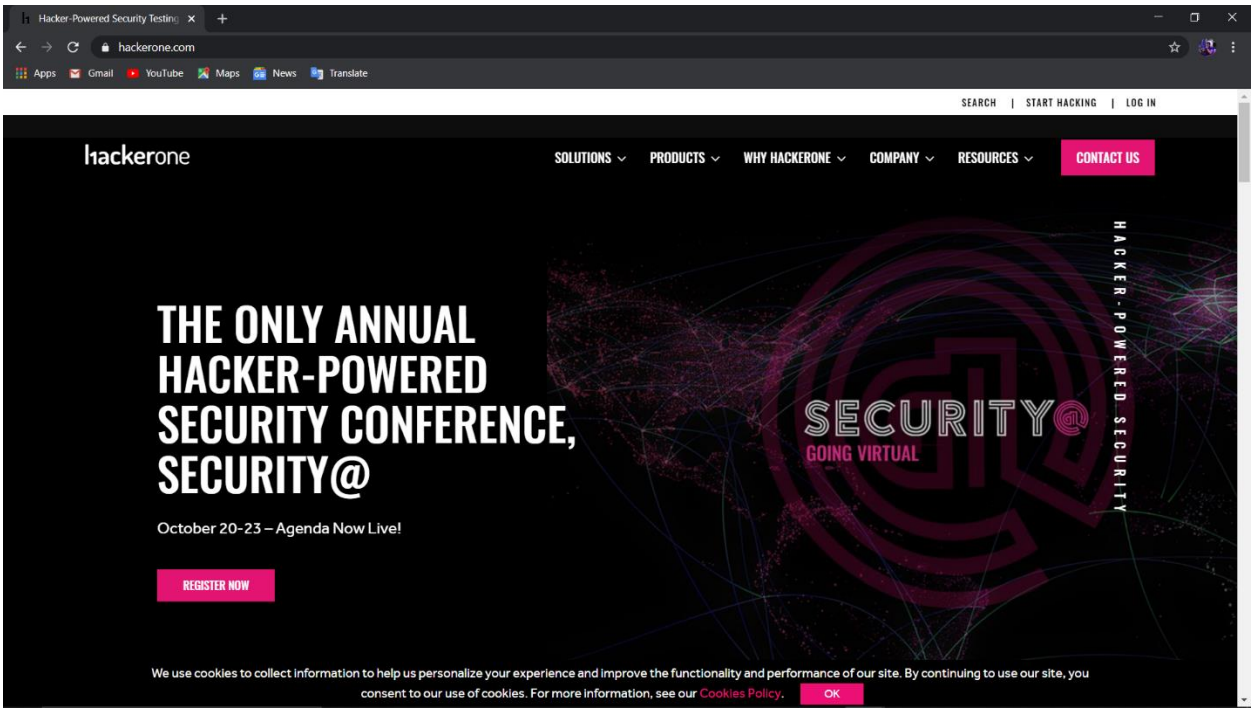
• Using Components with known vulnerabilities

• Insufficient logging and monitoring [3]

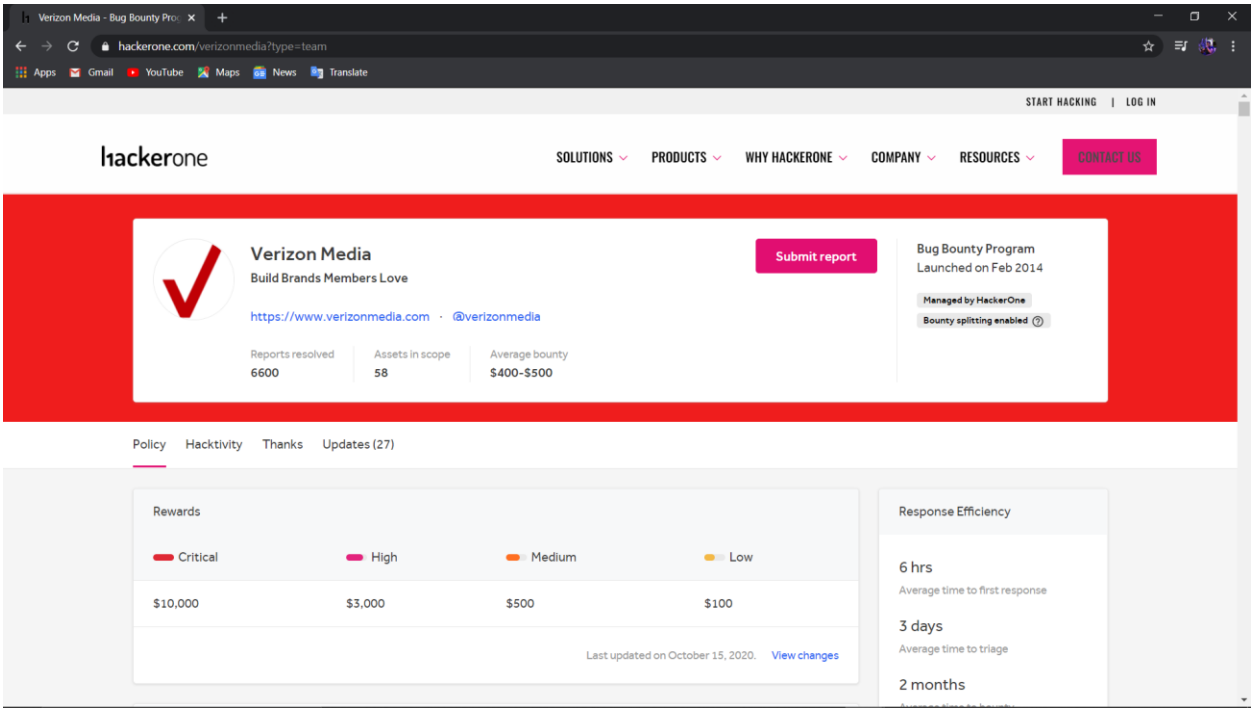
I decided to follow some of the OWASP testing guidelines and methodology for my web security auditing.

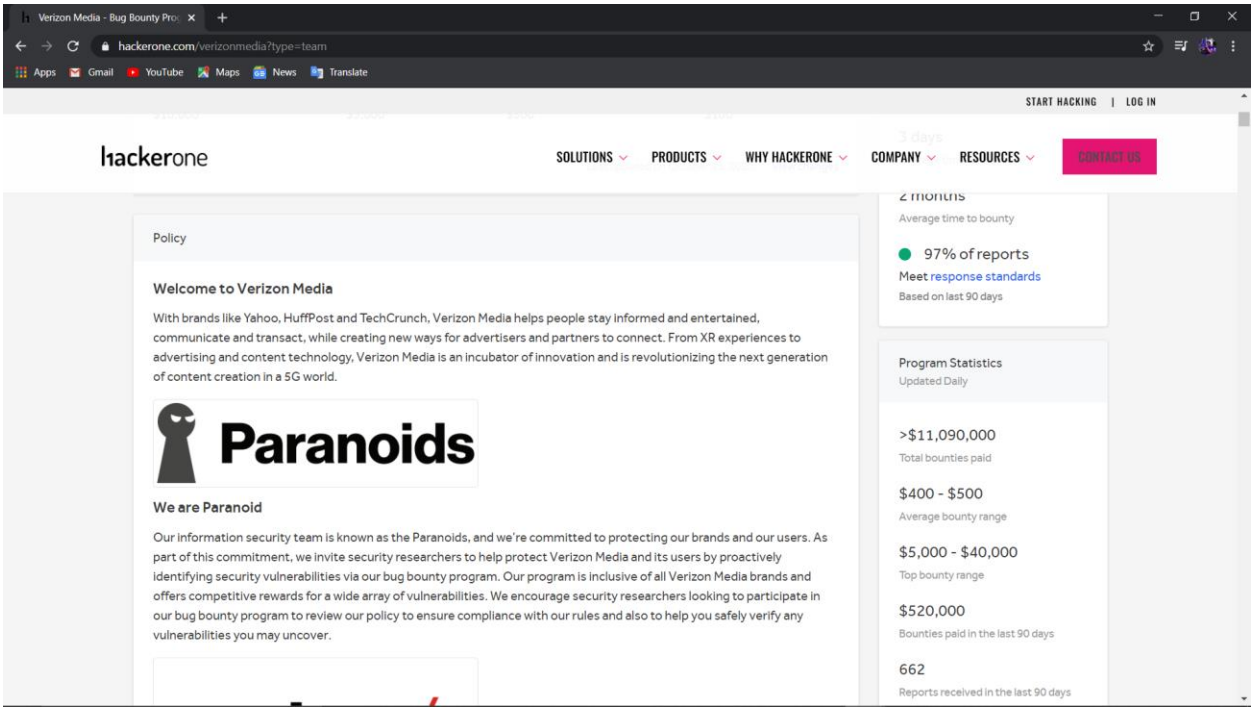
Domain selection

We have so many platforms to select for the domain for this web security audit. After going through some of these platforms and I was selected to HackerOne for selected to a domain for doing my web security audit. Hackerone is good vulnerability coordination and bug bounty platform. It connects with cybersecurity researchers. In addition, HackerOne also paid for these bug bounty programs.



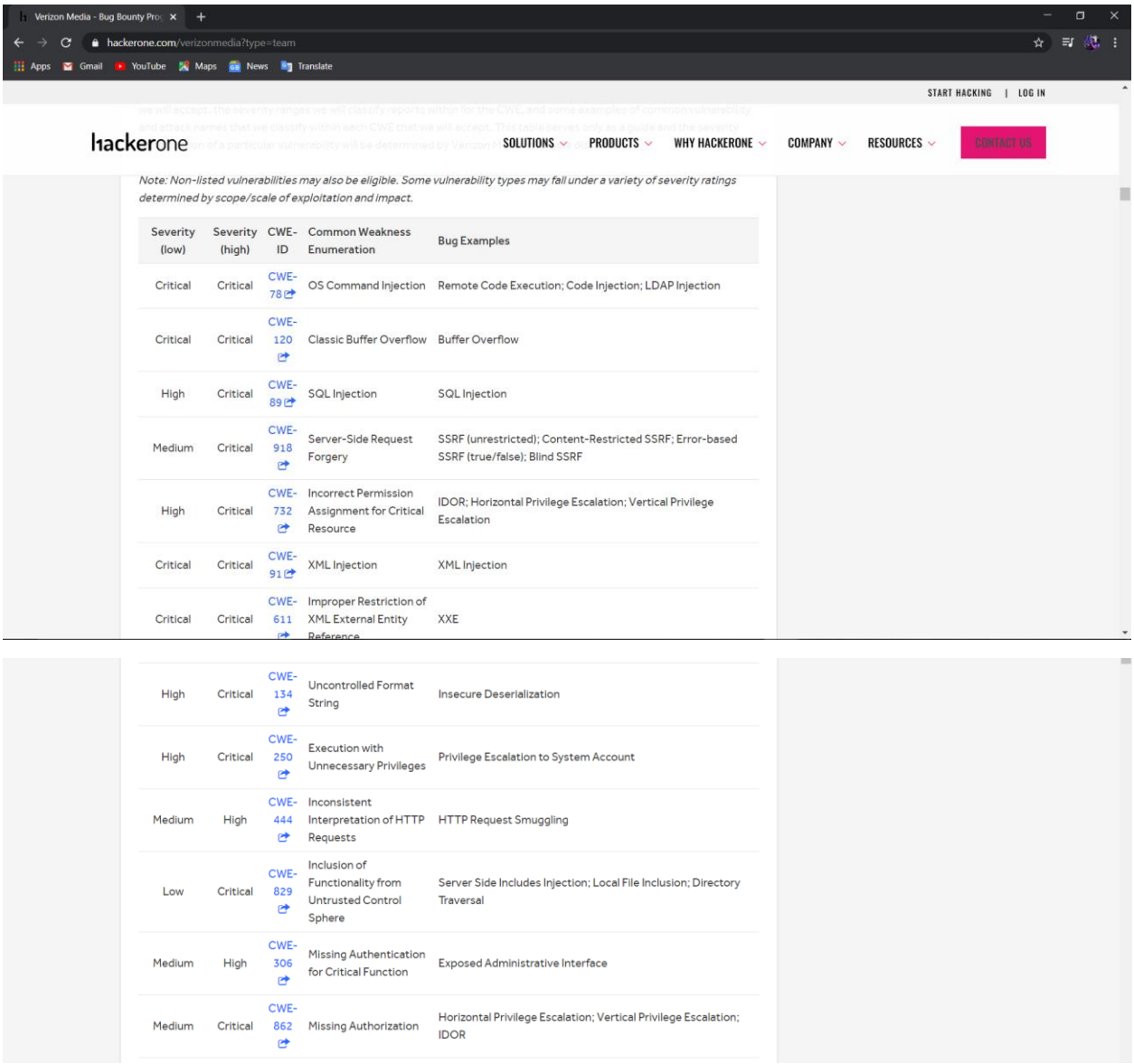
Then I searched permitted domains for doing my bug bounty program. This platform has so many permitted domains for doing security audits. Then I selected some of the domains from this permitted domains list and I did some consideration of the facts about I selected domains. In the Hackerone platform are given some description, some rules for want to consider when doing the bug bounty program and some important facts of the domain. Then I consider the facts and rules of the domains and I selected to https://www.verizonmedia.com/ domain to doing my web security audit.





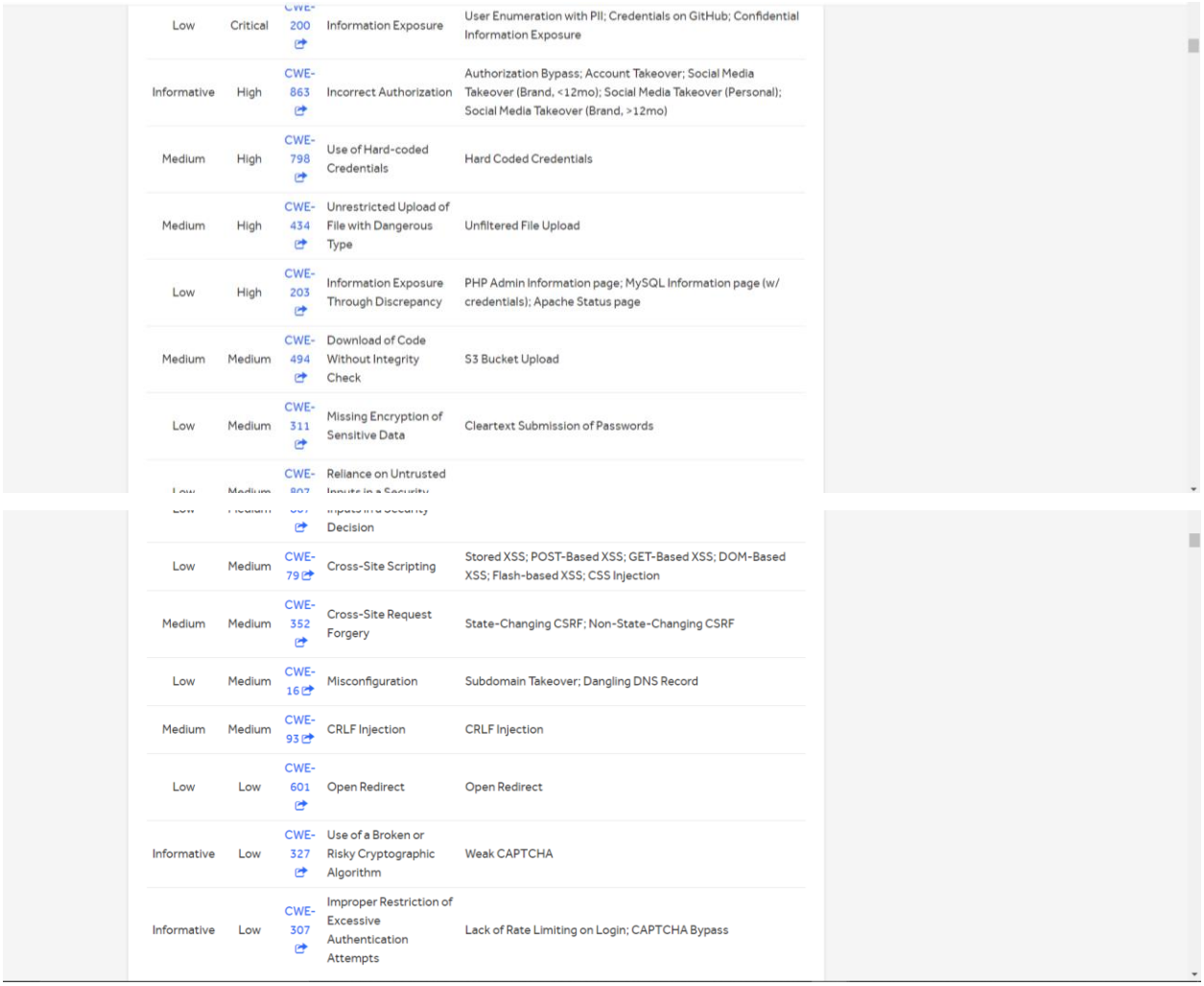
Then I again going through the rules and I understood what can we do in the audit and also what can not be doing in the audit. Also in the platform is given more details about what are the

responsibilities, Rewards, rules of engagement when we are doing adult for this domain. In addition, supply what is the valued vulnerabilities in this domain.



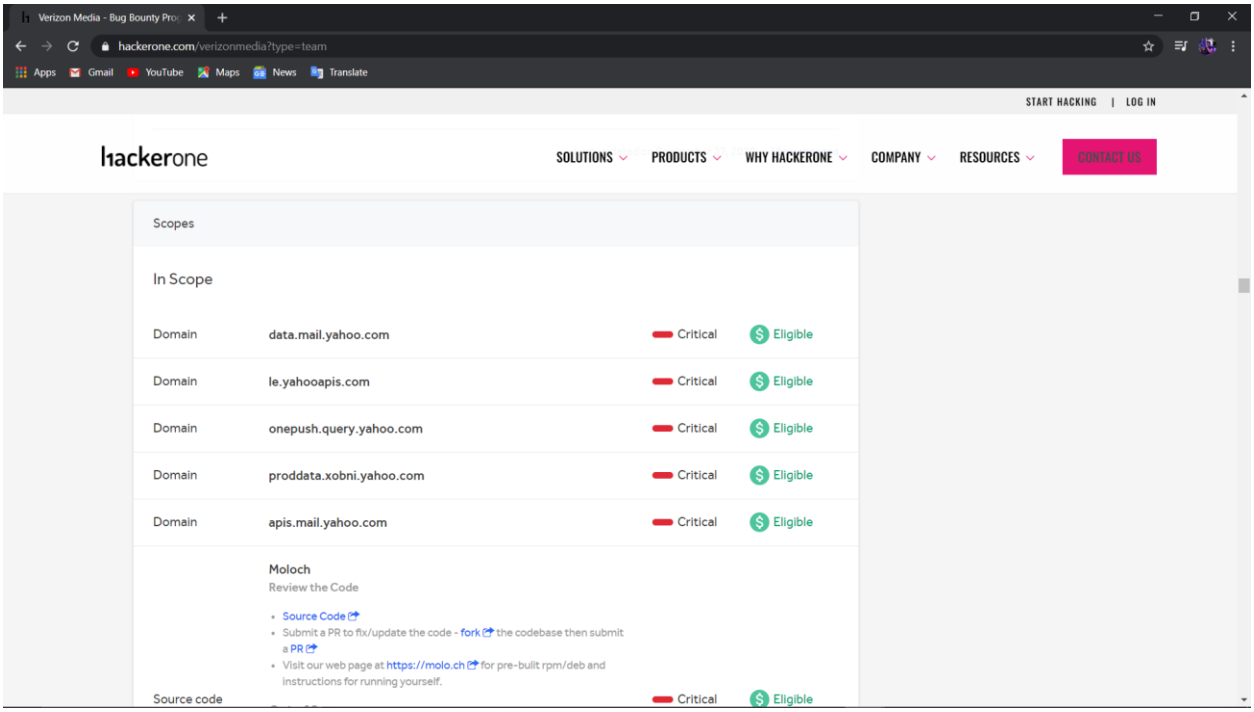
Note: Non-listed vulnerabilities may also be eligible. Some vulnerability types may fall under a variety of severity ratings determined by scope/scale of exploitation and impact.

Severity (low)	Severity (high)	CWE-ID	Common Weakness Enumeration	Bug Examples
Critical	Critical	CWE-78	OS Command Injection	Remote Code Execution; Code Injection; LDAP Injection
Critical	Critical	CWE-120	Classic Buffer Overflow	Buffer Overflow
High	Critical	CWE-89	SQL Injection	SQL Injection
Medium	Critical	CWE-918	Server-Side Request Forgery	SSRF (unrestricted); Content-Restricted SSRF; Error-based SSRF (true/false); Blind SSRF
High	Critical	CWE-732	Incorrect Permission Assignment for Critical Resource	IDOR; Horizontal Privilege Escalation; Vertical Privilege Escalation
Critical	Critical	CWE-91	XML Injection	XML Injection
Critical	Critical	CWE-611	Improper Restriction of XML External Entity Reference	XXE
High	Critical	CWE-134	Uncontrolled Format String	Insecure Deserialization
High	Critical	CWE-250	Execution with Unnecessary Privileges	Privilege Escalation to System Account
Medium	High	CWE-444	Inconsistent Interpretation of HTTP Requests	HTTP Request Smuggling
Low	Critical	CWE-829	Inclusion of Functionality from Untrusted Control Sphere	Server Side Includes Injection; Local File Inclusion; Directory Traversal
Medium	High	CWE-306	Missing Authentication for Critical Function	Exposed Administrative Interface
Medium	Critical	CWE-862	Missing Authorization	Horizontal Privilege Escalation; Vertical Privilege Escalation; IDOR



Low	Critical	CWE-200	Information Exposure	User Enumeration with PII; Credentials on GitHub; Confidential Information Exposure
Informative	High	CWE-863	Incorrect Authorization	Authorization Bypass; Account Takeover; Social Media Takeover (Brand, <12mo); Social Media Takeover (Personal); Social Media Takeover (Brand, >12mo)
Medium	High	CWE-798	Use of Hard-coded Credentials	Hard Coded Credentials
Medium	High	CWE-434	Unrestricted Upload of File with Dangerous Type	Unfiltered File Upload
Low	High	CWE-203	Information Exposure Through Discrepancy	PHP Admin Information page; MySQL Information page (w/ credentials); Apache Status page
Medium	Medium	CWE-494	Download of Code Without Integrity Check	S3 Bucket Upload
Low	Medium	CWE-311	Missing Encryption of Sensitive Data	Cleartext Submission of Passwords
Low	Medium	CWE-807	Reliance on Untrusted Inputs in a Security Decision	
Low	Medium	CWE-79	Cross-Site Scripting	Stored XSS; POST-Based XSS; GET-Based XSS; DOM-Based XSS; Flash-based XSS; CSS Injection
Medium	Medium	CWE-352	Cross-Site Request Forgery	State-Changing CSRF; Non-State-Changing CSRF
Low	Medium	CWE-16	Misconfiguration	Subdomain Takeover; Dangling DNS Record
Medium	Medium	CWE-93	CRLF Injection	CRLF Injection
Low	Low	CWE-601	Open Redirect	Open Redirect
Informative	Low	CWE-327	Use of a Broken or Risky Cryptographic Algorithm	Weak CAPTCHA
Informative	Low	CWE-307	Improper Restriction of Excessive Authentication Attempts	Lack of Rate Limiting on Login; CAPTCHA Bypass

And also HackerOne is supplied to scope to what subdomains can we audit. This is very important facts because through this scope we can know our limitations. Sometimes when we trying to access the subdomains which are out of scope, we have to chance banned from the domain. Hence this scope is helpful to us.



After finding and referring to this information and I started to information gathering part according to the OWASP checklist.

Information Gathering

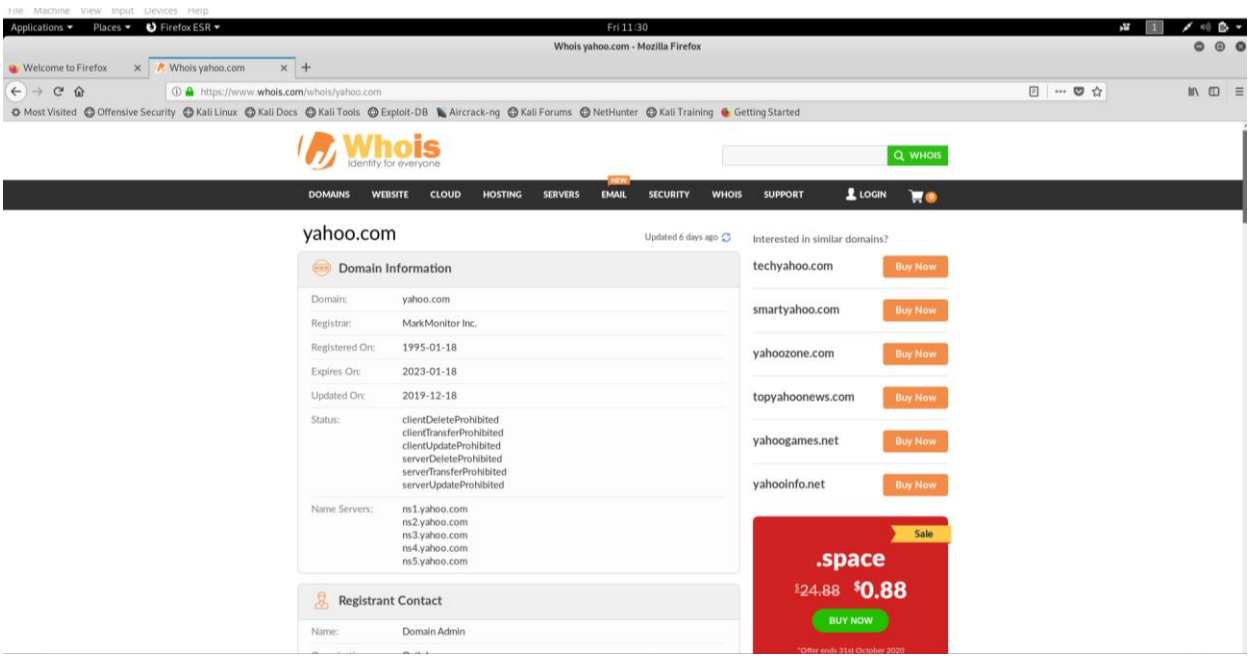
Most of the information about I selected domain is given in the platform. By that, we can get a clear idea about the domain. But when we are doing a web security audit, we want more details. Hence we have to do the information gathering part.

I used some tools for done information gathering.

- ✓ Sublist3r
- ✓ Crt.sh
- ✓ Nmap

Information of Domain name

I used the **"Whois"** feature to get more information about I selected domain. It includes server names, status, registered date, update date, and more details.

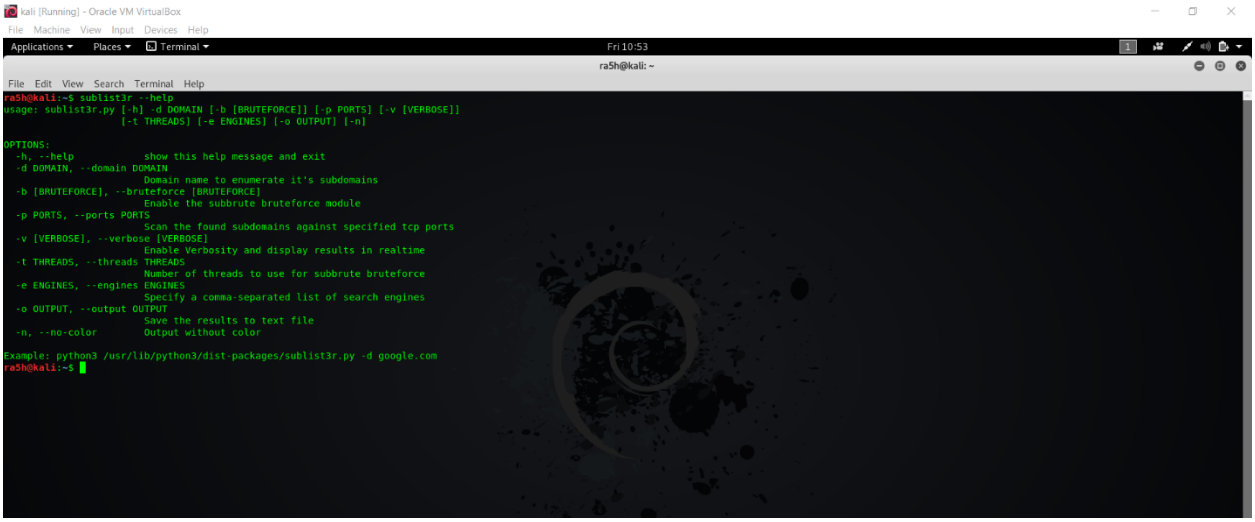


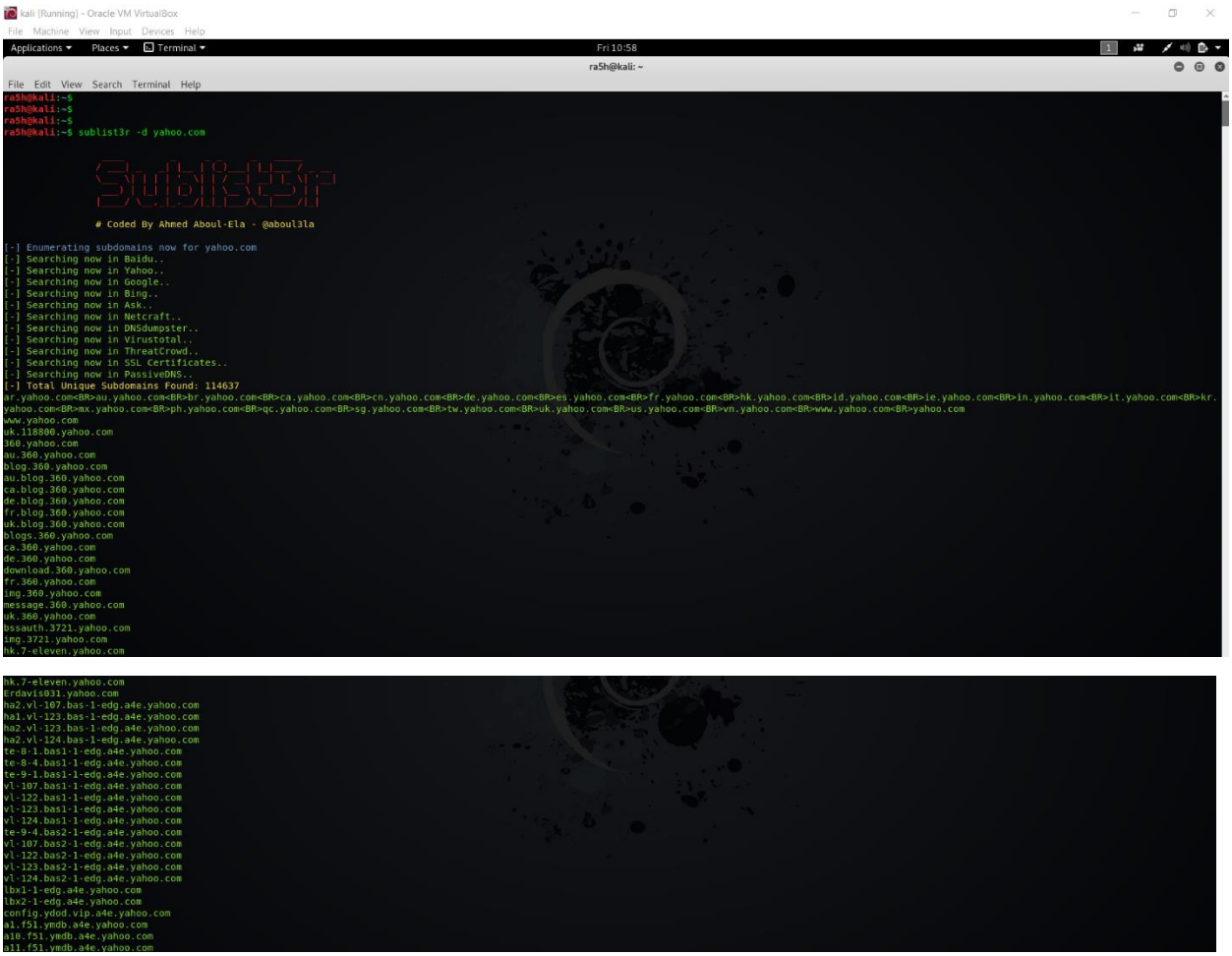

kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Firefox ESR
Fri 11:30
Whois yahoo.com - Mozilla Firefox
Welcome to Firefox
Whois yahoo.com
https://www.whois.com/whois/yahoo.com
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started
Email: domain-admin@oath.com
Raw Whois Data
Domain Name: yahoo.com
Registry Domain ID: 3643624_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2020-07-30T11:35:29-0700
Creation Date: 1995-01-18T00:00:00-0800
Registrar Registration Expiration Date: 2023-01-18T21:00:00-0800
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdatePrc
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransfe
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeletePrc
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdatePrc
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransfe
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeletePrc
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Oath Inc.
Registrant Street: 22000 AOL Way
Registrant City: Dulles
Registrant State/Province: VA
Registrant Postal Code: 20166
Registrant Country: US
Registrant Phone: +1.4083493300
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domain-admin@oath.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Oath Inc.
Admin Street: 22000 AOL Way
Admin City: Dulles
Admin State/Province: VA
Admin Postal Code: 20166
Admin Country: US
Admin Phone: +1.4083493300
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domain-admin@oath.com
Registry Tech ID:
Tech Name: Domain Admin
Tech Organization: Oath Inc.
Tech Street: 22000 AOL Way
Tech City: Dulles
Tech State/Province: VA
Tech Postal Code: 20166
Tech Country: US
Tech Phone: +1.4083493300
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domain-admin@oath.com
Name Server: ns4.yahoo.com
Name Server: ns1.yahoo.com
Name Server: ns2.yahoo.com
Name Server: ns5.yahoo.com
Name Server: ns3.yahoo.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-10-09T04:58:35-0700 <<<
For more information on WHOIS status codes, please visit:
https://www.icann.org/resources/pages/epp-status-codes
If you wish to contact this domain's Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).
Web-based WHOIS:
https://domains.markmonitor.com/whois
If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.
The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.
By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
(1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
(2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).
MarkMonitor reserves the right to modify these terms at any time.
By submitting this query, you agree to abide by this policy.
MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.
Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220

Sublist3r

Sublist3r is a tool for gather subdomains in the domains. When using this tool I can found subdomains in the domain which I selected. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster, and ReverseDNS. [4]

I am also used this sublist3r for my information gathering part. Then I able to find the subdomains of yahoo.com that I selected domain.

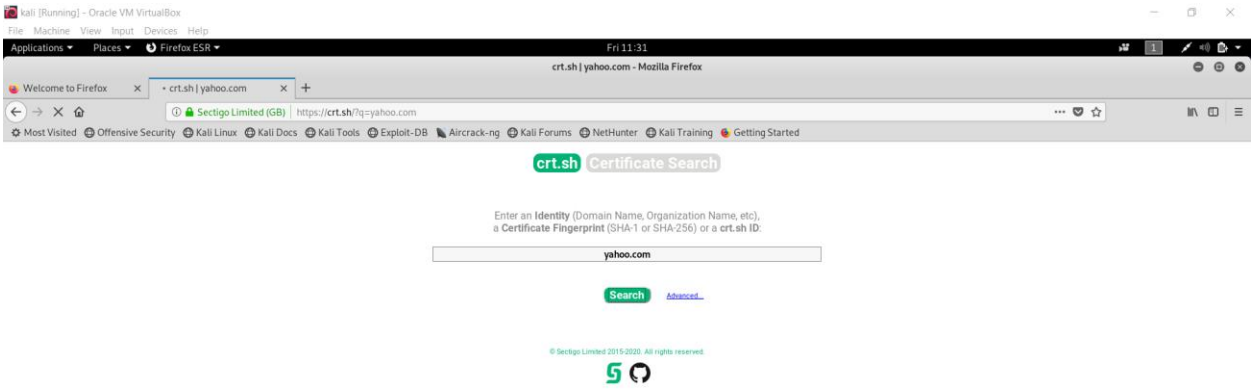


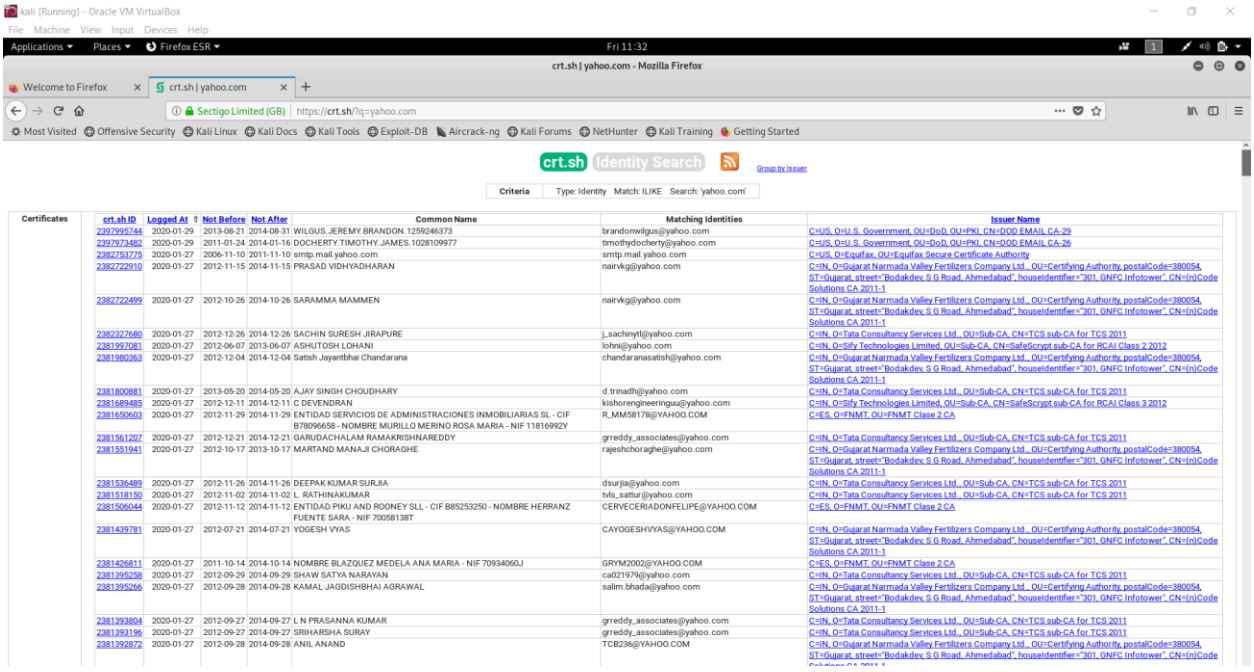


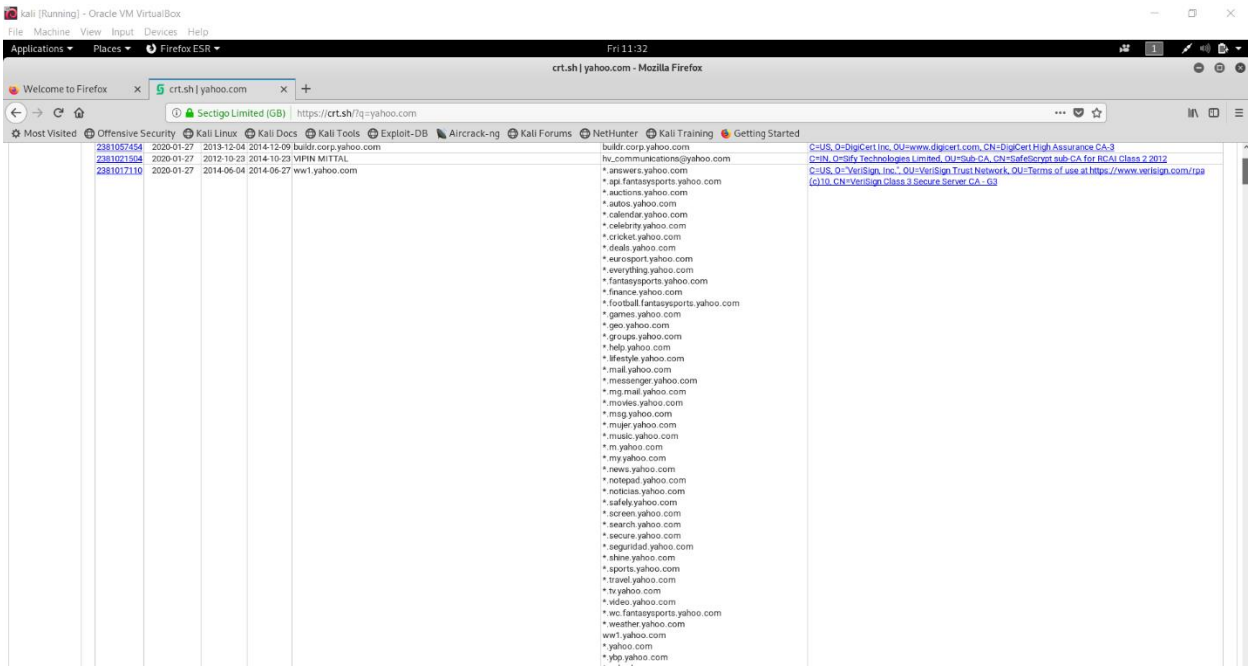
I used this sublist3r tool to find 114637 subdomains on yahoo.com, the domain I selected.

Crt.sh

Furthermore, I used "**Crt.sh"** to find subdomains for doing my web security auditing. **Crt.sh** is also like a sublist3r tool that also can find subdomains of the selected domain.







After these several stages, I selected some subdomains because this domain has so many subdomains and we can not do to scan all subdomains in that domain. Then I do vulnerability scans for I selected subdomains in the domain.

Then I shifted to another stage of the information-gathering part. Before doing a vulnerability scan I did a Nmap scan.

Several subdomains I selected,

- ✓ Mail.yahoo.com
- ✓ Onepush.query.yahoo.com
- ✓ Proddata.xobni.yahoo.com
- ✓ Data.mail.yahoo.com
- ✓ Le.yahoo.apis.com
- ✓ Apis.yahoo.mail.com

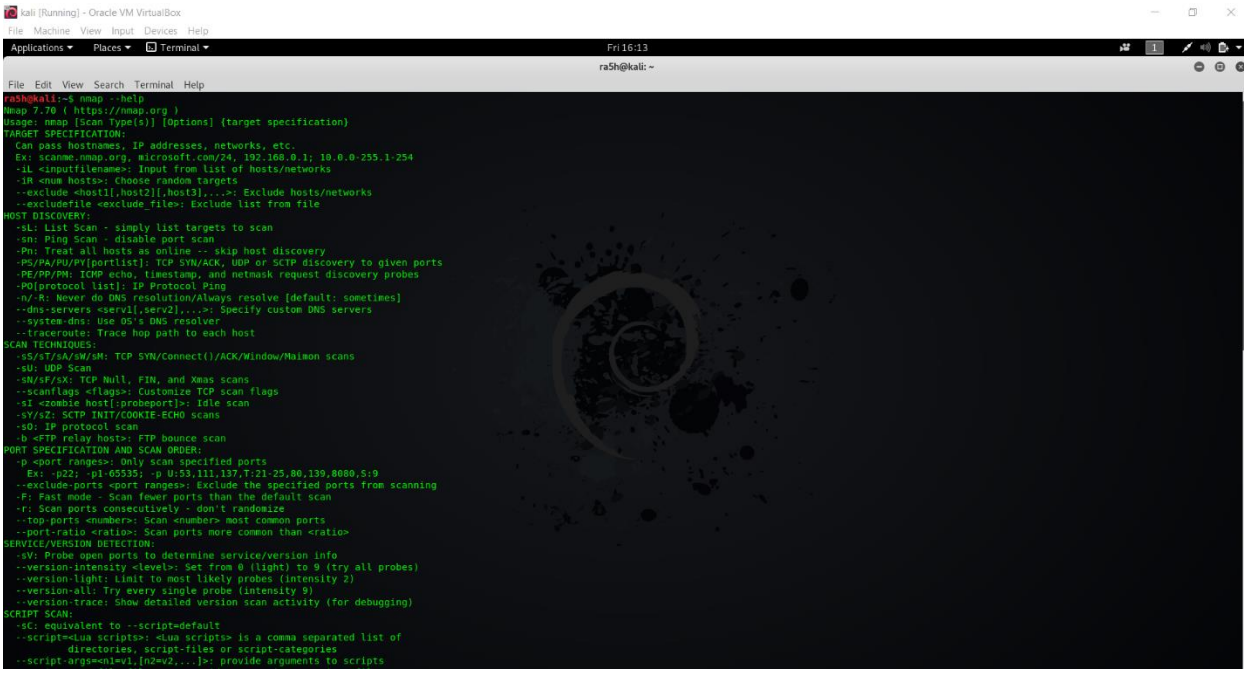
Nmap scan

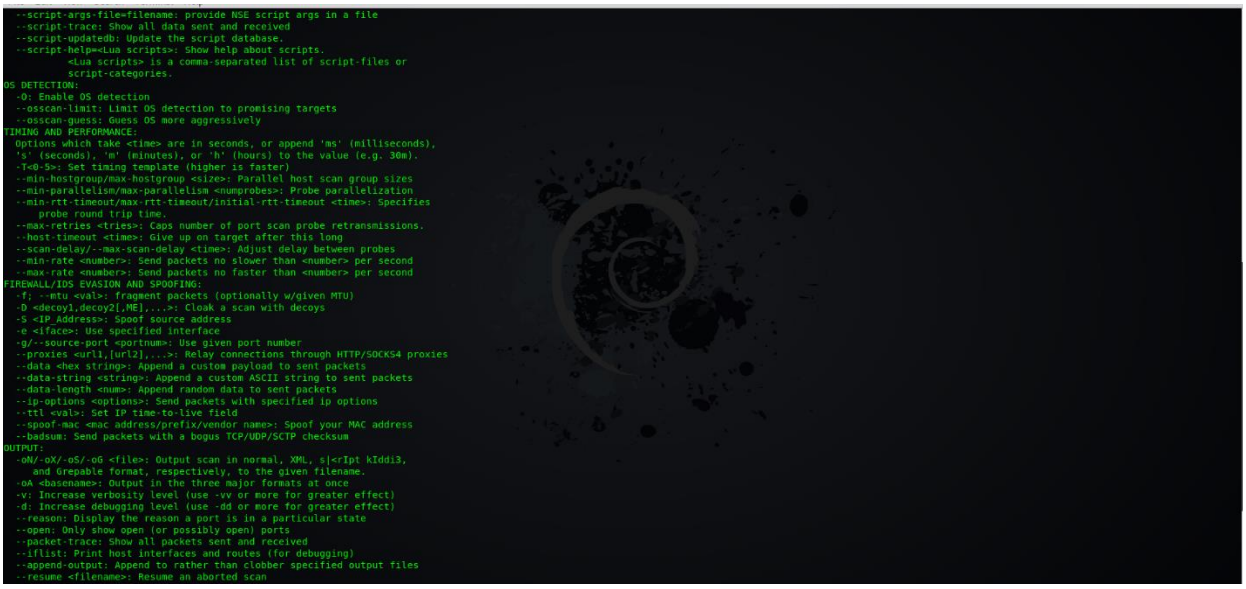
Nmap is short for network mapper. This Nmap is open source tools for network discovery and also vulnerability scanner. And also it is known as a network monitoring system. When using this Nmap scanning, we can identify,

- Open ports
- What devices are running on the system
- Available host

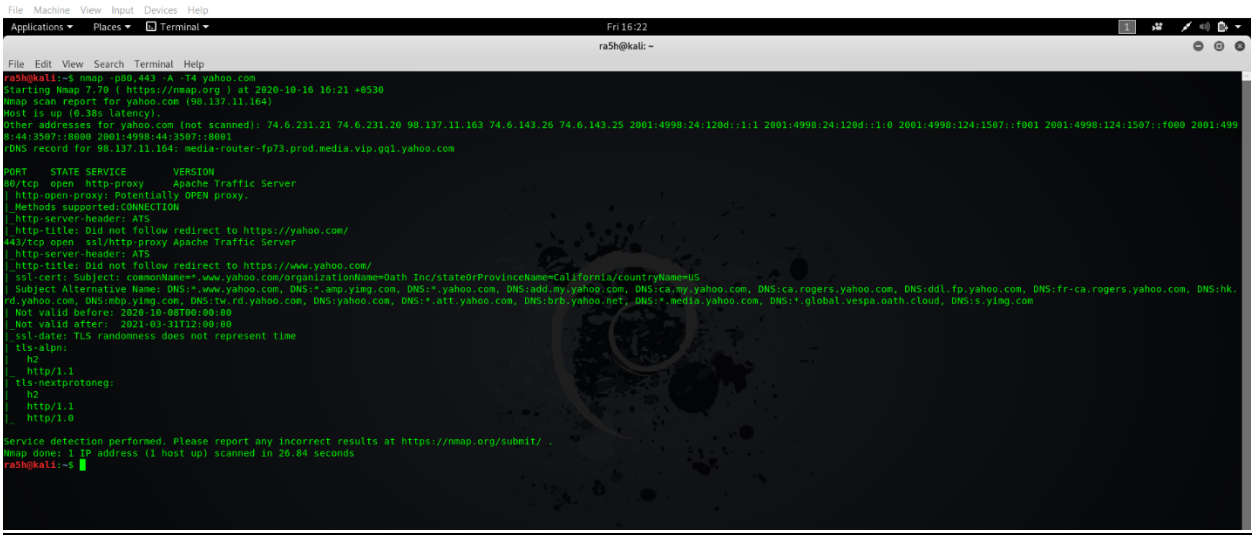
Nmap collects information by sending raw packet systems to the port. Listening to the feedback on those sent raw packets determines whether the port is open or closed. Nmap used transport layer protocol include UDP, TCP and also SCTP. The packets which Nmap sends return with IP addresses of ports and some of the other data in the ports and also system. through this Nmap scan we can able to get an idea of the network in the system. and also Nmap can identify the operating systems running on the network systems. It is known as OS fingerprinting. [5]

Nmap commands :





Nmap scan of yahoo.com



Command of the above screenshot shows, ports 80 and 443 mean HTTP and HTTPS scripts and –A mean an active OS detection, version detection and also script scanning. –T means timing template. And the last one is the target domain that I need to scan.

According to a Nmap scan of the yahoo.com, this domain used server as **ATS(Apache Traffic Server).**

After finishing this stage, I do a vulnerability scan as another part of my web security auditing.

Vulnerability scan

A vulnerability scan is an automated technology that attempts to identify vulnerabilities in the system. through this scan, we can identify shortcomings in the system. vulnerability scan has various types.

- External vulnerability scan
- Internal vulnerability scan
- Authenticated vulnerability scan
- Unauthenticated vulnerability scan [6]

Also, we have to use many tools for doing this vulnerability scan. Some are,

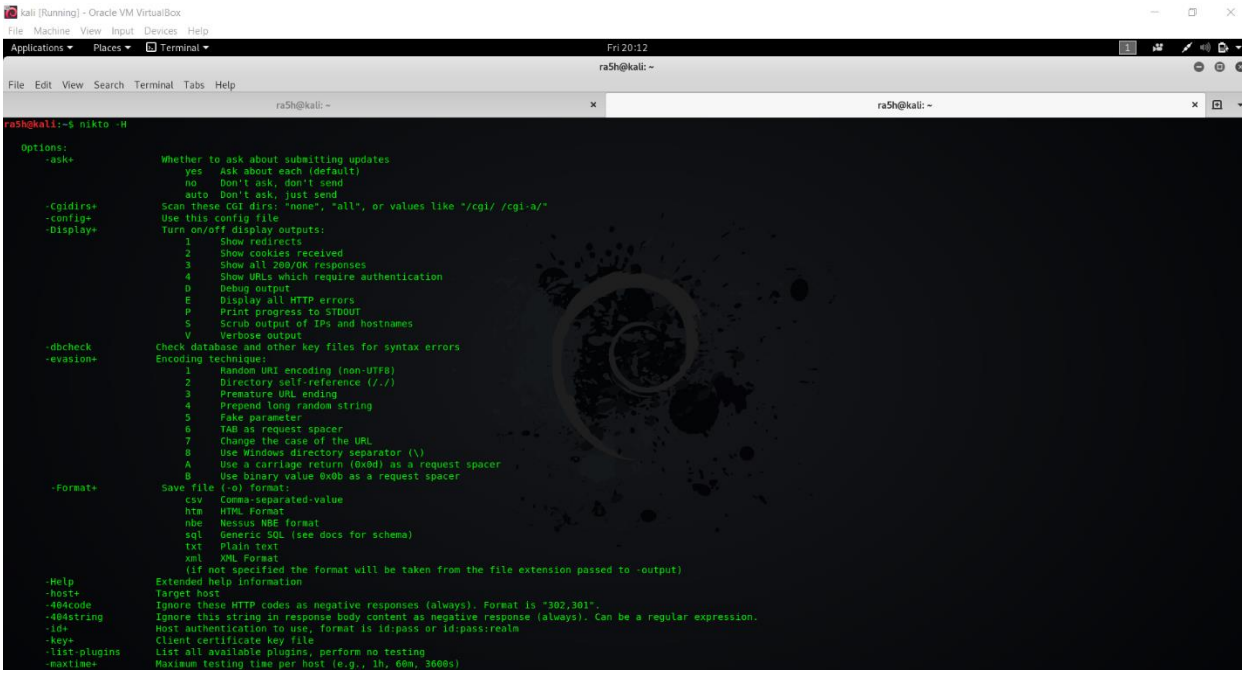
- Nikto scan
- Nessus
- Netsparker
- Burp

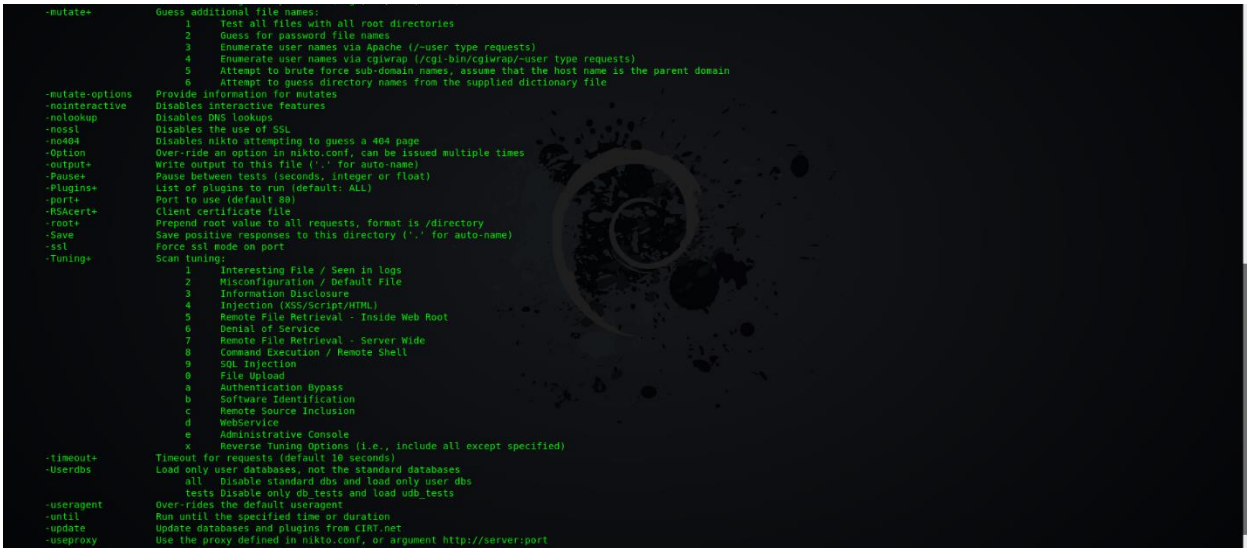
I selected **Nikto scan** and **Netsparker** tools from these tools to continue to my web security audit.

Nikto Scan

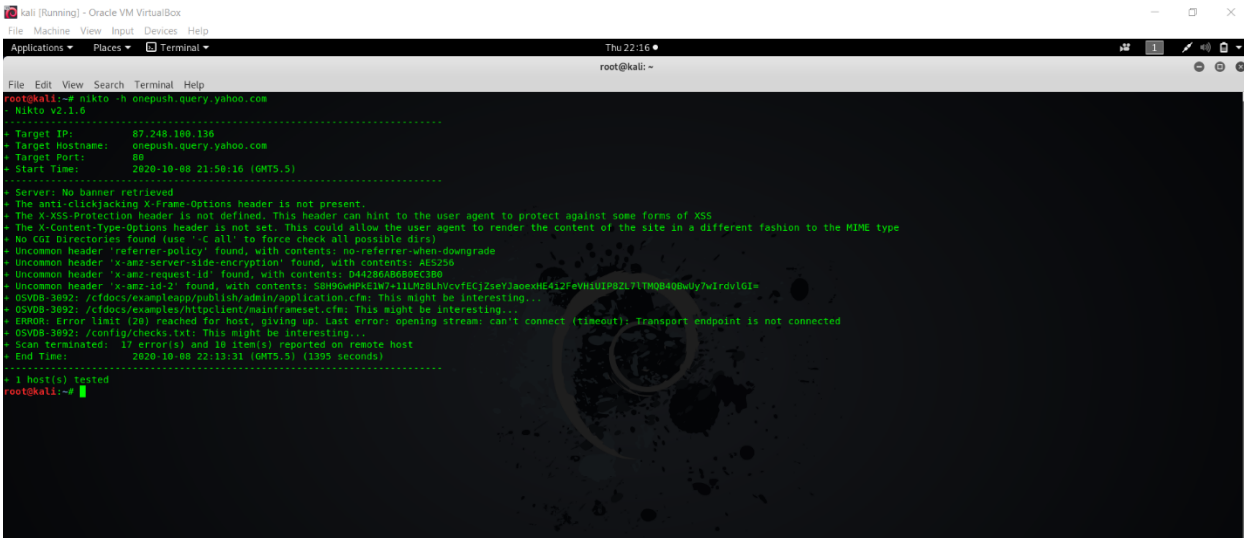
Nikto scan is a well know vulnerability scanner that scans web servers for vulnerable and dangerous files, outdated server software, miss configuration and other problems. It captures cookies received and then print it. This scanner helps to detect security-related issues in web script and web server configuration. Nikto is open-source software.

These are some keywords of Nikto :

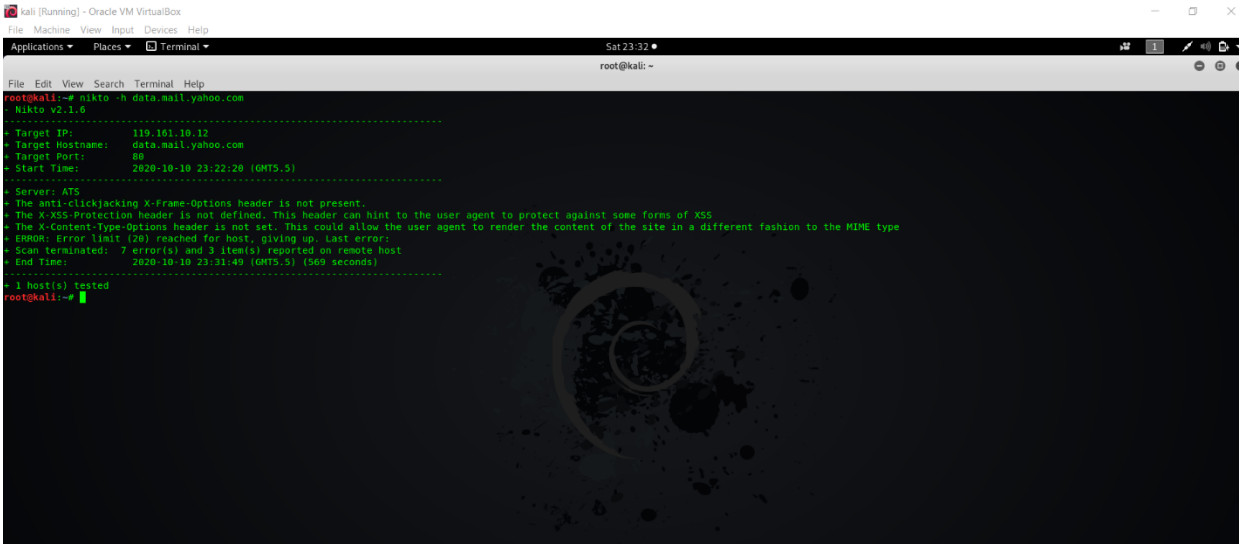




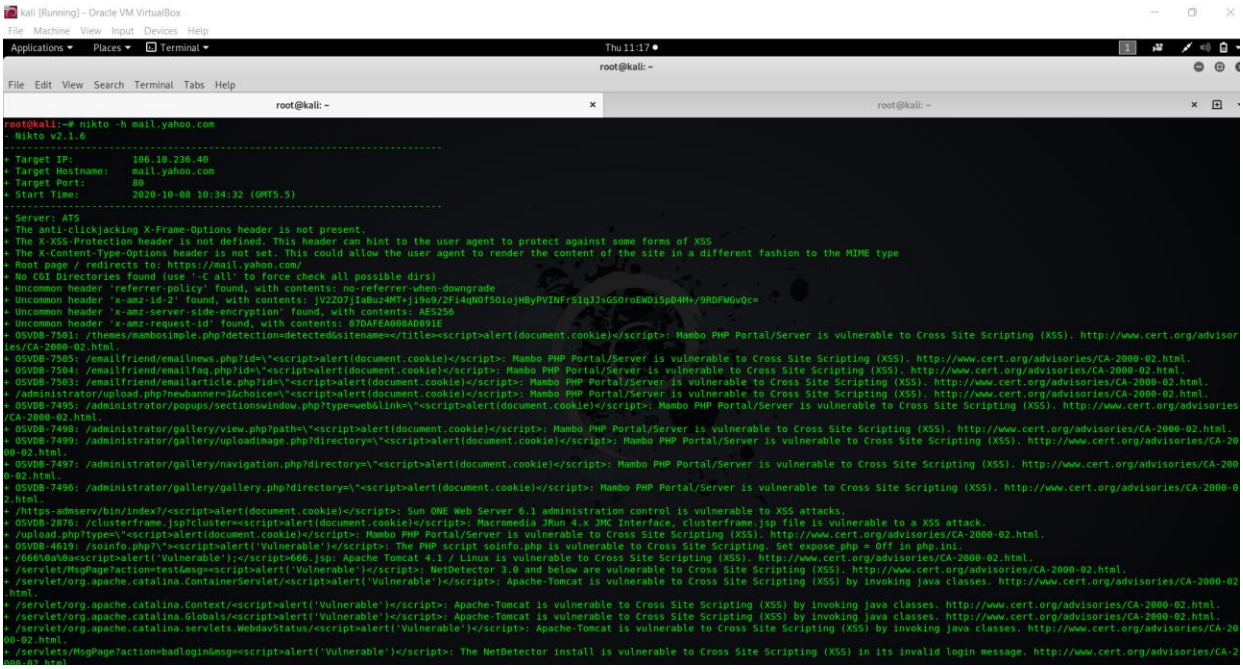
Nikto scan for Onepush.query.yahoo.com



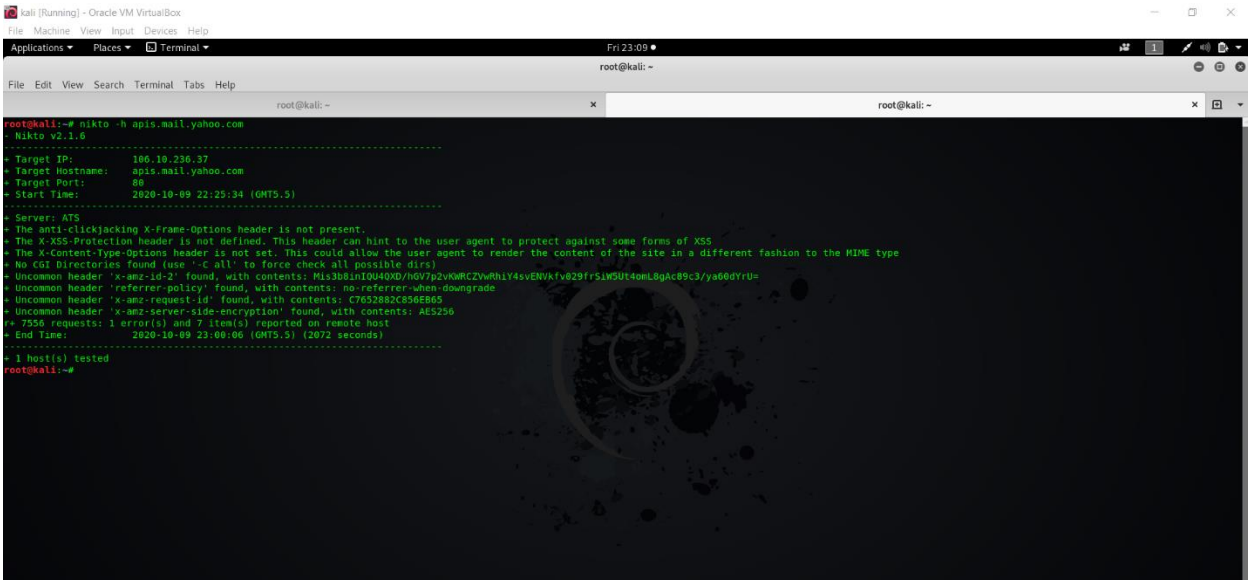
Nikto scan for data.mail.yahoo.com



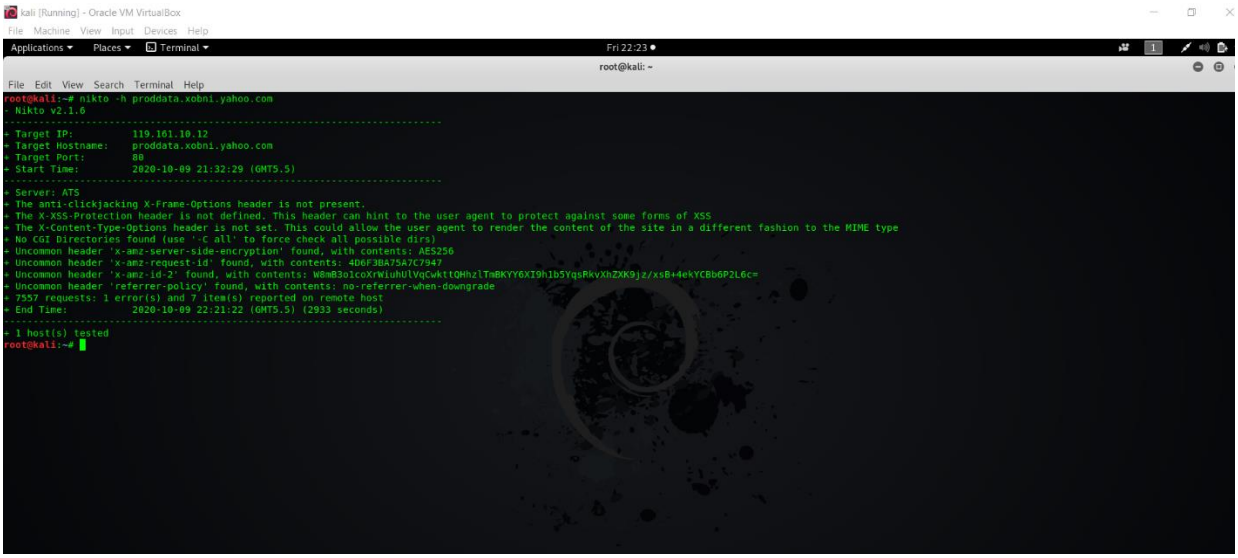
Nikto scan for mail.yahoo.com



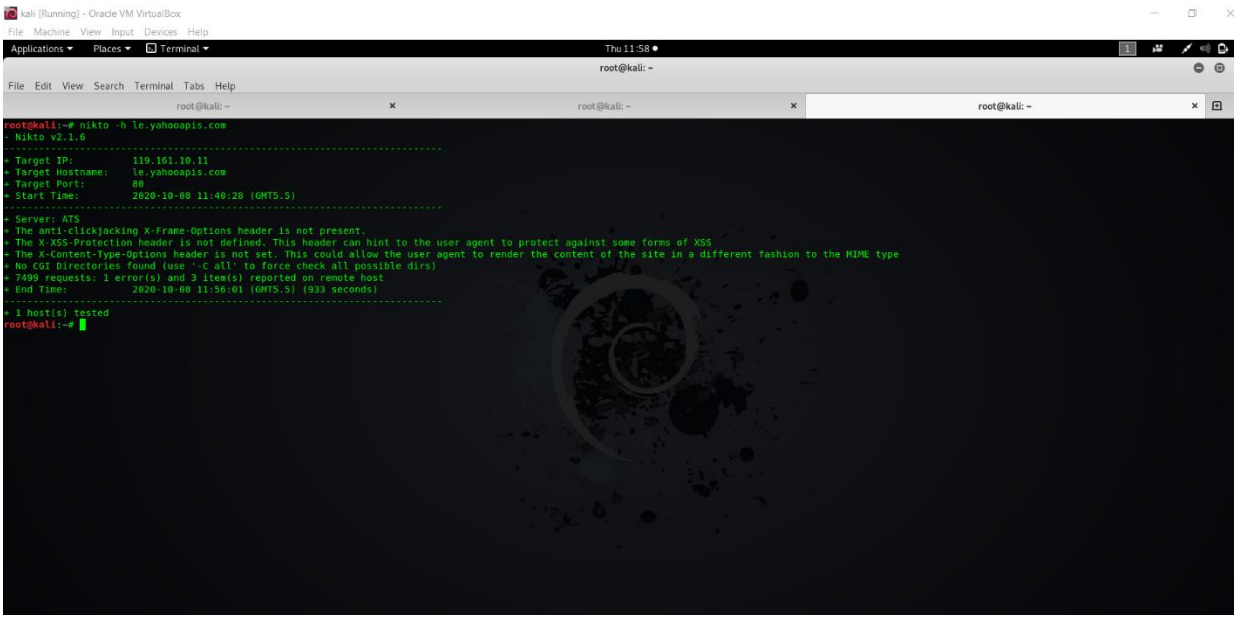
Nikto scan for apis.mail.yahoo.com



Nikto scan for proddata.xobni.yahoo.com



Nikto scan for le.yahooapis.com



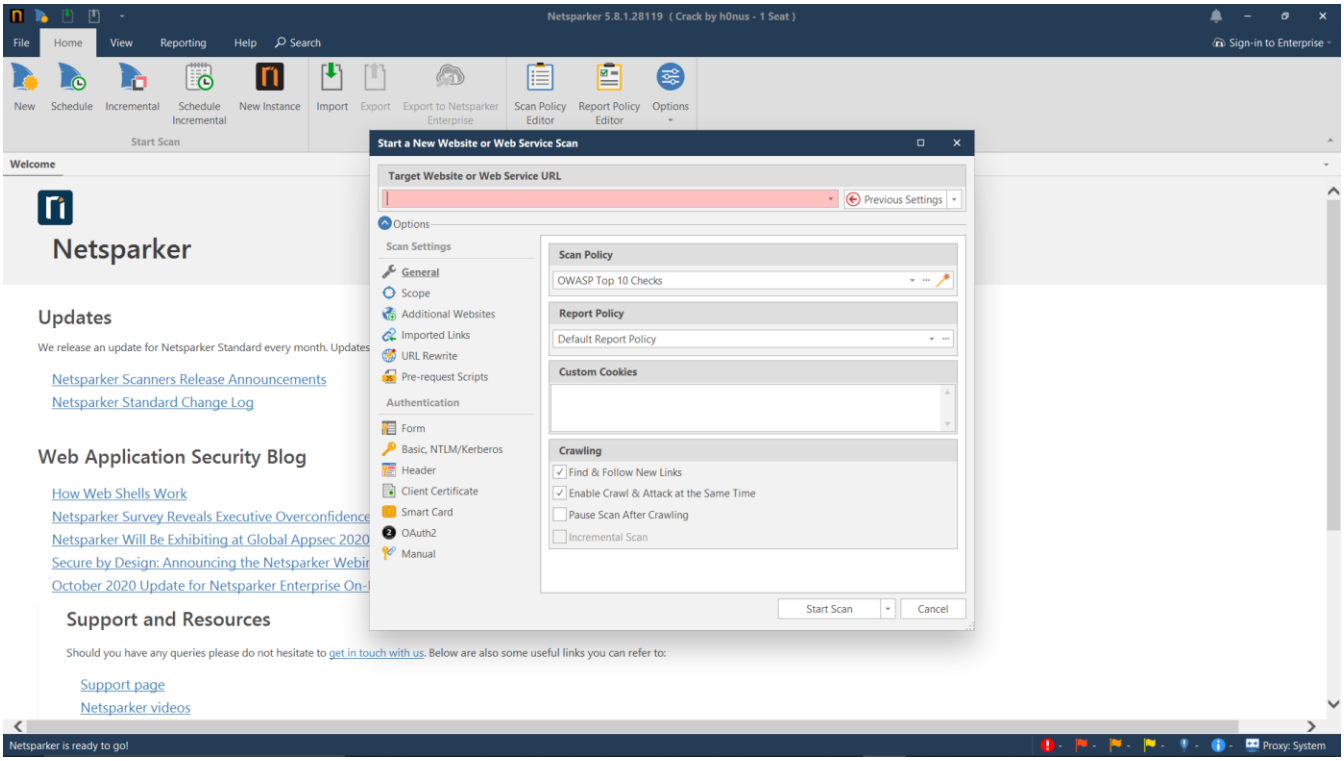
Netsparker

Netsparker is also an automated web application security scanner. It can scan web applications, web services and also websites. Netsparker can detect security issues of the system. and also it automatically discovers and protect your current web assets. Netsparker is not a just scanner it is a vulnerability management solution. Because the Netsparker provides so many facts of detected vulnerability. So we can easily identify what is the type of this vulnerability and also we can gain an understanding of the solution we can take to fix this vulnerability. One of the important of this application, it provides proof of the vulnerability. Netsparker can generate a proof when it identifies the following vulnerabilities, [7]

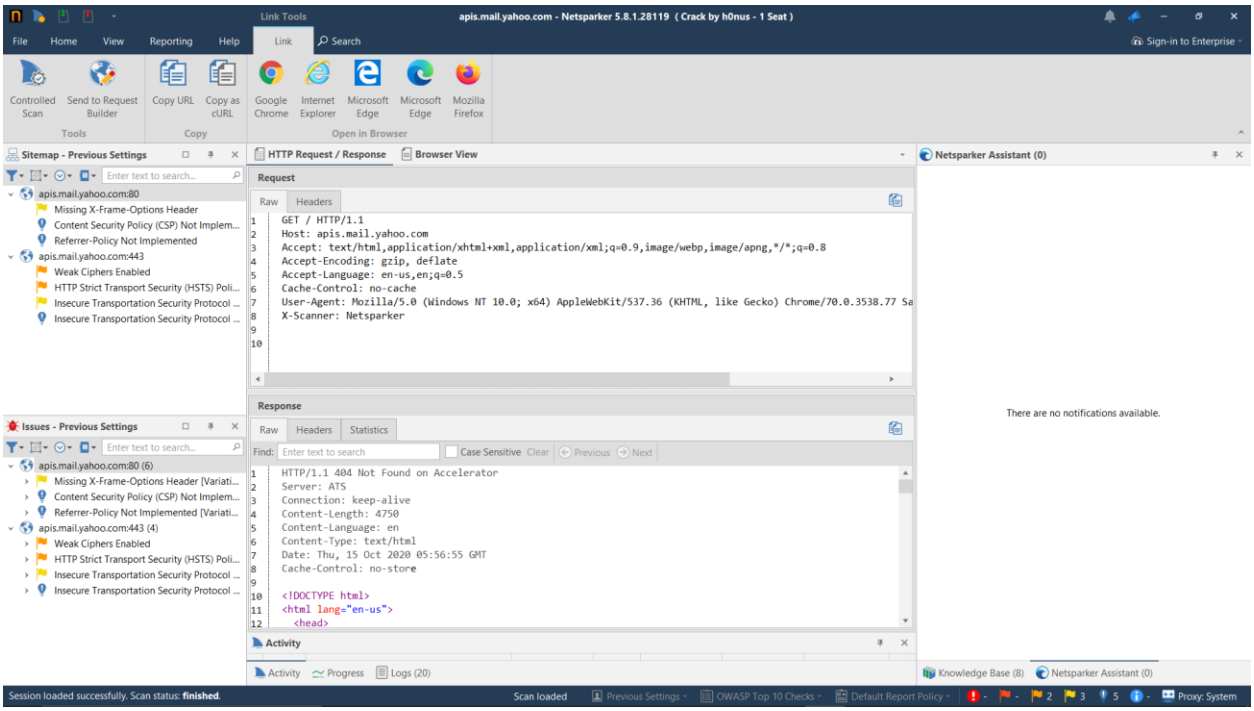
- SQL Injection
- Boolean SQL Injection
- Blind SQL Injection
- Remote File Inclusion (RFI)
- Command Injection
- Blind Command Injection
- XML External Entity (XXE) Injection
- Remote Code Evaluation
- Local File Inclusion (LFI)
- Server-side Template Injection
- Remote Code Execution
- Injection via Local File Inclusion

Also, lots of benefits have to this type of proof-based scanning. Furthermore, we can select the scan policy and also report policy in the Netsparker scanner.

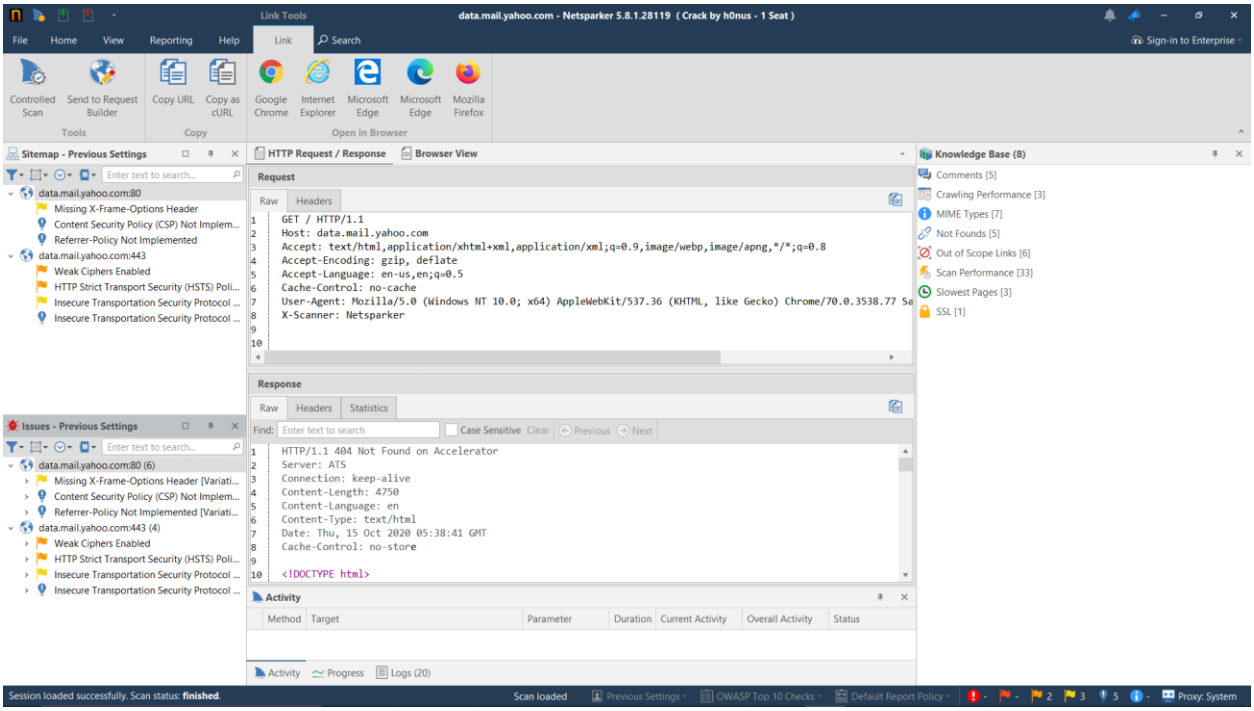
The interface of the Netsparker



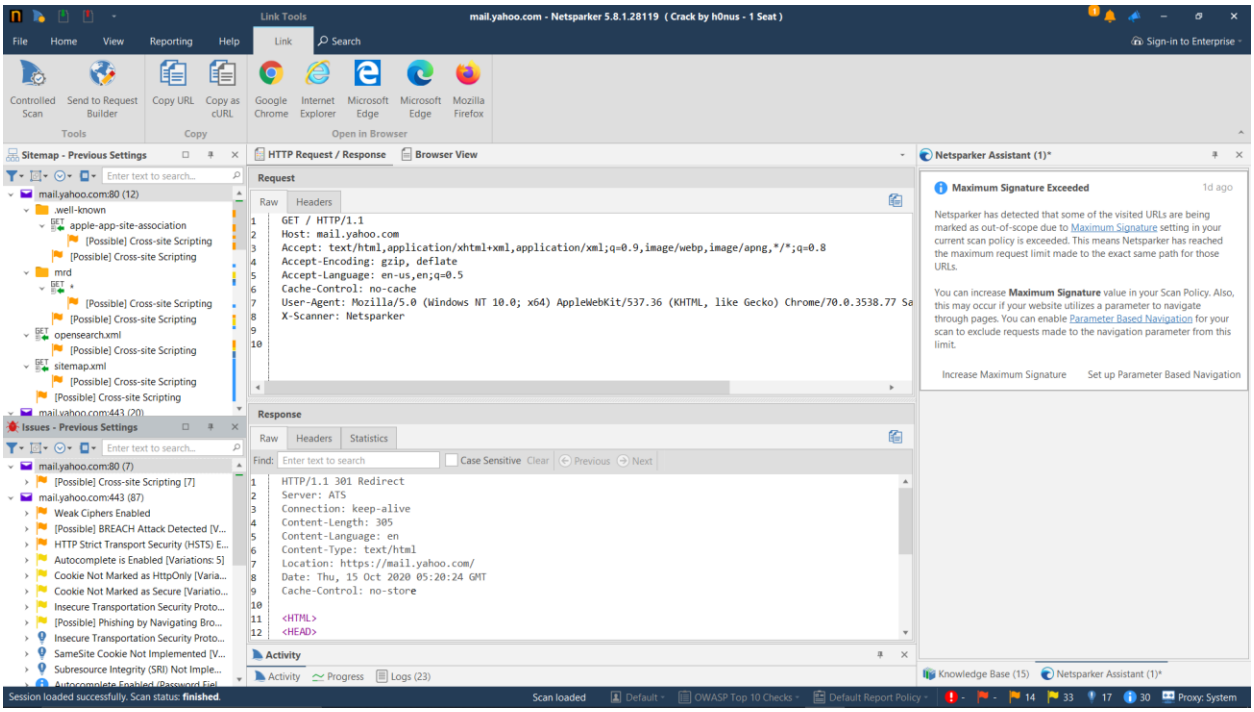
Netsparker scan of the onepushquery.yahoo.com



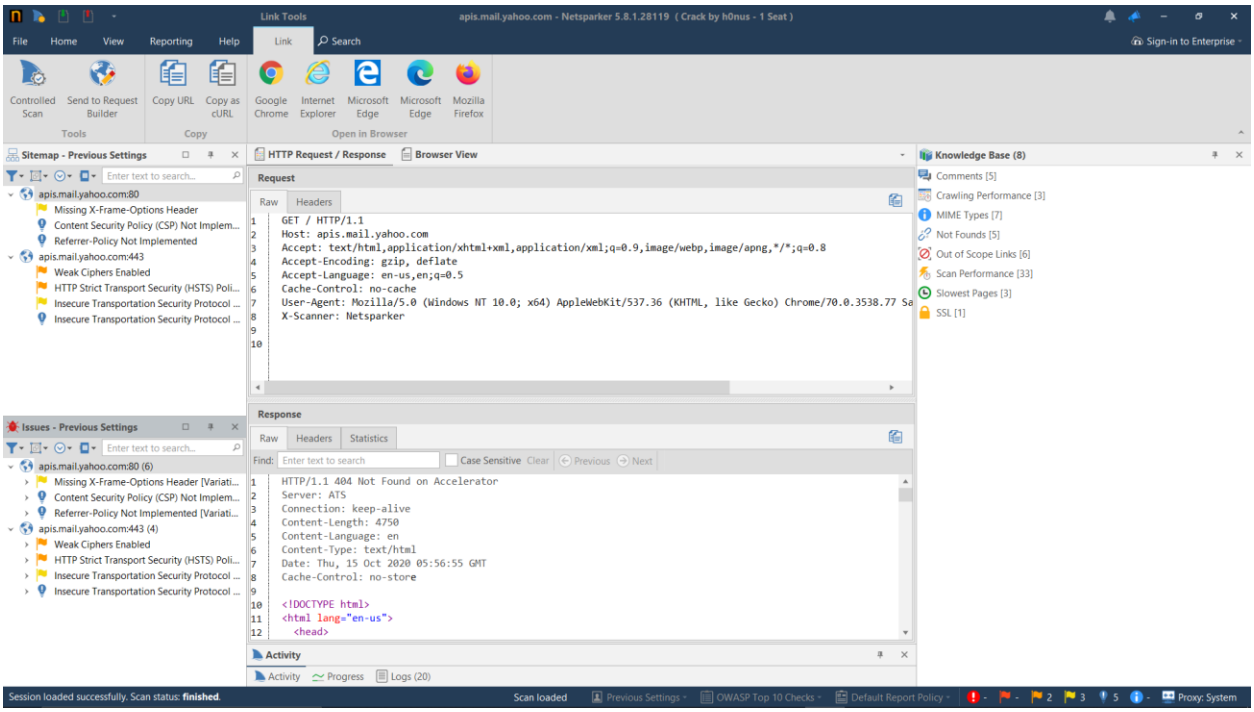
Netsparker scan of the data.mail.com



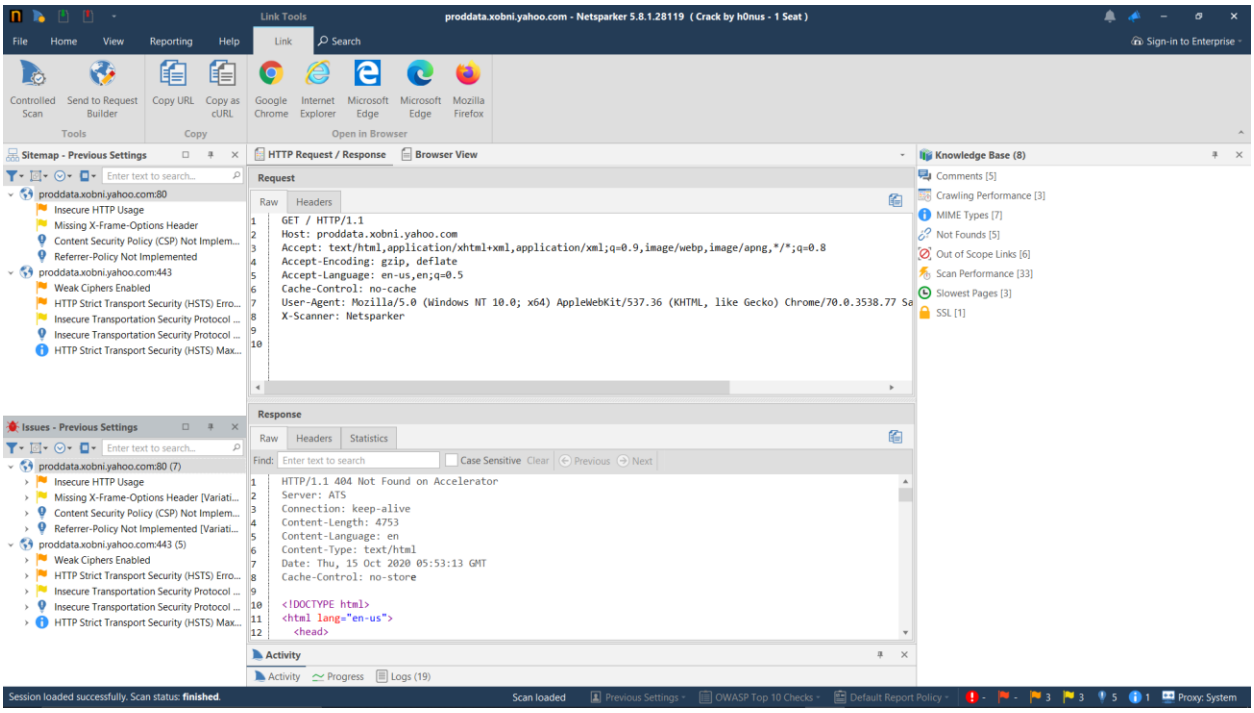
Netsparker scan of the mail.yahoo.com



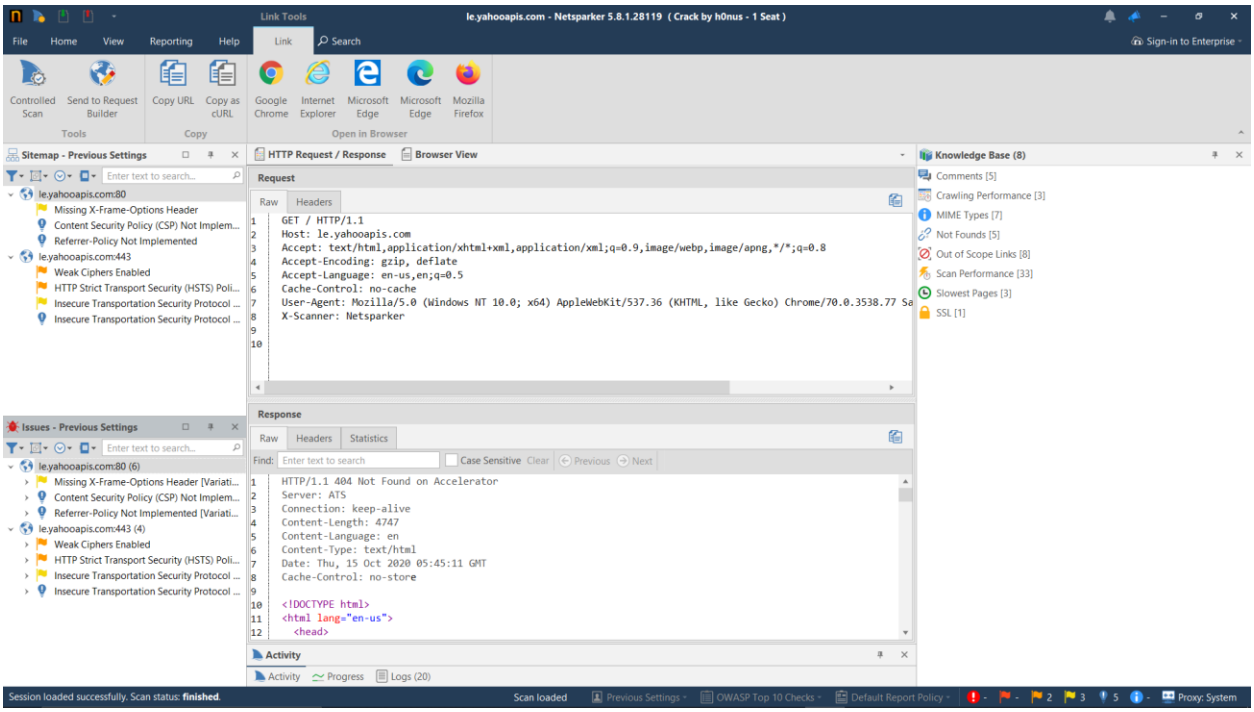
Netsparker scan of the apis.mail.yahoo



Netsparker scan of the proddata.xobni.yahoo.com



Netsparker scan of the le.yahooapis.com



After these scans of Nikto and also Netsparker I find some vulnerabilities of these subdomains.

Vulnerability analysis

Vulnerabilities identified in the Onepush.query.yahoo.com

- ✓ **Insecure HTTP Usage**

This insecure HTTP header usage is a medium vulnerability which identifies by Netsparker. The identity of this vulnerability according to OWASP is 2017-A3. What happens here is that when implemented target website however HTTP request is not redirected to HTTPS. This vulnerability is vulnerable to Man in the Middle (MITM) attack because the user will not able to get the benefits of HTTP strict transport security (HSTS) and almost renders the implementation is useless.

Solution
Configure webserver to redirect HTTP requests to HTTPS requests.

- ✓ **Weak Ciphers enabled**

This is a confirmed medium vulnerability identified by Netsparker. Classification of this vulnerability is OWASP 2017 –A3 or CWE-327. This vulnerability is identified during secure communication.
The impact of this weak ciphers enabled vulnerability is attackers can decrypt secure socket layer (SSL) traffic between web application and users.

Solutions
Configure webserver to disallow when using weak ciphers.
In the apache server, modify the SSLCipher suite.

- ✓ **Cookie not marked as HTTP only**

This vulnerability can expose to cross-site scripting attacks. Through this vulnerable attacker can easily hijack the victim's session.

- ✓ **Same-site cookie not implemented**
  This vulnerable can expose to the CSRF attack.

- ✓ **Missing X-frame option header**

- ✓ **Insecure transportation security protocol supported**

Vulnerabilities identified in the data.mail.yahoo.com

- ✓ **Missing X-frame option header**

  The x-frame option header missing means this application can be the risk of a clickjacking attack. A clickjacking attack is that prompts a user to click on a web page feature in malicious. This can cause to download malicious software into the users' devices.

  Solution

- Sending the proper X-Frame-Options in HTTP response headers.
  - **X-Frame-Options: DENY**

    It completely denies being loaded in frame/iframe.

  - **X-Frame-Options: SAMEORIGIN**

    It allows only if the site which wants to load has the same origin.

  - **X-Frame-Options: ALLOW-FROM <*URL*>**

    It grants a specific URL to load itself in an iframe.

- ✓ **HSTS Policy is not enabled**

- ✓ **Weak Ciphers enabled**

  This is a confirmed medium vulnerability identified by Netsparker. Classification of this vulnerability is OWASP 2017 –A3 or CWE-327. This vulnerability is identified during secure communication.

The impact of this weak ciphers enabled vulnerability is attackers can decrypt secure socket layer (SSL) traffic between web application and users.

Solutions

Configure webserver to disallow when using weak ciphers.

In the apache server, modify the SSLCipher suite.

- ✓ **Insecure transportation security protocol supported.**

Vulnerabilities identified in the mail.yahoo.com

- ✓ **Vulnerable to cross-site scripting**

  In here attackers can execute some dynamic scripts. This can cause several attacks. Mostly risk on hijacking attack. Other risks of this vulnerable are phishing attack, intercepting data and perform MiTM attack and changing the user interface.

  Solutions

  - Enabled content security policy(CSP).
  - Outputs and inputs are should be encoded.
  - Include well-structured whitelist libraries

- ✓ **Autocomplete is enable**

  In here, some sensitive data like username, password, credit card no and CVV are automatically filled. If the users select the save option and this sensitive data is going to be cached by the browser. And then attackers can steal these users' sensitive data.

  Solution

  The "Autocomplete" attribute is disabled.

- ✓ **Detected robot.txt file**

  In the Netsparker scan detected this text file that includes some sensitive data. So attackers might be can discover this file and then it issues to users' data.

- ✓ **Cross-site referrer leakage through referrer policy.**

  Through this vulnerability can leak some domain information through the referrer header. When we check the available option by using external reference and use one suit for your need.

Vulnerabilities identified in the apis.mail.yahoo.com

- ✓ **Weak Ciphers enabled.**

  This is a confirmed medium vulnerability identified by Netsparker. Classification of this vulnerability is OWASP 2017 –A3 or CWE-327. This vulnerability is identified during secure communication.

  The impact of this weak ciphers enabled vulnerability is attackers can decrypt secure socket layer (SSL) traffic between web application and users.

  Solutions

  Configure webserver to disallow when using weak ciphers.

  In the apache server, modify the SSLCipher suite.

- ✓ **HSTS Policy is not enabled.**

  HTST policy is using to communicate with the server to the user. HTST is the security policy of the web servers that implement for users to interact with a website using a secure (HTTPS) connection.

  Solution

  Configure webserver to redirect HTTP requests to HTTPS.

- ✓ **Missing X-Frame-Options Header**.

- ✓ **Referrer-Policy Not Implemented.**

  Referrer-Policy is a security header that implements to prevent cross-domain referer leakage. The lack of a Referrer-Policy header might affect the privacy of the users and also the website.

  Solutions

  Implement Referrer-Policy response header.

  Declare the meta tags.

Vulnerabilities identified in the proddata.xobni.yahoo.com

- ✓ **Insecure HTTP Usage.**

This insecure HTTP header usage is a medium vulnerability which identifies by Netsparker. The identity of this vulnerability according to OWASP is 2017-A3. What happens here is that when implemented target website however HTTP request is not redirected to HTTPS.

This vulnerability is vulnerable to Man in the Middle (MITM) attack because the user will not able to get the benefits of HTTP strict transport security (HSTS) and almost renders the implementation is useless.

Solution

Configure webserver to redirect HTTP requests to HTTPS requests.

- ✓ **Missing X-frame option header.**

The x-frame option header missing means this application can be the risk of a clickjacking attack. A clickjacking attack is that prompts a user to click on a web page feature in malicious. This can cause to download malicious software into the users' devices.

Solution

Sending the proper X-Frame-Options in HTTP response headers.

- ✓ **Referrer-Policy Not Implemented.**

Referrer-Policy is a security header that implements to prevent cross-domain referer leakage. The lack of a Referrer-Policy header might affect the privacy of the users and also the website.

Vulnerabilities identified in the le.yahooapis.com

- ✓ **Content Security Policy (CSP) Not Implemented.**

  CSP is used to mitigate Cross-site Scripting attacks. This vulnerability has not a direct impact on the website but if the website is vulnerable to a Cross-site Scripting attack, then CSP can prevent the successful exploitation of that vulnerability.

  Solution

  Enable CSP on the website by sending the Content-Security-Policy in HTTP response headers.

- ✓ **Weak Ciphers enabled.**

  This is a confirmed medium vulnerability identified by Netsparker. Classification of this vulnerability is OWASP 2017 –A3 or CWE-327. This vulnerability is identified during secure communication.

  The impact of this weak ciphers enabled vulnerability is attackers can decrypt secure socket layer (SSL) traffic between web application and users.

  Solutions

  Configure webserver to disallow when using weak ciphers.

  In the apache server, modify the SSLCipher suite.

- ✓ **(HSTS) Policy Not Enabled**

- ✓ **Referrer-Policy Not Implemented.**

  Referrer-Policy is a security header that implements to prevent cross-domain referer leakage. The lack of a Referrer-Policy header might affect the privacy of the users and also the website.

  Solutions

  Implement Referrer-Policy response header.

  Declare the meta tags.

Conclusion

Overall, through this web security audit performed on several subdomains that I selected in yahoo.com.While this testing I identified several critical vulnerabilities as well as a lot of medium vulnerabilities on these subdomains. Furthermore through this documentation provide an idea of web security auditing and also what benefits are coming from this audit to web application. Also in this documentation discussed how to perform web auditing and also what tools can use to do the audit. As well as a discussed result about what identified vulnerabilities are in I selected domain.

Today, most people are using web applications for their work. Also, they access their sensitive data through this web application. Therefore web applications want to follow a good security system because if not users' data have at risk. That's why security analysis is recommended for doing a web security audit and implement or improve their security. It can protect their users' data and also they can prevent cyber attacks.

References :

[1] J. Varghese, Website Security Audit, Astra, October 9, 2020.

[2] OWASP Mobile Top 10 Risks, Promon.

[3] OWASP Top 10 Security Risks & Vulnerabilities, Sucuri Guides.

[4] sublist3r Package Description, Kali Tools.

[5] M. Ferranti, What is Nmap? Why you need this network mapper, Network World , AUG 17, 2018.

[6] What is a Vulnerability Scan?, PACKETLABS.

[7] What is Netsparker?, Netsparker.