VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

FALL SEMESTER 2023-24

LAB ASSESSMENT -3

NAME:- Namit Mehrotra

Registration Number:- 21BCE0763

Course Name:- Information Security Analysis and Audit Lab BCSE353E

Slot:- L57+L58

Date:- 04-07-2023

EXERCISE 3-A-1: Static Malware Analysis

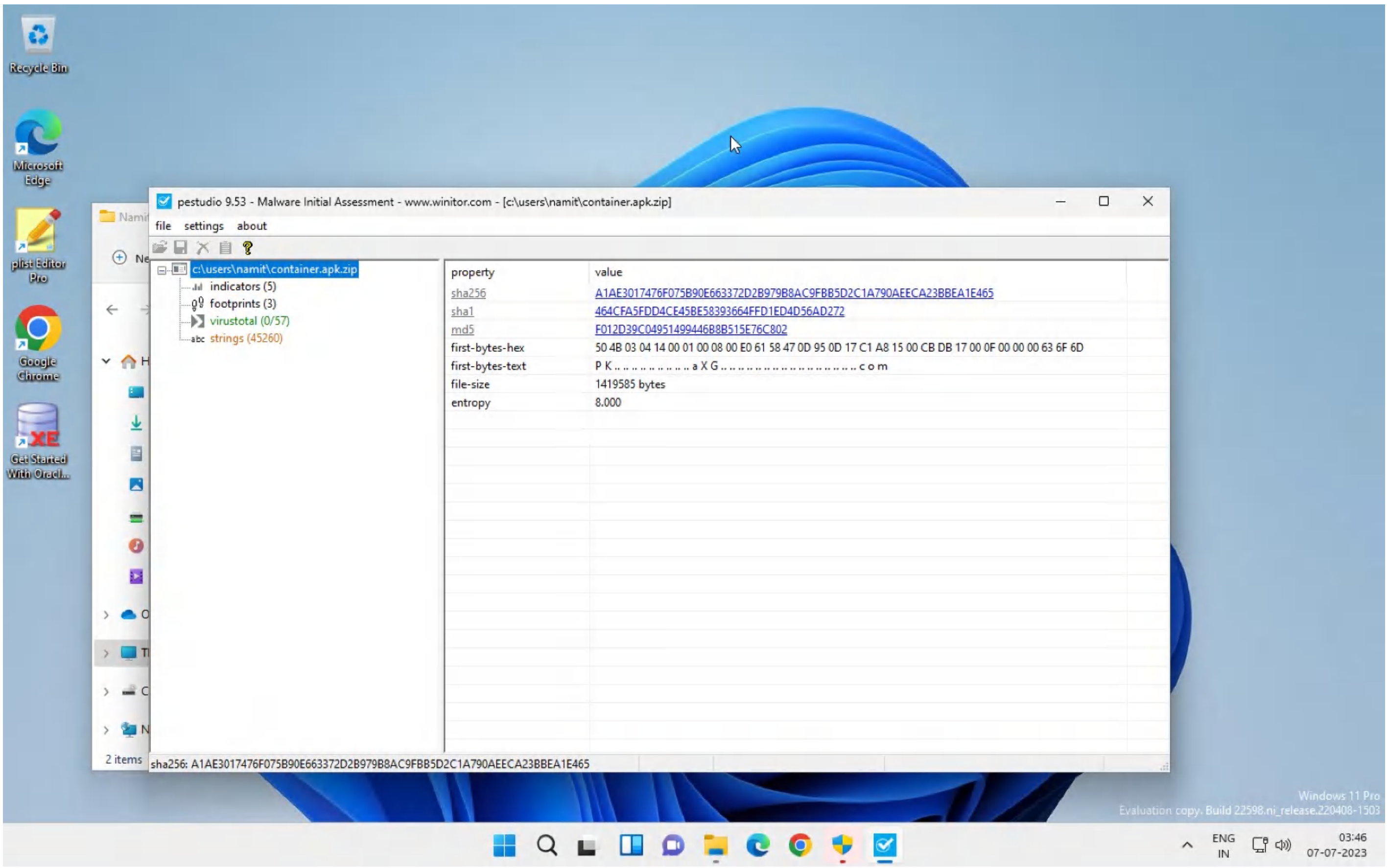
I. AIM: Performing Static Malware Analysis using PeStudio.

II. TOOLS REQUIRED:

1. Products: PeStudio in Windows 11
2. Internet browser: Microsoft Edge
3. Manufacturer: various

III. STEP BY STEP PROCEDURE:

1. Download the container.apk.zip file from the given link.
2. Open PeStudio.
3. Open the container.apk.zip as a zip file in PeStudio.



pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [c:\users\namit\container.apk.zip]

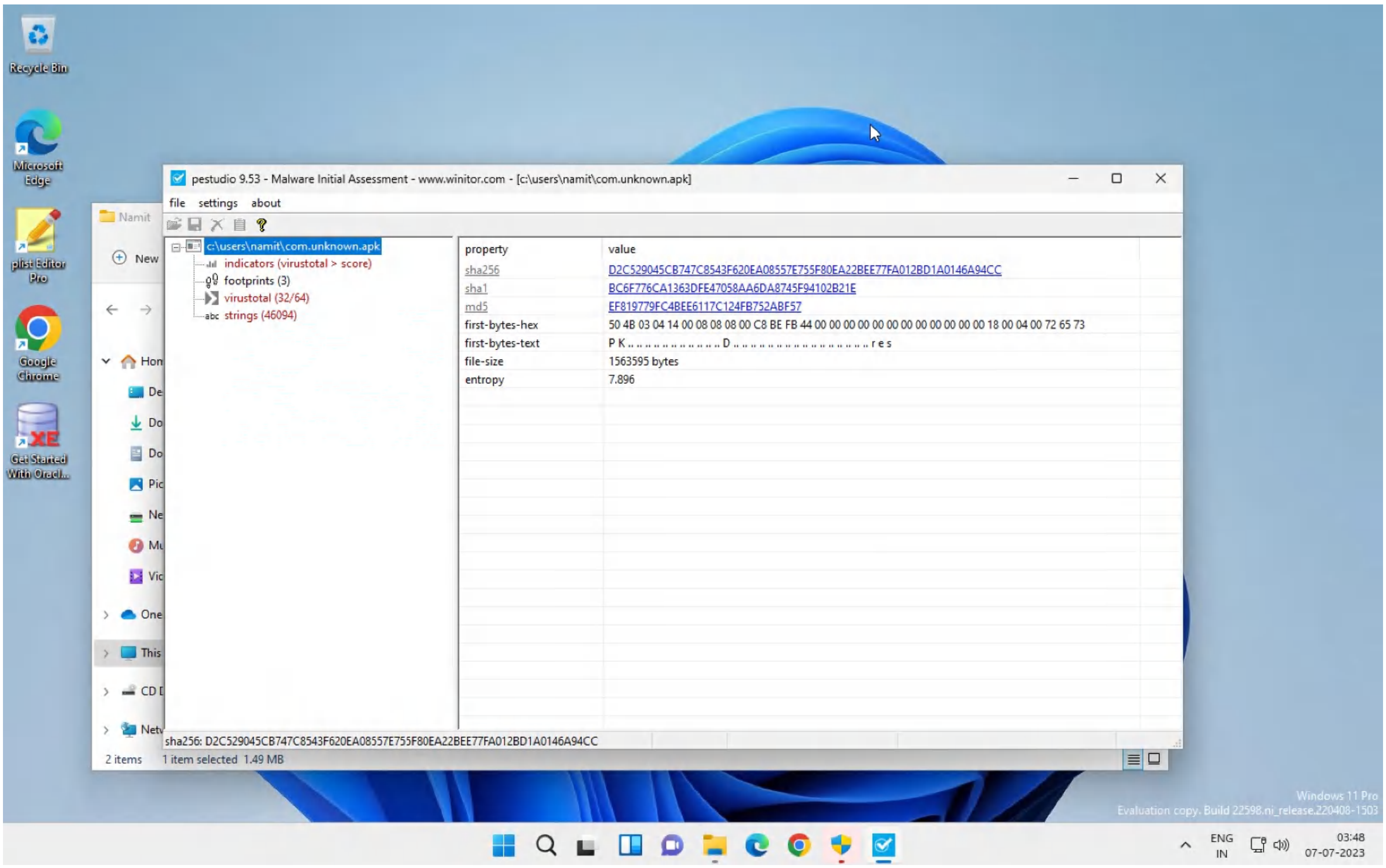
c:\users\namit\container.apk.zip
- indicators (5)
- footprints (3)
- virustotal (0/57)
- strings (45260)

property	value
sha256	A1AE3017476F075B90E663372D2B979B8AC9FBB5D2C1A790AEECA23BBEA1E465
sha1	464CFA5FDD4CE45BE58393664FFD1ED4D56AD272
md5	F012D39C04951499446B8B515E76C802
first-bytes-hex	50 4B 03 04 14 00 01 00 08 00 E0 61 58 47 0D 95 0D 17 C1 A8 15 00 CB DB 17 00 0F 00 00 00 63 6F 6D
first-bytes-text	P K . . . . a X G . . . . c o m
file-size	1419585 bytes
entropy	8.000

2 items

sha256: A1AE3017476F075B90E663372D2B979B8AC9FBB5D2C1A790AEECA23BBEA1E465

4. Now Extract The contents of the Zip File(The Actual apk file) Contents into a folder and open the folder using PeStudio.



pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [c:\users\namit\com.unknown.apk]

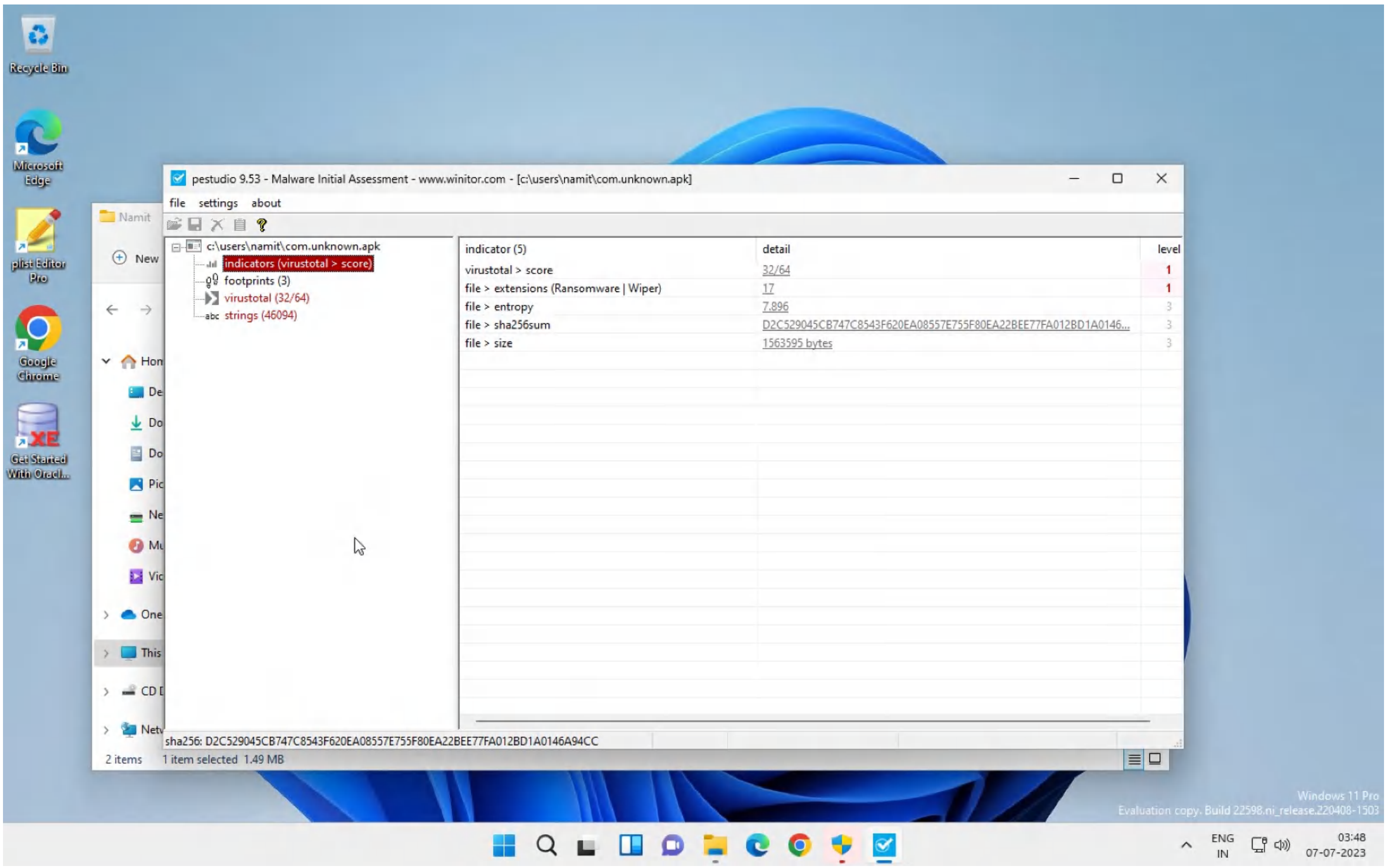
```
c:\users\namit\com.unknown.apk
  indicators (virustotal > score)
  footprints (3)
  virustotal (32/64)
  strings (46094)
```

property	value
sha256	D2C529045CB747C8543F620EA08557E755F80EA22BEE77FA012BD1A0146A94CC
sha1	BC6F776CA1363DFE47058AA6DA8745F94102B21E
md5	EF819779FC4BEE6117C124FB752ABF57
first-bytes-hex	50 4B 03 04 14 00 08 08 08 00 C8 BE FB 44 00 00 00 00 00 00 00 00 00 00 00 00 18 00 04 00 72 65 73
first-bytes-text	P K . . . . D . . . . r e s
file-size	1563595 bytes
entropy	7.896

sha256: D2C529045CB747C8543F620EA08557E755F80EA22BEE77FA012BD1A0146A94CC

2 items 1 item selected 1.49 MB

5. The Indicator Section shows malicious behavior detected in the file.



pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [c:\users\namit\com.unknown.apk]

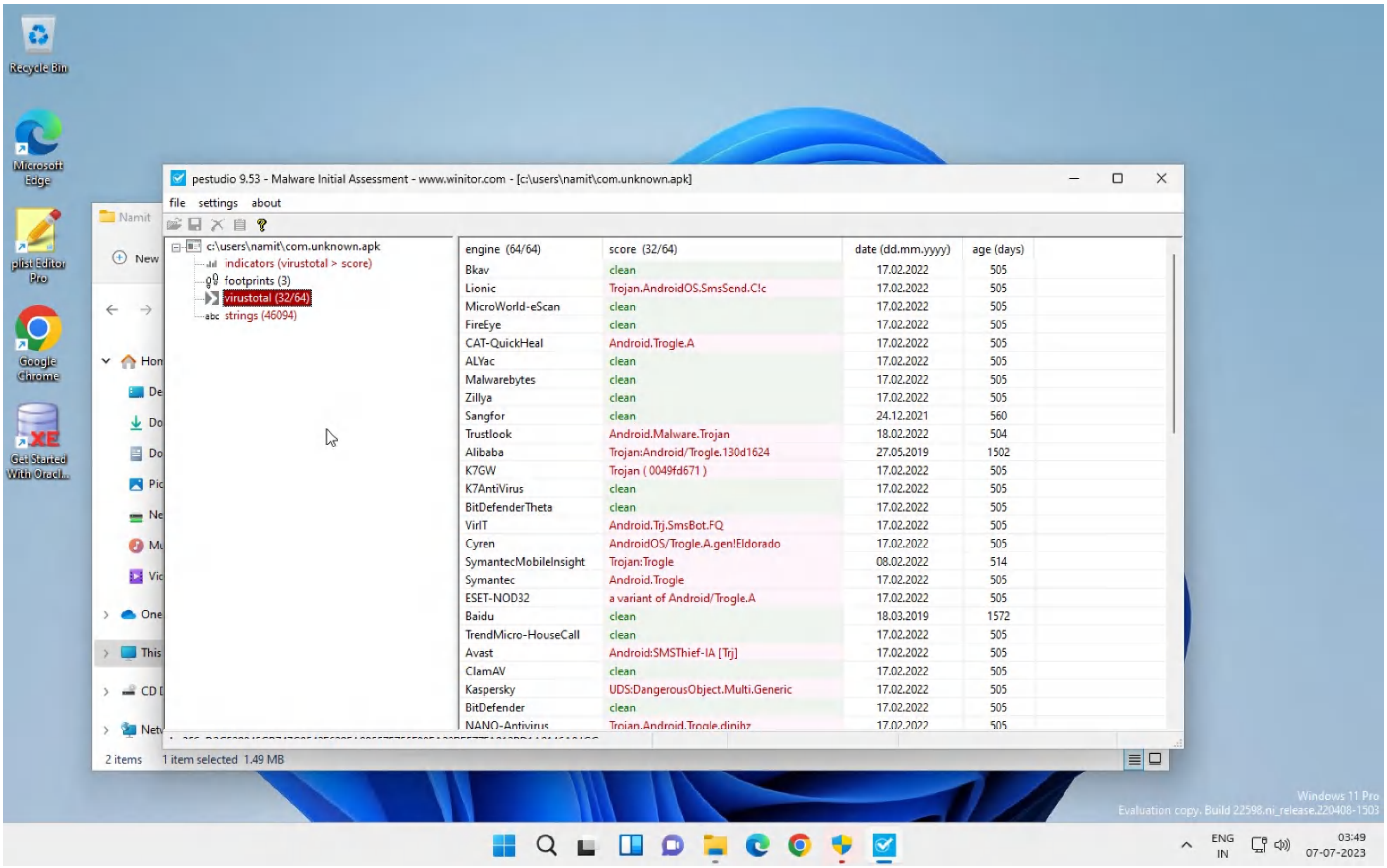
```
c:\users\namit\com.unknown.apk
  indicators (virustotal > score)
  footprints (3)
  virustotal (32/64)
  strings (46094)
```

indicator (5)	detail	level
virustotal > score	32/64	1
file > extensions (Ransomware | Wiper)	17	1
file > entropy	7.896	3
file > sha256sum	D2C529045CB747C8543F620EA08557E755F80EA22BEE77FA012BD1A0146...	3
file > size	1563595 bytes	3

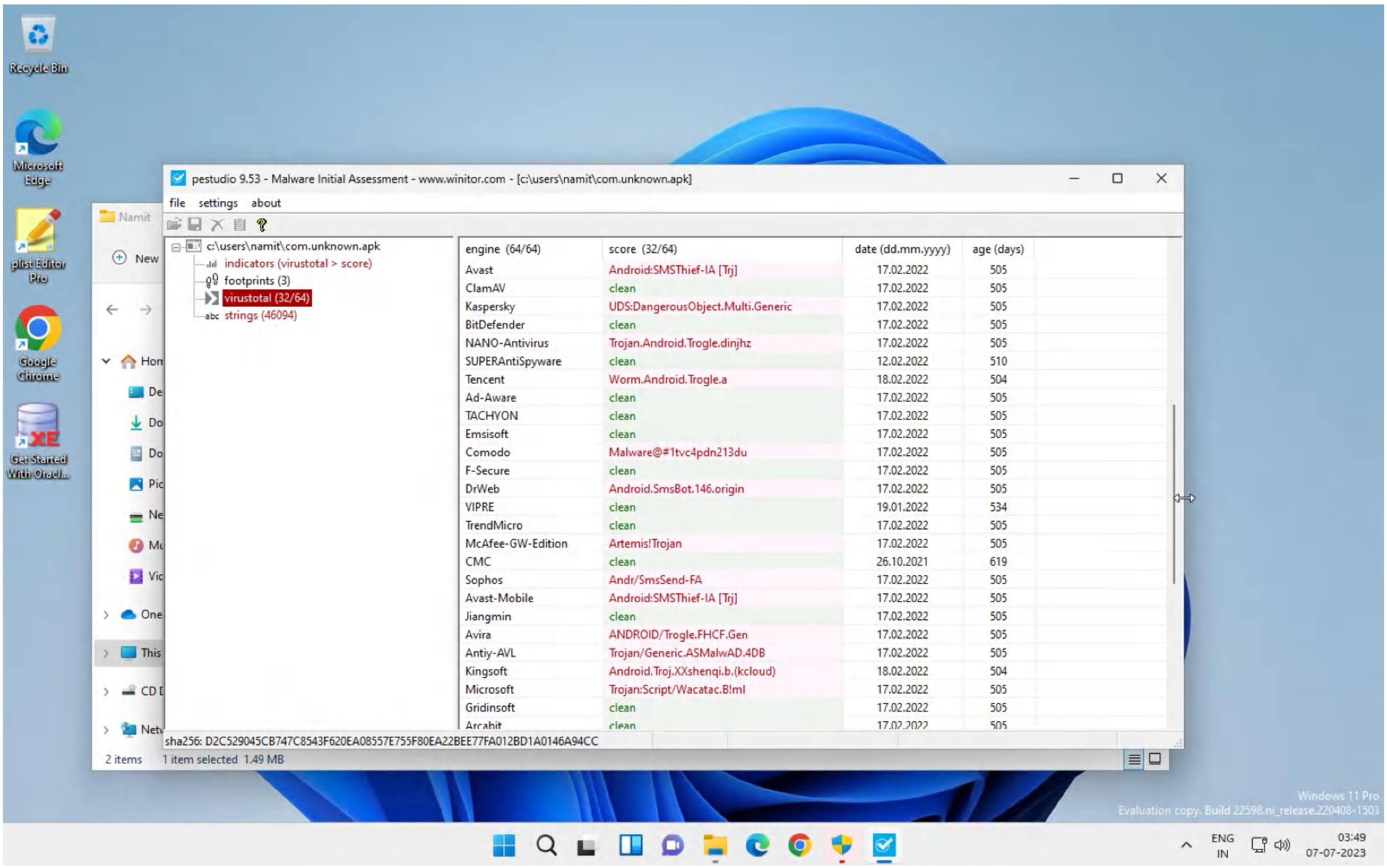
sha256: D2C529045CB747C8543F620EA08557E755F80EA22BEE77FA012BD1A0146A94CC

2 items 1 item selected 1.49 MB

6. The VirusTotal Section shows the scan of the given file from various antivirus softwares.


pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [c:\users\namit\com.unknown.apk]
file
settings
about
c:\users\namit\com.unknown.apk
indicators (virustotal > score)
footprints (3)
virustotal (32/64)
strings (46094)
2 items
1 item selected 1.49 MB
Windows 11 Pro
Evaluation copy. Build 22598.ni_release.220408-1503
ENG
IN
03:49
07-07-2023

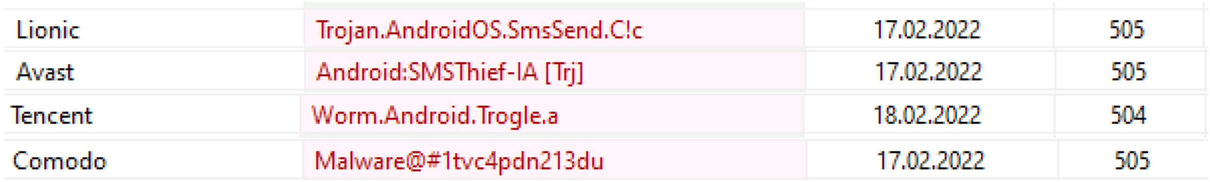
engine (64/64)	score (32/64)	date (dd.mm.yyyy)	age (days)
Bkav	clean	17.02.2022	505
Lionic	Trojan.AndroidOS.SmsSend.C!c	17.02.2022	505
MicroWorld-eScan	clean	17.02.2022	505
FireEye	clean	17.02.2022	505
CAT-QuickHeal	Android.Trogle.A	17.02.2022	505
ALYac	clean	17.02.2022	505
Malwarebytes	clean	17.02.2022	505
Zillya	clean	17.02.2022	505
Sangfor	clean	24.12.2021	560
Trustlook	Android.Malware.Trojan	18.02.2022	504
Alibaba	Trojan:Android/Trogle.130d1624	27.05.2019	1502
K7GW	Trojan (0049fd671)	17.02.2022	505
K7AntiVirus	clean	17.02.2022	505
BitDefenderTheta	clean	17.02.2022	505
VirIT	Android.Trj.SmsBot.FQ	17.02.2022	505
Cyren	AndroidOS/Trogle.A.gen!Eldorado	17.02.2022	505
SymantecMobileInsight	Trojan:Trogle	08.02.2022	514
Symantec	Android.Trogle	17.02.2022	505
ESET-NOD32	a variant of Android/Trogle.A	17.02.2022	505
Baidu	clean	18.03.2019	1572
TrendMicro-HouseCall	clean	17.02.2022	505
Avast	Android:SMSThief-IA [Trj]	17.02.2022	505
ClamAV	clean	17.02.2022	505
Kaspersky	UDS:DangerousObject.Multi.Generic	17.02.2022	505
BitDefender	clean	17.02.2022	505
NANO-Antivirus	Trojan.Android.Trogle.dinjhz	17.02.2022	505


pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [c:\users\namit\com.unknown.apk]
file
settings
about
c:\users\namit\com.unknown.apk
indicators (virustotal > score)
footprints (3)
virustotal (32/64)
strings (46094)
2 items
1 item selected 1.49 MB
Windows 11 Pro
Evaluation copy. Build 22598.ni_release.220408-1503
ENG
IN
03:49
07-07-2023

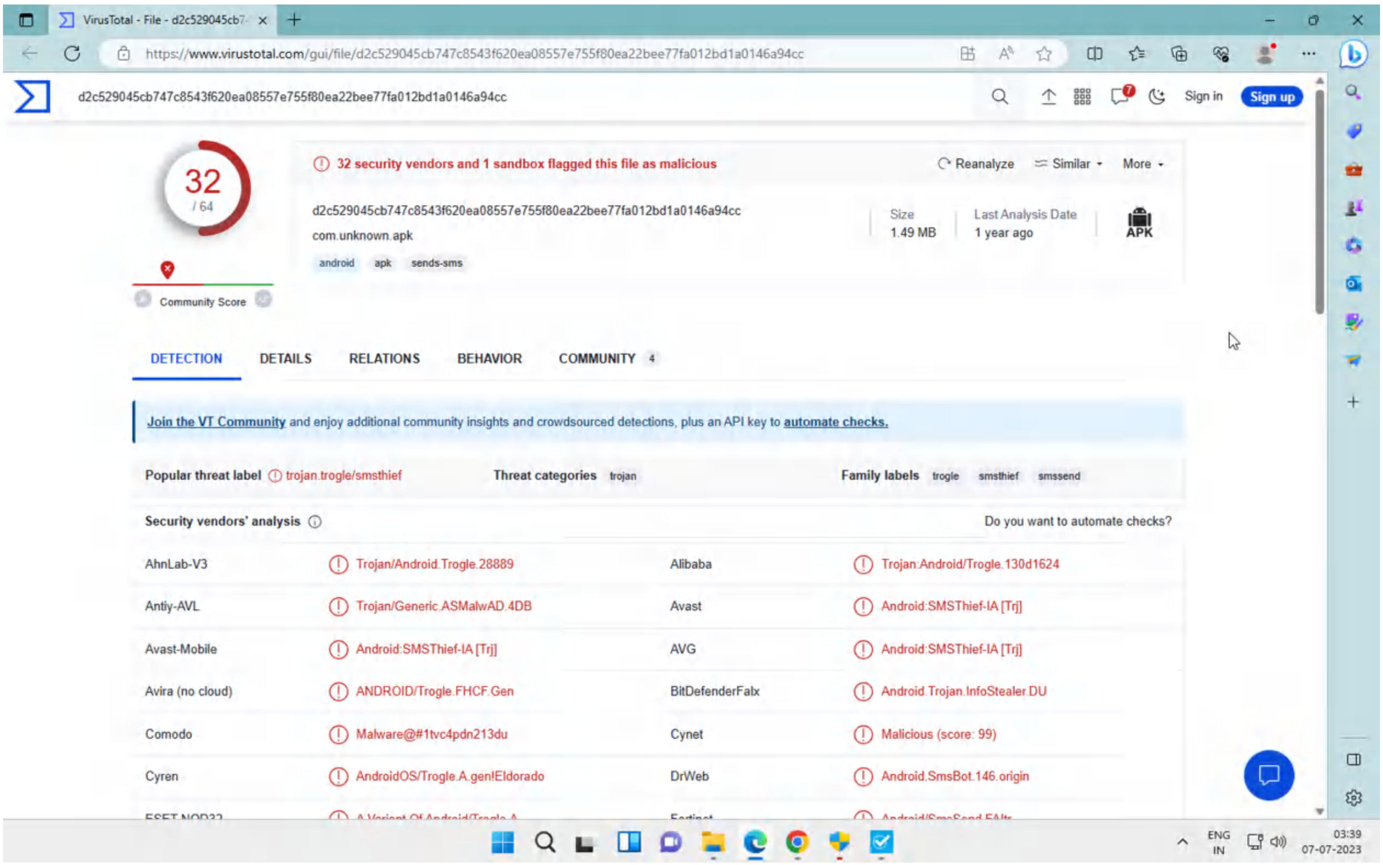
engine (64/64)	score (32/64)	date (dd.mm.yyyy)	age (days)
Avast	Android:SMSThief-IA [Trj]	17.02.2022	505
ClamAV	clean	17.02.2022	505
Kaspersky	UDS:DangerousObject.Multi.Generic	17.02.2022	505
BitDefender	clean	17.02.2022	505
NANO-Antivirus	Trojan.Android.Trogle.dinjhz	17.02.2022	505
SUPERAntiSpyware	clean	12.02.2022	510
Tencent	Worm.Android.Trogle.a	18.02.2022	504
Ad-Aware	clean	17.02.2022	505
TACHYON	clean	17.02.2022	505
Emsisoft	clean	17.02.2022	505
Comodo	Malware@#1tvc4pdn213du	17.02.2022	505
F-Secure	clean	17.02.2022	505
DrWeb	Android.SmsBot.146.origin	17.02.2022	505
VIPRE	clean	19.01.2022	534
TrendMicro	clean	17.02.2022	505
McAfee-GW-Edition	Artemis!Trojan	17.02.2022	505
CMC	clean	26.10.2021	619
Sophos	Andr/SmsSend-FA	17.02.2022	505
Avast-Mobile	Android:SMSThief-IA [Trj]	17.02.2022	505
Jiangmin	clean	17.02.2022	505
Avira	ANDROID/Trogle.FHCF.Gen	17.02.2022	505
Antiy-AVL	Trojan/Generic.ASMalwAD.4DB	17.02.2022	505
Kingsoft	Android.Troj.XXshenqi.b.(kcloud)	18.02.2022	504
Microsoft	Trojan:Script/Wacatac.B!ml	17.02.2022	505
Gridinsoft	clean	17.02.2022	505
Arcabit	clean	17.02.2022	505

sha256: D2C529045CB747C8543F620EA08557E755F80EA22BEE77FA012BD1A0146A94CC

7. LookUp The Viruses Online.



Lionic	Trojan.AndroidOS.SmsSend.C!c	17.02.2022	505
Avast	Android:SMSThief-IA [Trj]	17.02.2022	505
Tencent	Worm.Android.Trogle.a	18.02.2022	504
Comodo	Malware@#1tvc4pdn213du	17.02.2022	505



VirusTotal - File - d2c529045cb7
https://www.virustotal.com/gui/file/d2c529045cb747c8543f620ea08557e755f80ea22bee77fa012bd1a0146a94cc
d2c529045cb747c8543f620ea08557e755f80ea22bee77fa012bd1a0146a94cc
Sign in
Sign up
Reanalyze
Similar
More
Community Score
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 4
APK
ENG IN
03:39
07-07-2023

32 / 64

32 security vendors and 1 sandbox flagged this file as malicious

d2c529045cb747c8543f620ea08557e755f80ea22bee77fa012bd1a0146a94cc
com.unknown.apk
android apk sends-sms

Size 1.49 MB

Last Analysis Date 1 year ago

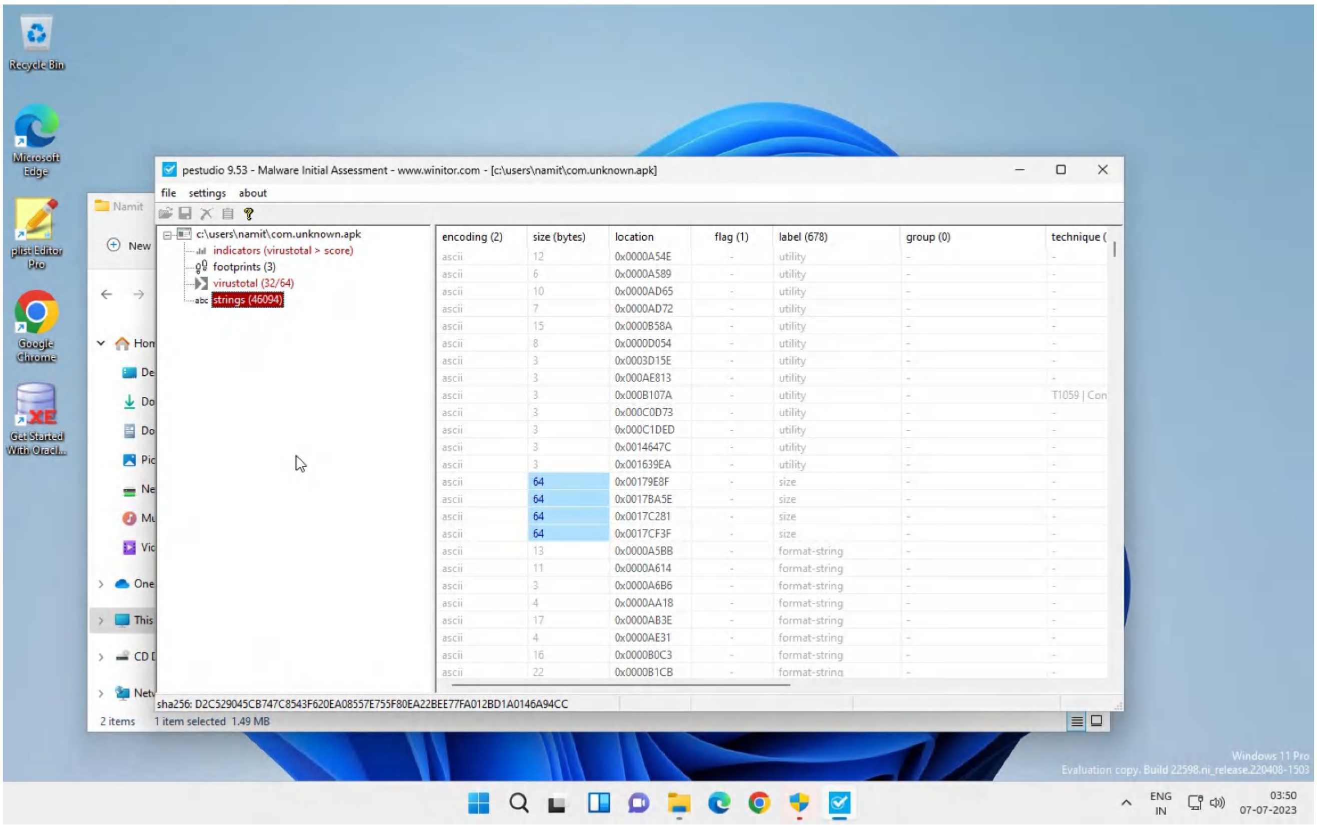
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.trogle/smsthief Threat categories trojan Family labels trogle smsthief smssend

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Android.Trogle.28889	Alibaba	Trojan:Android/Trogle.130d1624
Antiy-AVL	Trojan/Generic.ASMalwAD.4DB	Avast	Android:SMSThief-IA [Trj]
Avast-Mobile	Android:SMSThief-IA [Trj]	AVG	Android:SMSThief-IA [Trj]
Avira (no cloud)	ANDROID/Trogle.FHCF.Gen	BitDefenderFalx	Android.Trojan.InfoStealer.DU
Comodo	Malware@#1tvc4pdn213du	Cynet	Malicious (score: 99)
Cyren	AndroidOS/Trogle.A.gen!Eldorado	DrWeb	Android.SmsBot.146.origin

8. The Strings Section shows the actual contents of the file.



pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [c:\users\namit\com.unknown.apk]

c:\users\namit\com.unknown.apk
- indicators (virustotal > score)
- footprints (3)
- virustotal (32/64)
- strings (46094)

encoding (2)	size (bytes)	location	flag (1)	label (678)	group (0)	technique (
ascii	12	0x0000A54E	-	utility	-	-
ascii	6	0x0000A589	-	utility	-	-
ascii	10	0x0000AD65	-	utility	-	-
ascii	7	0x0000AD72	-	utility	-	-
ascii	15	0x0000B58A	-	utility	-	-
ascii	8	0x0000D054	-	utility	-	-
ascii	3	0x0003D15E	-	utility	-	-
ascii	3	0x000AE813	-	utility	-	-
ascii	3	0x000B107A	-	utility	-	T1059 | Con
ascii	3	0x000C0D73	-	utility	-	-
ascii	3	0x000C1DED	-	utility	-	-
ascii	3	0x0014647C	-	utility	-	-
ascii	3	0x001639EA	-	utility	-	-
ascii	64	0x00179E8F	-	size	-	-
ascii	64	0x0017BA5E	-	size	-	-
ascii	64	0x0017C281	-	size	-	-
ascii	64	0x0017CF3F	-	size	-	-
ascii	13	0x0000A5BB	-	format-string	-	-
ascii	11	0x0000A614	-	format-string	-	-
ascii	3	0x0000A6B6	-	format-string	-	-
ascii	4	0x0000AA18	-	format-string	-	-
ascii	17	0x0000AB3E	-	format-string	-	-
ascii	4	0x0000AE31	-	format-string	-	-
ascii	16	0x0000B0C3	-	format-string	-	-
ascii	22	0x0000B1CB	-	format-string	-	-

sha256: D2C529045CB747C8543F620EA08557E755F80EA22BEE77FA012BD1A0146A94CC

1 item selected 1.49 MB

IV. OBSERVATIONS:

a.)

1. Indicators like

   a. File> extension (Ransomware>Wiper)>count 17 is a level 1 threat thus it is confident malicious indicator.
   b. Strings>flags 8 ,level 1 threat thus it is a confident malicious indicator.
   c. Other indicators like file size etc are level 3 threats thus they are not confident malicious indicators

b.)

2. File is flagged as a Trojan (an application that poses to be useful but will actually harm the system) by Lionic, Avast etc.
3. It is flagged as a Worm by Tencent
4. It is flagged as a malware by Comodo
5. The age of all these rating is <360 i.e., these scans were done not more than a year ago.

V. INFERENCES:

1. The given “container.apk” file is not safe as it has some confident malicious indicators like extensions and flags.

2. It is also marked malicious by famous Antivirus Softwares like Avast, Quick Heal etc.

3. It is flagged as Trojan,Worm and Malware by these antivruses in the VirusTotal list.

EXERCISE 3-B-1: Web Application Attacks

I. **AIM:** Analyse the website www.megacorp.one using Firefox (browser) developer tools in Kali Linux.

II. TOOLS REQUIRED:

1. Products: developer tools in Kali Linux
2. Internet browser: Firefox
3. Manufacturer: various

III. STEP BY STEP PROCEDURE:

1. Web applications can be written in a variety of programming languages and frameworks, each of which can introduce specific types of vulnerabilities. However, the most common vulnerabilities are similar in concept, regardless of the underlying technology stack.

2. We will discuss web application vulnerability enumeration and exploitation. Although the complexity of vulnerabilities and attacks vary, we will demonstrate the exploitation of several common web application vulnerabilities listed in the OWASP Top 10 list.237 These attack vectors will serve as the basic building blocks used to construct more advanced attacks.

3. As a first step, we should gather information about the application. What does the application do? What language is it written in? What server software is the application running on? The answers to these and other basic questions will help guide us towards our first (or next) potential attack vector. As with many penetration testing disciplines, the goal of each attempted attack or exploit is to increase our permissions within the application or pivot to another application or target.

4. Each successful exploit along the way may grant access to new functionality or components within the application. We may need to successfully execute several exploits to advance from an unauthenticated user account access to any kind of shell on the system. Enumeration of new functionality is important each step of the way especially since attacks that previously failed may succeed in a new context. As penetration testers, we must continue to enumerate and adapt until we've exhausted all attack avenues or compromised the system.

5. It is important to identify the components that make up a web application before attempting to blindly exploit it. Many web application vulnerabilities are technology-agnostic.

6. Exploits and payloads need to be crafted based on the technological underpinnings of the application, such as the database software or operating system. Before launching any attacks on a web application, we should attempt to discover the technology stack in use, which generally consists of the following components:

   - Programming language and frameworks
   - Web server software
   - Database software
   - Server operating system

7. Firefox since it is the default browser in Kali Linux for in **inspecting urls**, File extensions, which are sometimes a part of a URL, can reveal the programming language the application was written in. Some of these, like .php, are straightforward, but other extensions are more cryptic and vary based on the frameworks in use. For example, a Java-based web application might use .jsp, .do, or .html.

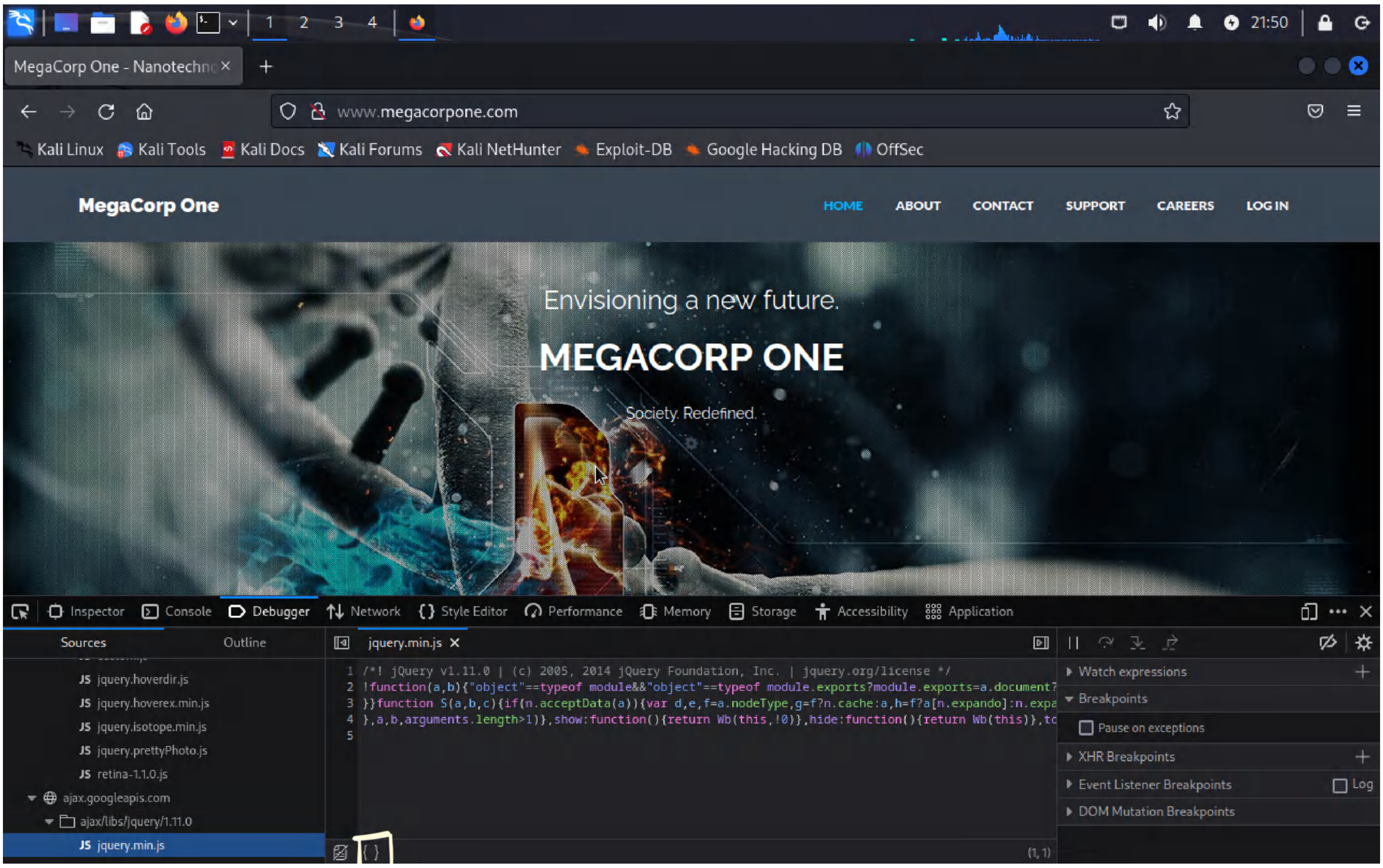
8. File extensions on web pages are becoming less common since many languages and frameworks now support the concept of routes, which allow developers to map a URI to a section of code. Applications leveraging routes use logic to determine what content is returned to the user and make URI extensions largely irrelevant.

9. Although **Inspecting Page Content** by URL inspection can provide some clues about the target web application, most context clues can be found in the source of the web page. The Firefox Debugger tool (found in the Web Developer menu or by pressing C B k) displays the page's resources and content, which varies by application. The Debugger tool may display JavaScript frameworks, hidden input fields, comments, client-side controls within HTML, JavaScript, and much more.

IV. OBSERVATIONS:

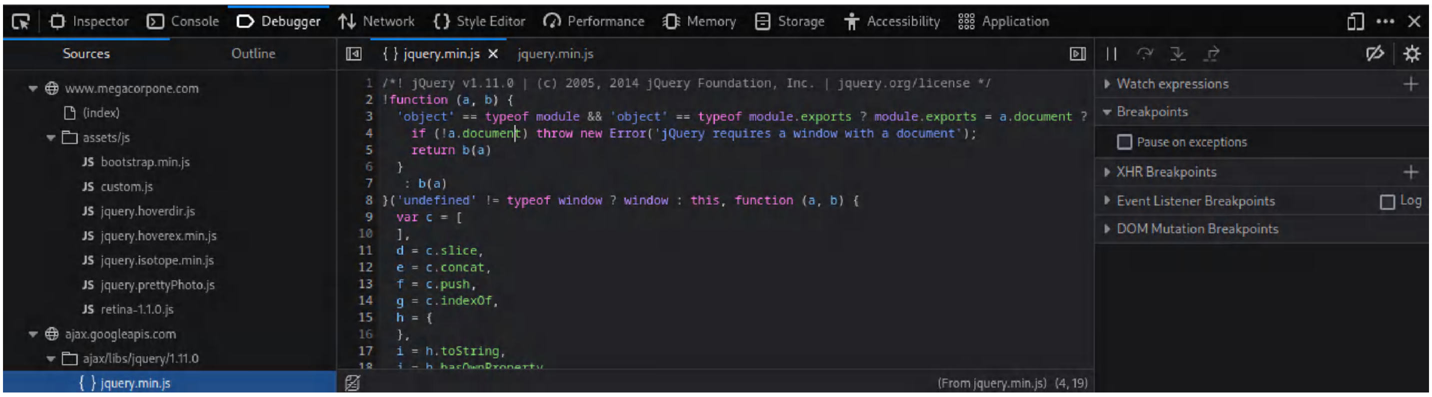
10. We can see that the application running on www.megacorpone.com uses jQuery238 version 1.11.0, a common JavaScript library. In this case, the developer minified239 the code, making it more compact and conserving resources but making it somewhat difficult to read.

Fortunately, we can “prettify” code within Firefox by clicking on the Pretty print source button with the double curly braces:



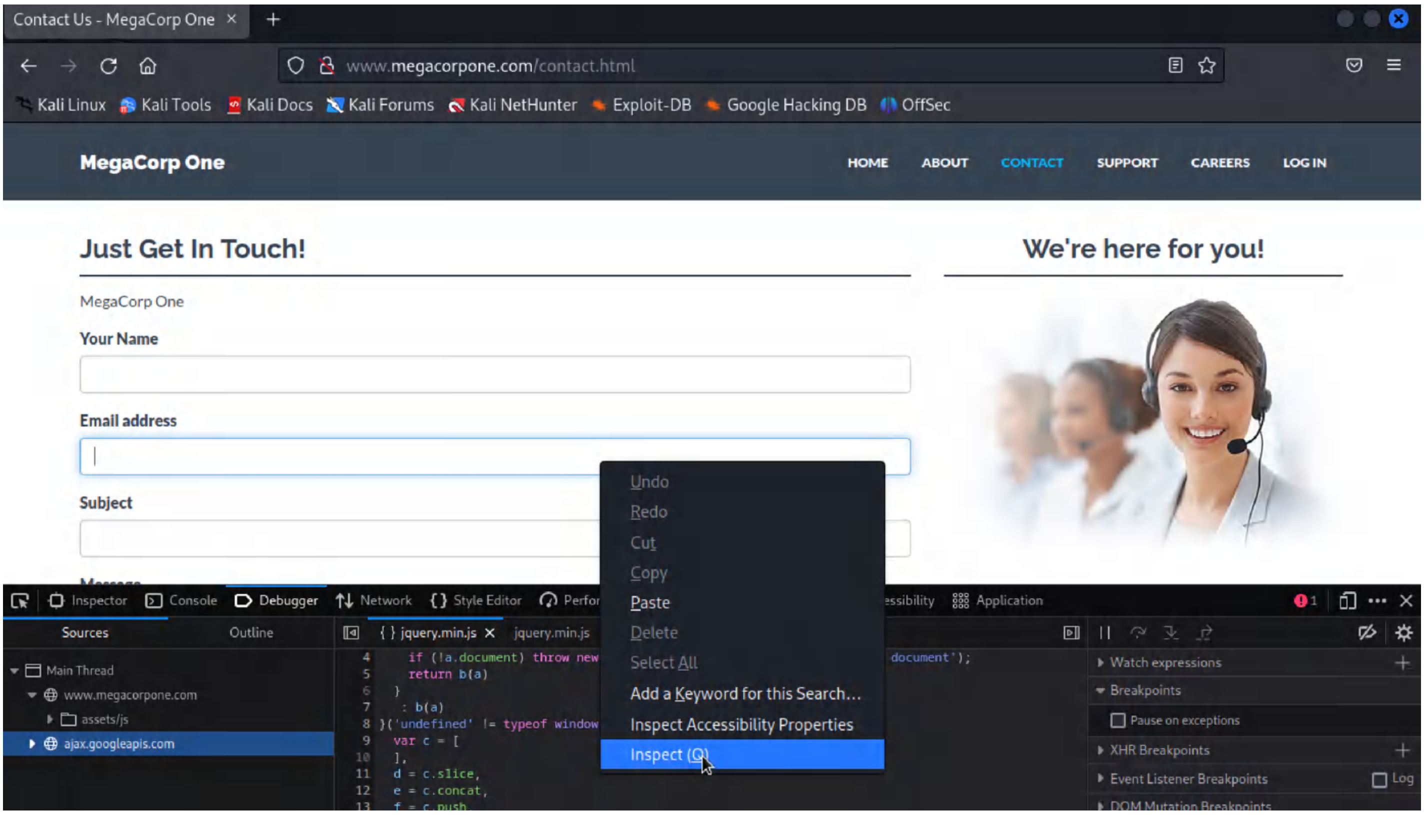
```
/*! jQuery v1.11.0 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?
}}function S(a,b,c){if(n.acceptData(a)){var d,e,f=a.nodeType,g=f?n.cache:a,h=f?a[n.expando]:n.expa
},a,b,arguments.length>1)},show:function(){return Wb(this,!0)},hide:function(){return Wb(this)},tc
```

11. After clicking the icon, Firefox will display the code in a format that is easier to read and follow:



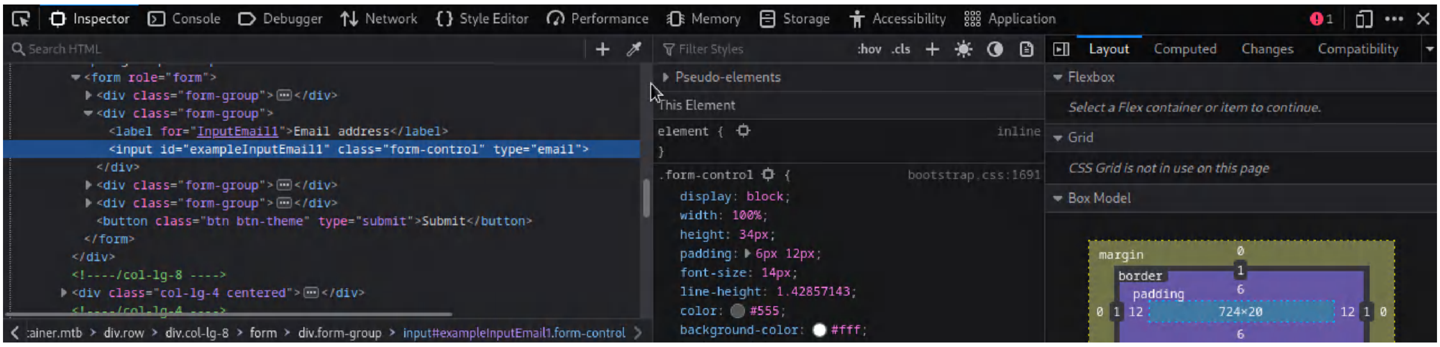
```
/*! jQuery v1.11.0 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */
!function (a, b) {
  'object' == typeof module && 'object' == typeof module.exports ? module.exports = a.document ?
    if (!a.document) throw new Error('jQuery requires a window with a document');
    return b(a)
  }
   : b(a)
}('undefined' != typeof window ? window : this, function (a, b) {
  var c = [
  ],
  d = c.slice,
  e = c.concat,
  f = c.push,
  g = c.indexOf,
  h = {
  },
  i = h.toString,
  j = h.hasOwnProperty
```

12. We can also use the Inspector tool to drill down into specific page content. Let’s use Inspector to examine the email input element from the “Contact” page by right-clicking the email address field on the page and selecting Inspect Element or using the shortcut Page Up.



```
    if (!a.document) throw new                          document');
    return b(a)
  }
   : b(a)
}('undefined' != typeof window
  var c = [
  ],
  d = c.slice,
  e = c.concat,
  f = c.push,
```

13. This will open the Inspector tool and highlight the HTML for the element we right-clicked on.

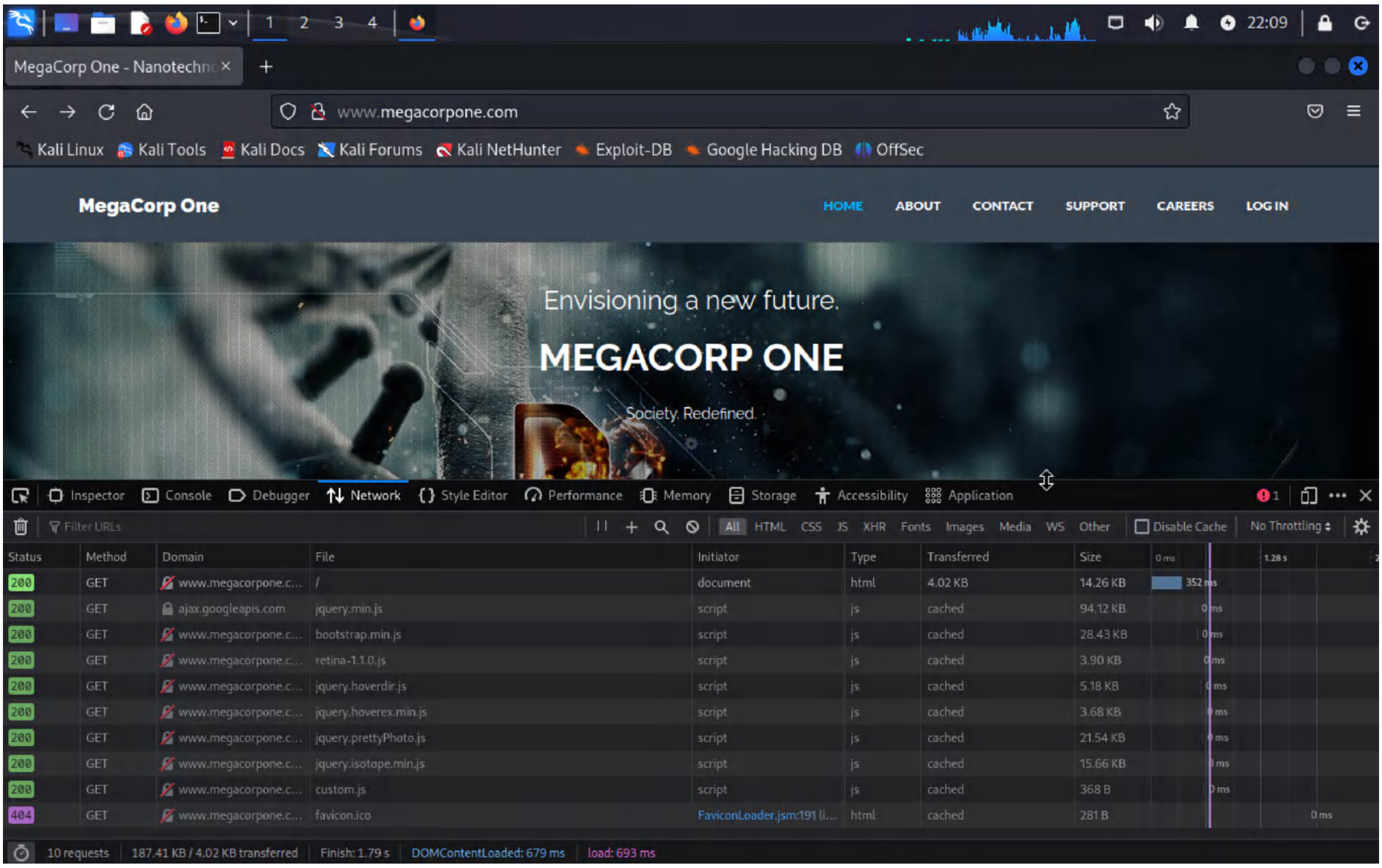


```
<form role="form">
  <div class="form-group">⋯</div>
  <div class="form-group">
    <label for="InputEmail1">Email address</label>
    <input id="exampleInputEmail1" class="form-control" type="email">
  </div>
  <div class="form-group">⋯</div>
  <div class="form-group">⋯</div>
  <button class="btn btn-theme" type="submit">Submit</button>
</form>
</div>
<!----/col-lg-8 ---->
<div class="col-lg-4 centered">⋯</div>
<!----/col-lg-4 ---->
```

```
element {                    inline
}
.form-control {              bootstrap.css:1691
  display: block;
  width: 100%;
  height: 34px;
  padding: 6px 12px;
  font-size: 14px;
  line-height: 1.42857143;
  color: #555;
  background-color: #fff;
```

This tool is especially useful for quickly finding hidden form fields in the HTMLsource.

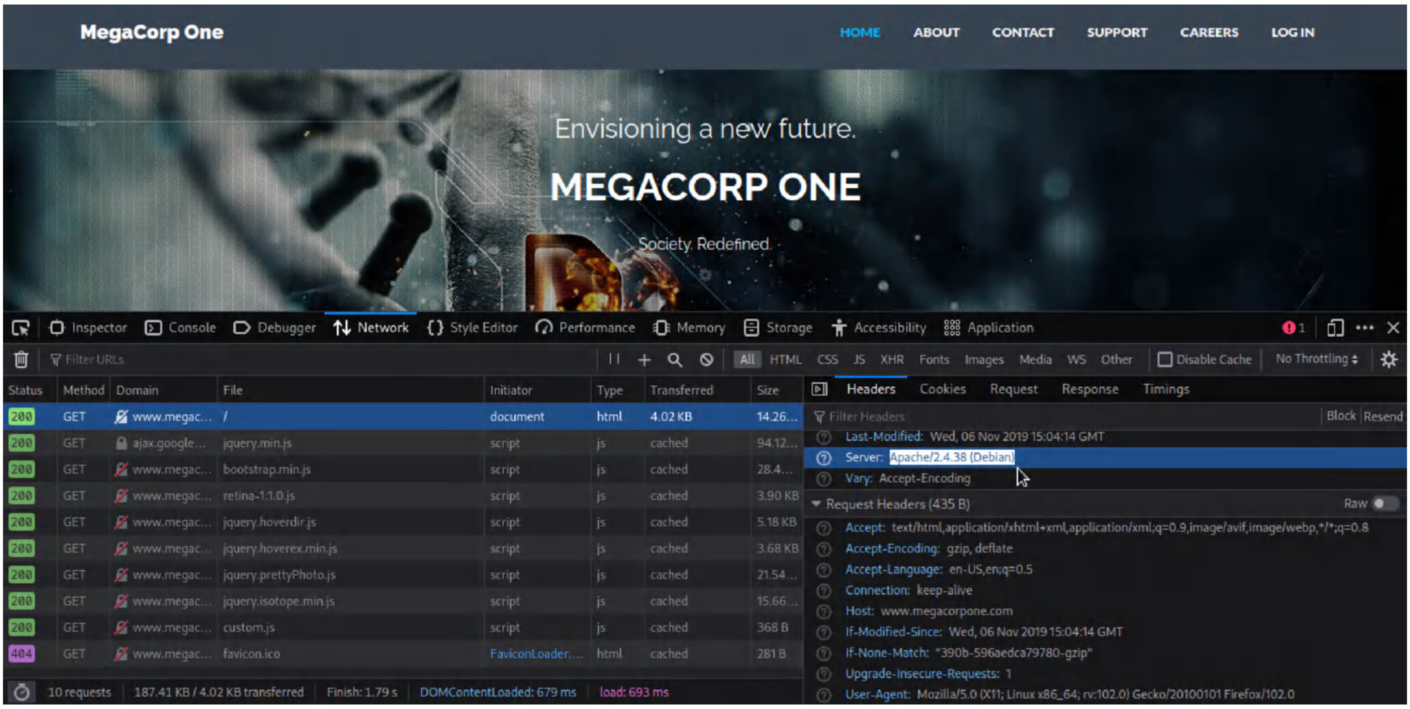
14. **Viewing Response Headers** - We can also search server responses for additional information. There are two types of tools we can use to accomplish this task. The first type of tool is a proxy, which intercepts requests and responses between a client and a webserver. We will explore proxies later in this module, but first we will explore the Network tool, launched from the Firefox Web Developer menu, to view HTTP requests and responses. This tool shows network activity that occurs after it launches, so we must refresh the page to see traffic.



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.megacorpone.c...	/	document	html	4.02 KB	14.26 KB
200	GET	ajax.googleapis.com	jquery.min.js	script	js	cached	94.12 KB
200	GET	www.megacorpone.c...	bootstrap.min.js	script	js	cached	28.43 KB
200	GET	www.megacorpone.c...	retina-1.1.0.js	script	js	cached	3.90 KB
200	GET	www.megacorpone.c...	jquery.hoverdir.js	script	js	cached	5.18 KB
200	GET	www.megacorpone.c...	jquery.hoverex.min.js	script	js	cached	3.68 KB
200	GET	www.megacorpone.c...	jquery.prettyPhoto.js	script	js	cached	21.54 KB
200	GET	www.megacorpone.c...	jquery.isotope.min.js	script	js	cached	15.66 KB
200	GET	www.megacorpone.c...	custom.js	script	js	cached	368 B
404	GET	www.megacorpone.c...	favicon.ico	FaviconLoader.jsm:191 (i...	html	cached	281 B

10 requests | 187.41 KB / 4.02 KB transferred | Finish: 1.79 s | DOMContentLoaded: 679 ms | load: 693 ms

We can click on a request to get more details about it, in this case the response headers:



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.megac...	/	document	html	4.02 KB	14.26...
200	GET	ajax.google...	jquery.min.js	script	js	cached	94.12...
200	GET	www.megac...	bootstrap.min.js	script	js	cached	28.4...
200	GET	www.megac...	retina-1.1.0.js	script	js	cached	3.90 KB
200	GET	www.megac...	jquery.hoverdir.js	script	js	cached	5.18 KB
200	GET	www.megac...	jquery.hoverex.min.js	script	js	cached	3.68 KB
200	GET	www.megac...	jquery.prettyPhoto.js	script	js	cached	21.54...
200	GET	www.megac...	jquery.isotope.min.js	script	js	cached	15.66...
200	GET	www.megac...	custom.js	script	js	cached	368 B
404	GET	www.megac...	favicon.ico	FaviconLoader....	html	cached	281 B

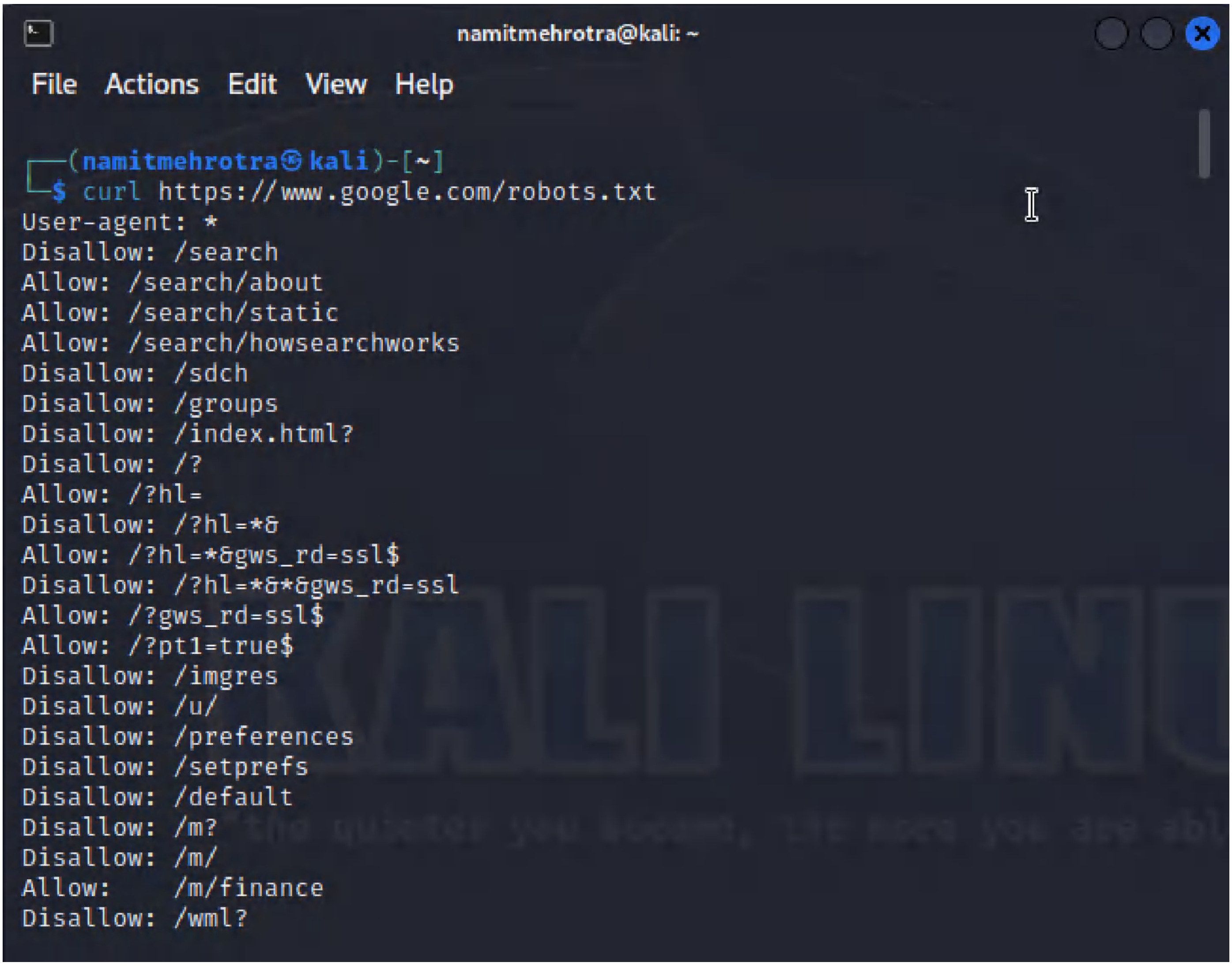
10 requests | 187.41 KB / 4.02 KB transferred | Finish: 1.79 s | DOMContentLoaded: 679 ms | load: 693 ms

```
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
Server: Apache/2.4.38 (Debian)
Vary: Accept-Encoding
Request Headers (435 B)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Host: www.megacorpone.com
If-Modified-Since: Wed, 06 Nov 2019 15:04:14 GMT
If-None-Match: "390b-596aedca79780-gzip"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
```

The “Server” header displayed above will often reveal at least the name of the web server software. In many default configurations, it also reveals the version number. Headers that start with “X-” are non-standard HTTP headers.240 The names or values often reveal additional information about the technology stack used by the application. Some examples of nonstandard headers include X-Powered-By, x-amz-cf-id, and X-Aspnet-Version. Further research into these names could reveal additional information, such as the “x-amz-cf-id” header, which indicates the application uses Amazon CloudFront.

15. **Inspecting Sitemaps** -Web applications can include sitemap files to help search engine bots crawl and index their sites. These files also include directives of which URLs not to crawl. These are usually sensitive pages or administrative consoles–exactly the sort of pages we are interested in.
16. The two most common sitemap filenames are robots.txt and sitemap.xml.

For example, we can retrieve the robots.txt file from www.google.com with curl:



```
┌──(namitmehrotra㉿kali)-[~]
└─$ curl https://www.google.com/robots.txt
User-agent: *
Disallow: /search
Allow: /search/about
Allow: /search/static
Allow: /search/howsearchworks
Disallow: /sdch
Disallow: /groups
Disallow: /index.html?
Disallow: /?
Allow: /?hl=
Disallow: /?hl=*&
Allow: /?hl=*&gws_rd=ssl$
Disallow: /?hl=*&*&gws_rd=ssl
Allow: /?gws_rd=ssl$
Allow: /?pt1=true$
Disallow: /imgres
Disallow: /u/
Disallow: /preferences
Disallow: /setprefs
Disallow: /default
Disallow: /m?
Disallow: /m/
Allow:    /m/finance
Disallow: /wml?
```

Allow and Disallow are directives for web crawlers indicating pages or directories that “polite” web crawlers may or may not access, respectively. Although the listed pages and directories in most cases may not be interesting and some may even be invalid, sitemap files should not be overlooked as they may contain clues about the website layout or other interesting information.

17. **Locating Administration Consoles**- Web servers often ship with remote administration web applications, or consoles, which are accessible via a particular URL and often listening on a specific TCP port.
Two common examples are the manager241 application for Tomcat and phpMyAdmin242 for MySQL hosted at /manager/html and /phpmyadmin respectively.

While these consoles can be restricted to local access or may be hosted on custom TCP ports, we often find them externally exposed by default configurations. Regardless, as penetration testers we should check the default console locations, identified in the application server software documentation. In the following section, we will also demonstrate tools that can be used to automate the search for these consoles and in a later section we will demonstrate exploitation techniques.

V. INFERENCES:

1. Based on the experiment conducted to analyze the website www.megacorp.one using Firefox developer tools in Kali Linux, several inferences can be drawn.

2. Firstly, the utilization of Firefox developer tools in Kali Linux allowed for comprehensive inspection and examination of the website's underlying code, network traffic, and performance metrics.

3. This provided valuable insights into the website's structure, potential vulnerabilities, and overall functionality. Furthermore, the experiment likely enabled the identification of any errors, bugs, or security loopholes present in the website, contributing to the enhancement of its overall security and user experience.

4. The combination of Firefox developer tools and Kali Linux proved to be a powerful combination for proficiently dissecting and understanding the technical aspects of the website www.megacorp.one.

EXERCISE 3-B-2: Web Application Assessment Tools using DIRB tool

I. **AIM:** To implement Web Application Assessment using DIRB tool in Kali Linux. Analyse the website www.megacorp.oneusing DIRB tool in Kali Linux.

II. TOOLS REQUIRED:

1. Products: DIRB tool in Kali Linux

2. Internet browser: Firefox

3. Manufacturer: various

III. STEP BY STEP PROCEDURE:

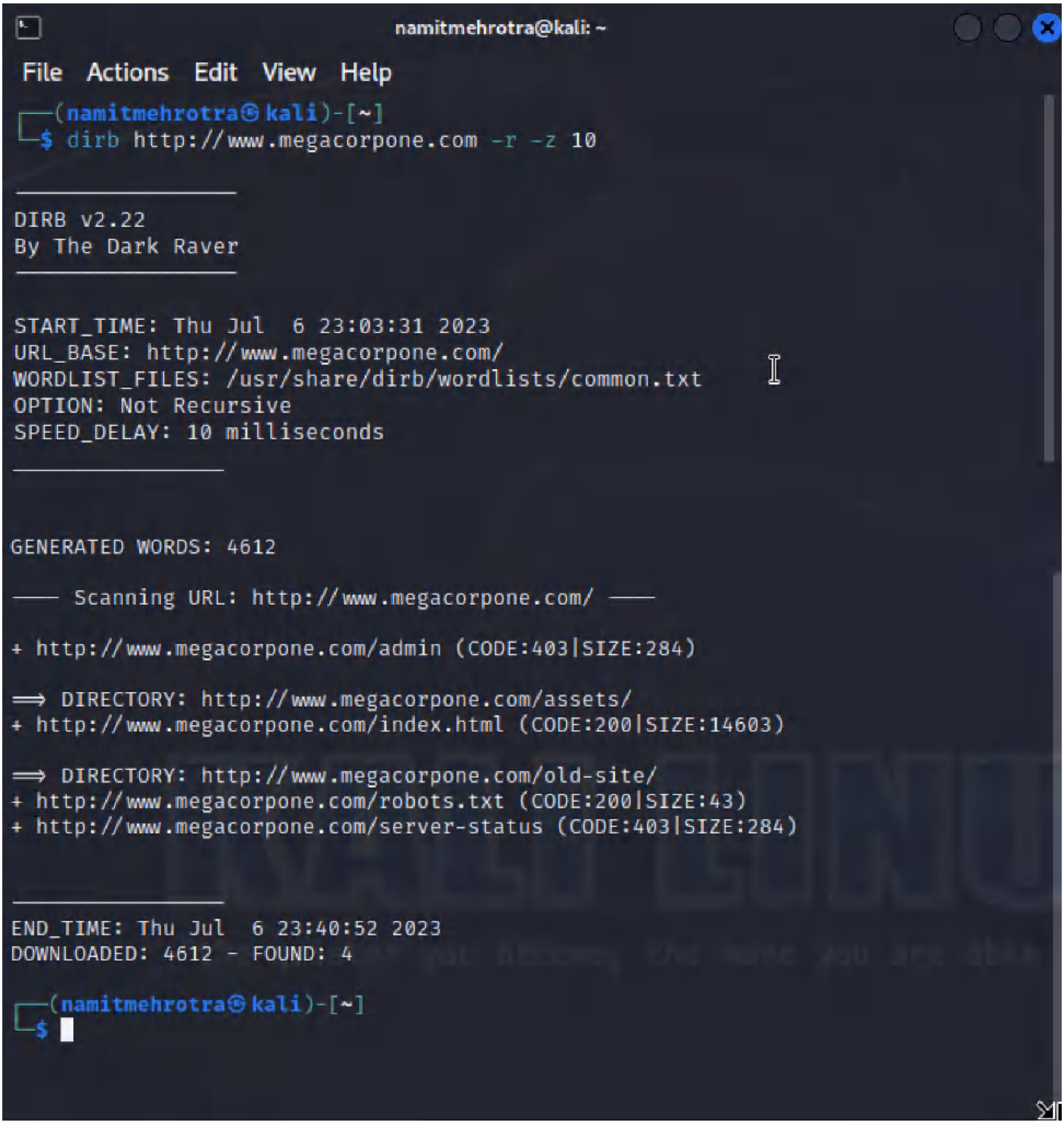
1. There are a variety of tools that can aid in discovering and exploiting web application vulnerabilities, many of which come pre-installed in Kali. In this section, we will explore some of these tools including a few simple browser extensions and in a later section we will shift our focus to manual vulnerability enumeration and exploitation.

2. DIRB243 is a web content scanner that uses a wordlist to find directories and pages by issuing requests to the server. DIRB can identify valid web pages on a web server even if the main index page is missing.

3. By default, DIRB will identify interesting directories on the server but it can also be customized to search for specific directories, use custom dictionaries, set a custom cookie or header on each request, and much more.

IV. OBSERVATIONS:

4. Let's run DIRB on www.megacorpone.com. We will supply several arguments: the URL to scan, -r to scan non-recursively, and -z 10 to add a 10 millisecond delay to each request:



```
┌──(namitmehrotra㉿kali)-[~]
└─$ dirb http://www.megacorpone.com -r -z 10

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jul  6 23:03:31 2023
URL_BASE: http://www.megacorpone.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Recursive
SPEED_DELAY: 10 milliseconds

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://www.megacorpone.com/ ----

+ http://www.megacorpone.com/admin (CODE:403|SIZE:284)

==> DIRECTORY: http://www.megacorpone.com/assets/
+ http://www.megacorpone.com/index.html (CODE:200|SIZE:14603)

==> DIRECTORY: http://www.megacorpone.com/old-site/
+ http://www.megacorpone.com/robots.txt (CODE:200|SIZE:43)
+ http://www.megacorpone.com/server-status (CODE:403|SIZE:284)


-----------------
END_TIME: Thu Jul  6 23:40:52 2023
DOWNLOADED: 4612 - FOUND: 4

┌──(namitmehrotra㉿kali)-[~]
└─$ 
```

5. According to the output in Listing 281, DIRB made 4,612 requests and reported the URL, status code, and size of nine distinct resources. By default, the tool will recurse into newly-discovered directories, but in this case, our non-recursive (-r) scan simply reports directories without descending into them. Obviously, we could begin with a non-recursive scan against a large target and recursively search interesting directories, or begin with a full recursive scan depending on our needs.

V. INFERENCES:

1. By conducting a web application assessment using the DIRB tool in Kali Linux to analyze the website www.megacorp.one, several inferences can be made.

2. Firstly, the DIRB tool's utilization allowed for the identification of hidden directories or files on the website that were not easily accessible through standard navigation.

3. This discovery could potentially reveal sensitive information or indicate poor security practices, thereby highlighting areas of concern for the website's administrators.

4. Additionally, the use of the DIRB tool enabled the detection of common web vulnerabilities, such as misconfigured or improperly protected directories, which could be exploited by malicious actors.

5. This assessment process served as an effective means of proactively identifying and addressing security weaknesses, ultimately helping to enhance the overall security posture of www.megacorp.one.

EXERCISE 3-B-3:Web Application Assessment using Burp Suite

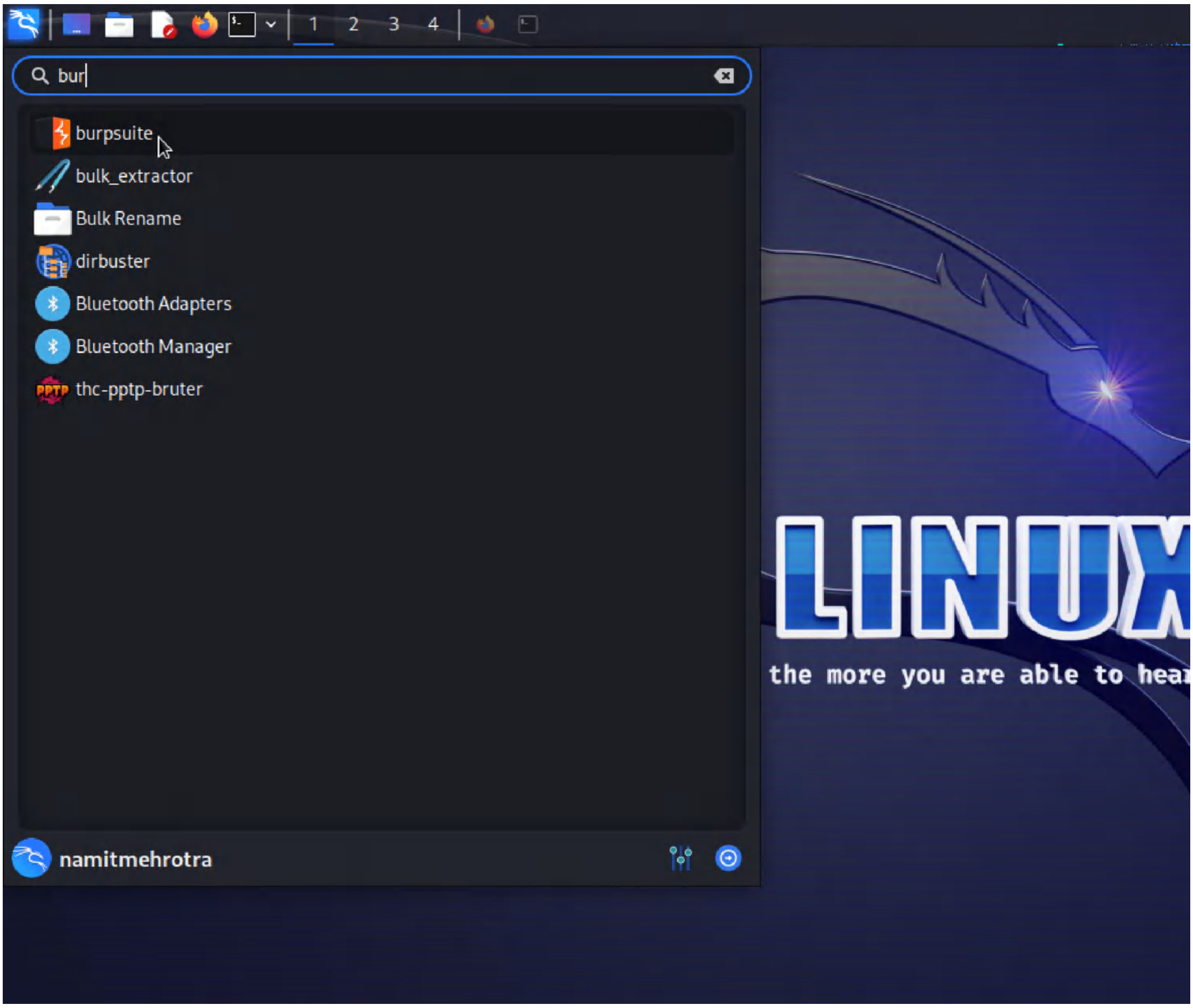
I. **AIM:** To implement the Web Application Assessment using Burp Suite in Kali Linux and Analyse the website www.megacorp.one using Burp Suite in Kali Linux.

II. TOOLS REQUIRED:

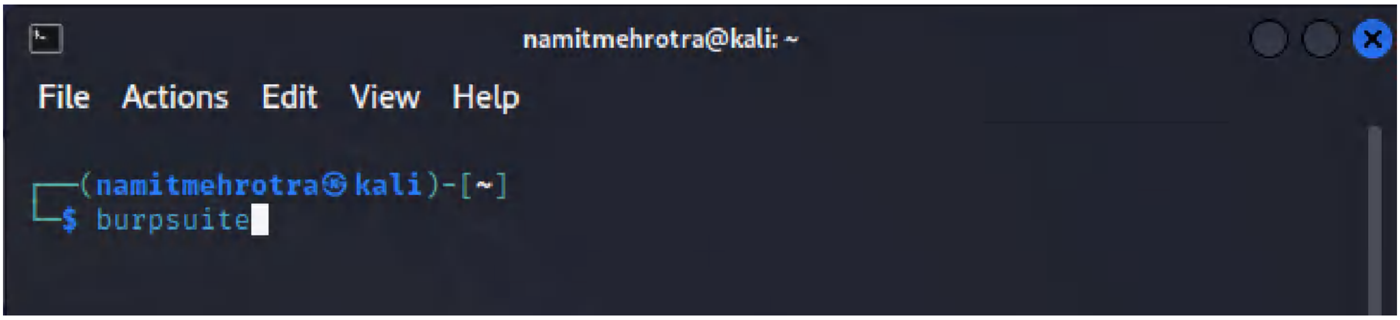
1. Products: Burpsuite tool in Kali Linux
2. Internet browser: Firefox
3. Manufacturer: various

III. STEP BY STEP PROCEDURE:

1. We can find it in Kali under Applications > 03 Web Application Analysis > burpsuite.

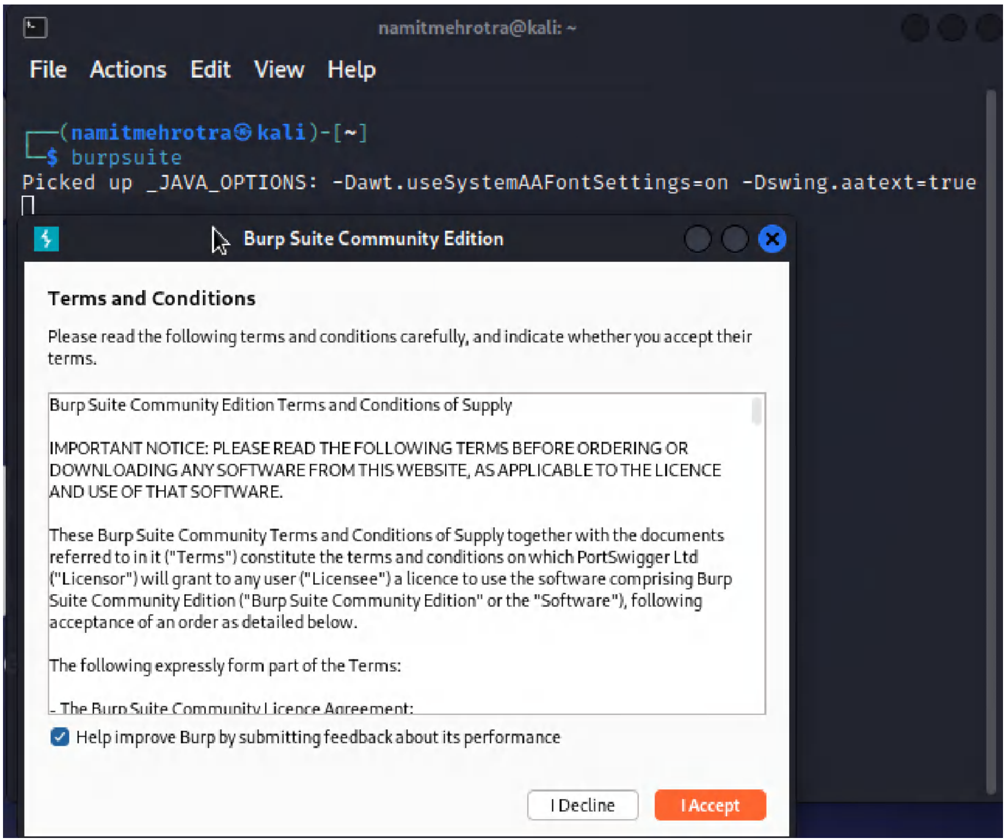


2. We can also launch it from the command line with burpsuite:



```
┌──(namitmehrotra㉿kali)-[~]
└─$ burpsuite
```

Once it launches, we'll choose Temporary project and click Next.



```
┌──(namitmehrotra㉿kali)-[~]
└─$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
```

Terms and Conditions

Please read the following terms and conditions carefully, and indicate whether you accept their terms.

Burp Suite Community Edition Terms and Conditions of Supply

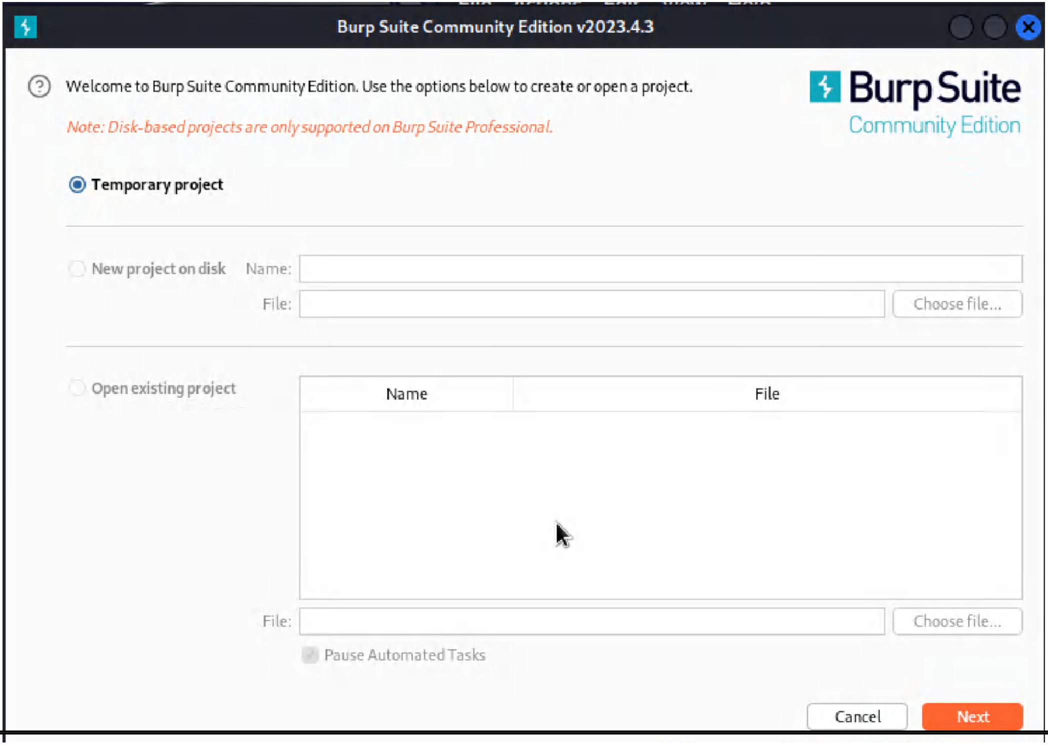
IMPORTANT NOTICE: PLEASE READ THE FOLLOWING TERMS BEFORE ORDERING OR DOWNLOADING ANY SOFTWARE FROM THIS WEBSITE, AS APPLICABLE TO THE LICENCE AND USE OF THAT SOFTWARE.

These Burp Suite Community Terms and Conditions of Supply together with the documents referred to in it ("Terms") constitute the terms and conditions on which PortSwigger Ltd ("Licensor") will grant to any user ("Licensee") a licence to use the software comprising Burp Suite Community Edition ("Burp Suite Community Edition" or the "Software"), following acceptance of an order as detailed below.

The following expressly form part of the Terms:

- The Burp Suite Community Licence Agreement;

☑ Help improve Burp by submitting feedback about its performance



Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● **Temporary project**

○ New project on disk Name:
File: Choose file...

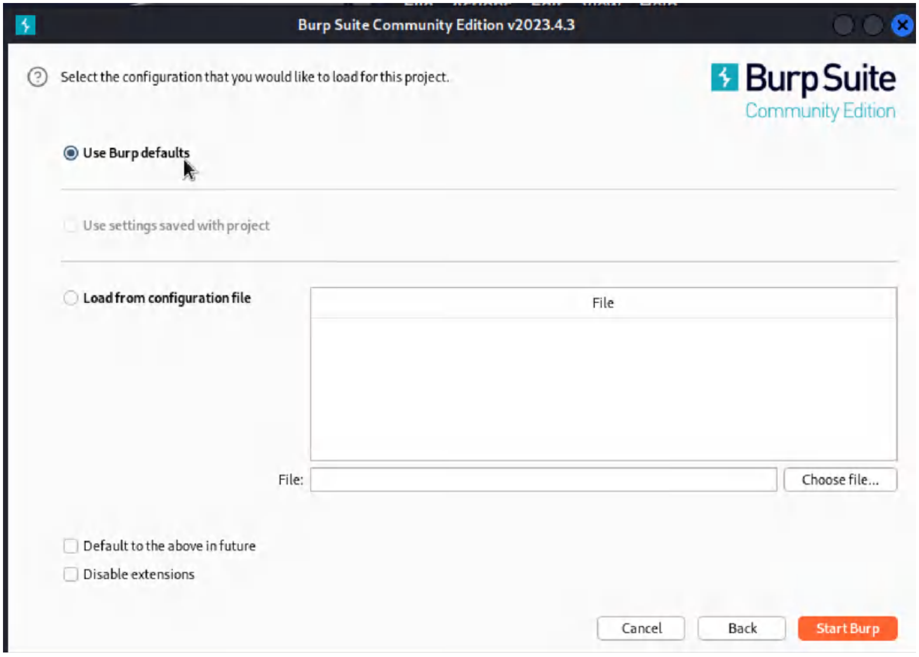
○ Open existing project

Name	File

File: Choose file...

☑ Pause Automated Tasks

3.In the next screen, choose the option to setup Burp using Burp defaults, and then press “Start Burp.



Burp Suite Community Edition v2023.4.3

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use settings saved with project

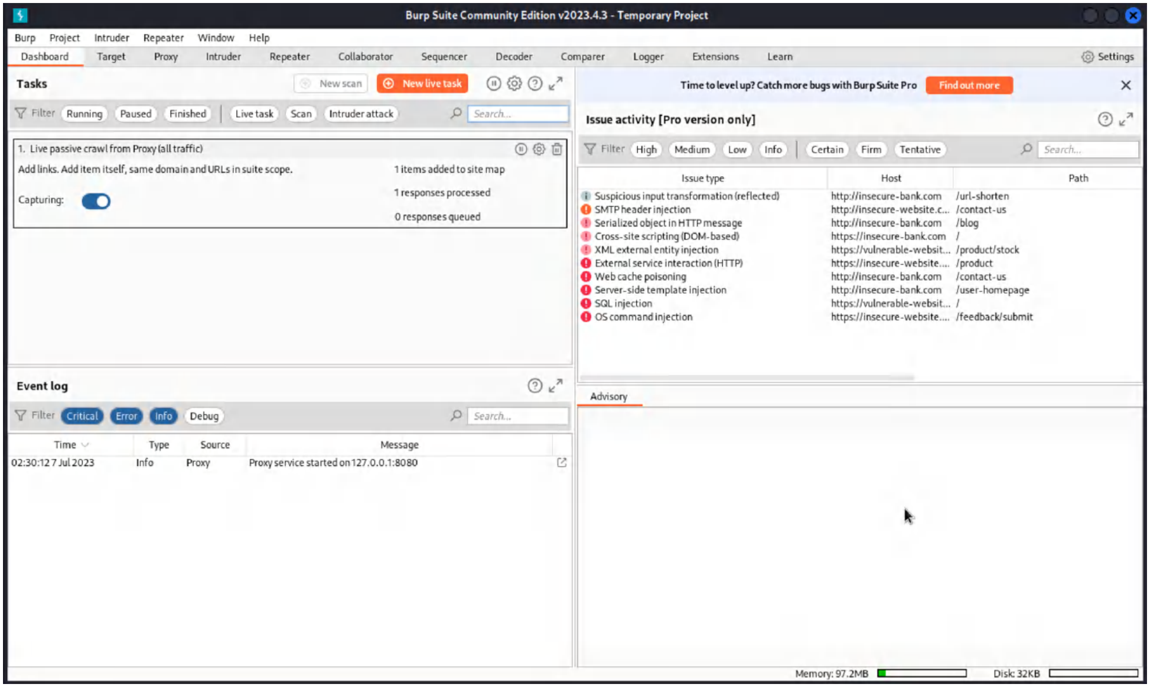
○ Load from configuration file

File:

□ Default to the above in future

□ Disable extensions

4. Once Burp Suite is opened, you will see a lot of tabs and other information. For now, all we will be worrying about is the Proxy tab, so you can navigate there now. Burp Suite recently updated to include its own built-in browser for using the local proxy with, which means we no longer must configure our browser to work with Burp manually and turn intercept mode off.



Burp Suite Community Edition v2023.4.3 - Temporary Project

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

1 items added to site map

1 responses processed

0 responses queued

Time to level up? Catch more bugs with Burp Suite Pro

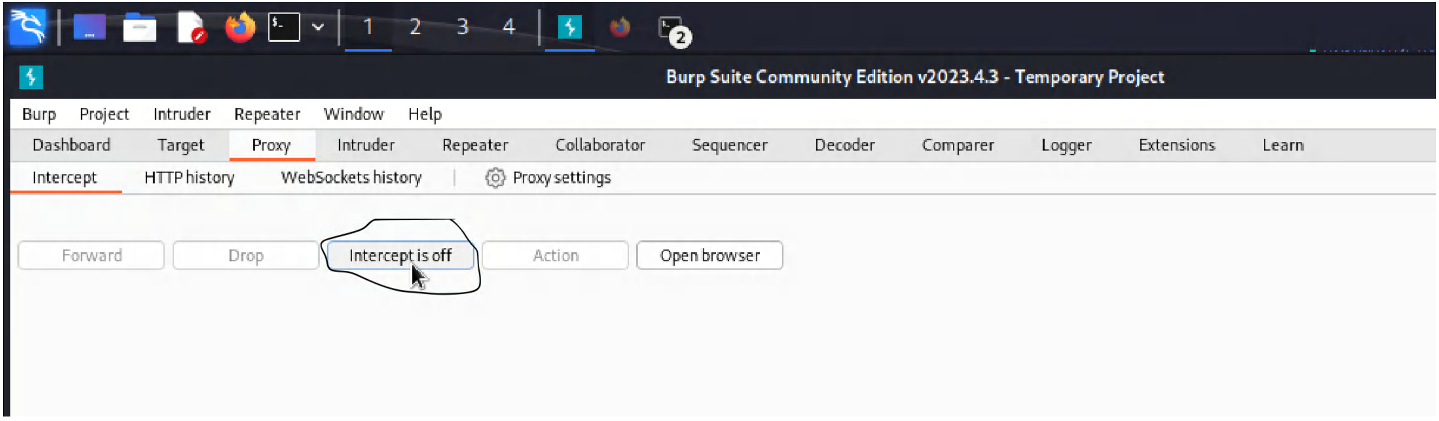
Issue activity [Pro version only]

Issue type	Host	Path
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
SMTP header injection	http://insecure-website.c...	/contact-us
Serialized object in HTTP message	http://insecure-bank.com	/blog
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-websit...	/product/stock
External service interaction (HTTP)	https://insecure-website....	/product
Web cache poisoning	http://insecure-bank.com	/contact-us
Server-side template injection	http://insecure-bank.com	/user-homepage
SQL injection	https://vulnerable-websit...	/
OS command injection	https://insecure-website....	/feedback/submit

Event log

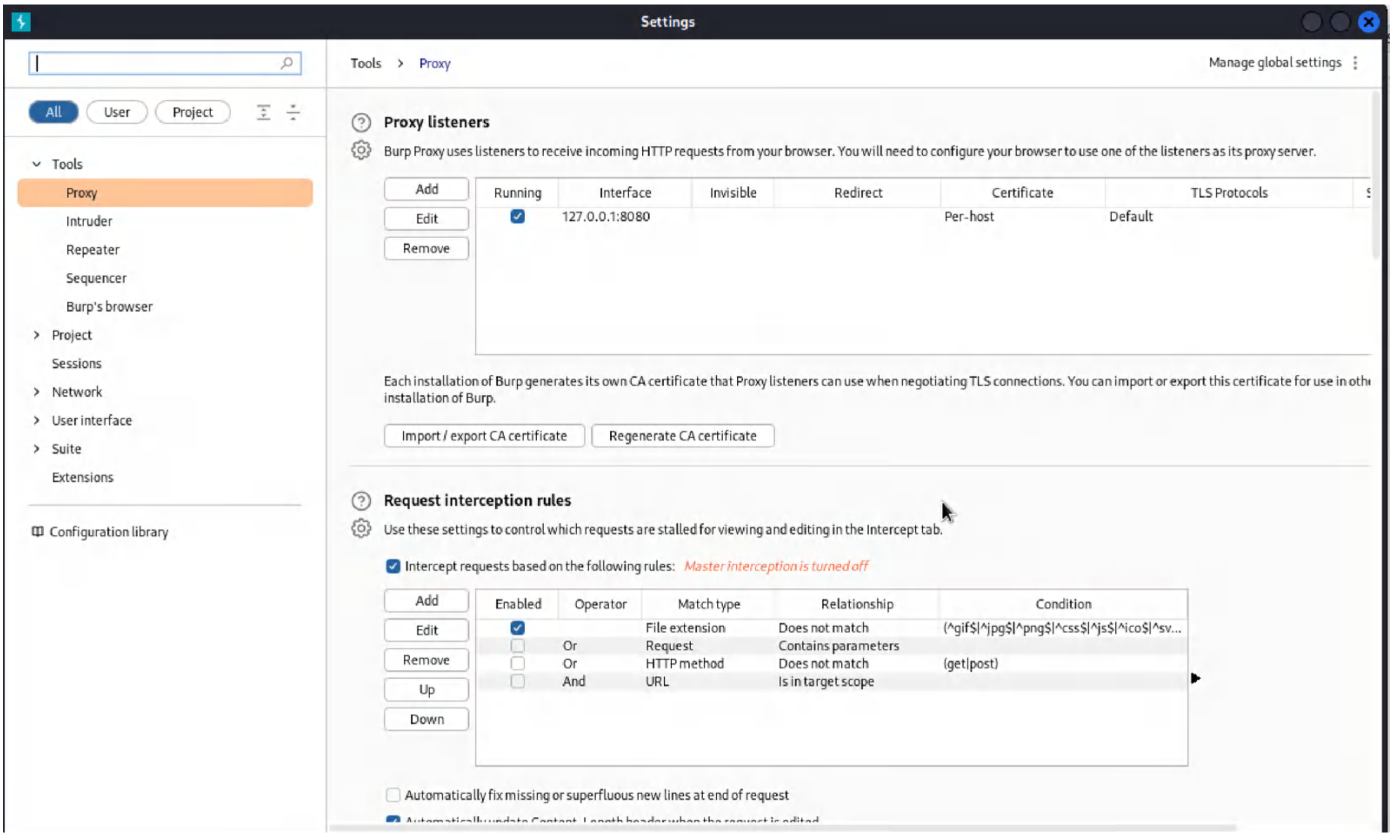
Time	Type	Source	Message
02:30:12 7 Jul 2023	Info	Proxy	Proxy service started on 127.0.0.1:8080

Memory: 97.2MB Disk: 32KB



Burp Suite Community Edition v2023.4.3 - Temporary Project

5. Next, we can review the proxy listener settings. The Options sub-tab shows what ports are listening for proxy requests.



Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in oth installation of Burp.

Request interception rules

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

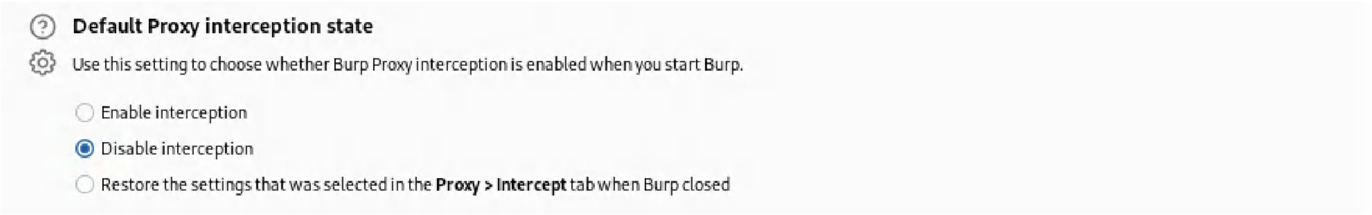
☑ Intercept requests based on the following rules: *Master interception is turned off*

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$|^sv...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

□ Automatically fix missing or superfluous new lines at end of request

☑ Automatically update Content-Length header when the request is edited

6. By default, Burp Suite enables a proxy listener on localhost:8080. This is the host and port that our browser must connect to in order to proxy traffic through Burp Suite. We will leave these default settings. The Intercept tool is enabled at start up in Burp Suite's default configuration. We can check this setting under User options > Misc > Proxy Interception. However, many users prefer to disable Intercept on startup, which can be done by selecting Always disable. Either way, we can still manually toggle Intercept on and off through Proxy > Intercept > Intercept is on/off.



Default Proxy interception state

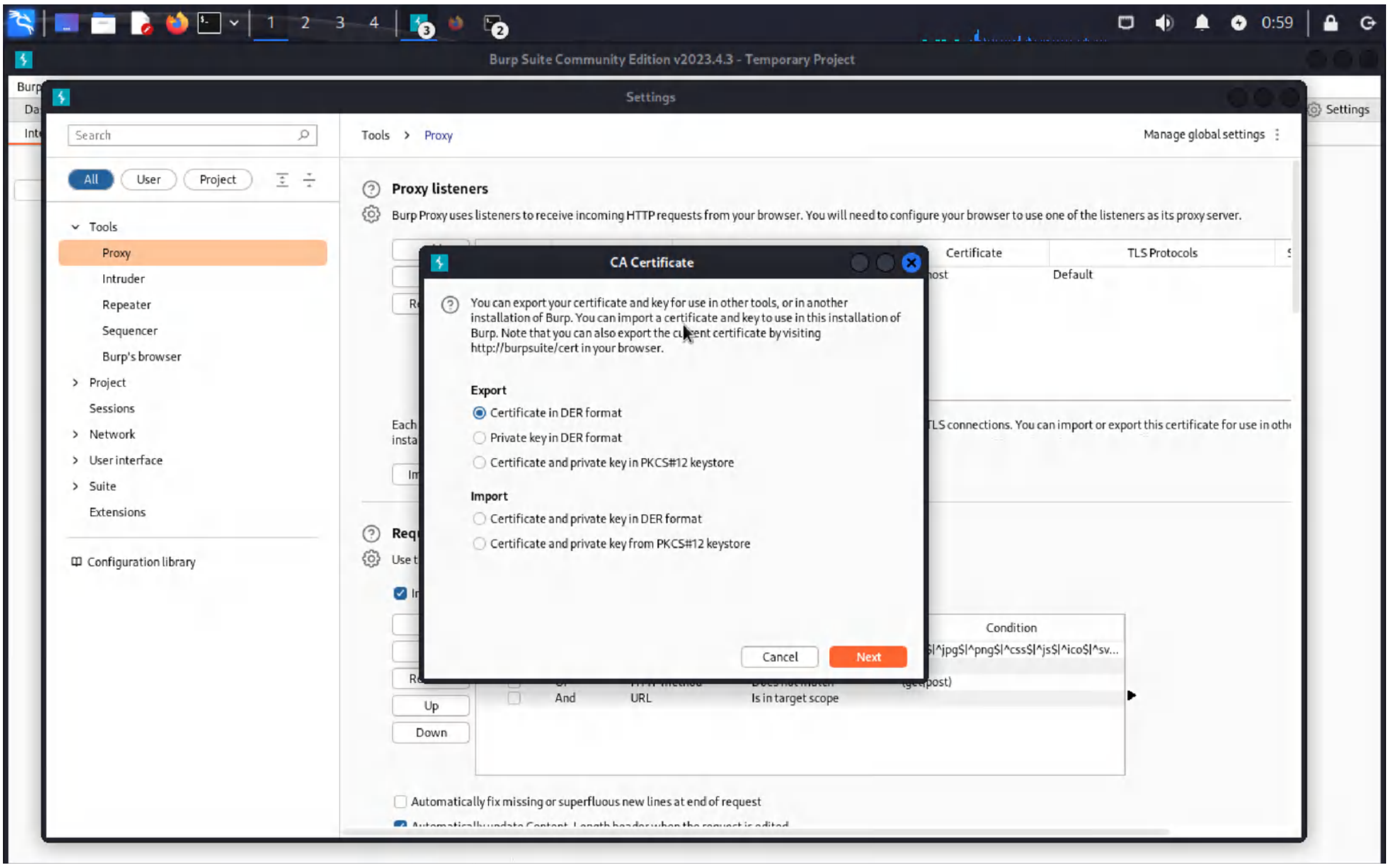
Use this setting to choose whether Burp Proxy interception is enabled when you start Burp.

○ Enable interception

● Disable interception

○ Restore the settings that was selected in the **Proxy > Intercept** tab when Burp closed

7. We will begin by learning how to use Burp with Firefox. Navigate to the proxy tab, and then to the options tab. Then, click on "Import/export CA Certificate". This is thecertificate which will allow our browser to trust Burp Suite. Then, browse to a location on your Kali VM where you want to save the file. It is important that, when you are saving the file, you save it with a .der extension, otherwise the file won't import correctly into Firefox.



Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

CA Certificate

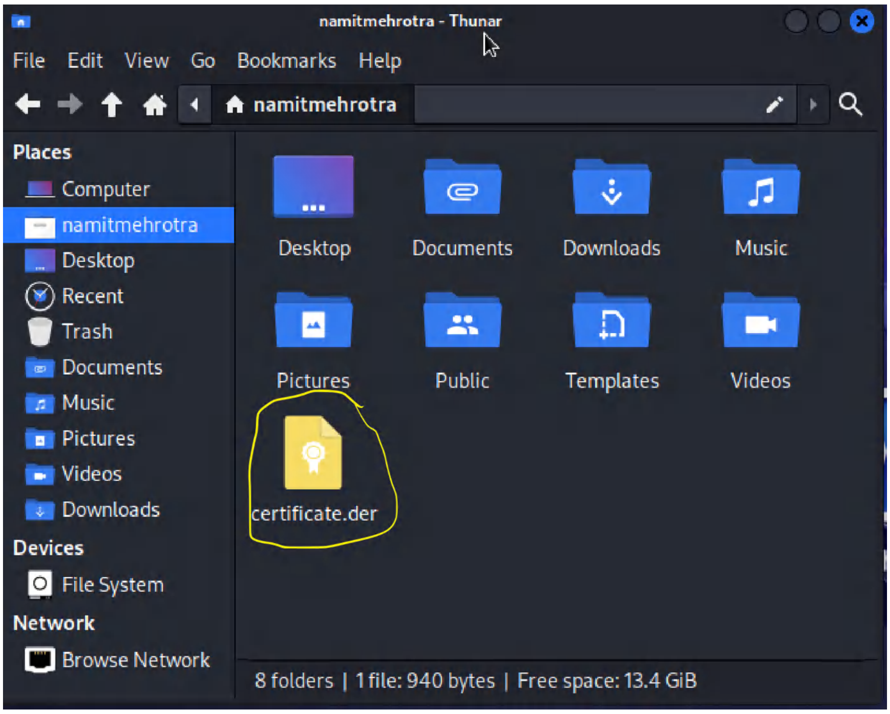
You can export your certificate and key for use in other tools, or in another installation of Burp. You can import a certificate and key to use in this installation of Burp. Note that you can also export the current certificate by visiting http://burpsuite/cert in your browser.

Export

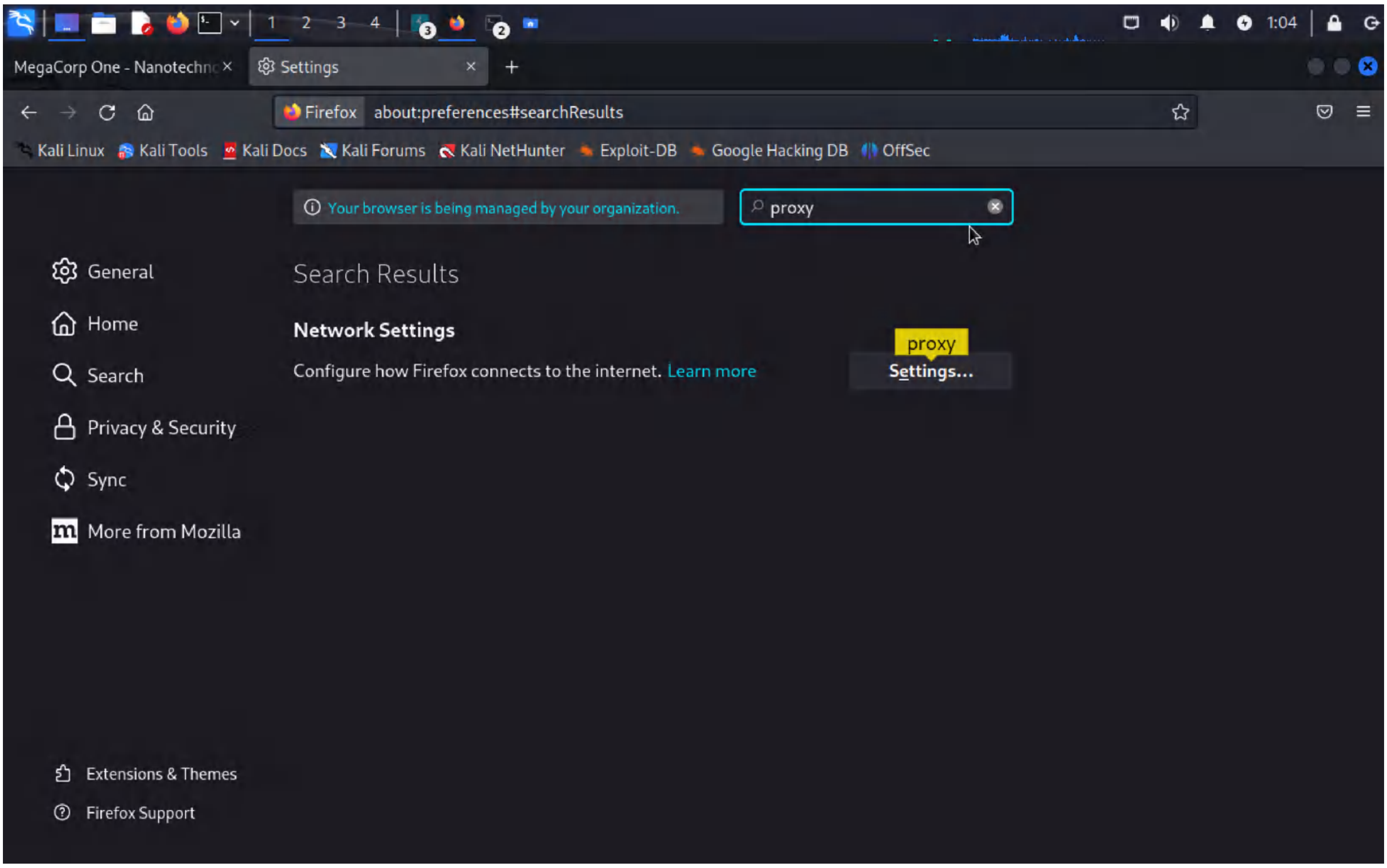
- ● Certificate in DER format
- ○ Private key in DER format
- ○ Certificate and private key in PKCS#12 keystore

Import

- ○ Certificate and private key in DER format
- ○ Certificate and private key from PKCS#12 keystore



8. Once this is done, open Web Browser (Firefox) in Kali and navigate to the options. Find “proxy” in Preferences’ search box. Click on the button called “Settings” under Network Settings.



Your browser is being managed by your organization.

proxy

Search Results

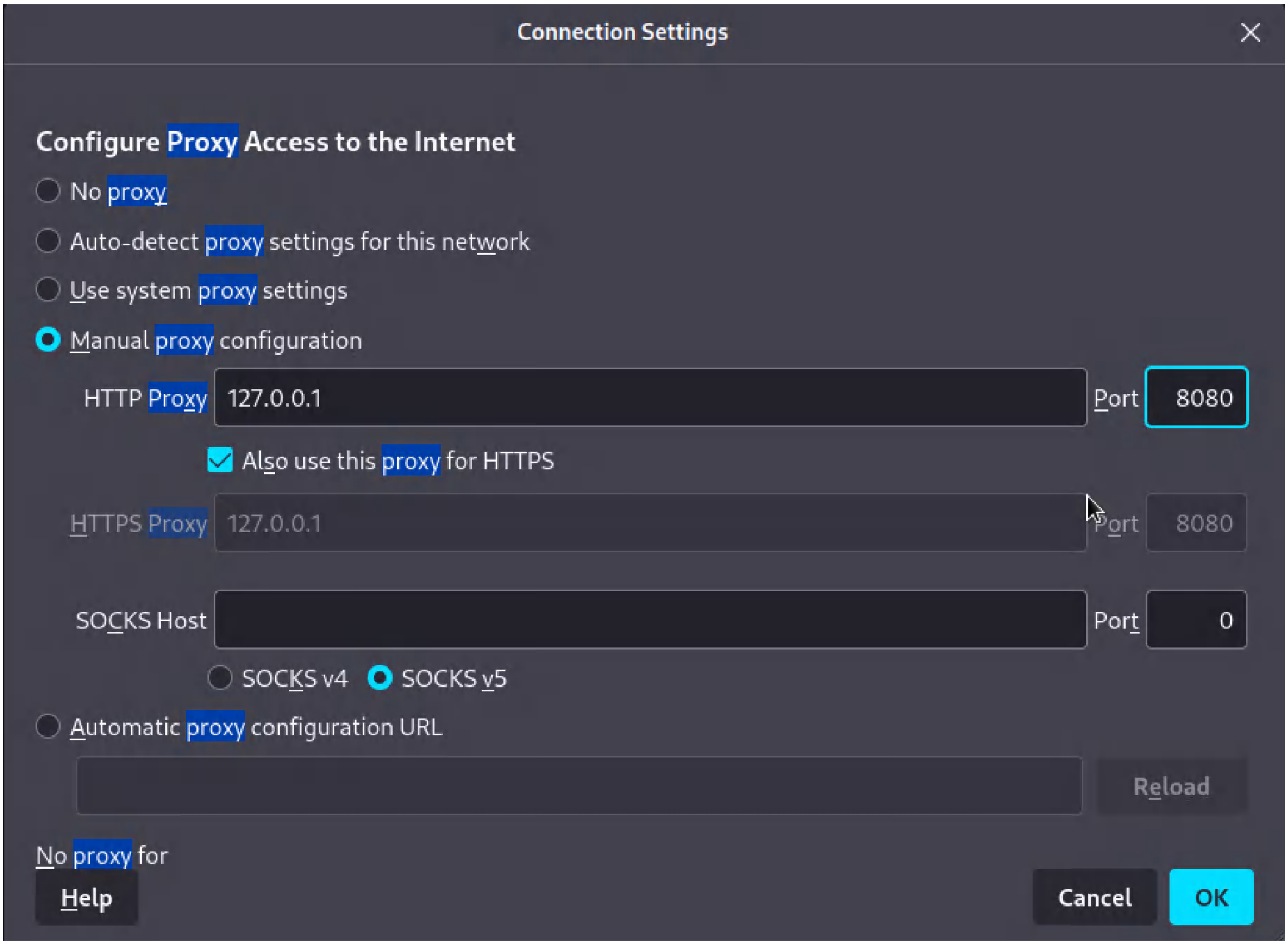
Network Settings

Configure how Firefox connects to the internet. Learn more

proxy

Settings...

9. Then, click Manual Proxy Configuration and enter the following details:



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

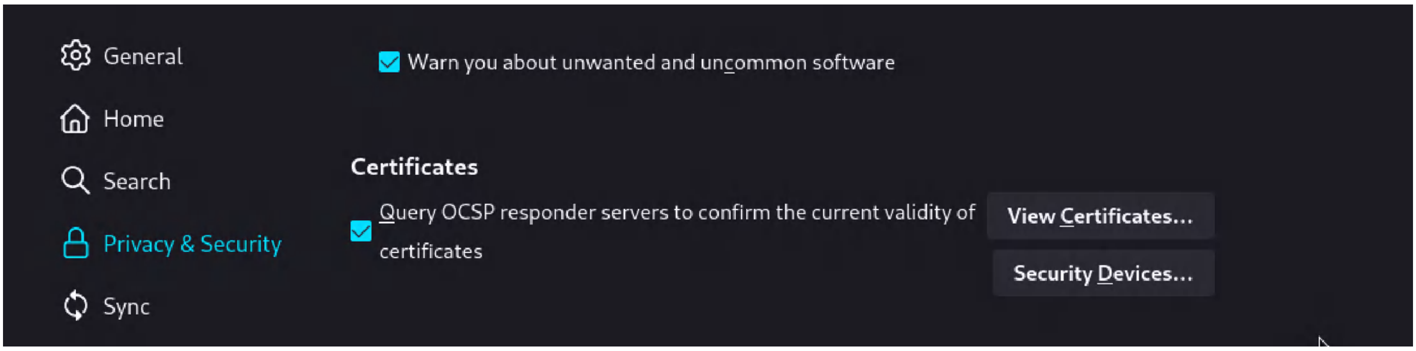
SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

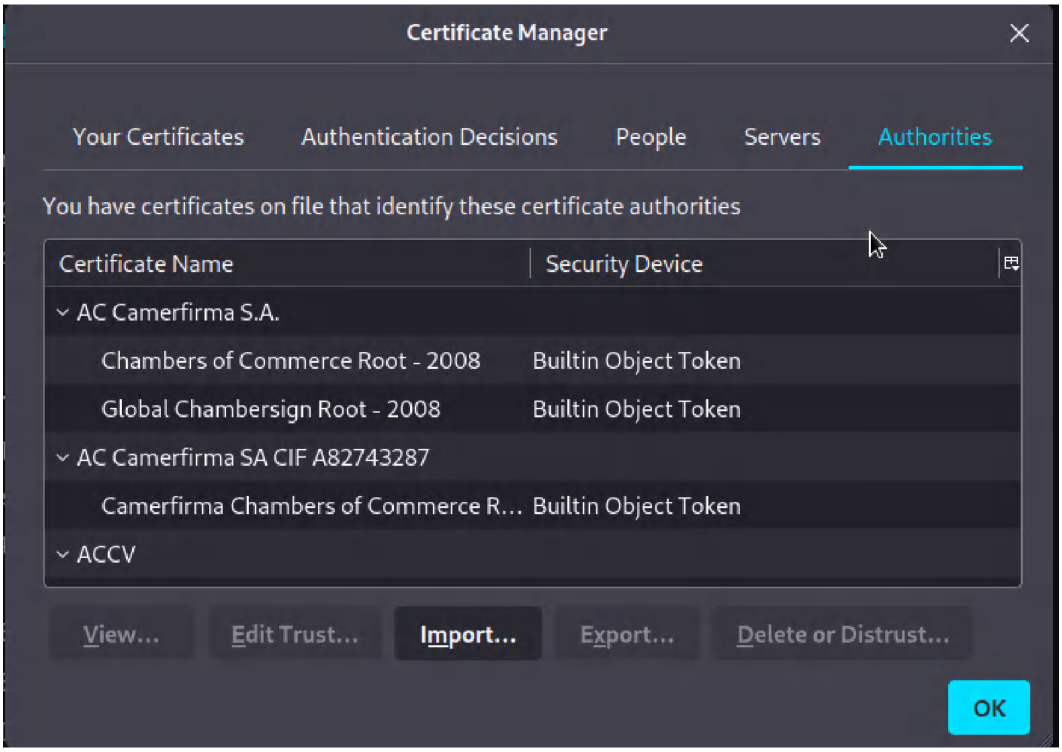
10. Once this is done, navigate to the Privacy & Security tab and then to the Certificates section. This is where we will import the certificate from Burp we saved earlier. To do this, press on “View Certificates” and click on “Import”.



☑ Warn you about unwanted and uncommon software

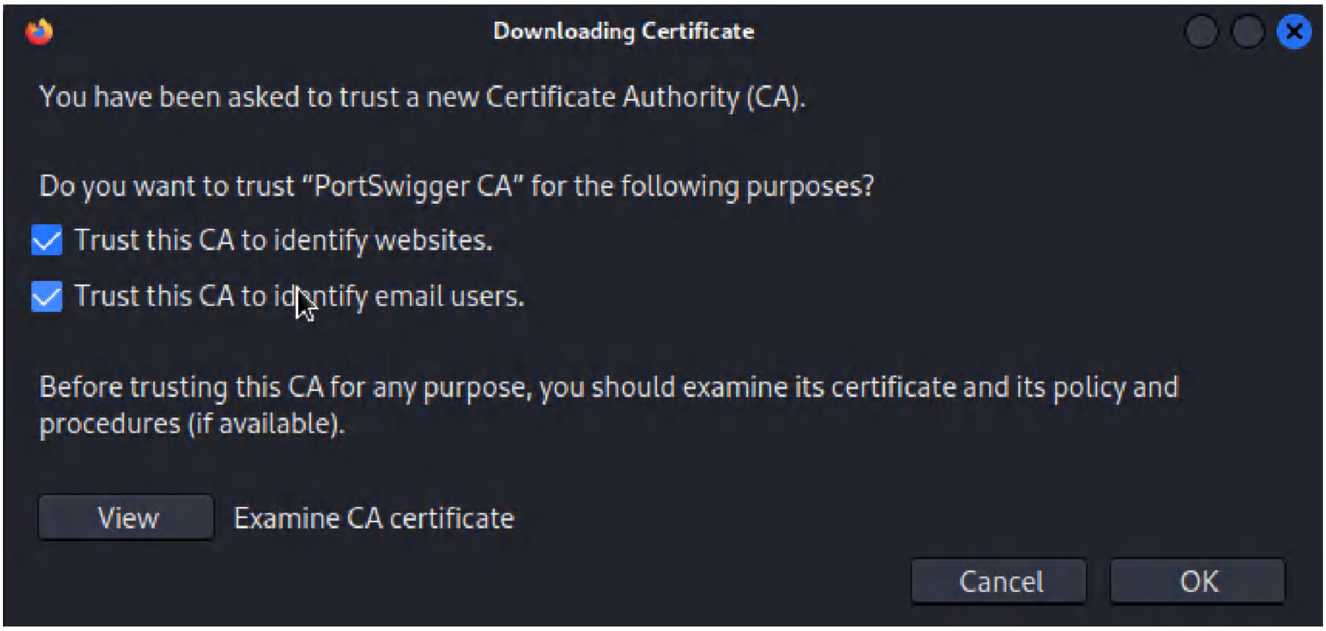
Certificates

☑ Query OCSP responder servers to confirm the current validity of certificates



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
⌄ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
⌄ AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce R...	Builtin Object Token
⌄ ACCV	



You have been asked to trust a new Certificate Authority (CA).

Do you want to trust “PortSwigger CA” for the following purposes?

☑ Trust this CA to identify websites.

☑ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Examine CA certificate

11. Great, Firefox is now configured to work with burp! To test it out, open Burp and Firefox. Ensure Intercept mode is turned ON, and search something in Firefox. If Burp Suite is not intercepting requests, you may have to navigate back to the proxy page. A pop-up might appear asking you to set up a listener. Simply press enable and Burp should then work properly. Your request should be captured in Burp Suite for you to manipulate or examine.

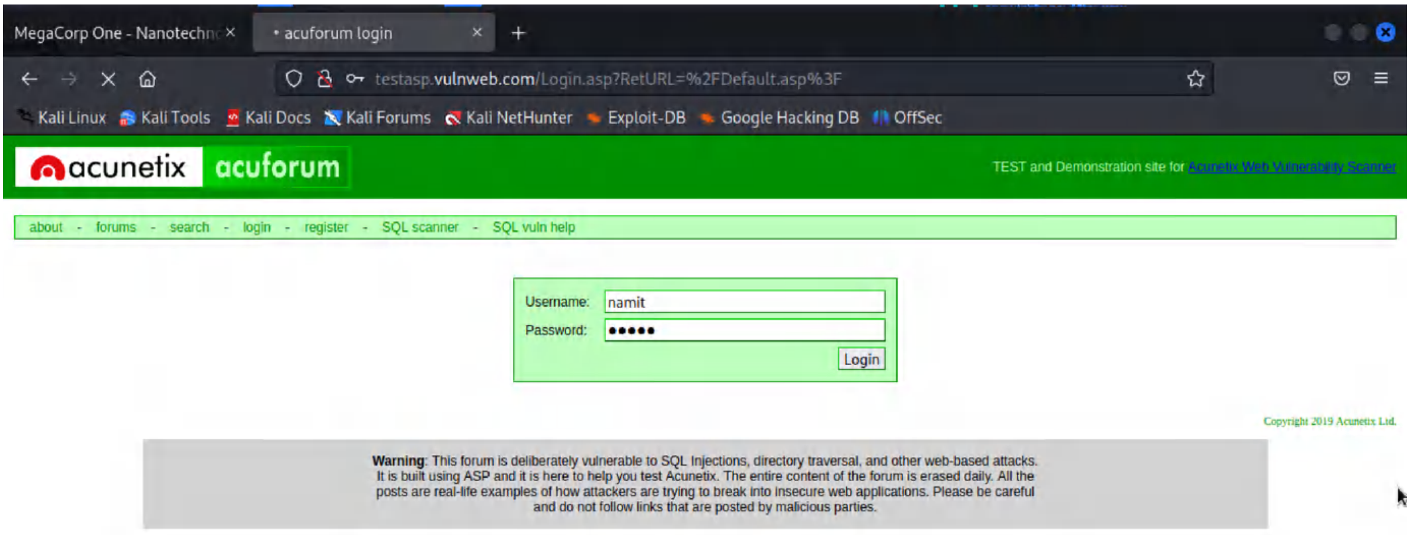
IV. OBSERVATIONS:

12. Now, we will learn how to use Burp to intercept browser network traffic.

Once the web browser opens, navigate to the following site:

http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F

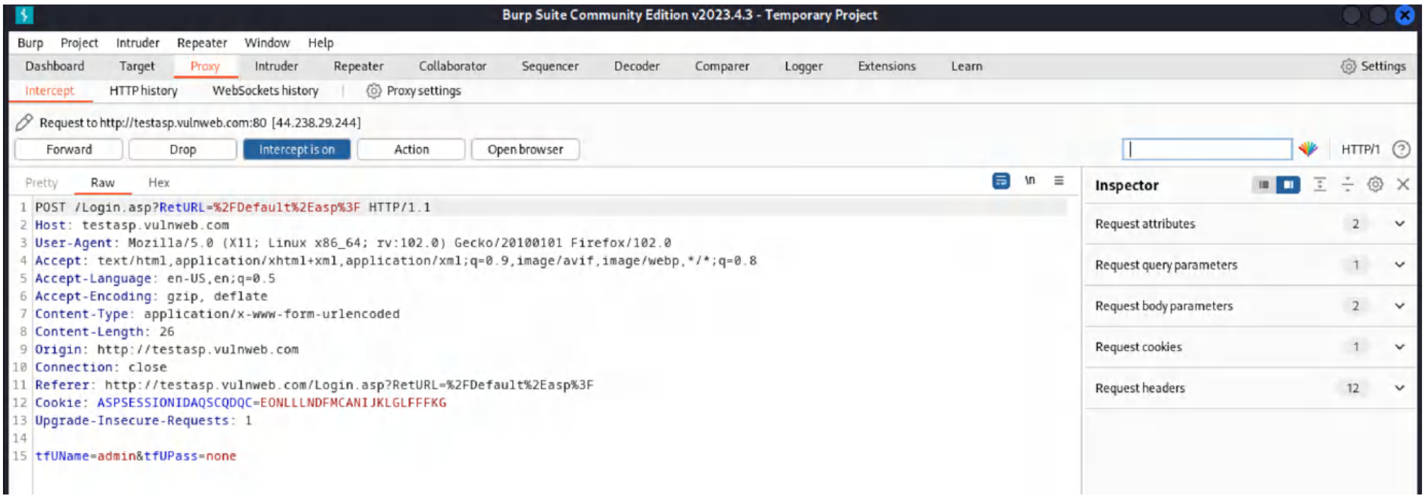
Once there, go back to Burp and turn ON intercept mode. Then, enter any username and password combination into the site and click "Login". As you will see, the page will remain in a loading state. This is because Burp has now intercepted the request we sent to the server, and is holding it for us to manipulate.


MegaCorp One - Nanotechn
acuforum login
testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
acunetix
acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register - SQL scanner - SQL vuln help
Login
Copyright 2019 Acunetix Ltd.

Username: namit

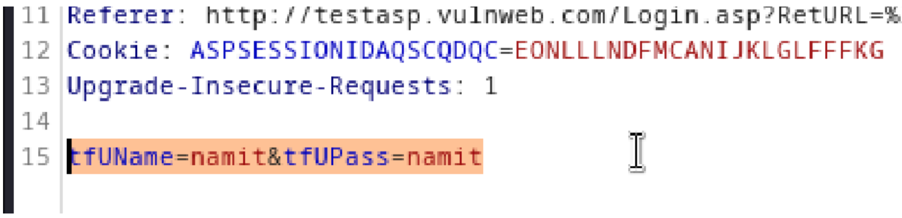
Password: •••••

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.



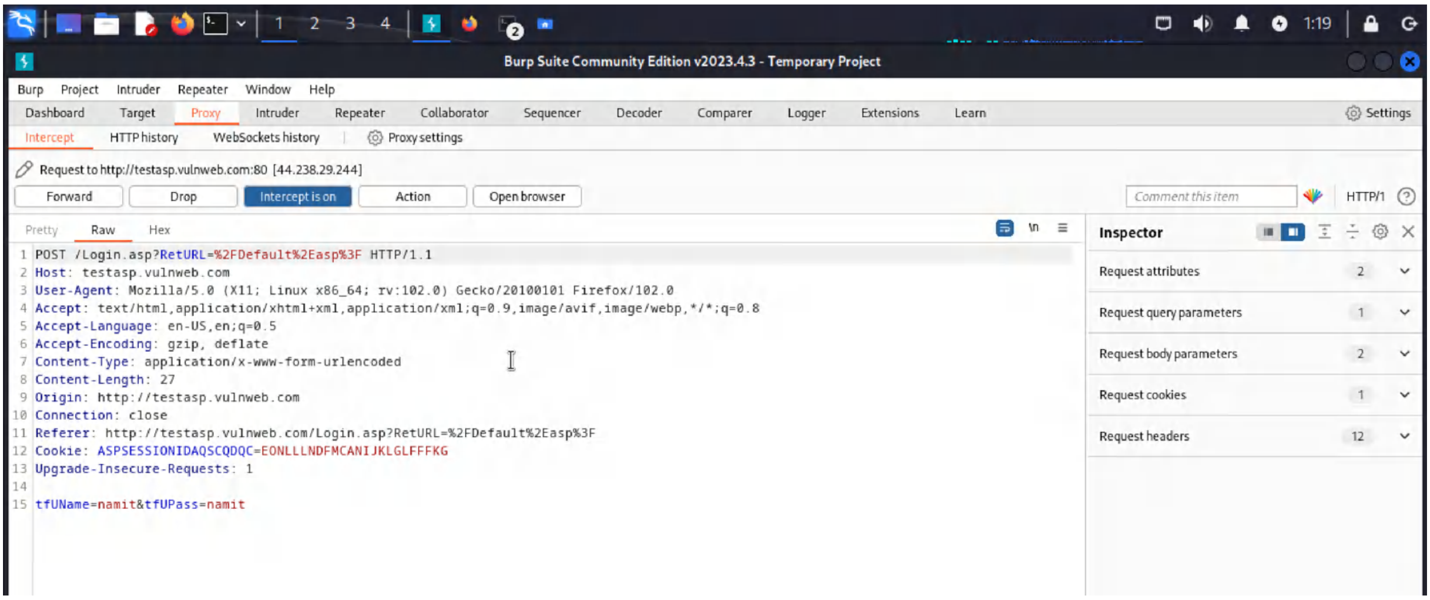
Request to http://testasp.vulnweb.com:80 [44.238.29.244]

```
POST /Login.asp?RetURL=%2FDefault%2Easp%3F HTTP/1.1
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://testasp.vulnweb.com
Connection: close
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
Cookie: ASPSESSIONIDAQSCQDQC=EONLLLNDFMCANIJKLGLFFFKG
Upgrade-Insecure-Requests: 1

tfUName=admin&tfUPass=none
```



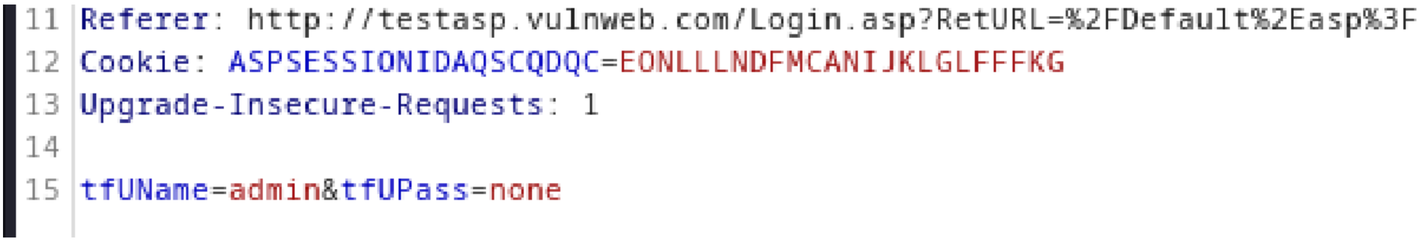
```
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
Cookie: ASPSESSIONIDAQSCQDQC=EONLLLNDFMCANIJKLGLFFFKG
Upgrade-Insecure-Requests: 1

tfUName=namit&tfUPass=namit
```

13. Go back to Burp and you will find the intercepted request, along with the username and password data that we entered. To navigate through the different requests Burp is intercepting, simply press the “Forward” button to send the request to the server and view the next request.

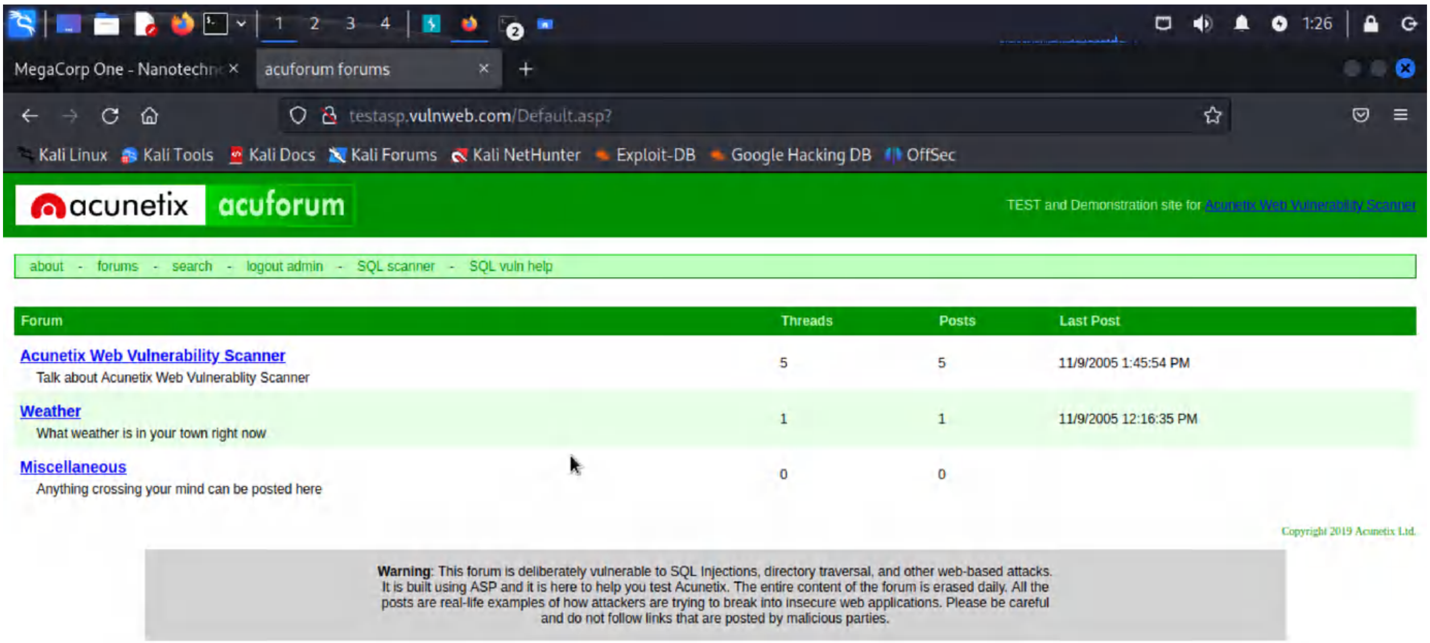

Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Comment this item HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 2
Request cookies 1
Request headers 12

Request to http://testasp.vulnweb.com:80 [44.238.29.244]

```
POST /Login.asp?RetURL=%2FDefault%2Easp%3F HTTP/1.1
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Origin: http://testasp.vulnweb.com
Connection: close
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
Cookie: ASPSESSIONIDAQSCQDQC=EONLLLNDFMCANIJKLGLFFFKG
Upgrade-Insecure-Requests: 1

tfUName=namit&tfUPass=namit
```



```
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
Cookie: ASPSESSIONIDAQSCQDQC=EONLLLNDFMCANIJKLGLFFFKG
Upgrade-Insecure-Requests: 1

tfUName=admin&tfUPass=none
```

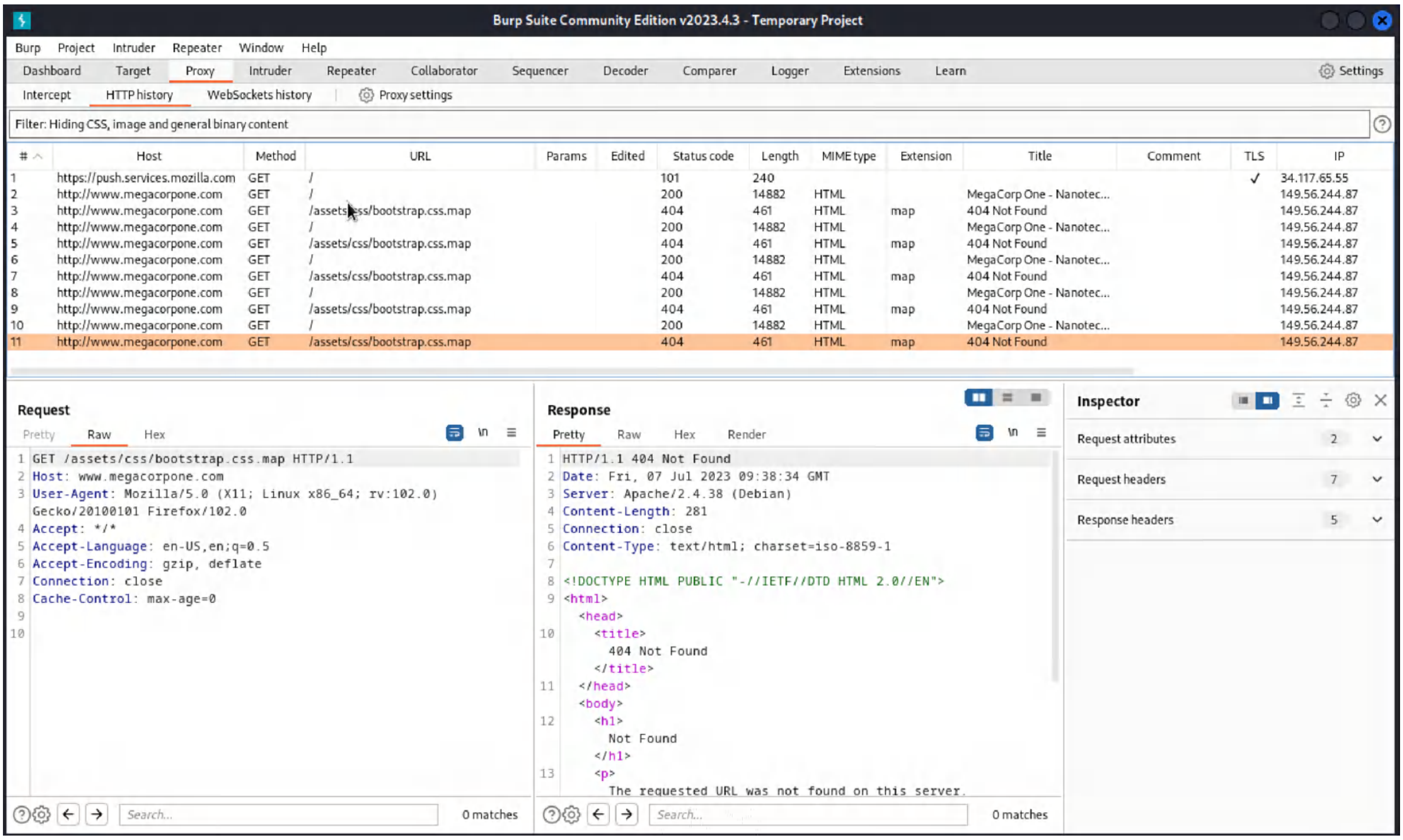

MegaCorp One - Nanotechn
acuforum forums
testasp.vulnweb.com/Default.asp?
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - logout admin - SQL scanner - SQL vuln help

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerablity Scanner	5	5	11/9/2005 1:45:54 PM
Weather What weather is in your town right now	1	1	11/9/2005 12:16:35 PM
Miscellaneous Anything crossing your mind can be posted here	0	0	

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

14. With the proxy enabled, we can close any extra open tabs and browse to http://www.megacorpone.com. We should see traffic in BurpSuite under Proxy > HTTP History.


Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request headers 7
Response headers 5
Search...
0 matches
Search...
0 matches

Filter: Hiding CSS, image and general binary content

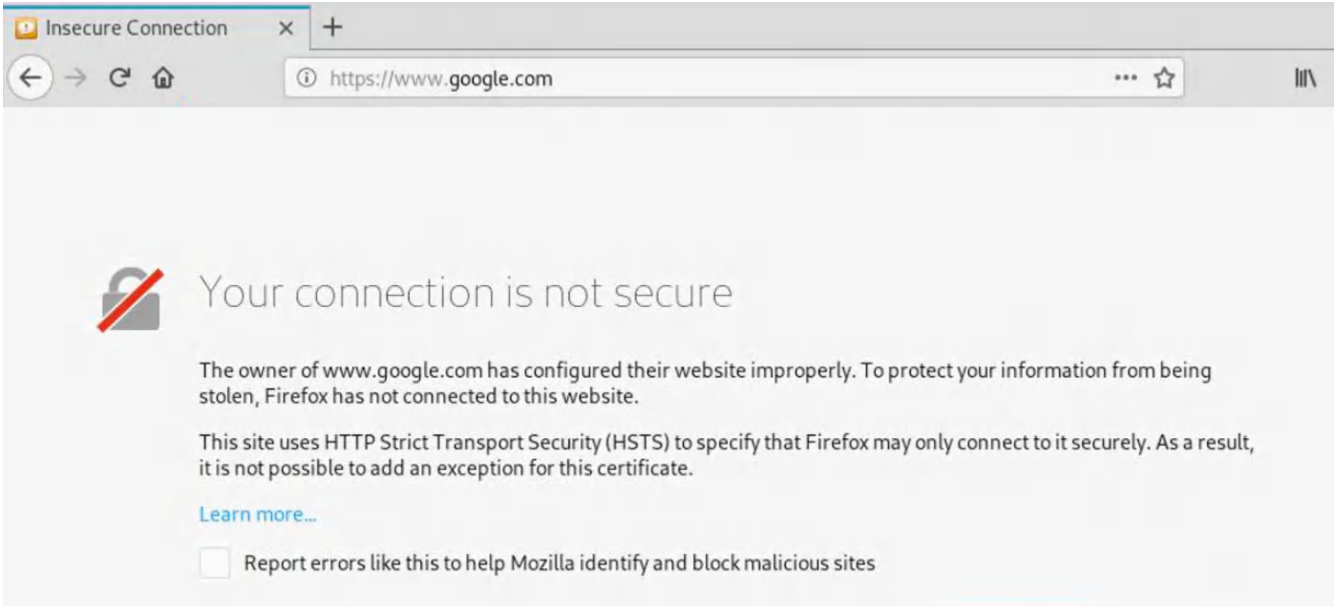
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP
1	https://push.services.mozilla.com	GET	/			101	240					✓	34.117.65.55
2	http://www.megacorpone.com	GET	/			200	14882	HTML		MegaCorp One - Nanotec...			149.56.244.87
3	http://www.megacorpone.com	GET	/assets/css/bootstrap.css.map			404	461	HTML	map	404 Not Found			149.56.244.87
4	http://www.megacorpone.com	GET	/			200	14882	HTML		MegaCorp One - Nanotec...			149.56.244.87
5	http://www.megacorpone.com	GET	/assets/css/bootstrap.css.map			404	461	HTML	map	404 Not Found			149.56.244.87
6	http://www.megacorpone.com	GET	/			200	14882	HTML		MegaCorp One - Nanotec...			149.56.244.87
7	http://www.megacorpone.com	GET	/assets/css/bootstrap.css.map			404	461	HTML	map	404 Not Found			149.56.244.87
8	http://www.megacorpone.com	GET	/			200	14882	HTML		MegaCorp One - Nanotec...			149.56.244.87
9	http://www.megacorpone.com	GET	/assets/css/bootstrap.css.map			404	461	HTML	map	404 Not Found			149.56.244.87
10	http://www.megacorpone.com	GET	/			200	14882	HTML		MegaCorp One - Nanotec...			149.56.244.87
11	http://www.megacorpone.com	GET	/assets/css/bootstrap.css.map			404	461	HTML	map	404 Not Found			149.56.244.87

```
GET /assets/css/bootstrap.css.map HTTP/1.1
Host: www.megacorpone.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cache-Control: max-age=0
```

```
HTTP/1.1 404 Not Found
Date: Fri, 07 Jul 2023 09:38:34 GMT
Server: Apache/2.4.38 (Debian)
Content-Length: 281
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head>
    <title>
      404 Not Found
    </title>
  </head>
  <body>
    <h1>
      Not Found
    </h1>
    <p>
      The requested URL was not found on this server.
```

15. If the browser hangs while loading the page, Intercept may be enabled. Switching it off will allow the traffic to flow uninterrupted. As we browse to additional pages, we should see more requests in the HTTP History tab.

At this point, Firefox is now proxying all of its traffic through Burp Suite. Up to this point, we've only looked at cleartext HTTP traffic. However, if we browse an HTTPS site while proxying traffic through Burp (such as https://www.google.com), we'll be presented with an "invalid certificate" warning:



Your connection is not secure

The owner of www.google.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

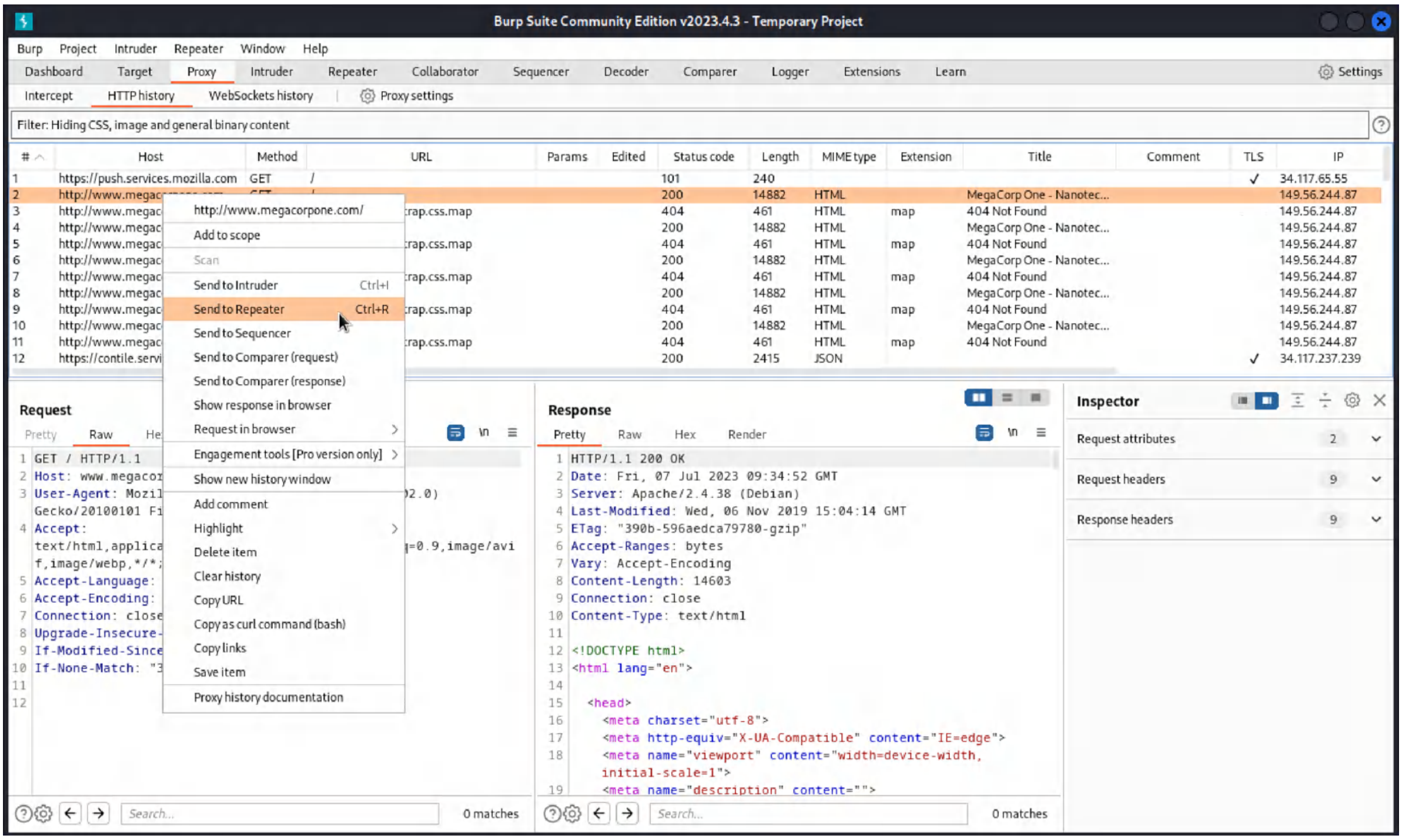
This site uses HTTP Strict Transport Security (HSTS) to specify that Firefox may only connect to it securely. As a result, it is not possible to add an exception for this certificate.

Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites

Burp can easily decrypt HTTPS traffic by generating its own SSL/TLS certificate, essentially manin-the-middling247 ourselves in order to capture the traffic. These warnings can be irritating but we can prevent them by issuing a new certificate and importing it into Firefox.

16. With the Repeater tool, we can easily modify requests, resend them, and review the responses. To see this in action, we can right-click a request from Proxy > HTTP History and select Send to Repeater.


Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
http://www.megacorpone.com/
Add to scope
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Engagement tools [Pro version only]
Show new history window
Add comment
Highlight
Delete item
Clear history
Copy URL
Copy as curl command (bash)
Copy links
Save item
Proxy history documentation
Request
Pretty Raw He
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request headers 9
Response headers 9
Search...
0 matches

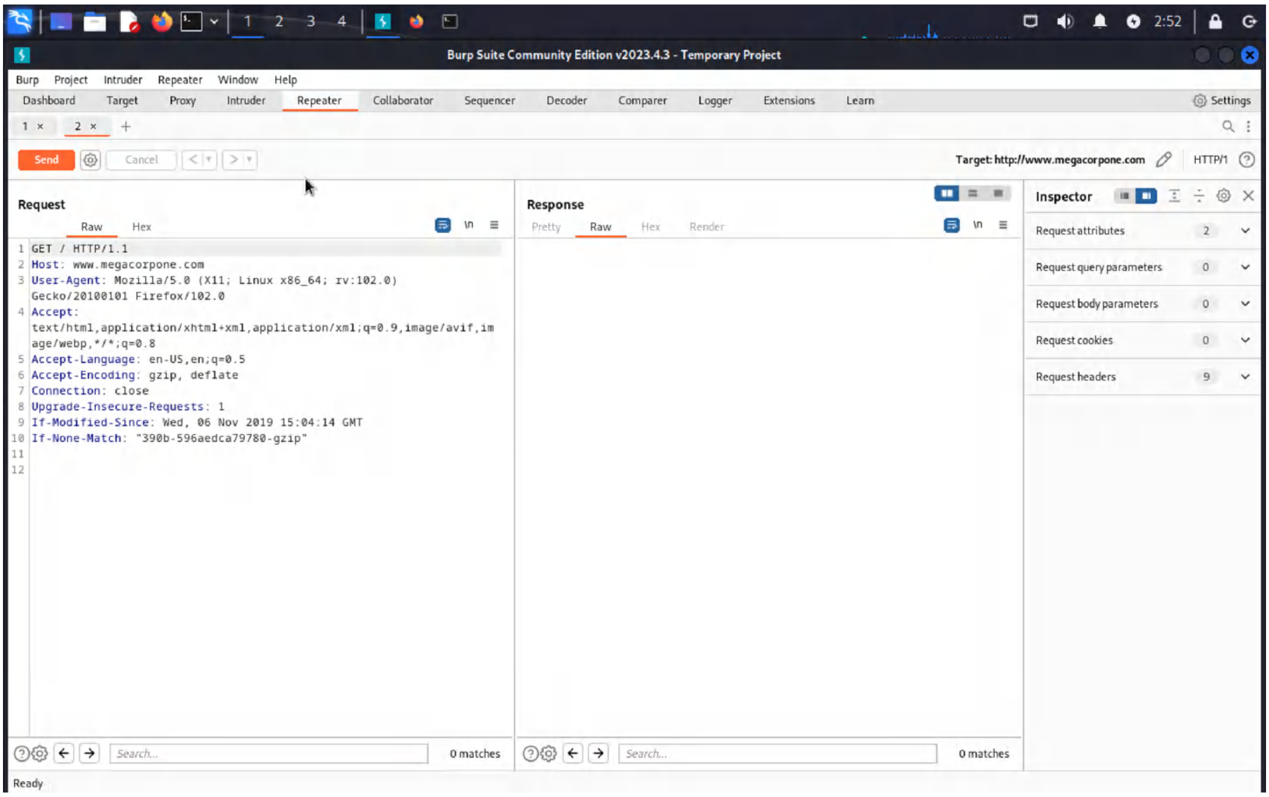
Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP
1	https://push.services.mozilla.com	GET	/			101	240					✓	34.117.65.55
2	http://www.megac					200	14882	HTML		MegaCorp One - Nanotec...			149.56.244.87
3	http://www.megac		rap.css.map			404	461	HTML	map	404 Not Found			149.56.244.87
4	http://www.megac					200	14882	HTML		MegaCorp One - Nanotec...			149.56.244.87
5	http://www.megac		rap.css.map			404	461	HTML	map	404 Not Found			149.56.244.87
6	http://www.megac					200	14882	HTML		MegaCorp One - Nanotec...			149.56.244.87
7	http://www.megac		rap.css.map			404	461	HTML	map	404 Not Found			149.56.244.87
8	http://www.megac					200	14882	HTML		MegaCorp One - Nanotec...			149.56.244.87
9	http://www.megac		rap.css.map			404	461	HTML	map	404 Not Found			149.56.244.87
10	http://www.megac					200	14882	HTML		MegaCorp One - Nanotec...			149.56.244.87
11	http://www.megac		rap.css.map			404	461	HTML	map	404 Not Found			149.56.244.87
12	https://contile.servi					200	2415	JSON				✓	34.117.237.239

```
GET / HTTP/1.1
Host: www.megacor
User-Agent: Mozil                                    2.0)
Gecko/20100101 Fi
Accept:
text/html,applica                                    =0.9,image/avi
f,image/webp,*/*;
Accept-Language:
Accept-Encoding:
Connection: close
Upgrade-Insecure-
If-Modified-Since
If-None-Match: "3
```

```
HTTP/1.1 200 OK
Date: Fri, 07 Jul 2023 09:34:52 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390b-596aedca79780-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 14603
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">

  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width,
    initial-scale=1">
    <meta name="description" content="">
```

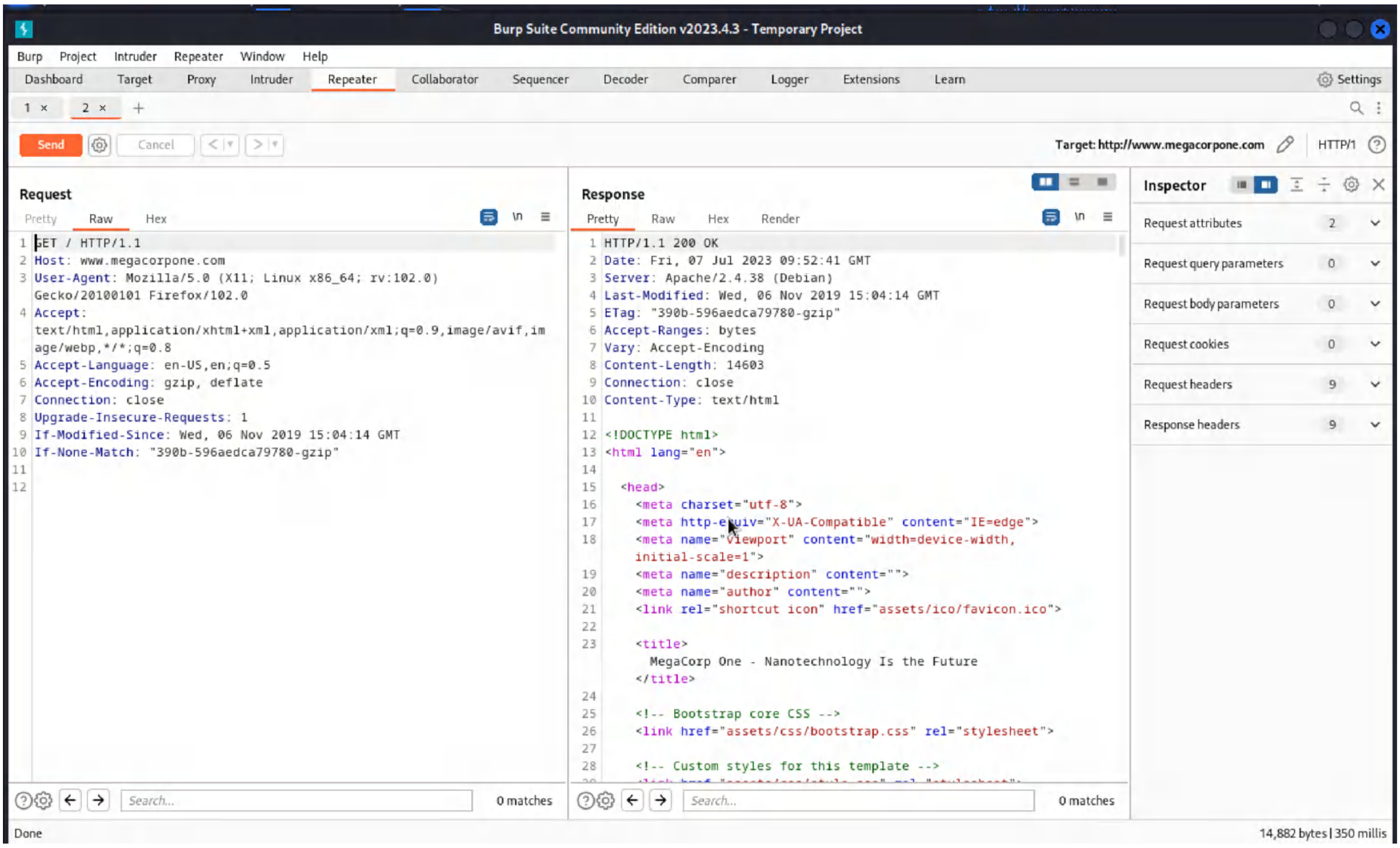
17. If we click on Repeater, we will have one sub-tab with the request on the left side of the window. We can send multiple requests to Repeater and it will display them on separate tabs. We can send the request to the server by clicking Send.



Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Send Cancel
Target: http://www.megacorpone.com HTTP/1
Request
Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 9
0 matches
Ready

```
GET / HTTP/1.1
Host: www.megacorpone.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Wed, 06 Nov 2019 15:04:14 GMT
If-None-Match: "390b-596aedca79780-gzip"
```

18. Burp Suite will display the raw server response on the right side of the window, which includes the response headers and unrendered response content.



Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Send Cancel
Target: http://www.megacorpone.com HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 9
Response headers 9
0 matches
Done
14,882 bytes | 350 millis

```
GET / HTTP/1.1
Host: www.megacorpone.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Wed, 06 Nov 2019 15:04:14 GMT
If-None-Match: "390b-596aedca79780-gzip"
```

```
HTTP/1.1 200 OK
Date: Fri, 07 Jul 2023 09:52:41 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390b-596aedca79780-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 14603
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">

  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width,
    initial-scale=1">
    <meta name="description" content="">
    <meta name="author" content="">
    <link rel="shortcut icon" href="assets/ico/favicon.ico">

    <title>
      MegaCorp One - Nanotechnology Is the Future
    </title>

    <!-- Bootstrap core CSS -->
    <link href="assets/css/bootstrap.css" rel="stylesheet">

    <!-- Custom styles for this template -->
```

19. Web application exploitation often requires a great deal of trial and error as we submit and modify requests and monitor the responses. Repeater is very useful for this as we can quickly tweak elements of the request and resend them without waiting for our browser to render every response.

V. INFERENCES:

1. By conducting a web application assessment using Burp Suite in Kali Linux to analyze the website www.megacorp.one, several inferences can be drawn.

2. Firstly, Burp Suite's intercepting proxy feature allowed for the thorough examination of HTTP requests and responses, providing insights into the website's underlying structure, communication patterns, and potential vulnerabilities.

3. This allowed for the identification of security weaknesses such as cross-site scripting (XSS), SQL injection, or insecure direct object references (IDOR), which could be exploited by malicious actors. Additionally, the active scanning capabilities of Burp Suite aided in the automated discovery of common vulnerabilities and misconfigurations within the website, enhancing the efficiency and effectiveness of the assessment process.

4. The comprehensive reporting functionality of Burp Suite further facilitated the communication of identified vulnerabilities to the website administrators, enabling prompt remediation actions. Overall, the use of Burp Suite in Kali Linux provided a robust framework for analyzing the website www.megacorp.one, helping to enhance its security posture and protect against potential threats.

EXERCISE 3-B-4: Web Application Assessment using Nikto tool

I. AIM: Analyse the website www.megacorp.one using Nikto tool in Kali Linux.

II. TOOLS REQUIRED:

1. Products: Nikto tool in Kali Linux
2. Internet browser: Firefox
3. Manufacturer: various

III. STEP BY STEP PROCEDURE:

1. Nikto248 is a highly configurable Open Source web server scanner that tests for thousands of dangerous files and programs, vulnerable server versions and various server configuration issues. It performs well, but is not designed for stealth as it will send many requests and embed information about itself in the User-Agent249 header.

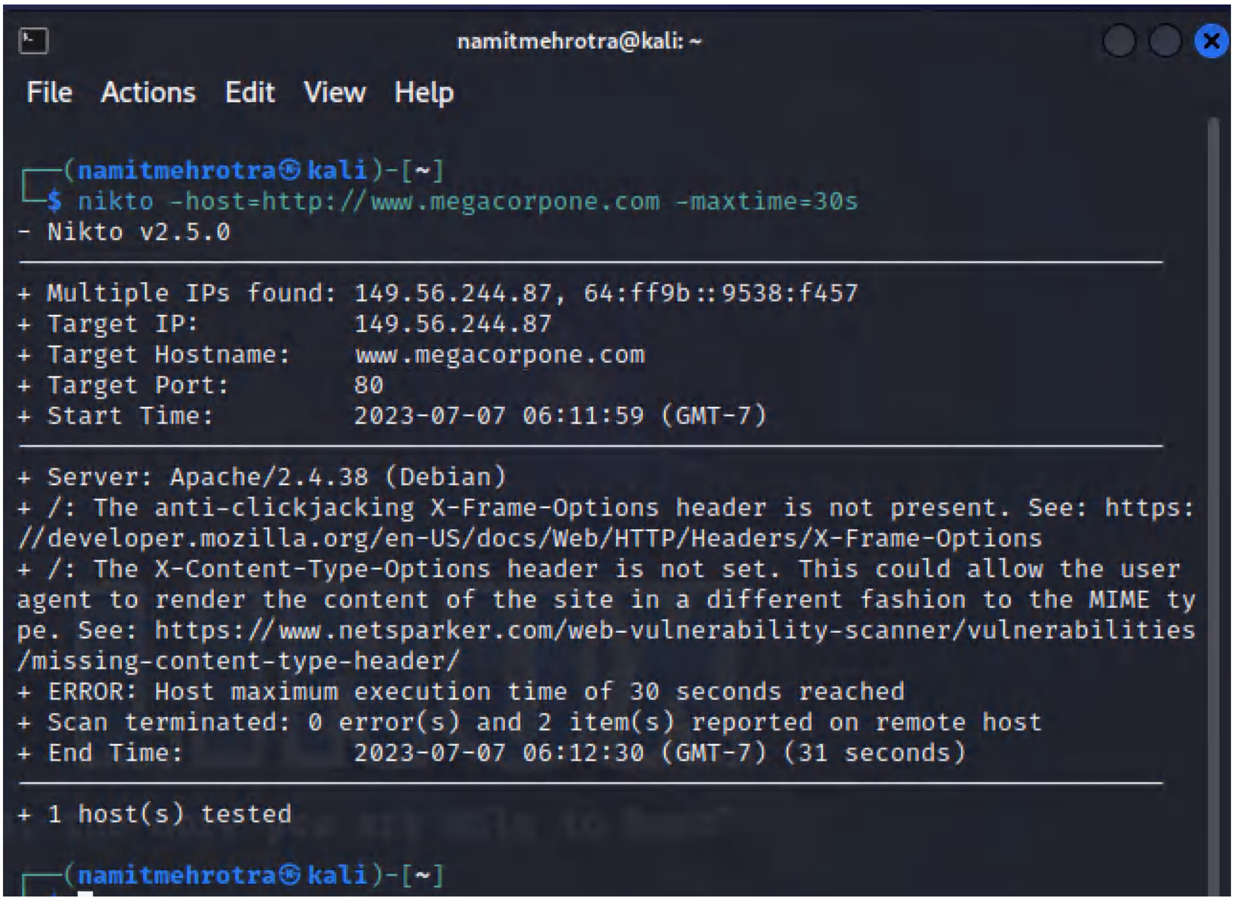
2. Nikto can scan multiple servers and ports and will scan as many pages as it can find. On sites with heavy content, such as an ecommerce site, a Nikto scan can take several hours to complete. We have two options to control the scan duration. The simplest option is to set the -maxtime option, which will halt the scan after the specified time limit. This does not optimize the scan in any way. Nikto will simply stop scanning. Our second option is to tune250 the scan with the -T option.

3. We can use this feature to control which types of tests we want to run. There are times when we do not want to run all the tests built in to Nikto, such as verifying if a certain class of vulnerabilities is present. Tuning a scan is invaluable in these situations.

4. Nikto is especially useful for catching low-hanging fruit, reporting non-standard server headers, and catching server configuration errors.

5. To demonstrate this, let’s run Nikto against www.megacorpone.com. We’ll specify the host we want to scan (host=http://www.megacorpone.com) and for the sake of this demonstration, we’ll use -maxtime=30s to limit the scan duration to 30 seconds:

IV. OBSERVATIONS:



```
┌──(namitmehrotra㉿kali)-[~]
└─$ nikto -host=http://www.megacorpone.com -maxtime=30s
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 149.56.244.87, 64:ff9b::9538:f457
+ Target IP:          149.56.244.87
+ Target Hostname:    www.megacorpone.com
+ Target Port:        80
+ Start Time:         2023-07-07 06:11:59 (GMT-7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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 ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ ERROR: Host maximum execution time of 30 seconds reached
+ Scan terminated: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2023-07-07 06:12:30 (GMT-7) (31 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(namitmehrotra㉿kali)-[~]
```

Although we limited the scan duration, the output in Listing 283 still provided some interesting information. For example, it identified that the version of Apache running on the server is out of date and past its end-of-life.

We have only demonstrated a fraction of the tools available in Kali Linux in this brief introduction, but the tools we have covered so far will serve us well for the demonstrations that follow in the rest of the module.

V. INFERENCES:

1. Analyzing the website www.megacorp.one using the Nikto tool in Kali Linux provided valuable insights into its security posture.

2. Nikto's scanning capabilities uncovered common vulnerabilities, misconfigurations, and outdated software versions, highlighting potential weaknesses that could be exploited. The detection of server-side vulnerabilities, such as insecure CGI scripts, helped identify possible attack vectors.

3. By generating detailed reports, Nikto facilitated effective communication of these findings to the website administrators for timely remediation.

4. This analysis with Nikto in Kali Linux proved instrumental in assessing and enhancing the overall security of www.megacorp.one, fortifying it against potential threats.