Sri Lanka Institute of Information Technology

Individual Assignment IE2062 – Web Security

Reg no.:IT19974606

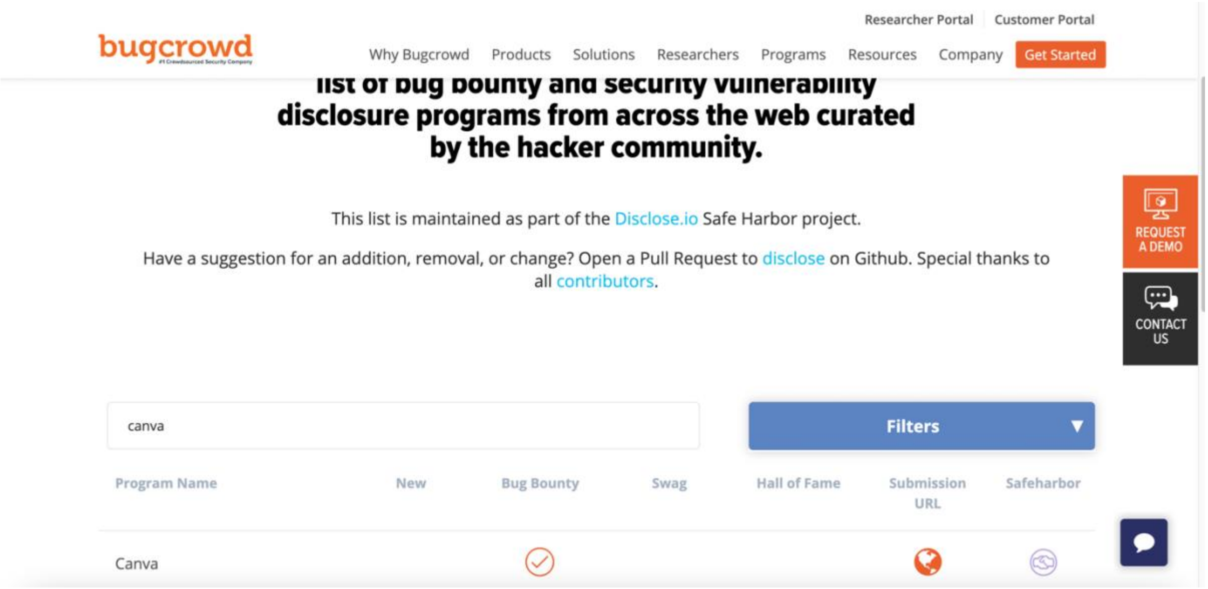
Name: K.S Mahappukorala

Introduction

What is a web audit?

The auditing of a website entails a detailed examination of all elements that influence search engine visibility. This typical technique gives you a complete picture of all your websites, traffic, and specific pages. The website audit has been completed solely for marketing purposes. The goal is to identify flaws in web-based campaigns. The website audit starts with a general website examination to identify the steps that need to be taken to improve SEO. The SEO audit on-site and off-site, which can include broken links, duplicate meta-descriptions, HTML validation, web site statistics, mistakes, index pages, and site speed, can all provide recommendations for improving search web ranks. There are various reasons for a website audit, but the most essential ones are usually SEO and content marketing. An SEO-based website audit identifies weak places in a website's SEO score and leads to a better knowledge of its SEO status. The content audit is used to assess participation and evaluate modifications to the content strategy in order to improve the website's performance.

To do a web audit, we must first choose a website. I utilized the website "Bugcrowd" for this. Bugcrowd is a website that participates in the bug bounty program. There are numerous websites where you may conduct a web audit. We chose a website from among several that were presented to us.



list of bug bounty and security vulnerability disclosure programs from across the web curated by the hacker community.

This list is maintained as part of the Disclose.io Safe Harbor project.

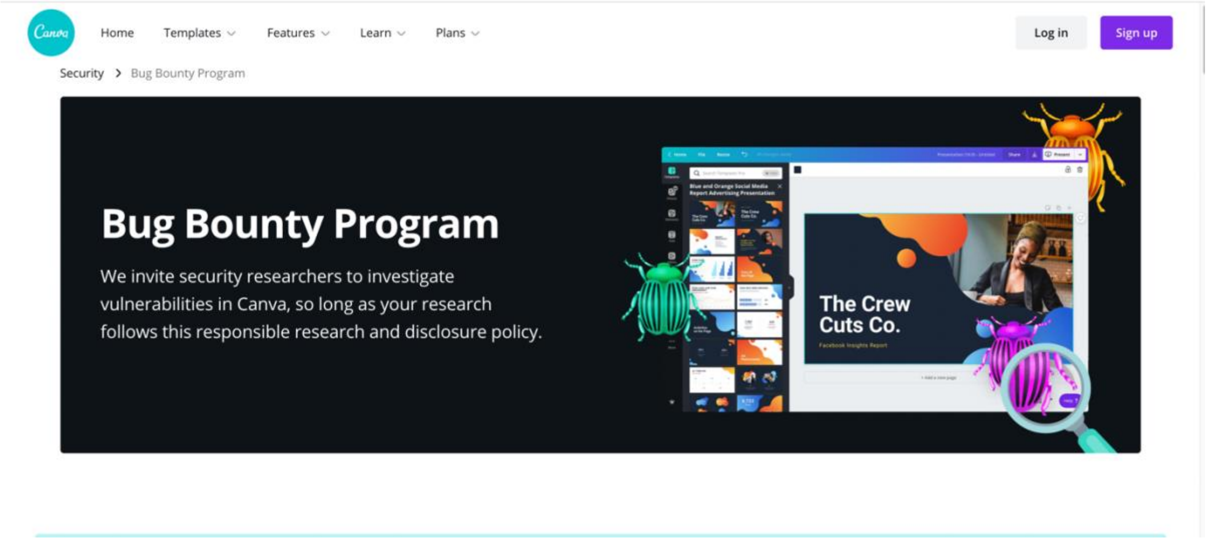
Have a suggestion for an addition, removal, or change? Open a Pull Request to disclose on Github. Special thanks to all contributors.

Program Name	New	Bug Bounty	Swag	Hall of Fame	Submission URL	Safeharbor
Canva		✓			●	○

And for my assignment I used the “Canva” site

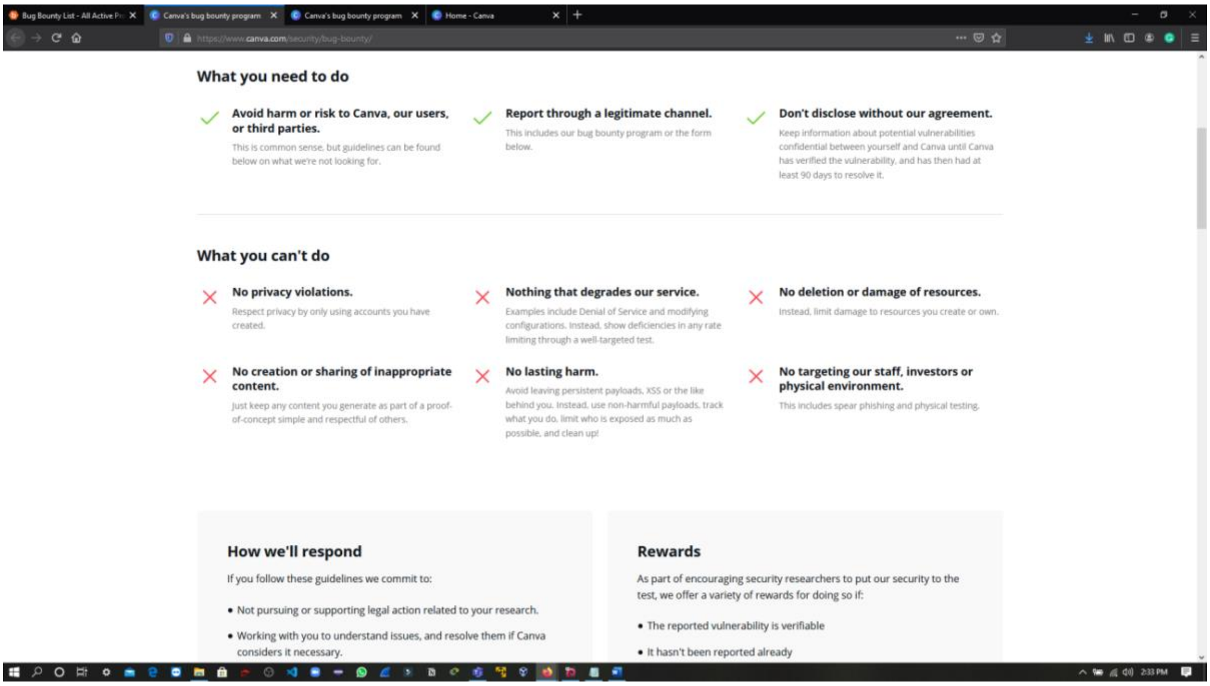
Canva is a graphic design tool for making social media graphics, presentations, posters, documents, and other visual content. Users can use the templates provided in the app. The platform is free to use, however paid memberships such as Canva Pro and Canva for Enterprise are available for those that want more features.

- Canva is a free graphic design website that can be used to create invites, business cards, Instagram posts, and other things.
- Customizing thousands of templates is simple and straightforward thanks to a drag-and-drop interface.
- Canva's broad feature set allows you to modify photographs even if you don't have a lot of experience with picture editing.



Bug Bounty Program

We invite security researchers to investigate vulnerabilities in Canva, so long as your research follows this responsible research and disclosure policy.



Bug Bounty List - All Active Pr
Canva's bug bounty program
Canva's bug bounty program
Home - Canva
https://www.canva.com/security/bug-bounty/
2:33 PM

What you need to do

✓ **Avoid harm or risk to Canva, our users, or third parties.**
This is common sense, but guidelines can be found below on what we're not looking for.

✓ **Report through a legitimate channel.**
This includes our bug bounty program or the form below.

✓ **Don't disclose without our agreement.**
Keep information about potential vulnerabilities confidential between yourself and Canva until Canva has verified the vulnerability, and has then had at least 90 days to resolve it.

What you can't do

✗ **No privacy violations.**
Respect privacy by only using accounts you have created.

✗ **Nothing that degrades our service.**
Examples include Denial of Service and modifying configurations. Instead, show deficiencies in any rate limiting through a well-targeted test.

✗ **No deletion or damage of resources.**
Instead, limit damage to resources you create or own.

✗ **No creation or sharing of inappropriate content.**
Just keep any content you generate as part of a proof-of-concept simple and respectful of others.

✗ **No lasting harm.**
Avoid leaving persistent payloads, XSS or the like behind you. Instead, use non-harmful payloads, track what you do, limit who is exposed as much as possible, and clean up!

✗ **No targeting our staff, investors or physical environment.**
This includes spear phishing and physical testing.

How we'll respond

If you follow these guidelines we commit to:

- Not pursuing or supporting legal action related to your research.
- Working with you to understand issues, and resolve them if Canva considers it necessary.

Rewards

As part of encouraging security researchers to put our security to the test, we offer a variety of rewards for doing so if:

- The reported vulnerability is verifiable
- It hasn't been reported already

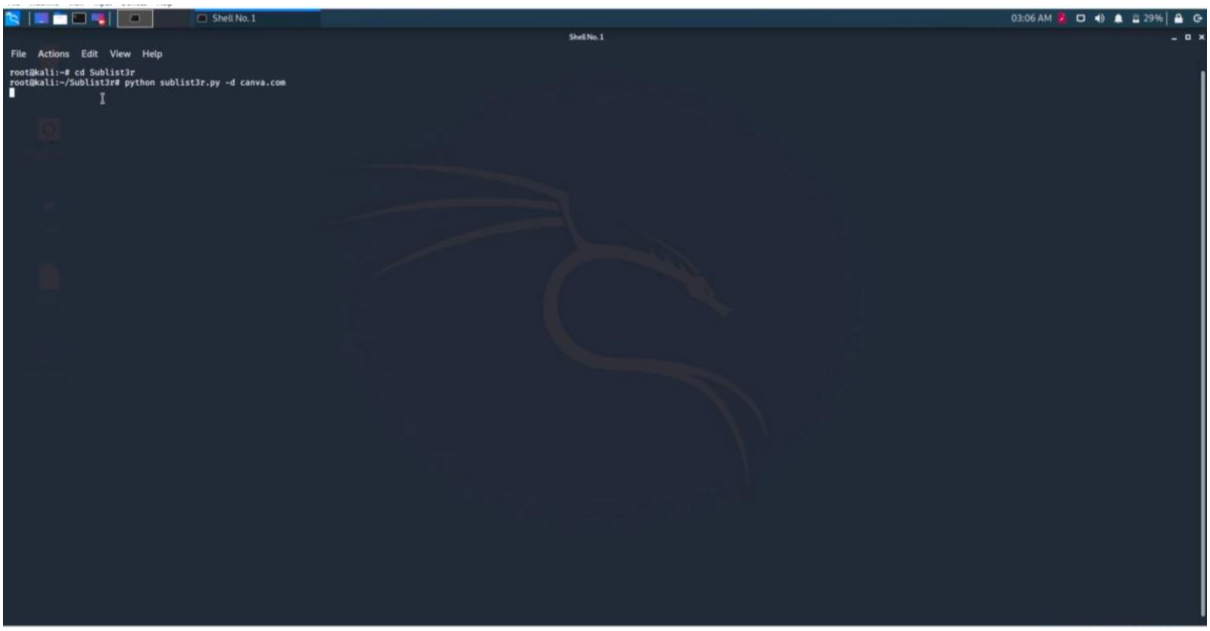
As seen in the diagram above, they have specified what they want from us and what they do not anticipate us to do during the online audit.

- What you should do:
  - Avoid causing harm or putting Canva, our users, or third parties in danger. · Make a formal report through a reputable source.
  - Do not reveal without our permission.

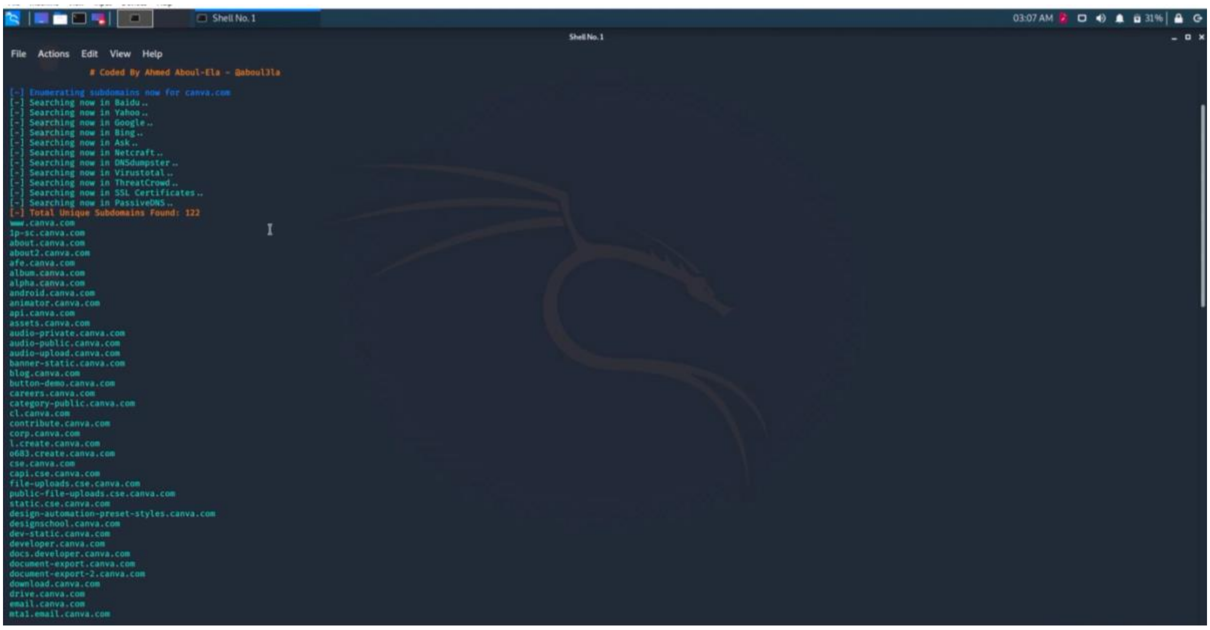
- What you can't do: o No invasions of privacy; o No resource deletion or harm.
  - No long-term consequences o Nothing that damages our service
  - No inappropriate content should be created or shared.
  - We will not attack our employees, investors, or physical environment.

• This assignment stipulates that the domain we choose must have at least 50 subdomains.

Sublist3r is a python utility that uses OSINT to enumerate website subdomains. It assists penetration testers and bug hunters in gathering and collecting subdomains for the site they are targeting. Sublist3r uses a variety of search engines to find subdomains, including Google, Yahoo, Bing, Baidu, and Ask. Sublist3r also uses Netcraft, Virustotal, ThreatCrowd, DNSdumpster, and ReverseDNS to find subdomains.



```
root@kali:~# cd Sublist3r
root@kali:~/Sublist3r# python sublist3r.py -d canva.com
```

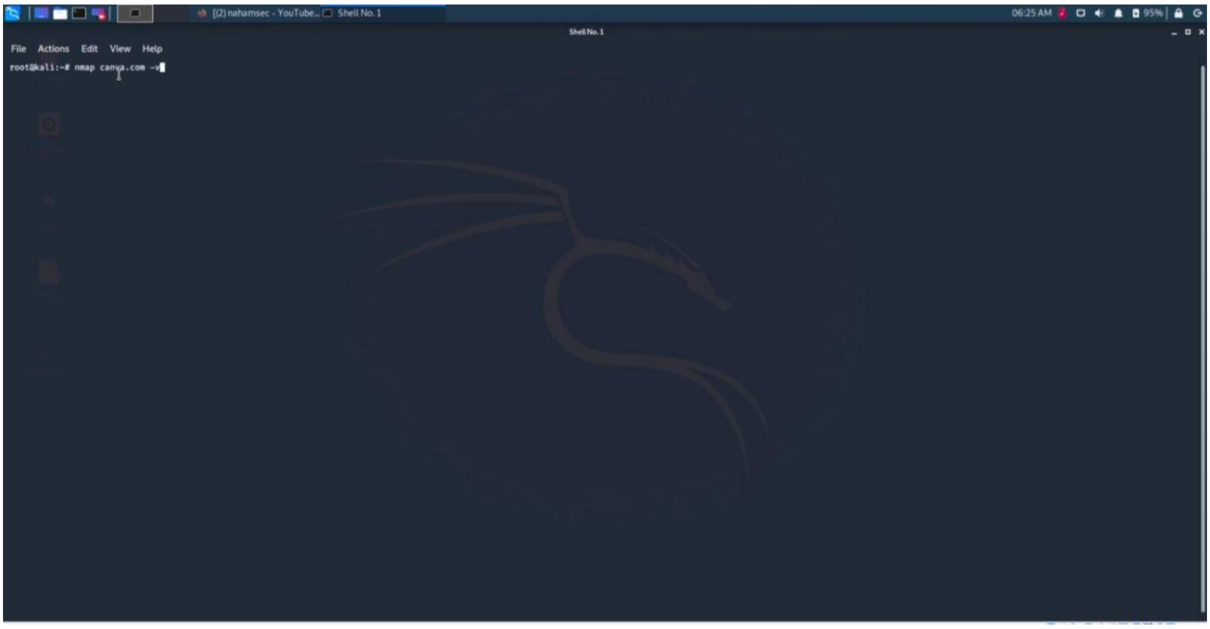


```
                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for canva.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 122
www.canva.com
1p-sc.canva.com
about.canva.com
about2.canva.com
afe.canva.com
album.canva.com
alpha.canva.com
android.canva.com
animator.canva.com
api.canva.com
assets.canva.com
audio-private.canva.com
audio-public.canva.com
audio-upload.canva.com
banner-static.canva.com
blog.canva.com
button-demo.canva.com
careers.canva.com
category-public.canva.com
cl.canva.com
contribute.canva.com
corp.canva.com
l.create.canva.com
o683.create.canva.com
cse.canva.com
capi.cse.canva.com
file-uploads.cse.canva.com
public-file-uploads.cse.canva.com
static.cse.canva.com
design-automation-preset-styles.canva.com
designschool.canva.com
dev-static.canva.com
developer.canva.com
docs.developer.canva.com
document-export.canva.com
document-export-2.canva.com
download.canva.com
drive.canva.com
email.canva.com
mta1.email.canva.com
```

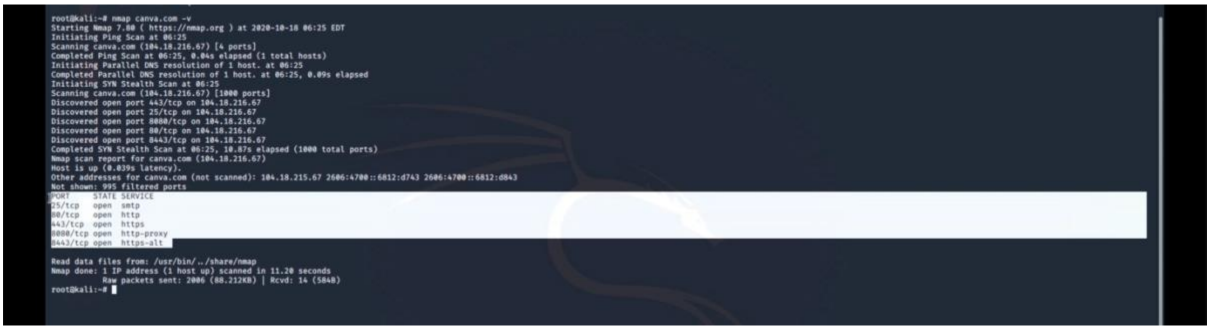
According to the details in the above figure there are 122 sub domains

In my first effort, I attempted to exploit the site that I chose without first evaluating the site's vulnerabilities using several tools. Those attempts, however, were futile because the site was far more secure than I had imagined. Then I looked for ways to conduct a web audit properly. Nahamsec's "YouTube" videos on the issue given me some insight into web audits. According to the video, the recon must be done correctly by finding vulnerabilities and obtaining as much information as possible about the site before attempting the exploitation.

Nmap (Network Mapper) is a free and open-source vulnerability scanner and network discovery tool. Nmap is a network administrator's tool for determining what devices are running on their systems, locating available hosts and the services they provide, discovering open ports, and detecting security threats.


[(2) nahamsec - YouTube... Shell No. 1
06:25 AM
95%
Shell No. 1
File Actions Edit View Help

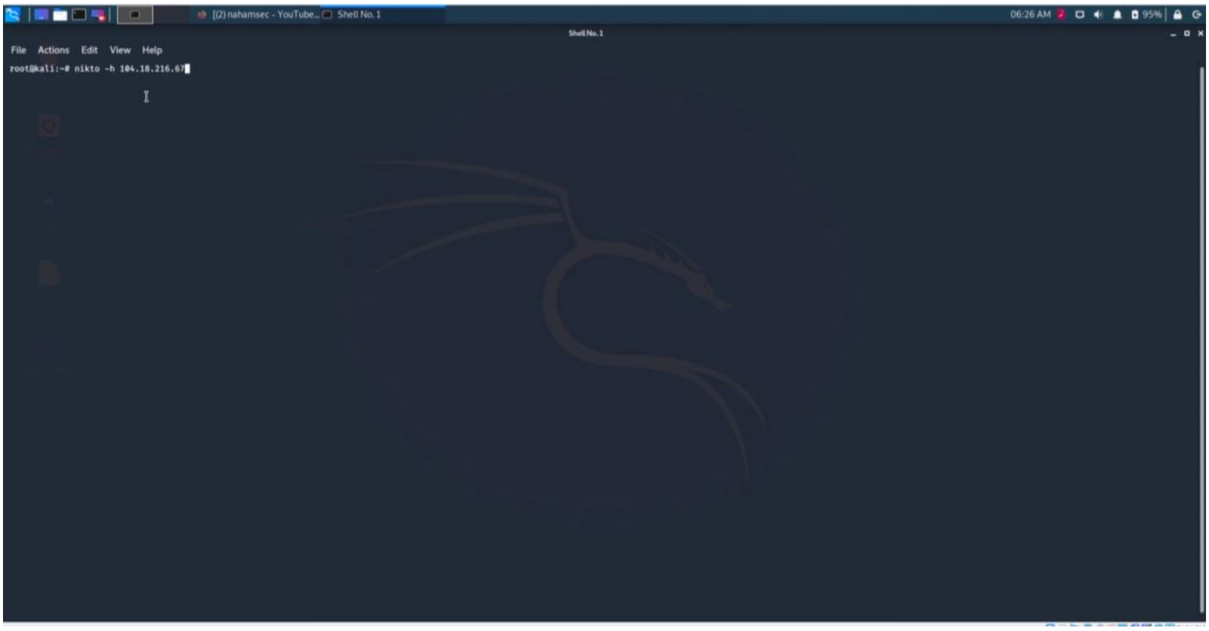
```
root@kali:~# nmap canva.com -v
```



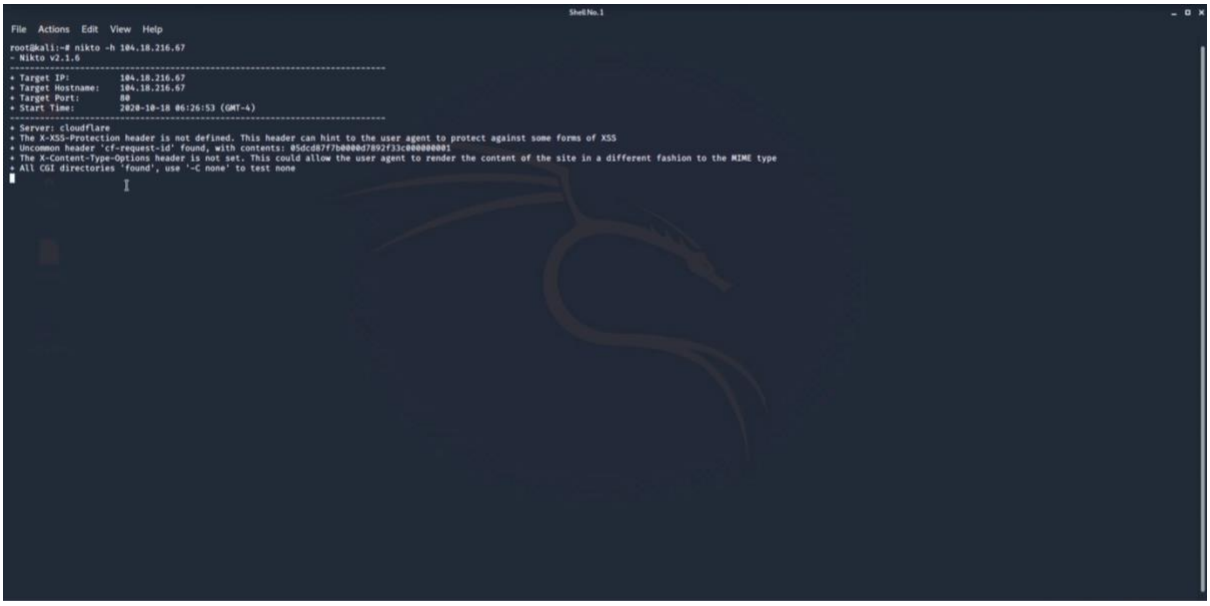
```
root@kali:~# nmap canva.com -v
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-18 06:25 EDT
Initiating Ping Scan at 06:25
Scanning canva.com (104.18.216.67) [4 ports]
Completed Ping Scan at 06:25, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:25
Completed Parallel DNS resolution of 1 host. at 06:25, 0.09s elapsed
Initiating SYN Stealth Scan at 06:25
Scanning canva.com (104.18.216.67) [1000 ports]
Discovered open port 443/tcp on 104.18.216.67
Discovered open port 25/tcp on 104.18.216.67
Discovered open port 8080/tcp on 104.18.216.67
Discovered open port 80/tcp on 104.18.216.67
Discovered open port 8443/tcp on 104.18.216.67
Completed SYN Stealth Scan at 06:25, 10.87s elapsed (1000 total ports)
Nmap scan report for canva.com (104.18.216.67)
Host is up (0.039s latency).
Other addresses for canva.com (not scanned): 104.18.215.67 2606:4700::6812:d743 2606:4700::6812:d843
Not shown: 995 filtered ports
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.20 seconds
           Raw packets sent: 2006 (88.212KB) | Rcvd: 14 (584B)
root@kali:~#
```

This figure shows how I used the Nmap tool to gather information about my domain and detected five open ports as well as the domain's IP address.

Nikto is an open-source vulnerability scanner written in Perl that provides extra vulnerability scanning particular to web servers. It was first released in late 2001. It scans web servers for 6400 potentially harmful files and scripts, 1200 out-of-date server versions, and approximately 300 version-specific issues.

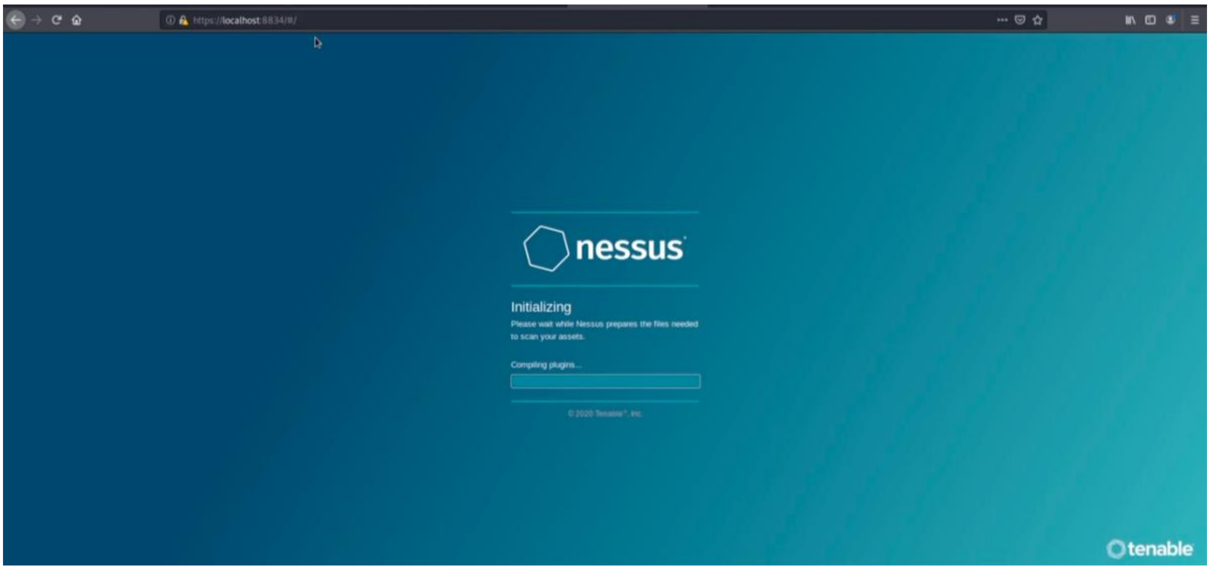


```
root@kali:~# nikto -h 104.18.216.67
```



```
root@kali:~# nikto -h 104.18.216.67
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          104.18.216.67
+ Target Hostname:    104.18.216.67
+ Target Port:        80
+ Start Time:         2020-10-18 06:26:53 (GMT-4)
---------------------------------------------------------------------------
+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'cf-request-id' found, with contents: 05dcd87f7b0000d7892f33c000000001
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
```

Nessus is a remote security scanning application that examines a computer and alerts you if it finds any vulnerabilities that malevolent hackers could exploit to obtain access to any computer on your network. It accomplishes this by doing over 1200 checks on a specific machine, determining whether any of these attacks might be used to break into or harm the machine.

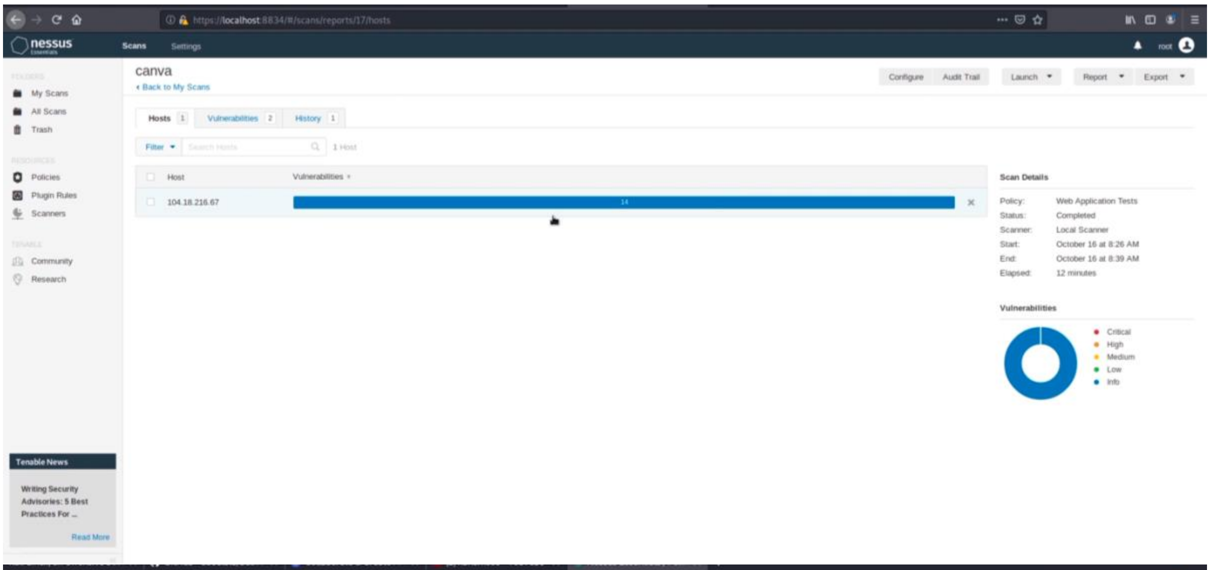


Initializing

Please wait while Nessus prepares the files needed to scan your assets.

Compiling plugins...

© 2020 Tenable®, Inc.



canva

‹ Back to My Scans

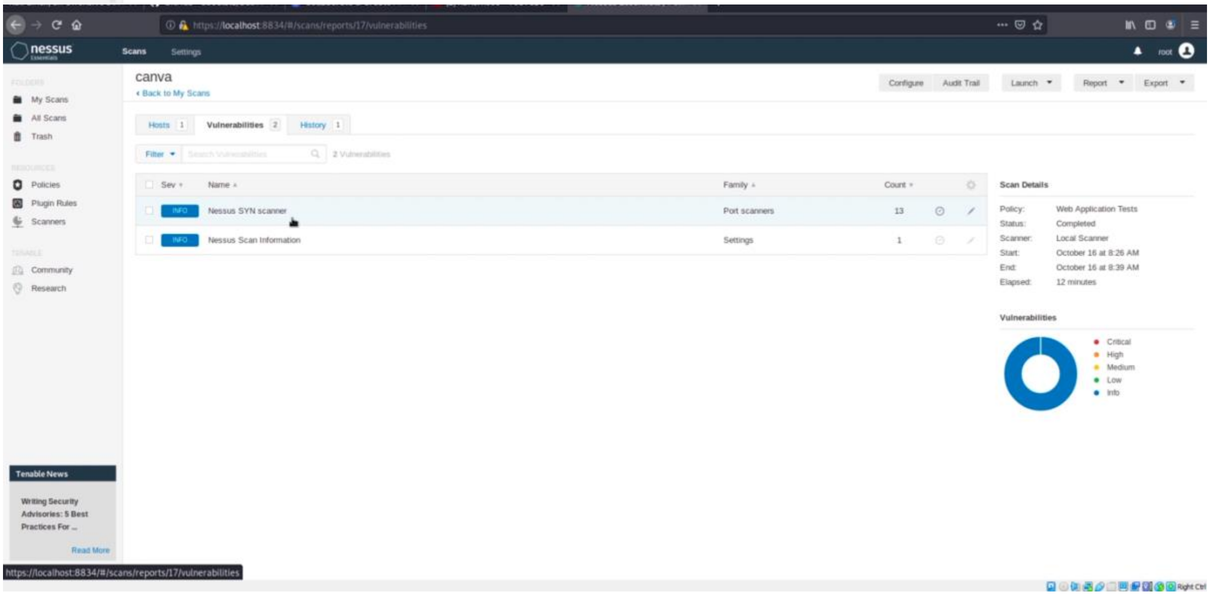
1 Host

Host	Vulnerabilities
104.18.216.67	14

Scan Details

Policy:	Web Application Tests
Status:	Completed
Scanner:	Local Scanner
Start:	October 16 at 8:26 AM
End:	October 16 at 8:39 AM
Elapsed:	12 minutes

Vulnerabilities



canva

‹ Back to My Scans

2 Vulnerabilities

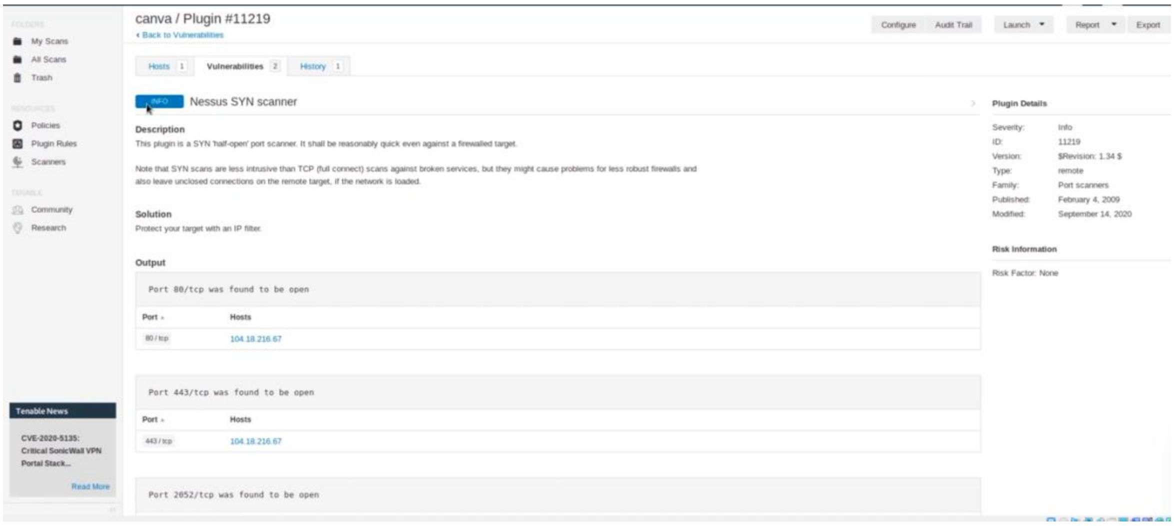
Sev	Name	Family	Count
INFO	Nessus SYN scanner	Port scanners	13
INFO	Nessus Scan Information	Settings	1

Scan Details

Policy:	Web Application Tests
Status:	Completed
Scanner:	Local Scanner
Start:	October 16 at 8:26 AM
End:	October 16 at 8:39 AM
Elapsed:	12 minutes

Vulnerabilities

https://localhost:8834/#/scans/reports/17/vulnerabilities



canva / Plugin #11219

‹ Back to Vulnerabilities

INFO Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

```
Port 80/tcp was found to be open
```

Port	Hosts
80 / tcp	104.18.216.67

```
Port 443/tcp was found to be open
```

Port	Hosts
443 / tcp	104.18.216.67

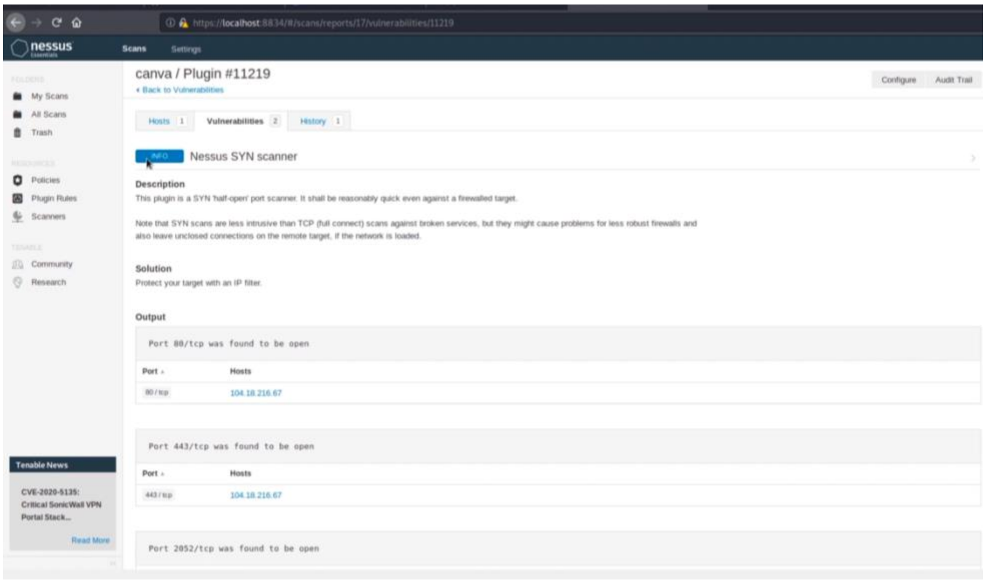
```
Port 2052/tcp was found to be open
```

Plugin Details

Severity:	Info
ID:	11219
Version:	$Revision: 1.34 $
Type:	remote
Family:	Port scanners
Published:	February 4, 2009
Modified:	September 14, 2020

Risk Information

Risk Factor: None



canva / Plugin #11219

Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

```
Port 80/tcp was found to be open
```

Port	Hosts
80 / tcp	104.18.216.67

```
Port 443/tcp was found to be open
```

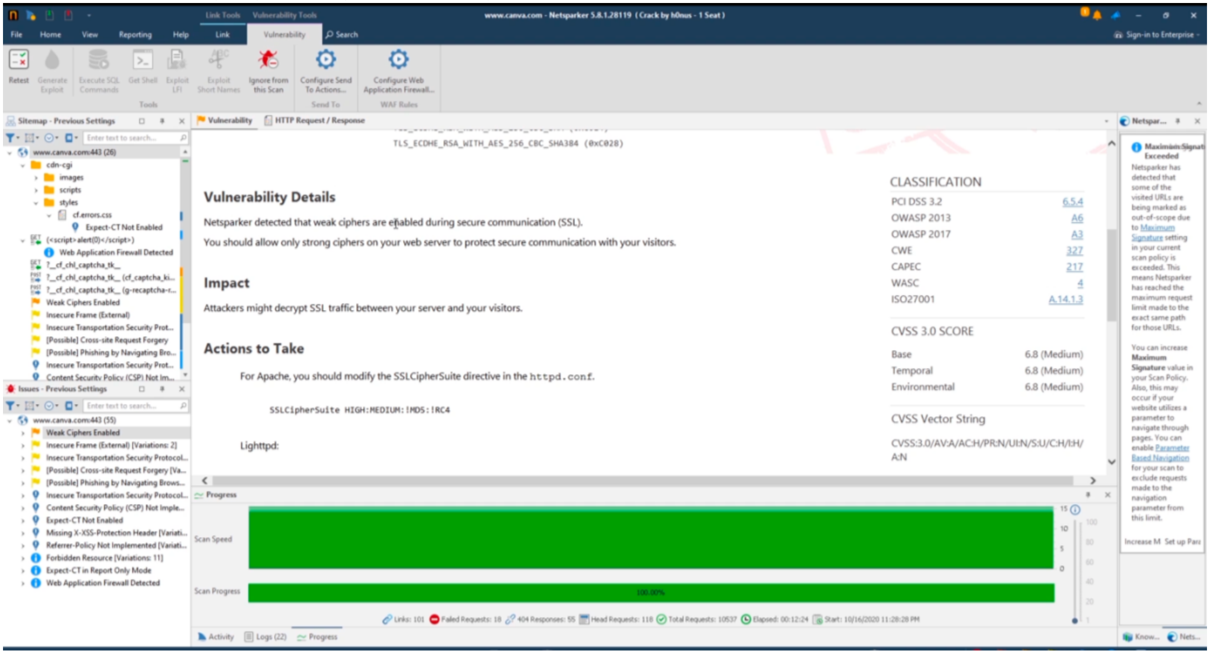
Port	Hosts
443 / tcp	104.18.216.67

```
Port 2052/tcp was found to be open
```

CVE-2020-5135: Critical SonicWall VPN Portal Stack...

report by nessus as a result, the nessuss scan was not successful because I did not receive any high or critical vulnerabilities.

Netspaker is automated web application security scanner that allows you to scan websites, web apps, and web services for security issues while remaining fully customisable. Netsparker can scan any web application, independent of the platform or programming language used to create it. Netsparker is the only online web application security scanner that exploits discovered vulnerabilities in a read-only and secure manner to confirm concerns. It also provides evidence of the vulnerability, so you don't have to waste time manually validating it. For example, if a SQL injection vulnerability is found, the database name will be displayed as proof of exploit.



www.canva.com:443 (26)
- cdn-cgi
  - images
  - scripts
  - styles
    - cf.errors.css
      - Expect-CT Not Enabled
- (<script>alert(0)</script>)
  - Web Application Firewall Detected
- ?__cf_chl_captcha_tk__
- ?__cf_chl_captcha_tk__ (cf_captcha_ki...
- ?__cf_chl_captcha_tk__ (g-recaptcha-r...
- Weak Ciphers Enabled
- Insecure Frame (External)
- Insecure Transportation Security Prot...
- [Possible] Cross-site Request Forgery
- [Possible] Phishing by Navigating Bro...
- Insecure Transportation Security Prot...
- Content Security Policy (CSP) Not Im...

www.canva.com:443 (55)
- Weak Ciphers Enabled
- Insecure Frame (External) [Variations: 2]
- Insecure Transportation Security Protocol...
- [Possible] Cross-site Request Forgery [Va...
- [Possible] Phishing by Navigating Brows...
- Insecure Transportation Security Protocol...
- Content Security Policy (CSP) Not Imple...
- Expect-CT Not Enabled
- Missing X-XSS-Protection Header [Variati...
- Referrer-Policy Not Implemented [Variati...
- Forbidden Resource [Variations: 11]
- Expect-CT in Report Only Mode
- Web Application Firewall Detected

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
```

Vulnerability Details

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Actions to Take

For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

CLASSIFICATION

PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

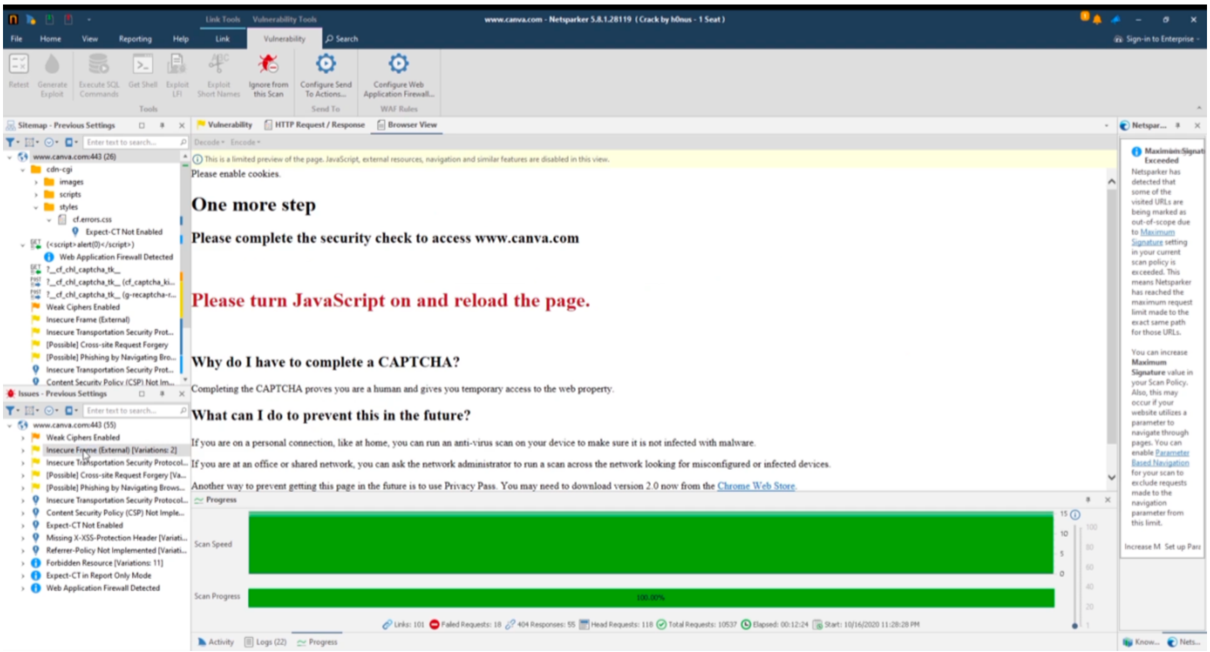
Maximum Signature Exceeded

Netsparker has detected that some of the visited URLs are being marked as out-of-scope due to Maximum Signature setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the exact same path for those URLs.

You can increase **Maximum Signature** value in your Scan Policy. Also, this may occur if your website utilizes a parameter to navigate through pages. You can enable Parameter Based Navigation for your scan to exclude requests made to the navigation parameter from this limit.

Increase M   Set up Para

Links: 101   Failed Requests: 18   404 Responses: 55   Head Requests: 118   Total Requests: 10537   Elapsed: 00:12:24   Start: 10/16/2020 11:28:28 PM



www.canva.com:443 (26)
- cdn-cgi
  - images
  - scripts
  - styles
    - cf.errors.css
      - Expect-CT Not Enabled
- (<script>alert(0)</script>)
  - Web Application Firewall Detected
- ?__cf_chl_captcha_tk__
- ?__cf_chl_captcha_tk__ (cf_captcha_ki...
- ?__cf_chl_captcha_tk__ (g-recaptcha-r...
- Weak Ciphers Enabled
- Insecure Frame (External)
- Insecure Transportation Security Prot...
- [Possible] Cross-site Request Forgery
- [Possible] Phishing by Navigating Bro...
- Insecure Transportation Security Prot...
- Content Security Policy (CSP) Not Im...

www.canva.com:443 (55)
- Weak Ciphers Enabled
- Insecure Frame (External) [Variations: 2]
- Insecure Transportation Security Protocol...
- [Possible] Cross-site Request Forgery [Va...
- [Possible] Phishing by Navigating Brows...
- Insecure Transportation Security Protocol...
- Content Security Policy (CSP) Not Imple...
- Expect-CT Not Enabled
- Missing X-XSS-Protection Header [Variati...
- Referrer-Policy Not Implemented [Variati...
- Forbidden Resource [Variations: 11]
- Expect-CT in Report Only Mode
- Web Application Firewall Detected

This is a limited preview of the page. JavaScript, external resources, navigation and similar features are disabled in this view.

Please enable cookies.

One more step

Please complete the security check to access www.canva.com

Please turn JavaScript on and reload the page.

Why do I have to complete a CAPTCHA?

Completing the CAPTCHA proves you are a human and gives you temporary access to the web property.

What can I do to prevent this in the future?

If you are on a personal connection, like at home, you can run an anti-virus scan on your device to make sure it is not infected with malware.

If you are at an office or shared network, you can ask the network administrator to run a scan across the network looking for misconfigured or infected devices.

Another way to prevent getting this page in the future is to use Privacy Pass. You may need to download version 2.0 now from the Chrome Web Store.

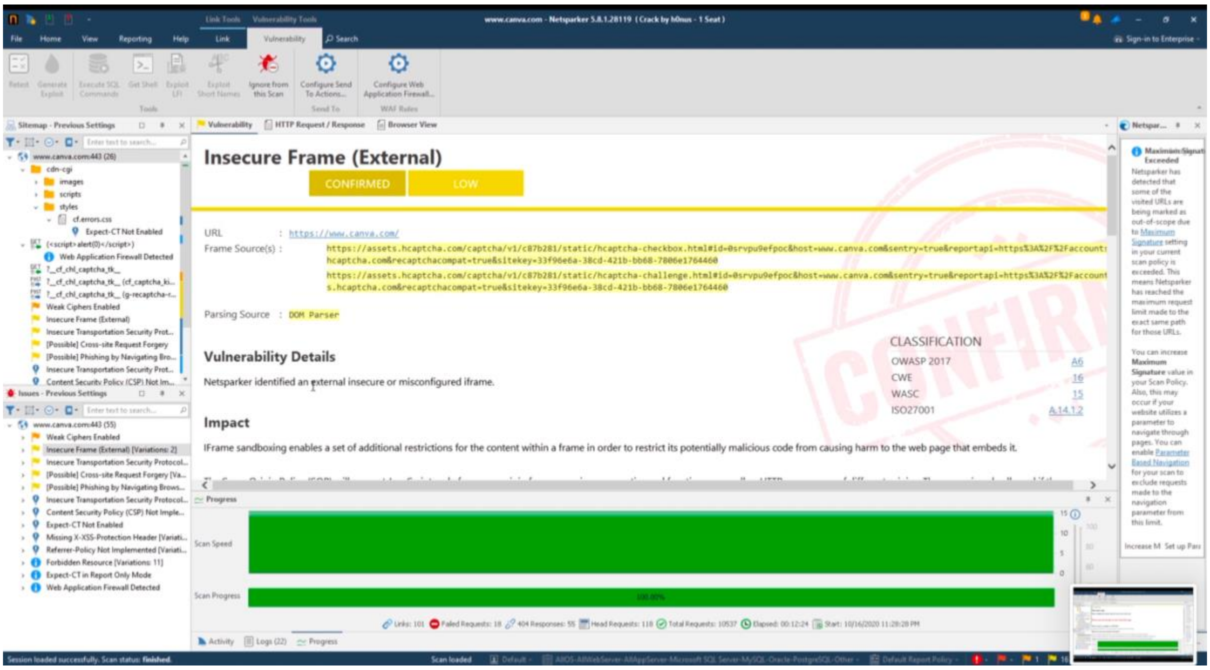
Maximum Signature Exceeded

Netsparker has detected that some of the visited URLs are being marked as out-of-scope due to Maximum Signature setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the exact same path for those URLs.

You can increase **Maximum Signature** value in your Scan Policy. Also, this may occur if your website utilizes a parameter to navigate through pages. You can enable Parameter Based Navigation for your scan to exclude requests made to the navigation parameter from this limit.

Increase M   Set up Para

Links: 101   Failed Requests: 18   404 Responses: 55   Head Requests: 118   Total Requests: 10537   Elapsed: 00:12:24   Start: 10/16/2020 11:28:28 PM


www.canva.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Link Tools
Vulnerability Tools
Link
Vulnerability
Search
Sign-in to Enterprise
Retest
Generate Exploit
Execute SQL Commands
Get Shell
Exploit LFI
Exploit Short Names
Ignore from this Scan
Configure Send To Actions...
Configure Web Application Firewall...
Tools
Send To
WAF Rules
Sitemap - Previous Settings
Enter text to search...
www.canva.com:443 (26)
cdn-cgi
images
scripts
styles
cf.errors.css
Expect-CT Not Enabled
(<script>alert(0)</script>)
Web Application Firewall Detected
?__cf_chl_captcha_tk__
?__cf_chl_captcha_tk__ (cf_captcha_ki...
?__cf_chl_captcha_tk__ (g-recaptcha-r...
Weak Ciphers Enabled
Insecure Frame (External)
Insecure Transportation Security Prot...
[Possible] Cross-site Request Forgery
[Possible] Phishing by Navigating Bro...
Insecure Transportation Security Prot...
Content Security Policy (CSP) Not Im...
Issues - Previous Settings
www.canva.com:443 (55)
Weak Ciphers Enabled
Insecure Frame (External) [Variations: 2]
Insecure Transportation Security Protocol...
[Possible] Cross-site Request Forgery [Va...
[Possible] Phishing by Navigating Brows...
Insecure Transportation Security Protocol...
Content Security Policy (CSP) Not Imple...
Expect-CT Not Enabled
Missing X-XSS-Protection Header [Variati...
Referrer-Policy Not Implemented [Variati...
Forbidden Resource [Variations: 11]
Expect-CT in Report Only Mode
Web Application Firewall Detected
Vulnerability
HTTP Request / Response
Browser View
Netspar...
Progress
Scan Speed
Scan Progress
100.00%
Activity
Logs (22)
Progress
Increase M
Set up Par

Insecure Frame (External)

CONFIRMED LOW

URL : https://www.canva.com/

Frame Source(s) :

```
https://assets.hcaptcha.com/captcha/v1/c87b281/static/hcaptcha-checkbox.html#id=0srvpu9efpoc&host=www.canva.com&sentry=true&reportapi=https%3A%2F%2Faccount
hcaptcha.com&recaptchacompat=true&sitekey=33f96e6a-38cd-421b-bb68-7806e1764460
https://assets.hcaptcha.com/captcha/v1/c87b281/static/hcaptcha-challenge.html#id=0srvpu9efpoc&host=www.canva.com&sentry=true&reportapi=https%3A%2F%2Faccount
s.hcaptcha.com&recaptchacompat=true&sitekey=33f96e6a-38cd-421b-bb68-7806e1764460
```

Parsing Source : DOM Parser

Vulnerability Details

Netsparker identified an external insecure or misconfigured iframe.

CLASSIFICATION	
OWASP 2017	A6
CWE	16
WASC	15
ISO27001	A.14.1.2

Impact

IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

Maximum Signature Exceeded

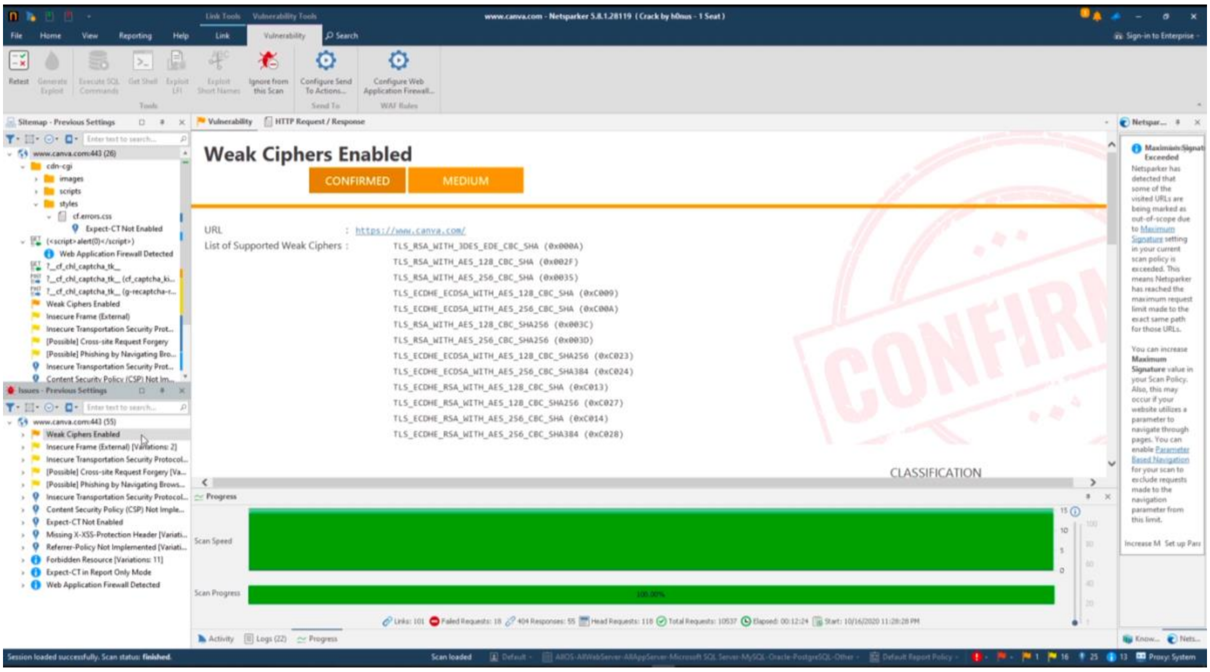
Netsparker has detected that some of the visited URLs are being marked as out-of-scope due to Maximum Signature setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the exact same path for those URLs.

You can increase **Maximum Signature** value in your Scan Policy. Also, this may occur if your website utilizes a parameter to navigate through pages. You can enable Parameter Based Navigation for your scan to exclude requests made to the navigation parameter from this limit.

Links: 101 Failed Requests: 18 404 Responses: 55 Head Requests: 118 Total Requests: 10537 Elapsed: 00:12:24 Start: 10/16/2020 11:28:28 PM

Session loaded successfully. Scan status: **finished.**

Scan loaded Default AllOS-AllWebServer-AllAppServer-Microsoft SQL Server-MySQL-Oracle-PostgreSQL-Other Default Report Policy



Weak Ciphers Enabled

CONFIRMED MEDIUM

URL : https://www.canva.com/

List of Supported Weak Ciphers :

```
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
```

CLASSIFICATION

Maximum Signature Exceeded

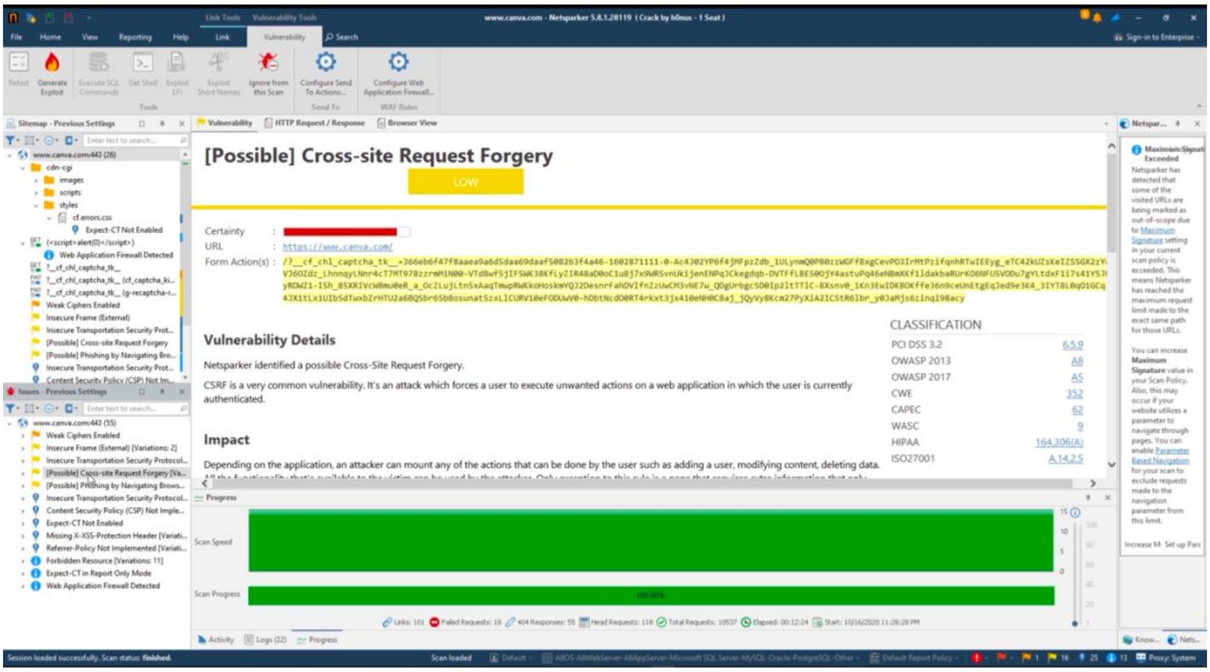
Netsparker has detected that some of the visited URLs are being marked as out-of-scope due to Maximum Signature setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the exact same path for those URLs.

You can increase **Maximum Signature** value in your Scan Policy. Also, this may occur if your website utilizes a parameter to navigate through pages. You can enable Parameter Based Navigation for your scan to exclude requests made to the navigation parameter from this limit.

Links: 101 Failed Requests: 18 404 Responses: 55 Head Requests: 118 Total Requests: 10537 Elapsed: 00:12:24 Start: 10/16/2020 11:28:28 PM

Session loaded successfully. Scan status: **finished.**

Scan loaded Default AllOS-AllWebServer-AllAppServer-Microsoft SQL Server-MySQL-Oracle-PostgreSQL-Other Default Report Policy


Link Tools Vulnerability Tools
File Home View Reporting Help Link Vulnerability Search
Retest Generate Exploit Execute SQL Commands Get Shell Exploit LFI Exploit Short Names Ignore from this Scan Configure Send To Actions... Configure Web Application Firewall...
Tools Send To WAF Rules
Sign-in to Enterprise
Vulnerability HTTP Request / Response Browser View
LOW
Scan Speed
Scan Progress
100.00%
Activity Logs (22) Progress
Know... Nets...

www.canva.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)

Sitemap - Previous Settings

- www.canva.com:443 (26)
  - cdn-cgi
    - images
    - scripts
    - styles
      - cf.errors.css
        - Expect-CT Not Enabled
  - (<script>alert(0)</script>)
    - Web Application Firewall Detected
  - ?__cf_chl_captcha_tk__
  - ?__cf_chl_captcha_tk__ (cf_captcha_ki...
  - ?__cf_chl_captcha_tk__ (g-recaptcha-r...
  - Weak Ciphers Enabled
  - Insecure Frame (External)
  - Insecure Transportation Security Prot...
  - [Possible] Cross-site Request Forgery
  - [Possible] Phishing by Navigating Bro...
  - Insecure Transportation Security Prot...
  - Content Security Policy (CSP) Not Im...

Issues - Previous Settings

- www.canva.com:443 (55)
  - Weak Ciphers Enabled
  - Insecure Frame (External) [Variations: 2]
  - Insecure Transportation Security Protocol...
  - [Possible] Cross-site Request Forgery [Va...
  - [Possible] Phishing by Navigating Brows...
  - Insecure Transportation Security Protocol...
  - Content Security Policy (CSP) Not Imple...
  - Expect-CT Not Enabled
  - Missing X-XSS-Protection Header [Variati...
  - Referrer-Policy Not Implemented [Variati...
  - Forbidden Resource [Variations: 11]
  - Expect-CT in Report Only Mode
  - Web Application Firewall Detected

[Possible] Cross-site Request Forgery

LOW

Certainty :

URL : https://www.canva.com/

Form Action(s) : /?__cf_chl_captcha_tk__=366eb6f47f8aaea9a6d5daa69daaf5082b3f4a46-1602871111-0-Ac4J02YP6f4jMFpzZdb_1ULynmQ0PB0zzWGFfBxgCevPO3IrMtPzifqnhRTwIEEyg_eTC42kUZsKeIZSSGX2zY VJ6OZdz_LhnnqyLNnr4cT7MT978zzrmMiN00-VTd8wf5jIFSWK38KfLyZIR48aD0oC1uBj7x9WRSvnUkijenENPqJCkegdqb-DVTFfLBE50OjY4astuPq46eN8mXXf1ldakbaRUrKO6NFUSVODu7gYLtdxF1i7s41YSJ yRDWZ1-ISh_85XRIVcWBmu0eR_a_OcZLujLtn5xAaqTmwpRWKkoHoskmYQJ2DesnrFahDVlfnZzUwCM3vNE7w_QDgUrbgcSD0Ip2ltTTlC-BXsnv0_1Kn3EwIDKBOKffe36n9ceUnEtgEqJed9e3K4_3IYT8L0qO1GCq 4JX1tLx1UIbSdTwxbZrHTU2a6BQSbr6Sb8osunatSzxLlCURV10eFODUwV0-hDbtNcdO0RT4rkxt3jx410eNH0C8aj_jQyVy8Kcm27PyXiA2ICStR6lbr_y0JaMjs6zinqi98acy

Vulnerability Details

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data.

CLASSIFICATION

PCI DSS 3.2	6.5.9
OWASP 2013	A8
OWASP 2017	A5
CWE	352
CAPEC	62
WASC	9
HIPAA	164.306(A)
ISO27001	A.14.2.5

Progress

Links: 101 Failed Requests: 18 404 Responses: 55 Head Requests: 118 Total Requests: 10537 Elapsed: 00:12:24 Start: 10/16/2020 11:28:28 PM

Netspar...

Maximum Signature Exceeded

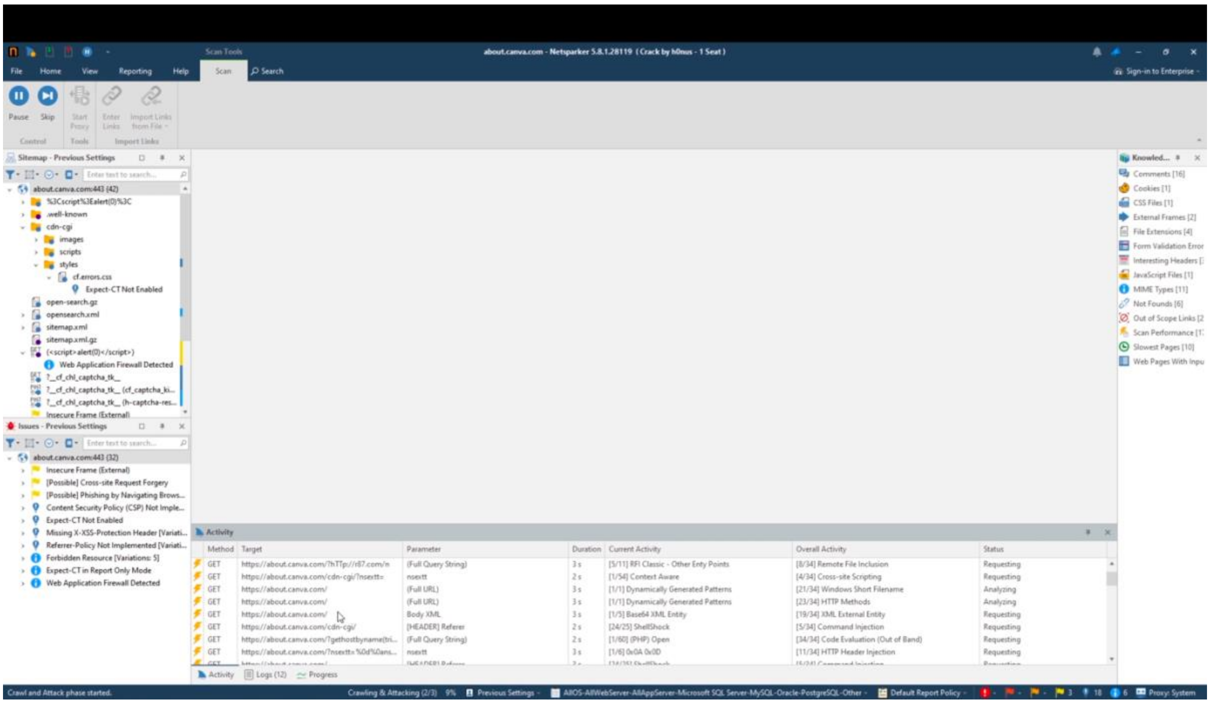
Netsparker has detected that some of the visited URLs are being marked as out-of-scope due to Maximum Signature setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the exact same path for those URLs.

You can increase **Maximum Signature** value in your Scan Policy. Also, this may occur if your website utilizes a parameter to navigate through pages. You can enable Parameter Based Navigation for your scan to exclude requests made to the navigation parameter from this limit.

Increase M Set up Par

Session loaded successfully. Scan status: **finished.**

Scan loaded Default AllOS-AllWebServer-AllAppServer-Microsoft SQL Server-MySQL-Oracle-PostgreSQL-Other Default Report Policy 1 16 25 13 Proxy: System


Scan Tools
File Home View Reporting Help Scan Search
Pause Skip Start Proxy Enter Links Import Links from File
Control Tools Import Links
Sign-in to Enterprise
Activity Logs (12) Progress

about.canva.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)

Sitemap - Previous Settings

- about.canva.com:443 (42)
  - %3Cscript%3Ealert(0)%3C
  - .well-known
  - cdn-cgi
    - images
    - scripts
    - styles
      - cf.errors.css
        - Expect-CT Not Enabled
  - open-search.gz
  - opensearch.xml
  - sitemap.xml
  - sitemap.xml.gz
  - (<script>alert(0)</script>)
    - Web Application Firewall Detected
  - ?__cf_chl_captcha_tk__
  - ?__cf_chl_captcha_tk__ (cf_captcha_ki...
  - ?__cf_chl_captcha_tk__ (h-captcha-res...
  - Insecure Frame (External)

Issues - Previous Settings

- about.canva.com:443 (32)
  - Insecure Frame (External)
  - [Possible] Cross-site Request Forgery
  - [Possible] Phishing by Navigating Brows...
  - Content Security Policy (CSP) Not Imple...
  - Expect-CT Not Enabled
  - Missing X-XSS-Protection Header [Variati...
  - Referrer-Policy Not Implemented [Variati...
  - Forbidden Resource [Variations: 5]
  - Expect-CT in Report Only Mode
  - Web Application Firewall Detected

Knowled...

- Comments [16]
- Cookies [1]
- CSS Files [1]
- External Frames [2]
- File Extensions [4]
- Form Validation Error
- Interesting Headers [
- JavaScript Files [1]
- MIME Types [11]
- Not Founds [6]
- Out of Scope Links [2
- Scan Performance [1
- Slowest Pages [10]
- Web Pages With Inpu

Activity

Method	Target	Parameter	Duration	Current Activity	Overall Activity	Status
GET	https://about.canva.com/?hTTp://r87.com/n	(Full Query String)	3 s	[5/11] RFI Classic - Other Enty Points	[8/34] Remote File Inclusion	Requesting
GET	https://about.canva.com/cdn-cgi/?nsextt=	nsextt	2 s	[1/54] Context Aware	[4/34] Cross-site Scripting	Requesting
GET	https://about.canva.com/	(Full URL)	3 s	[1/1] Dynamically Generated Patterns	[21/34] Windows Short Filename	Analyzing
GET	https://about.canva.com/	(Full URL)	3 s	[1/1] Dynamically Generated Patterns	[23/34] HTTP Methods	Analyzing
GET	https://about.canva.com/	Body XML	3 s	[1/5] Base64 XML Entity	[19/34] XML External Entity	Requesting
GET	https://about.canva.com/cdn-cgi/	[HEADER] Referer	2 s	[24/25] ShellShock	[5/34] Command Injection	Requesting
GET	https://about.canva.com/?gethostbyname(tri...	(Full Query String)	2 s	[1/60] (PHP) Open	[34/34] Code Evaluation (Out of Band)	Requesting
GET	https://about.canva.com/?nsextt=%0d%0ans...	nsextt	3 s	[1/6] 0x0A 0x0D	[11/34] HTTP Header Injection	Requesting

Crawl and Attack phase started.

Crawling & Attacking (2/3) 9% Previous Settings AllOS-AllWebServer-AllAppServer-Microsoft SQL Server-MySQL-Oracle-PostgreSQL-Other Default Report Policy 3 18 6 Proxy: System

Conclusion

To do my site audit, I employed a variety of technologies , Sublist3r, Nmap, Nikto, Nessuss, and Netsparker are the tools in question. However, none of the above scans revealed any high, critical, or impactful vulnerabilities in the canva.com domain. As a result, in my opinion, canva.com is a significantly more secure web application.