



Sri Lanka Institute of Information Technology

IE2062-Web Security

IT Number	Name
IT22581402	C.D.Aluthge

Information gathering and reconnaissance phase

- a. Subdomain enumeration
 - i. Recon-ng
- b. Getting alive subdomains
 - i. Nslookup
- c. DNS enumeration
 - i. Dnsrecon
- d. Public devices enumeration
 - i. Censys
- e. Find WAF (web application firewall) protection.
 - i. Wafwoof
- f. Find open ports.
 - i. Nmap
- g. Exploitation
 - i. sqlmap

vulnerability analysis phase

1. Target domain: <http://www.booking.com>



- a. Weak Ciphers Enabled (Confirmed)
- b. [Possible] Phishing by Navigating Browser Tabs
- c. Web Application Firewall Detected
- d. Unexpected Redirect Response Body (Too Large)
- e. Forbidden Resource
- f. Missing X-XSS-Protection Header

Conclusion

Scope:

One popular online travel agency (OTA) that makes it easier to book hotels, flights, rental cars, and other travel-related services is Booking.com. Since its founding in 1996, it has developed into one of the biggest and most well-known travel platforms worldwide. Travelers can look up and reserve a variety of lodging options in locations all over the world, including as hostels, hotels, apartments, villas, and more. To assist consumers in making well-informed booking selections, the portal offers comprehensive details, photographs, reviews, and ratings for each property. Booking.com provides a range of travel-related incentives and discounts in addition to customer support services.


Booking.com



LKR   List your property [Register](#) [Sign in](#)



[Stays](#) [Flights](#) [Car rentals](#) [Attractions](#) [Airport taxis](#)

Find your next stay

Search deals on hotels, homes, and much more...

 Where are you going?

 Check-in Date —  Check-out Date

 2 adults · 0 children · 1 room 

[Search](#)


Offers

Promotions, deals, and special offers for you

Planning a trip to the 2024 Summer Games?

Brussels is a quick train ride from all the action


[Explore Brussels](#)
























































Seize the moment!

Save 15% or more when you book and stay before October 2024

[Find Getaway Deals](#)



In Scope:

Asset name 	Type 	Coverage 	Max. severity 	Bounty 	Last update 	Resolved Reports 
https://iphone-xml.booking.com/json/	URL	In scope	 Critical	 Eligible	Nov 29, 2023	0 (0%)
https://secure-iphone-xml.booking.com/json/	URL	In scope	 Critical	 Eligible	Dec 13, 2023	0 (0%)
supplier.auth.toag.booking.com	Domain	In scope	 Critical	 Eligible	Jan 24, 2023	0 (0%)
metasearch-api.booking.com	Domain	In scope	 Critical	 Eligible	Nov 7, 2023	0 (0%)
experiences.booking.com	Domain	In scope	 Critical	 Eligible	Nov 7, 2023	0 (0%)
webhooks.booking.com	Domain	In scope	 Critical	 Eligible	Nov 29, 2023	0 (0%)
paybridge.booking.com	Domain	In scope	 Critical	 Eligible	Dec 13, 2023	0 (0%)
phone-validation.taxi.booking.com	Domain	In scope	 Critical	 Eligible	Dec 13, 2023	0 (0%)
autocomplete.booking.com	Domain	In scope	 Critical	 Eligible	Nov 29, 2023	0 (0%)
distribution-xml.booking.com	Domain	In scope	 Critical	 Eligible	Nov 29, 2023	0 (0%)
paynotifications.booking.com	Domain	In scope	 Critical	 Eligible	Dec 13, 2023	0 (0%)
supply-xml.booking.com	Domain	In scope	 Critical	 Eligible	Dec 13, 2023	0 (0%)
portal.taxi.booking.com	Domain	In scope	 Critical	 Eligible	Nov 29, 2023	0 (0%)
secure-supply-xml.booking.com	Domain	In scope	 Critical	 Eligible	Nov 29, 2023	0 (0%)
http://secure-iphone-xml.booking.com/json/	URL	In scope	 Critical	 Eligible	Dec 13, 2023	0 (0%)
kyc-onboarding.booking.com	Domain	In scope	 Critical	 Eligible	Dec 13, 2023	0 (0%)
teleport.fareharbor.engineering	Domain	In scope	 Critical	 Eligible	Mar 19, 2024	0 (0%)
paymentcomponent.booking.com	Domain	In scope	 Critical	 Eligible	Dec 13, 2023	0 (0%)
spark.fareharbor.com	Domain	In scope	 Critical	 Eligible	Feb 20, 2024	0 (0%)
flights.booking.com	Domain	In scope	 Critical	 Eligible	Nov 6, 2023	0 (0%)
indicative-pricing.taxi.booking.com	Domain	In scope	 Critical	 Eligible	Dec 13, 2023	0 (0%)
taxi.booking.com	Domain	In scope	 Critical	 Eligible	Nov 6, 2023	0 (0%)
<div>New</div> marketing.fareharbor.com	Domain	In scope	 Critical	 Eligible	<div>Updated</div> Apr 16, 2024	0 (0%)

New	readonly.fareharbor.com	Domain	In scope	<div>Critical</div>	Eligible	Updated Apr 16, 2024	0 (0%)
New	demo.fareharbor.com	Domain	In scope	<div>Critical</div>	Eligible	Updated Apr 16, 2024	0 (0%)
	taxis.booking.com	Domain	In scope	<div>Critical</div>	Eligible	Dec 13, 2023	0 (0%)
New	sites.fareharbor.com	Domain	In scope	<div>Critical</div>	Eligible	Updated Apr 16, 2024	0 (0%)
	chat.booking.com	Domain	In scope	<div>Critical</div>	Eligible	Nov 29, 2023	0 (0%)
	widget.rentalcars.com	Domain	In scope	<div>Critical</div>	Eligible	Nov 15, 2023	0 (0%)
	cars.booking.com	Domain	In scope	<div>Critical</div>	Eligible	Jul 13, 2023	0 (0%)
	careers.booking.com	Domain	In scope	<div>Critical</div>	Eligible	Nov 6, 2023	0 (0%)
	www.fareharbor.com	Domain	In scope	<div>Critical</div>	Eligible	Mar 5, 2024	0 (0%)
	secure.booking.com	Domain	In scope	<div>Critical</div>	Eligible	Nov 6, 2023	0 (0%)
	account.booking.com	Domain	In scope	<div>Critical</div>	Eligible	Nov 6, 2023	0 (0%)
*.rentalcars.com if there's any vulnerabilities raised on this asset that are owned by a third party we will not be accepting those reports		Wildcard	In scope	<div>Critical</div>	Eligible	Feb 29, 2024	0 (0%)
	accommodations.booking.com	Domain	In scope	<div>Critical</div>	Eligible	Nov 29, 2023	0 (0%)
	booking.com	Domain	In scope	<div>Critical</div>	Eligible	Nov 6, 2023	0 (0%)
	admin.booking.com	Domain	In scope	<div>Critical</div>	Eligible	Nov 29, 2023	0 (0%)
*.booking.com if there's any vulnerabilities raised on this asset that are owned by a third party we will not be accepting those reports		Wildcard	In scope	<div>Critical</div>	Eligible	Feb 29, 2024	0 (0%)

Out of Scope:

www.booking.com/bbmanage/*	Wildcard	Out of scope	<div><div></div></div> None	🚫 Ineligible	Mar 19, 2024	0 (0%)
www.booking.com/bbmanage/data/*	Wildcard	Out of scope	<div><div></div></div> None	🚫 Ineligible	Mar 19, 2024	0 (0%)
secure.booking.com/orgnode/*	Wildcard	Out of scope	<div><div></div></div> None	🚫 Ineligible	Mar 19, 2024	0 (0%)
business.booking.com/	Domain	Out of scope	<div><div></div></div> None	🚫 Ineligible	Mar 19, 2024	0 (0%)
spadmin.booking.com/	Domain	Out of scope	<div><div></div></div> None	🚫 Ineligible	Mar 19, 2024	0 (0%)
secure.booking.com/company/*	Wildcard	Out of scope	<div><div></div></div> None	🚫 Ineligible	Mar 19, 2024	0 (0%)
https://www.booking.com/bbm.html	URL	Out of scope	<div><div></div></div> None	🚫 Ineligible	Mar 19, 2024	0 (0%)
https://secure.booking.com/companyjoin.html	URL	Out of scope	<div><div></div></div> None	🚫 Ineligible	Mar 19, 2024	0 (0%)
https://secure.booking.com/enterprise/signon.en-gb.html	URL	Out of scope	<div><div></div></div> None	🚫 Ineligible	Mar 19, 2024	0 (0%)
https://ugcupload.booking.com/upload_bbttool_company_logo	URL	Out of scope	<div><div></div></div> None	🚫 Ineligible	Mar 19, 2024	0 (0%)
https://fareharbor.com/demo/	URL	Out of scope	<div><div></div></div> None	🚫 Ineligible	Mar 19, 2024	0 (0%)

OWASP top 10 vulnerabilities

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery
- Broken Access Control

When users are unable to adequately impose limitations on what they can access or do within a system, this is known as broken access control. This vulnerability makes

it possible for unauthorized individuals to access private data or carry out tasks that shouldn't be permitted. Insecure references to objects, improperly configured permissions, and a lack of authentication checks are the causes of it. Because it can result in illegal data exposure, manipulation, or system penetration, it's a major problem.

Cryptographic Failures

Cryptographic collapses are the result of poor algorithms, incorrect implementations, or improper management of encryption keys, which compromise the security of information encrypted via encryption techniques. Undermining security safeguards and perhaps leading in data breaches, this can lead to unauthorized access to or exposure of sensitive data.

Injection

Injection: it is a type of security vulnerability in which untrusted data is sent to an interpreter as part of a command or query. Most often, attackers use this to inject malicious code into input fields, for example, login forms or search boxes. The interpreter then executes this code, which can give the attacker unauthorized access to data, alter the application's behavior, or gain full control over the system. There are many types of injections, such as SQL injection, where the attackers manipulate database queries, or cross-site scripting, where the malicious script is injected into a web page that other users view.

Insecure Design

Insecure design means the security flaws within the fundamental system or application design born out of insufficient attention to security at the design time.

Consequently, systems have vulnerabilities that enable unauthorized system access or breaches. Examples are poor user authentication or no network segmentation. To fix insecure design, significant changes to the architecture are needed to develop the designs securely.

Security Misconfiguration

Imagine you accidentally leave your front door closed but not locked. That's what a security misconfiguration is like. Essentially, it's not properly securing your software systems, servers, or web applications. This can include default settings, shipped insecurely, or unnecessary features. Unauthorized users might target such vulnerabilities to access your info or disrupt the operation. Therefore, one should monitor and update security measures continuously to avoid misconfiguration.

Vulnerable and Outdated Components

Vulnerable components are software elements that are known to contain security flaws that could be exploited by hackers. However, software components that have not received an upgrade in a long time are known as outdated components, and they may not include important security updates and bug fixes. In order to maintain a secure system environment, both sorts of components present security concerns and should be routinely updated and monitored.

Identification and Authentication Failures

When systems are unable to accurately confirm user identities or authenticate their access credentials, identification and authentication failures take place. Whereas authentication failures are caused by an inability to verify user identities, identification failures are the consequence of incorrect user recognition. In order to identify and fix system vulnerabilities, strong authentication procedures and frequent

security assessments are essential. These failures might result in unauthorized access and security breaches.

Software and Data Integrity Failures

Software code or data accuracy, consistency, and reliability are jeopardized in software and data integrity issues. Data integrity problems are caused by mistakes, unauthorized access, or cyberattacks, whereas programming errors, malicious code, or unauthorized alterations are the causes of software integrity problems. To reduce risks and guarantee system security and dependability, preventive measures include backups, data encryption, access controls, and regular updates.

Security Logging and Monitoring Failures

Failed security logging and monitoring systems result in a delayed detection of security incidents and higher risks since they are unable to reliably capture and evaluate security-related events. Monitoring failures are caused by insufficient tools or response protocols, whereas logging failures are caused by misconfigurations or deactivated logging systems. Organizations should establish strong response protocols, use comprehensive logging practices, deploy efficient monitoring tools like SIEM tools, train security teams, and continuously improve logging and monitoring configurations in light of best practices and emerging threats in order to address these failures. By taking these steps, cybersecurity defenses are strengthened and the effects of security events are lessened

Server-Side Request Forgery

A security flaw known as server-side request forgery (SSRF) allows attackers to take control of a susceptible server and send unwanted requests, usually to external or internal systems. Unauthorized access, data loss, and more exploitation may result from this. Input validation, whitelisting authorized resources, network segmentation, and access controls are all part of prevention. Frequent security testing improves

overall system security by assisting in the identification and mitigation of SSRF threats.

Information gathering and reconnaissance phase.

The objective is to gather as much pertinent data as you can about the intended system or organization. Understanding the target's infrastructure, seeing potential vulnerabilities, and organizing additional security testing operations are all made easier with the aid of this information.

Domain: <http://www.booking.com>

Subdomain enumeration

- Recon-ng

Recon-ng is an open-source reconnaissance tool with Python foundation that is used for penetration testing and security evaluations. It collects data from domains, IPs, emails, and social media platforms using a modular framework with different modules. The advantages of recon-ng are its flexibility for scripting and automation, integration with many data sources, and data enrichment capabilities. It is used by security experts to gather and evaluate intelligence, spot possible weaknesses, and

improve overall security posture during the first reconnaissance phase. Its vibrant community guarantees continuous upgrades and support, which makes it an invaluable addition to cybersecurity toolkits.

Proof of concept:

```
(deshan@kali)~]
$ recon-ng
[*] Version check disabled.
```



Sponsored by ...



more you are able to hear"



[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

Proof of concept:

```
Source Options:
  default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>     string representing a single input
  <path>       path to a file containing a list of inputs
  query <sql>  database query returning one column of inputs

[recon-ng][default][google_site_web] > options set source booking.com
SOURCE => booking.com
[recon-ng][default][google_site_web] > run

BOOKING.COM

[*] Searching Google for: site:booking.com
[*] Country: None
[*] Host: partner.booking.com "the quieter you become, the more you are able to hear"
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
```

```
[1] Recon modules
[recon-ng][default] > marketplace search google
[*] Searching module index for 'google'...
```

Path	Version	Status	Updated	D	K
recon/domains-hosts/google_site_web	1.0	installed	2019-06-24		

```

D = Has dependencies. See info for details.
K = Requires keys. See info for details.
[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules ...
[recon-ng][default] > show info
Shows various framework items
Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>
[recon-ng][default] > marketplace search google
[*] Searching module index for 'google'...
```

Path	Version	Status	Updated	D	K
recon/domains-hosts/google_site_web	1.0	installed	2019-06-24		

```

D = Has dependencies. See info for details.
K = Requires keys. See info for details.
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > info
    Name: Google Hostname Enumerator
    Author: Tim Tomes (@lanmaster53)
    Version: 1.0
Description:
    Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.
Options:
    Name      Current Value  Required  Description
    SOURCE    skinport.com    yes       source of input (see 'info' for details)
```

Proof of concept:

```

[*] _____
[*] Country: None
[*] Host: news.booking.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: www.booking.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: careers.booking.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
```

```

[*] -----
[*] Country: None
[*] Host: careers.booking.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: developers.booking.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: business.booking.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----

[*]
[*] Country: None
[*] Host: join.booking.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Searching Google for: site:booking.com -site:partner.booking.com -site:news.booking.com -site:www.booking.
com -site:careers.booking.com -site:developers.booking.com -site:business.booking.com -site:cruises.booking.co
m -site:www.sustainability.booking.com -site:join.booking.com
[*] Country: None
[*] Host: admin.booking.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----

```

Proof of concept:

```

[*] Searching Google for: site:booking.com -site:partner.booking.com -site:news.booking.com -site:www.booking.com -site:careers.booking.com -site:developers.booking.com -site:business.booking.com -site:cruises.booking.com -site:www.sustainability.booking.com -site:join.booking.com -site:admin.booking.com -site:affiliates.support.booking.com -site:discover.booking.com -site:connectivity.booking.com -site:secure.booking.com -site:jobs.booking.com -site:connect.booking.com -site:blog.booking.com -site:partnerships.booking.com -site:cars.booking.com -site:transportaffiliates.support.booking.com
[*] Country: None
[*] Host: account.booking.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]

[*] Searching Google for: site:booking.com -site:partner.booking.com -site:news.booking.com -site:www.booking.com -site:careers.booking.com -site:developers.booking.com -site:business.booking.com -site:cruises.booking.com -site:www.sustainability.booking.com -site:join.booking.com -site:admin.booking.com -site:affiliates.support.booking.com -site:discover.booking.com -site:connectivity.booking.com -site:secure.booking.com -site:jobs.booking.com -site:connect.booking.com -site:blog.booking.com -site:partnerships.booking.com -site:cars.booking.com -site:transportaffiliates.support.booking.com -site:account.booking.com
[*] Country: None
[*] Host: taxi.booking.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]

[*] Searching Google for: site:booking.com -site:partner.booking.com -site:news.booking.com -site:www.booking.com -site:careers.booking.com -site:developers.booking.com -site:business.booking.com -site:cruises.booking.com -site:www.sustainability.booking.com -site:join.booking.com -site:admin.booking.com -site:affiliates.support.booking.com -site:discover.booking.com -site:connectivity.booking.com -site:secure.booking.com -site:jobs.booking.com -site:connect.booking.com -site:blog.booking.com -site:partnerships.booking.com -site:cars.booking.com -site:transportaffiliates.support.booking.com -site:account.booking.com -site:taxi.booking.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 201.

[*] No New Subdomains Found on the Current Page. Jumping to Result 6301.
[*] Searching Google for: site:booking.com -site:partner.booking.com -site:news.booking.com -site:www.booking.com -site:careers.booking.com -site:developers.booking.com -site:business.booking.com -site:cruises.booking.com -site:www.sustainability.booking.com -site:join.booking.com -site:admin.booking.com -site:affiliates.support.booking.com -site:discover.booking.com -site:connectivity.booking.com -site:secure.booking.com -site:jobs.booking.com -site:connect.booking.com -site:blog.booking.com -site:partnerships.booking.com -site:cars.booking.com -site:transportaffiliates.support.booking.com -site:account.booking.com -site:taxi.booking.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 6401.
[*] Searching Google for: site:booking.com -site:partner.booking.com -site:news.booking.com -site:www.booking.com -site:careers.booking.com -site:developers.booking.com -site:business.booking.com -site:cruises.booking.com -site:www.sustainability.booking.com -site:join.booking.com -site:admin.booking.com -site:affiliates.support.booking.com -site:discover.booking.com -site:connectivity.booking.com -site:secure.booking.com -site:jobs.booking.com -site:connect.booking.com -site:blog.booking.com -site:partnerships.booking.com -site:cars.booking.com -site:transportaffiliates.support.booking.com -site:account.booking.com -site:taxi.booking.com
[!] Google CAPTCHA triggered. No bypass available.

SUMMARY

[*] 22 total (22 new) hosts found.
[recon-ng][default][google_site_web] >

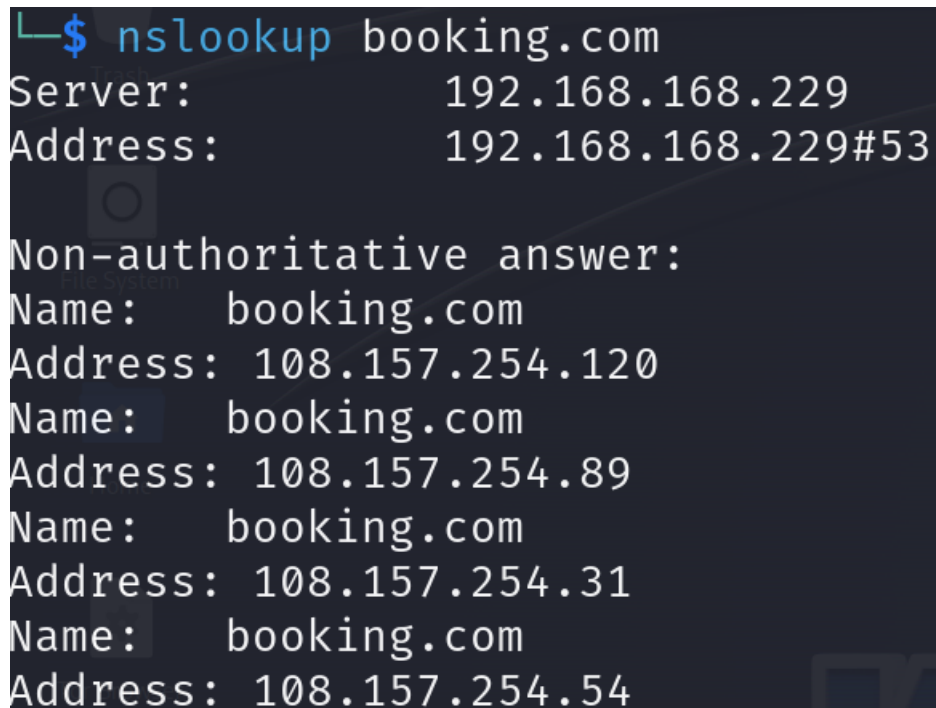
```

Getting alive subdomains

- Nslookup

A command-line utility called `nslookup` is used to query DNS (Domain Name System) servers and get DNS-related data. In addition to performing reverse DNS lookups and retrieving other DNS records like A, AAAA, MX, NS, PTR, and TXT records, it resolves domain names to IP addresses. It is flexible for diagnosing DNS problems, validating DNS configurations, and testing DNS servers because it may be used in both interactive and non-interactive modes. Network administrators and cybersecurity experts frequently utilize `nslookup`, which runs on several platforms, for DNS-related activities and diagnostics.

Proof of concept:

A terminal window with a dark background. The command 'nslookup booking.com' is entered at the prompt. The output shows the server IP as 192.168.168.229 and the address as 192.168.168.229#53. Below this, it indicates a 'Non-authoritative answer:' and lists four A records for booking.com with IP addresses 108.157.254.120, 108.157.254.89, 108.157.254.31, and 108.157.254.54.

```
└─$ nslookup booking.com
Server:          192.168.168.229
Address:         192.168.168.229#53

Non-authoritative answer:
Name:   booking.com
Address: 108.157.254.120
Name:   booking.com
Address: 108.157.254.89
Name:   booking.com
Address: 108.157.254.31
Name:   booking.com
Address: 108.157.254.54
```

DNS enumeration

- Dnsrecon

For security evaluations and penetration tests, DNSRecon is a powerful open-source tool for DNS reconnaissance that finds and counts DNS information. It is particularly good at finding subdomains, enumerating DNS records (A, AAAA, MX, NS, SOA, TXT), transferring DNS zones, and it can handle wordlist-based and brute-force attacks. With its automation, customization, and integration features, it's a useful tool for figuring out possible attack points, comprehending target infrastructure, and raising security awareness in general. DNSRecon is still a dependable option for DNS reconnaissance operations because of its community support and frequent updates.

Proof of concept:

```
(deshan@kali)-[~]
$ dnsrecon -d booking.com -D /user/share/wordlists/dnsmap.txt -t std --xml booking.xml
[*] std: Performing General Enumeration against: booking.com ...
[-] DNSSEC is not configured for booking.com
[*] SOA ns-1288.awsdns-33.org 205.251.197.8
[*] SOA ns-1288.awsdns-33.org 2600:9000:5305:800::1
[*] NS ns-1288.awsdns-33.org 205.251.197.8
[*] NS ns-1288.awsdns-33.org 2600:9000:5305:800::1
[*] NS ns-716.awsdns-25.net 205.251.194.204
[*] NS ns-716.awsdns-25.net 2600:9000:5302:cc00::1
[*] NS ns-508.awsdns-63.com 205.251.193.252
[*] NS ns-508.awsdns-63.com 2600:9000:5301:fc00::1
[*] NS ns-1959.awsdns-52.co.uk 205.251.199.167
[*] NS ns-1959.awsdns-52.co.uk 2600:9000:5307:a700::1
[*] MX mx-b-0032a201.gslb.pphosted.com 185.132.181.145
[*] MX mx-a-0032a201.gslb.pphosted.com 185.132.181.145
[*] A booking.com 108.157.254.120
[*] A booking.com 108.157.254.31
[*] A booking.com 108.157.254.54
[*] A booking.com 108.157.254.89
[*] TXT booking.com logmein-domain-confirmation 90DIFG9EEUT8U8R4895Y87H
[*] TXT booking.com fastly-domain-delegation-0344411-343733-2021_0223
[*] TXT booking.com globalsign-domain-verification=jpcnVg6kuHYyEz5op6ZzxI2E53gePoVqca7RgL0aNq
[*] TXT booking.com wrike-verification=NDM5MTUzODoyMTFknjJmZWMSMDk5MTVjOWY2YTQ2MWI4MmVhNjRkZjBmNjg3NzhmZTJhZTQ2NjYxMmVlNjNmMDJkZWRRkN2Vi
```

Proof of concept:

```

[*] TXT booking.com _globalsign-domain-verification=FSlSaYMuHsfff-JRsSpJSonQOV0_jwrwl5kQpFdTb
[*] TXT booking.com ZOOM_verify_rRPrFA9oTH2bxFkJeQTzA
[*] TXT booking.com intersight=f7b95d6ad5339839c1253d5e47c1c32ff8276909334ff7173890c54f4730e68a
[*] TXT booking.com miro-verification=a08b425a7aa0b2b93256f4b504ee72afe8f9e0b9
[*] TXT booking.com f3n3z6cw35fkl9lnb6q72dczy2z7d2gy
[*] TXT booking.com ecostruxure-it-verification=881dfd3b-5776-4fc0-a5f6-190a0ac842f8
[*] TXT booking.com google-site-verification=IqETr3m1Iq2apdhg2tJndtOH5xn_C0PrLSBL4UpB9WU
[*] TXT booking.com google-site-verification=qKQzyXjxHLM4q1X-7PdrurR3p1QjjINz2QD_MBvAmyU
[*] TXT booking.com v=spf1 include:%{ir}.*%{v}.*%{d}.spf.has.pphosted.com -all
[*] TXT booking.com google-site-verification=z4muhl35r1aT-msc5R269P03RkaZHc7zzn6omxkiedI
[*] TXT booking.com onetrust-domain-verification=3fce180bf9e54d5b97a7c9e1ce3cb10c
[*] TXT booking.com MS=ms35392088
[*] TXT booking.com sending_domain1012722=80cff31442c5f4e1b9c51346939d5bf298d9eff5f69d465476631c95f588ac9
0
[*] TXT booking.com Dynatrace-site-verification=3a88fcl1a-195c-455d-ab87-88d09191496b__drhtlct978bncn9utek
6qddqapk
[*] TXT booking.com asv=93db973d8bc6fd37d0c9e0c3feebff95
[*] TXT booking.com gwt5v1xngwj1f6zq7khv3bp4xnxbgmkg
[*] TXT booking.com mandrill_verify.e-1764xQVEGJ2x07f-WGHg
[*] TXT booking.com smartsheet-site-validation=zF2Qh0qhBS307AjSZMdaAVW2E7GB1VLL
[*] TXT booking.com docker-verification=0ebe0b8e-6bd1-4f94-b0b3-344bd07052ed
[*] TXT booking.com adobe-idp-site-verification=040db58f-cfb9-4203-a555-bfcd15b24b86
[*] TXT booking.com atlassian-domain-verification=PEQekniknktLbMzMw6Ifb9G9YWzhgcGHZIne34xYo7zW9/rzVsM/6qZ
SUWdIVAmR

[*] TXT booking.com google-site-verification=WMDRc5NqQj7RWff1N8L0_Ikc08kSr-iUa3C0Zczl9QA
[*] TXT booking.com docusign=1ddc2bf3-a249-4127-a351-f22dc75077d3
[*] TXT booking.com google-site-verification=1eOMDGAH7nc_P5U-8MWPqSTU40og02u0CODDvbcmoMw
[*] TXT booking.com google-site-verification=Yse39yHdmcUPiSTGNVY-eI27sv3TBfQVLBPgWHiins
[*] TXT booking.com _globalsign-domain-verification=9Xqu2bonefjuoUF-XmyjAptAfuE-yStJz6wy9UnH-C
[*] TXT booking.com google-site-verification=w40NMRTpNbdr8FXV33gtkD3qLFHastApR2UgHgggf8
[*] TXT booking.com _globalsign-domain-verification=l_BNpBANK-rKZRYXJ9UKBfv9o6EEuuenkBrGpYNYo0
[*] TXT booking.com apple-domain-verification=immERz8LzjEgeSoW
[*] TXT booking.com VkJHqtn1JPDHrgqwbz8C30fmoABFhxVfjIOtLVLUK06CUwKgd2mevDGtnDhWZcNbxEGk39D0ezbHay8XSv1zv
Q=
[*] TXT booking.com cisco-ci-domain-verification=45d8573a6620606f09d1556681408112c9f9754309b02423c380eee5
d287bd8f
[*] TXT booking.com atlassian-domain-verification=F3hugs/a4ZZHwjGTLmlb12IMA3TIRiz3ifqw4TKRz9tWk0LoyBBXfwc
775aT/juy
[*] TXT booking.com google-site-verification=_dm8LZJlohRuCXhYRFe8COWc0JNx7c6AVF1vWpP52nE
[*] TXT _dmarc.booking.com v=DMARC1; p=reject; rua=mailto:dmarc_rua@emaildefense.proofpoint.com,mailto:bo
oking@dmarc.postmastery.eu; ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com
[*] Enumerating SRV Records
[+] SRV _xmpp-server._tcp.booking.com wx2i-k.wbx2.com 170.72.238.12 5269
[+] SRV _xmpp-server._tcp.booking.com wx2i-k.wbx2.com 170.72.238.82 5269
[+] SRV _xmpp-server._tcp.booking.com wx2i-k.wbx2.com 170.72.238.62 5269
[+] SRV _sipfederationtls._tcp.booking.com sipfed.online.lync.com 52.112.191.65 5061
[+] 4 Records Found
[*] Saving records to XML file: booking.xml

```

Public devices enumeration

- Censys

Censys is a potent internet scanning tool that scans and monitors devices, networks, and services online all the time. It performs thorough scans, keeps track of SSL/TLS

certificates, keeps an eye on attack surfaces, finds vulnerabilities, and offers threat information. Large volumes of data may be searched and analyzed, processes can be automated with the help of the API, and Censys can be integrated into security workflows. In the connected digital world of today, Censys is useful for asset discovery, vulnerability management, compliance monitoring, and proactive risk reduction.

Proof of concept

SummaryHistoryWHOISExploreOpen in GreyNoiseRaw Data

Basic Information

Reverse DNS

server-18-238-192-123.sfo53.r.cloudfront.net

Forward DNS

spoey.com, glucoatrust.com, server-18-238-192-123.sfo53.r.cloudfront.net, aphysique.mattguetta.com, income2retire.com, ...

Routing

18.238.192.0/22 via AMAZON-02, US (AS16509)

Services (2)

80/HTTP, 443/HTTP

HTTP 80/TCP

04/28/2024 01:05 UTC

Software

Amazon CloudFront Load Balancer

VIEW ALL DATA

GO

Details

http://18.238.192.123/

Status

403 Forbidden

Body Hash

sha1:c1c72c0861240985ae8bb08020ce0a9b73b85055

HTML Title

ERROR: The request could not be satisfied

Response Body

EXPAND

Geographic Location

City

San Jose

State

California

Country

United States (US)

Coordinates

37.33939, -121.89496

Timezone

America/Los_Angeles

HTTP 443/TCP

04/29/2024 01:33 UTC

Software

Amazon CloudFront Load Balancer

VIEW ALL DATA

GO

Details

http://18.238.192.123:443/

Status

400 Bad Request

Body Hash

sha1:5cd1a28ad4446876f664e448f593a8c6183c0d95

HTML Title

ERROR: The request could not be satisfied

Response Body

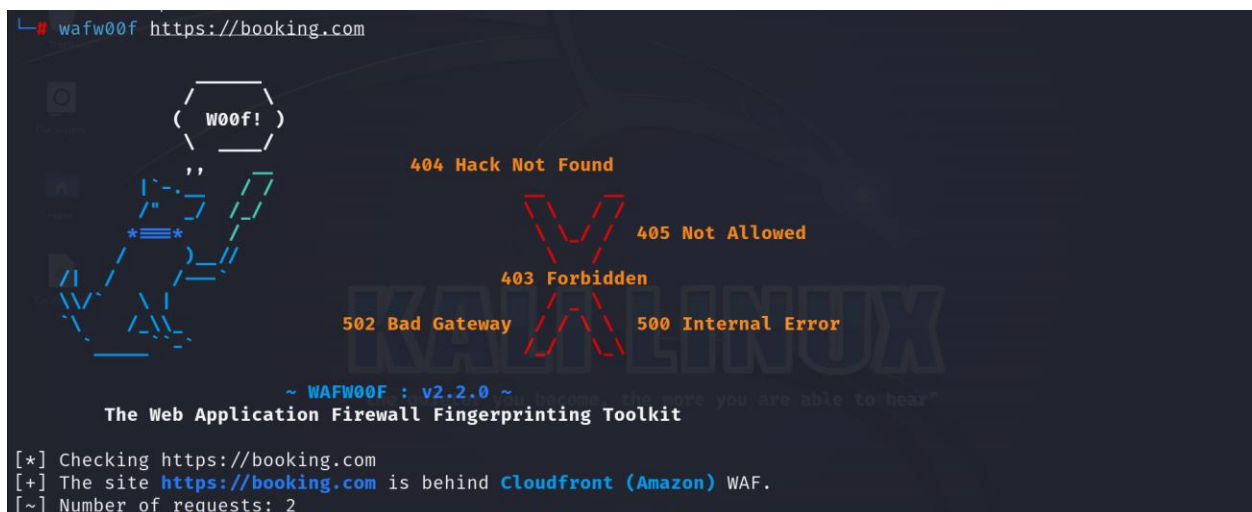
EXPAND

Find WAF (web application firewall) protection.

- Wafwoof

Wafw00f is an open-source program that uses content patterns, HTTP responses, and header analysis to detect and fingerprint web application firewalls (WAFs). It gives testers and security experts information about the particular WAF technology or vendor being used as well as assists them in determining whether a web application is protected by a WAF. In addition to being user-friendly and seamlessly integrating with automated testing workflows, Wafw00f also keeps an updated database of WAF signatures and offers community support. It is a useful tool for security assessment and reconnaissance jobs, supporting the creation of efficient testing plans and workarounds.

Proof of concept:



```
└─$ wafw00f https://booking.com

  ( W00f! )

 404 Hack Not Found
 405 Not Allowed
 403 Forbidden
 502 Bad Gateway
 500 Internal Error

~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://booking.com
[+] The site https://booking.com is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2
```

Find open ports.

- Nmap

Nmap, sometimes known as "Network Mapper," is a potent open-source network scanning program used for vulnerability analysis, security audits, and network discovery. It is particularly good at operating system detection, host discovery, port scanning, and service version detection. Because it supports custom scripting and automation, Nmap's scripting engine (NSE) is adaptable to a wide range of security activities and integration requirements. Because of its dependability, adaptability, and large feature set, network administrators, security experts, and penetration testers frequently use it for network reconnaissance, security audits, and network monitoring.

```
(root@kali)-[~]
# nmap -sV -A -T4 booking.com

Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-30 23:02 +0530
Nmap scan report for booking.com (108.157.254.54)
Host is up (0.0027s latency).
Other addresses for booking.com (not scanned): 108.157.254.31 108.157.254.120 108.157.254.89
rDNS record for 108.157.254.54: server-108-157-254-54.sin2.r.cloudfront.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  tcpwrapped
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://booking.com/
443/tcp   open  tcpwrapped
|_http-server-header: CloudFront
|_http-title: ERROR: The request could not be satisfied
| ssl-cert: Subject: commonName=*.booking.com/organizationName=Booking.com BV/countryName=NL
| Subject Alternative Name: DNS:*.booking.com, DNS:booking.com
| Not valid before: 2023-06-12T00:00:00
|_Not valid after: 2024-05-18T23:59:59

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|webcam|firewall
Running (JUST GUESSING): 2N embedded (93%), Grandstream embedded (93%), Garmin embedded (89%), Cisco ASA 9.X (
87%), FireBrick embedded (85%)
OS CPE: cpe:/h:2n:helios cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite cpe:/a:cisco:adaptive_security_ap
pliance_software:9.2 cpe:/h:firebrick:fb2700
Aggressive OS guesses: 2N Helios IP VoIP doorbell (93%), Grandstream GXP1105 VoIP phone (93%), Garmin Virb Eli
te action camera (89%), Cisco Adaptive Security Appliance (ASA 9.2) (87%), FireBrick FB2700 firewall (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1 0.29 ms server-108-157-254-54.sin2.r.cloudfront.net (108.157.254.54)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.96 seconds
```


Exploitation

- sqlmap

Web applications with SQL injection vulnerabilities can be automatically found and exploited with SQLMap, an open-source penetration testing tool. It employs a number of detecting methods, supports a number of database management systems, and provides customization choices. Security experts and penetration testers find SQLMap useful as it automates testing, enumeration, data extraction, and reporting procedures during security assessments. It should, therefore, be utilized sensibly, morally, and with the appropriate authorization to test programs and systems.

```

└─$ sqlmap -u booking.com

[1.7.9#stable]
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability
and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:33:30 /2024-05-01/

[00:33:31] [INFO] testing connection to the target URL
got a 301 redirect to 'https://booking.com/'. Do you want to follow? [Y/n] Y
[00:33:38] [WARNING] potential CAPTCHA protection mechanism detected
you have not declared cookie(s), while server wants to set its own ('px_init=0;bkng=11UmFuZG9tS...BxttMrI%3D;b
kng_sso_auth=CAIQsOnuTRp...s3MC0IMS49;pcm_consent=analytical%...ion%3Dnone'). Do you want to use those [Y/n] Y
[00:33:45] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:33:48] [INFO] testing if the target URL content is stable
[00:33:51] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.
site.com/index.php?id=1'). You are advised to rerun with '--forms --crawl=2'
[00:33:51] [WARNING] your sqlmap version is outdated

```

Vulnerability analysis phase

I used tool like netsparker to process and catch bugs and vulnerabilities are based on OWASP top 10.

Targeted Domain: - <http://www.booking.com>

- **Netsparker**

An automated web application security scanner known for its precision and extensive vulnerability finding capabilities is called Netsparker. It simplifies the procedure for examining online applications and finds many security flaws, such as SQL injection, XSS, and misconfigurations. With its ability to provide comprehensive reports for compliance audits and vulnerability monitoring, Netsparker seamlessly interacts with development workflows. Because of its intuitive interface, sophisticated features like support for continuous monitoring and authentication, and free support and upgrades, it's a great resource for security experts and companies looking to effectively strengthen their web application security posture.

Vulnerability title

- **Weak cipher enabled (confirmed).**

Vulnerability description

The "Weak Ciphers Enabled" vulnerability stems from the use of outdated or insecure cryptographic ciphers in SSL/TLS configurations, exposing systems to cryptographic attacks. Weak ciphers like DES, RC4, and MD5 lack the necessary security standards and are prone to exploitation. You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact assessment

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

Affected components

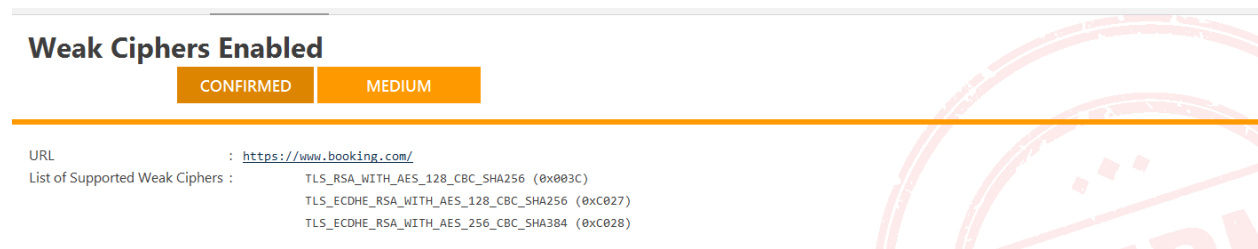
When HTTP Strict Transport Security (HSTS) is not there, there are security vulnerabilities associated with different parts of a web application and its infrastructure. The web server configuration, network traffic, user sessions, data integrity while in transit, adherence to compliance standards, and user trust and experience are among the components that are impacted.

How to mitigate?

Some changes must be made to the system registry. Editing the registry incorrectly can cause serious damage to your system. Before making changes to the registry,

you should back up any valuable data on your computer. Configure your web server to disallow the use of weak ciphers.

Proof of concept:



Other vulnerabilities were identified during the scan

- HTTP Strict Transport Security (HSTS) Errors and Warnings

HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM

Certainty :
URL : <https://www.booking.com/>

Error	Resolution
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

Vulnerability Details

Netsparker detected errors during parsing of Strict-Transport-Security header.

Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Remedy

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
 - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
 - The max-age must be at least 31536000 seconds (1 year)
 - The includeSubDomains directive must be specified
 - The preload directive must be specified
- If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

- Missing X-Frame-Options Header

Missing X-Frame-Options Header

LOW

Certainty :
URL : <https://www.booking.com/.well-known/>

Vulnerability Details

Netsparker detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

CLASSIFICATION	
OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ISO27001	A.14.2.5

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Remedy

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.

X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.

X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

Employing defensive code in the UI to ensure that the current frame is the most top level window.

Security.txt Detected

Security.txt Detected

INFORMATION

Certainty :

URL : <https://www.booking.com/.well-known/security.txt>

Injection URL : <http://www.booking.com/.well-known/security.txt>

Vulnerability Details

Netsparker detected a security.txt file with potentially sensitive content.

Impact

Depending on the content of the file, an attacker might discover hidden directories and files.


CLASSIFICATION

OWASP PC	C7
ISO27001	A.18.1.3

Expect-CT Not Enabled

Expect-CT Not Enabled

BEST PRACTICE

Certainty : 
URL : <https://www.booking.com/.well-known/>

Vulnerability Details

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissued certificates to be used.

CLASSIFICATION

CWE	16
WASC	15
ISO27001	A.14.1.2

Remedy

Configure your web server to respond with Expect-CT header.

Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"

Note: We strongly suggest you to use Expect-CT header in **report-only mode** first. If everything goes well and your certificate is ready, go with the Expect-CT enforce mode. To use **report-only mode** first, omit **enforce** flag and see the browser's behavior with your deployed certificate.

Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"

- Content Security Policy (CSP) Contains Out of Scope report-uri Domain

Content Security Policy (CSP) Contains Out of Scope report-uri Domain

INFORMATION

Certainty : 
URL : <https://www.booking.com/.well-known/>
Report Uri With Different Host : <https://nellie.booking.com/csp-report-uri?type=report&tag=112&pid=60d9869062b800b8&e=UmFuZG9tSVYkc2R1Iyh9YfUju7BdQA0xL1-dyBR0AfoTm8LhFLFuNx1FvbiJrvyfM58za3uJc>

Vulnerability Details

Netsparker detected that your CSP declaration contains `report-uri` value that points to an out of scope external domain. This domain will be aware of the CSP violation occurs on your website and some sensitive data will be disclosed to this site.

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
ISO27001	A.14.2.5

Remedy

If you trust this domain you can ignore this issue. However if you do not trust this external domain, remove it from `report-uri` directive.

- HTTP Strict Transport Security (HSTS) Max-Age Value Too Low

HTTP Strict Transport Security (HSTS) Max-Age Value Too Low

INFORMATION

Certainty : 
URL : <https://www.booking.com/>

Vulnerability Details

HTTP Strict Transport Security (HSTS) header's max-age value is lower than the recommended value.

Remedy

It is recommended to set the max-age to a big value like 31536000 (12 months) or 63072000 (24 months).

External References

[HTTP Strict Transport Security \(HSTS\) HTTP Header](#)
[Wikipedia - HTTP Strict Transport Security Implementation](#)

CLASSIFICATION

OWASP PC	C1
CWE	16
WASC	15
ISO27001	A.14.1.2

Conclusion

The research conducted a thorough security audit of the prominent trip booking platform Booking.com, with an emphasis on data collection, vulnerability detection, and mitigation techniques. Several vulnerabilities were discovered using tools such as Recon-ng, nslookup, Dnsrecon, Censys, Wafw00f, Nmap, sqlmap, and Netsparker, which included weak ciphers, missing security headers, banned resources, and unexpected redirects. These vulnerabilities increase the risk of data leakage, unauthorized access, and potential exploitation by malicious actors. Mitigation options were recommended, including setting the web server to reject weak ciphers and implementing missing security headers. Regular security evaluations and updates are recommended to maintain a strong security posture and safeguard user data from potential threats. The paper emphasizes the crucial role of proactive security measures in protecting online platforms and maintaining user confidence and data integrity.