# 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

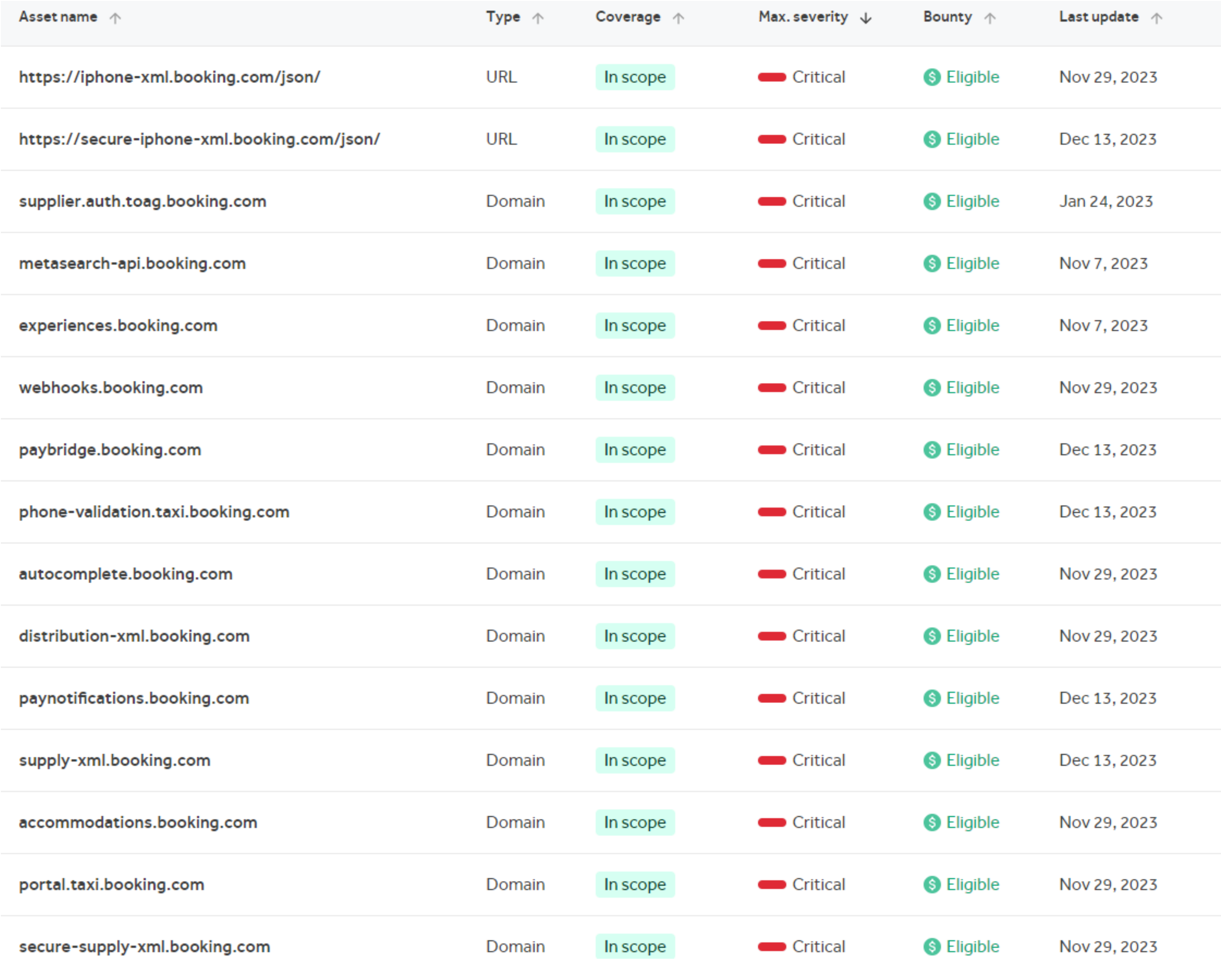
- SSRF
- XXE
- Subdomain takeover in *.booking.com domains

**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.

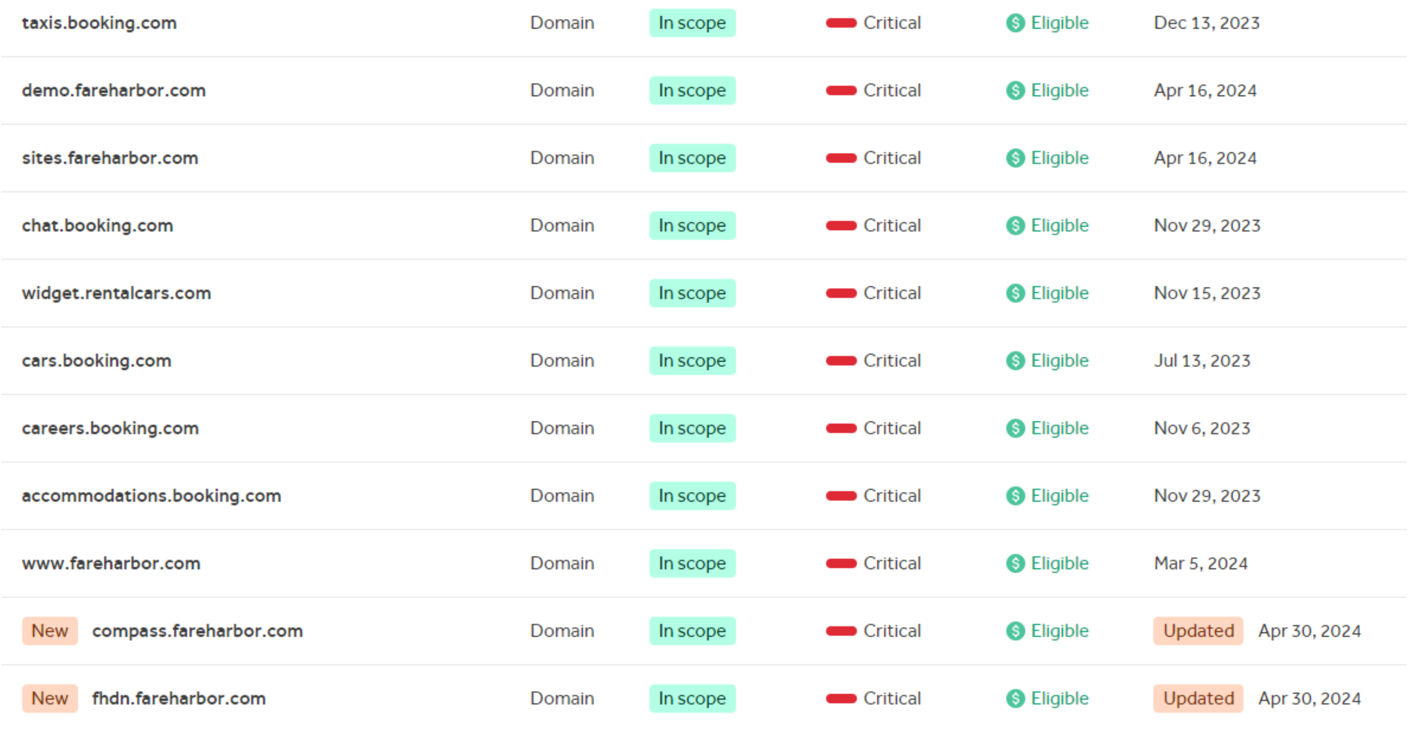
**The following issues are outside the scope of our vulnerability rewards program:**

- 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

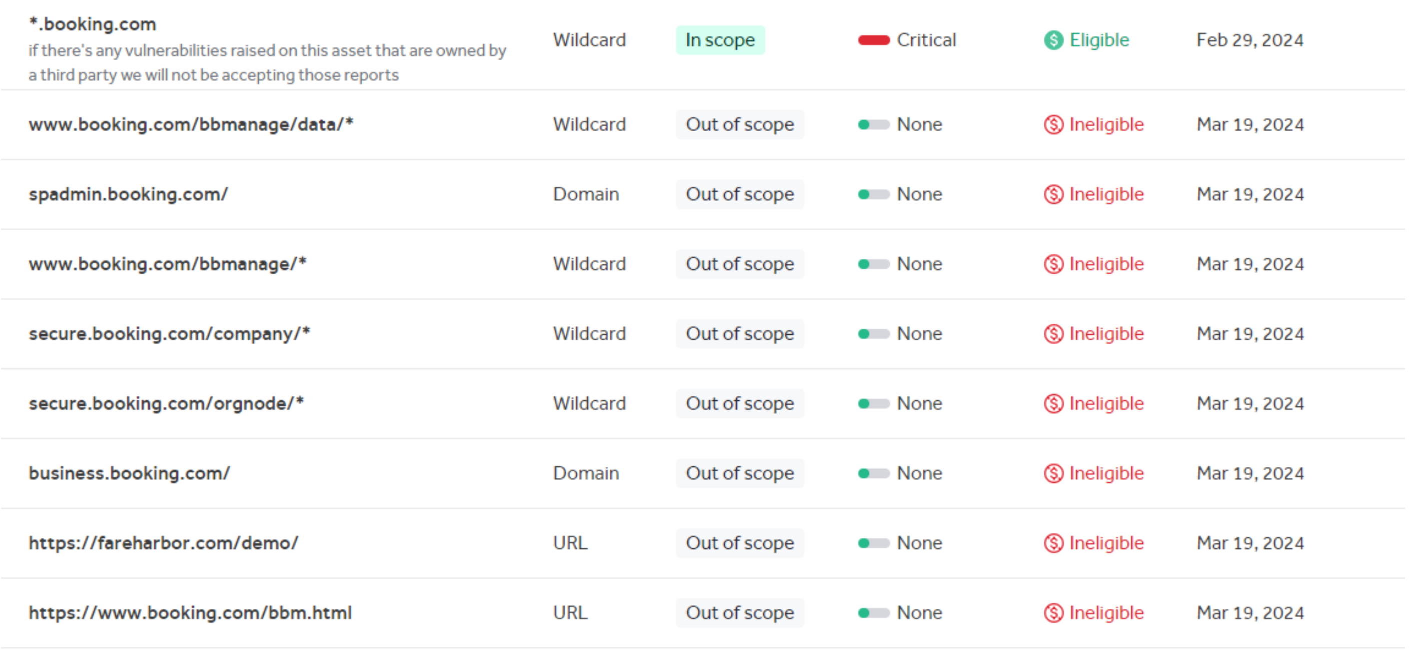
- Any vulnerabilities requiring significant and unlikely interaction by the victim, such as disabling browser controls
- Content spoofing without embedded HTML or JavaScript
- Hypothetical issues that do not have any practical impact
- Infrastructure vulnerabilities, including:
- Issues related to SSL 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 |



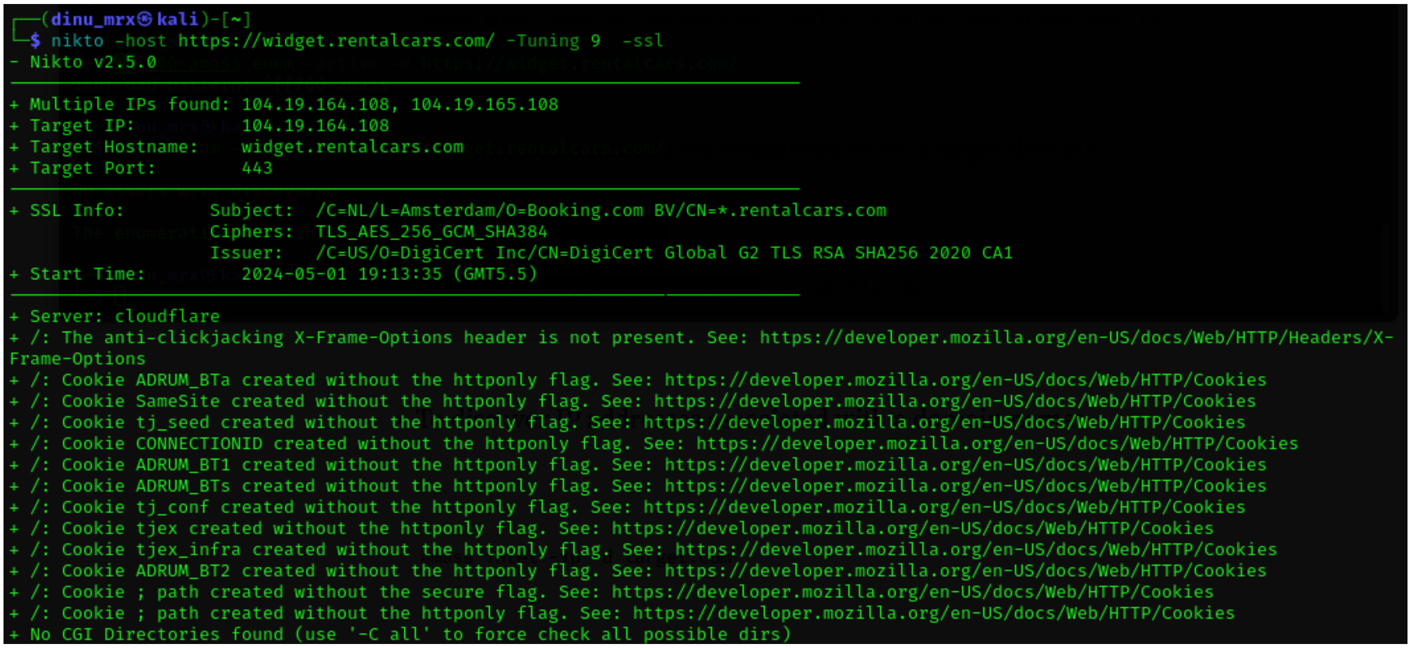
| | | | | | |
|---|---|---|---|---|---|
| taxis.booking.com | Domain | In scope | Critical | Eligible | Dec 13, 2023 |
| demo.fareharbor.com | Domain | In scope | Critical | Eligible | Apr 16, 2024 |
| sites.fareharbor.com | Domain | In scope | Critical | Eligible | Apr 16, 2024 |
| chat.booking.com | 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 |



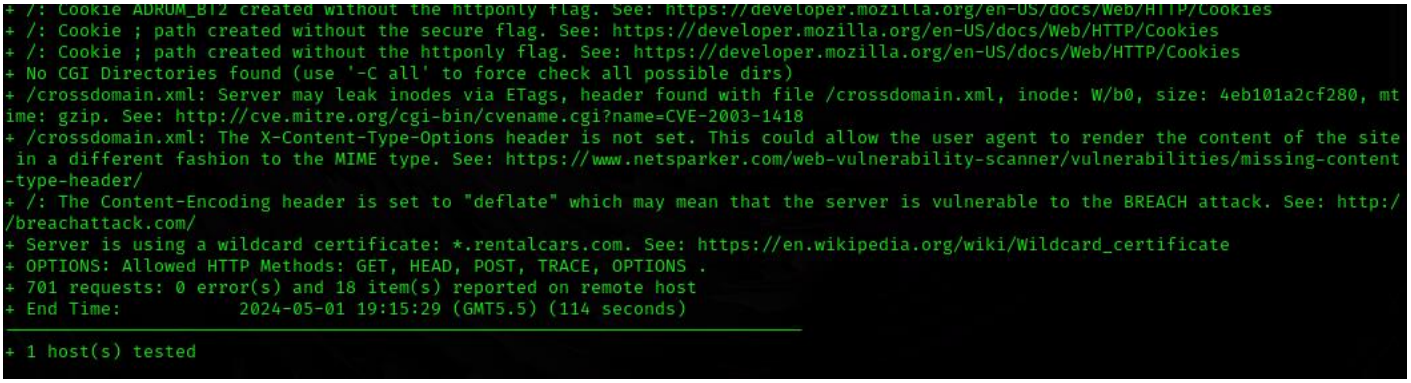
| | | | | | |
|---|---|---|---|---|---|
| *.booking.com<br>if there's any vulnerabilities raised on this asset that are owned by a third party we will not be accepting those reports | Wildcard | In scope | Critical | Eligible | Feb 29, 2024 |
| www.booking.com/bbmanage/data/* | Wildcard | Out of scope | 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://widget.rentalcars.com/

result obtain from nikto



```
┌──(dinu_mrx㉿kali)-[~]
└─$ nikto -host https://widget.rentalcars.com/ -Tuning 9  -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.19.164.108, 104.19.165.108
+ Target IP:          104.19.164.108
+ Target Hostname:    widget.rentalcars.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=NL/L=Amsterdam/O=Booking.com BV/CN=*.rentalcars.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
+ Start Time:         2024-05-01 19:13:35 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-
Frame-Options
+ /: Cookie ADRUM_BTa created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie SameSite created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie tj_seed created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie CONNECTIONID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ADRUM_BT1 created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ADRUM_BTs created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie tj_conf created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie tjex created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie tjex_infra created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ADRUM_BT2 created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ; path created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ; path created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```



```
+ /: Cookie ADRUM_BT2 created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ; path created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie ; path created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /crossdomain.xml: Server may leak inodes via ETags, header found with file /crossdomain.xml, inode: W/b0, size: 4eb101a2cf280, mt
ime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /crossdomain.xml: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
 in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content
-type-header/
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http:/
/breachattack.com/
+ Server is using a wildcard certificate: *.rentalcars.com. See: https://en.wikipedia.org/wiki/Wildcard_certificate
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, TRACE, OPTIONS .
+ 701 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2024-05-01 19:15:29 (GMT5.5) (114 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

According to the nikto The content-Encoding header is set to “deflate” where it may mean the server is vulnerable to breach attacks.

BREACH is a category of vulnerabilities and not a specific instance affecting a specific piece of software. To be vulnerable, a web application must:

- Be served from a server that uses HTTP-level compression
- Reflect user-input in HTTP response bodies
- Reflect a secret (such as a CSRF token) in HTTP response bodies.

Additionally, while not strictly a requirement, the attack is helped greatly by responses that remain mostly the same (modulo the attacker's guess). This is because the difference in size of the responses measured by the attacker can be quite small. Any noise in the side-channel makes the attack more difficult (though not impossible).

It is important to note that the attack is agnostic to the version of TLS/SSL, and does not require TLS-layer compression. Additionally, the attack works against any cipher suite. Against a stream cipher, the attack is simpler; the difference in sizes across response bodies is much more granular in this case. If a block cipher is used, additional work must be done to align the output to the cipher text blocks.

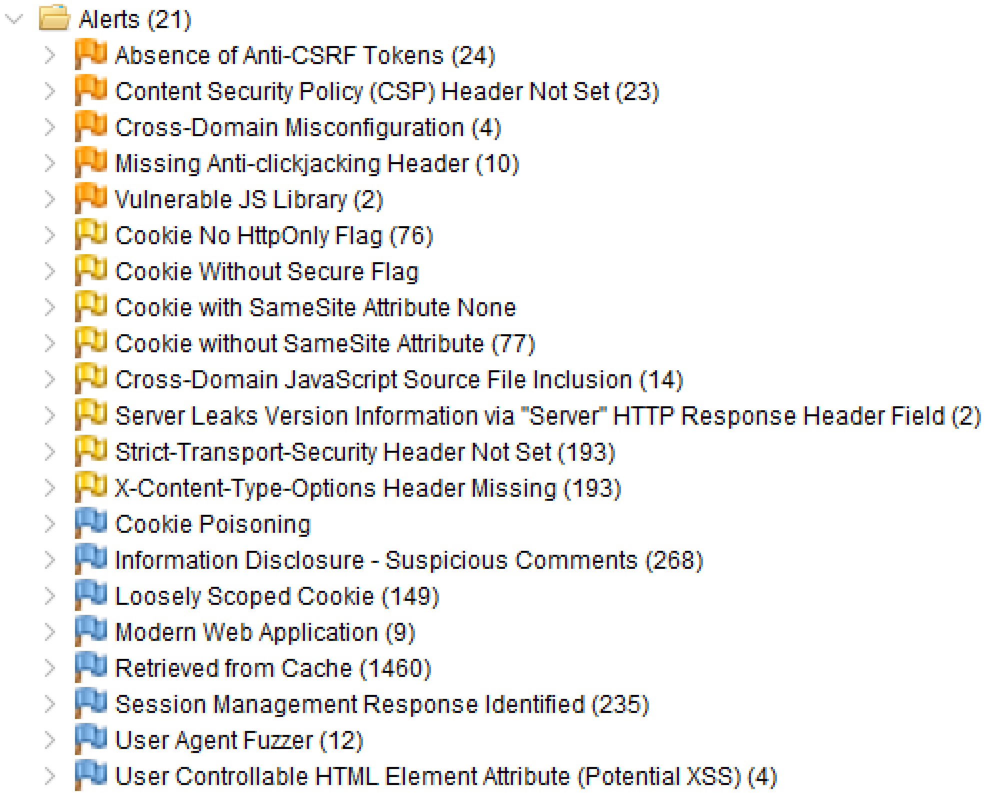
https://www.breachattack.com/

And also it shows that the server may leak inodes via ETags, header found with file /crossdomain.xml, inode: W/b0, size: 4eb101a2cf280, mtime: gzip.

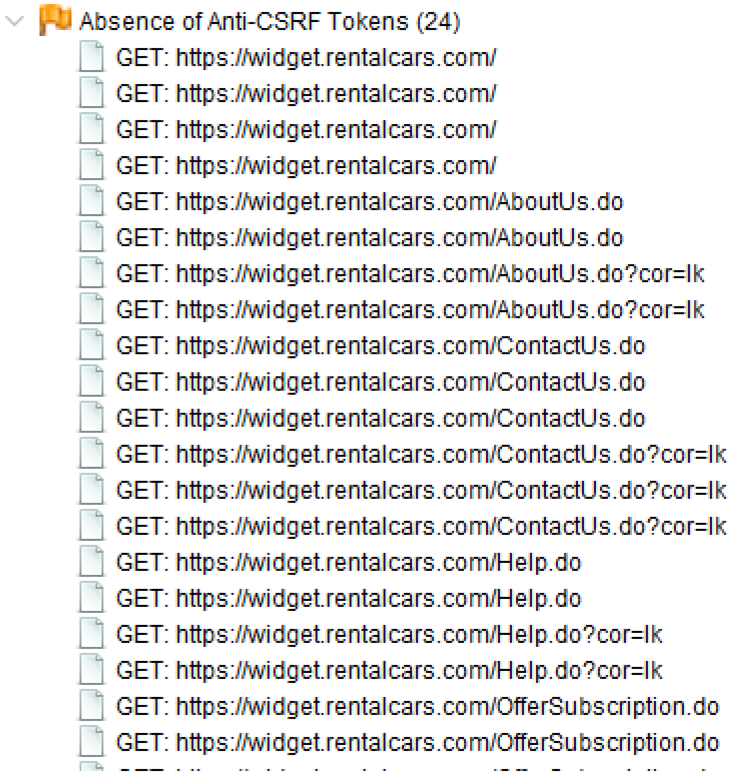
Apache HTTP Server 1.3.22 through 1.3.27 on OpenBSD allows remote attackers to obtain sensitive information via (1) the ETag header, which reveals the inode number, or (2) multipart MIME boundary, which reveals child process IDs (PID).

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418

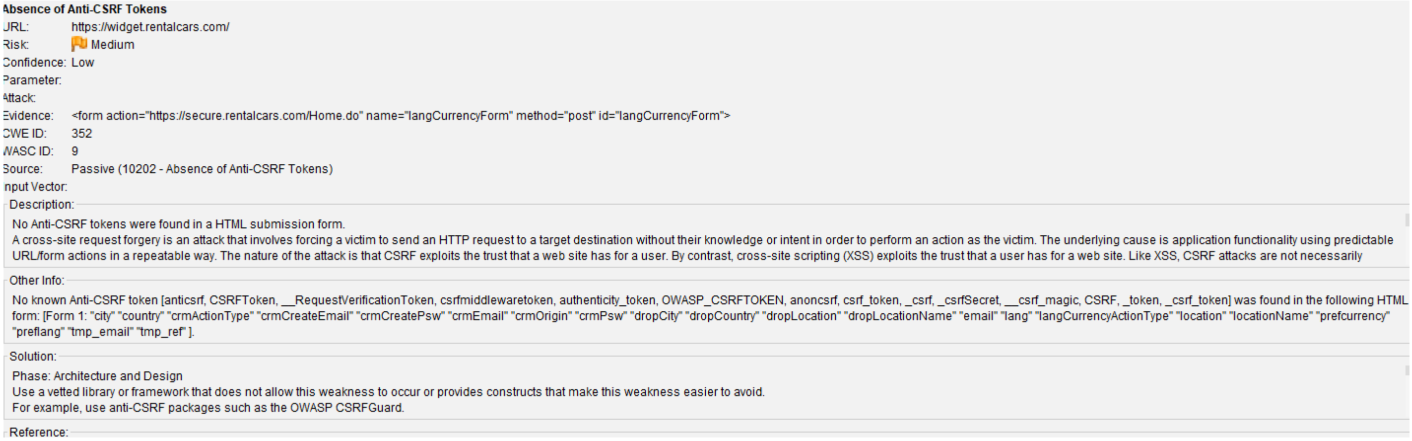
The automated scan through the OWSAP ZAP gives the following results



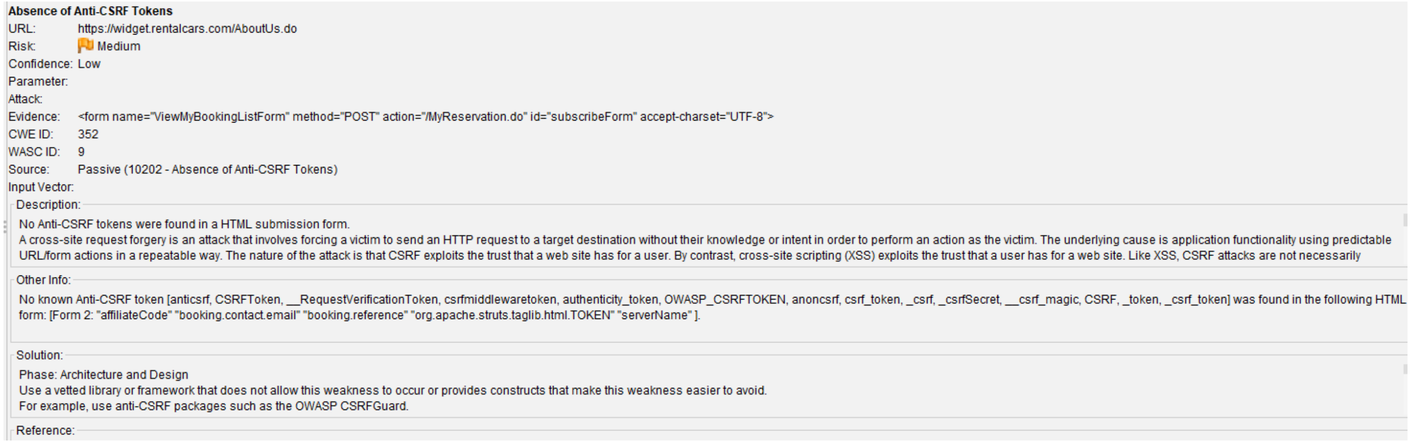
- Alerts (21)
  - Absence of Anti-CSRF Tokens (24)
  - Content Security Policy (CSP) Header Not Set (23)
  - Cross-Domain Misconfiguration (4)
  - Missing Anti-clickjacking Header (10)
  - Vulnerable JS Library (2)
  - Cookie No HttpOnly Flag (76)
  - Cookie Without Secure Flag
  - Cookie with SameSite Attribute None
  - Cookie without SameSite Attribute (77)
  - Cross-Domain JavaScript Source File Inclusion (14)
  - Server Leaks Version Information via "Server" HTTP Response Header Field (2)
  - Strict-Transport-Security Header Not Set (193)
  - X-Content-Type-Options Header Missing (193)
  - Cookie Poisoning
  - Information Disclosure - Suspicious Comments (268)
  - Loosely Scoped Cookie (149)
  - Modern Web Application (9)
  - Retrieved from Cache (1460)
  - Session Management Response Identified (235)
  - User Agent Fuzzer (12)
  - User Controllable HTML Element Attribute (Potential XSS) (4)



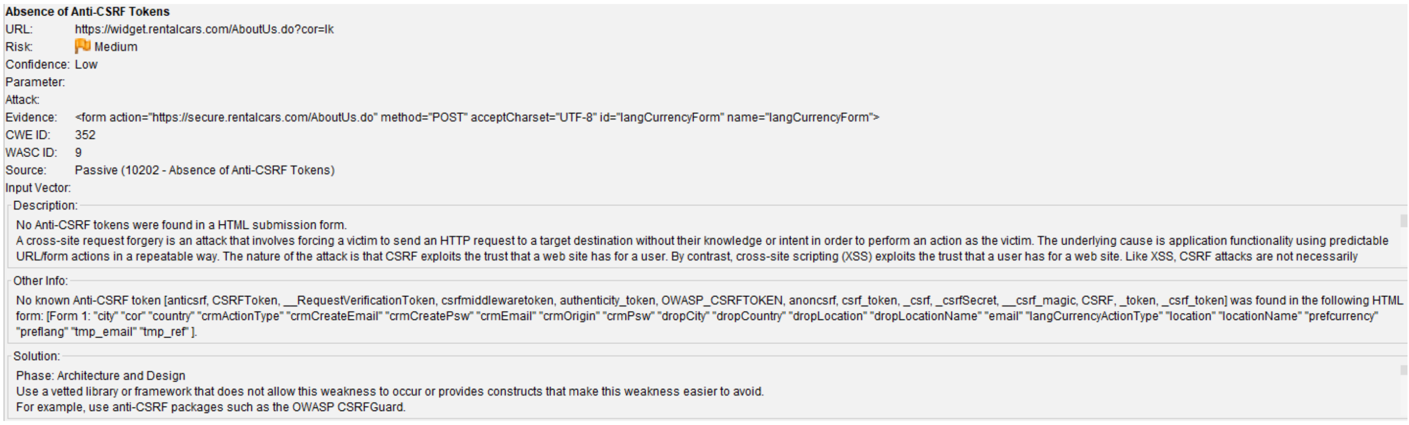
```
Absence of Anti-CSRF Tokens (24)
    GET: https://widget.rentalcars.com/
    GET: https://widget.rentalcars.com/
    GET: https://widget.rentalcars.com/
    GET: https://widget.rentalcars.com/
    GET: https://widget.rentalcars.com/AboutUs.do
    GET: https://widget.rentalcars.com/AboutUs.do
    GET: https://widget.rentalcars.com/AboutUs.do?cor=lk
    GET: https://widget.rentalcars.com/AboutUs.do?cor=lk
    GET: https://widget.rentalcars.com/ContactUs.do
    GET: https://widget.rentalcars.com/ContactUs.do
    GET: https://widget.rentalcars.com/ContactUs.do
    GET: https://widget.rentalcars.com/ContactUs.do?cor=lk
    GET: https://widget.rentalcars.com/ContactUs.do?cor=lk
    GET: https://widget.rentalcars.com/ContactUs.do?cor=lk
    GET: https://widget.rentalcars.com/Help.do
    GET: https://widget.rentalcars.com/Help.do
    GET: https://widget.rentalcars.com/Help.do?cor=lk
    GET: https://widget.rentalcars.com/Help.do?cor=lk
    GET: https://widget.rentalcars.com/OfferSubscription.do
    GET: https://widget.rentalcars.com/OfferSubscription.do
```



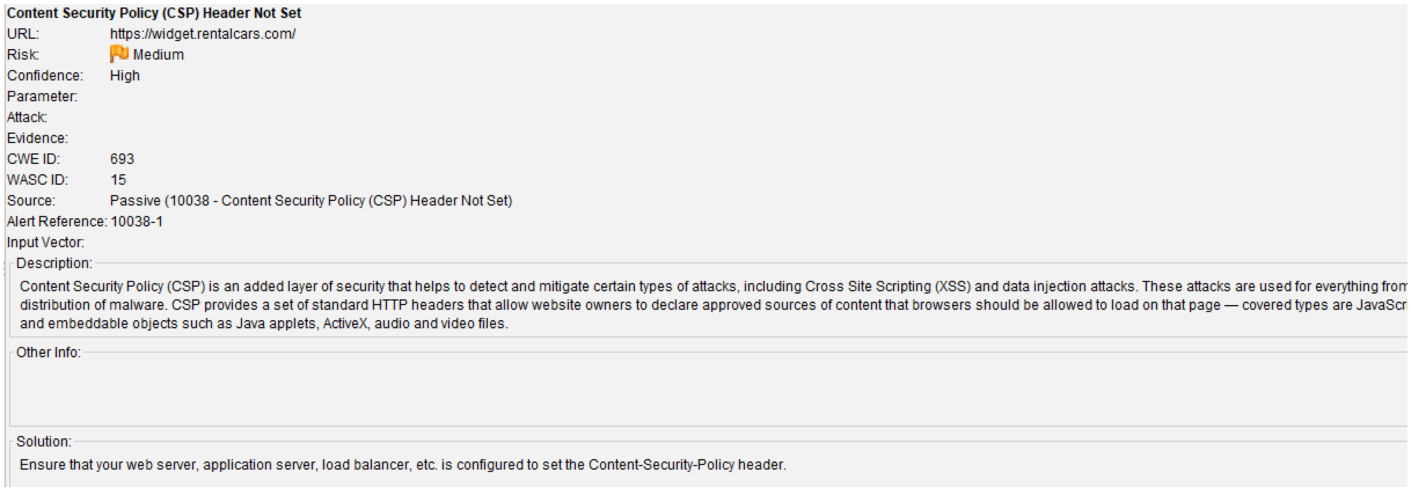
```
Absence of Anti-CSRF Tokens
URL:          https://widget.rentalcars.com/
Risk:         Medium
Confidence:   Low
Parameter:
Attack:
Evidence:     <form action="https://secure.rentalcars.com/Home.do" name="langCurrencyForm" method="post" id="langCurrencyForm">
CWE ID:       352
WASC ID:      9
Source:       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 user has for a web site. Like XSS, CSRF attacks are not necessarily
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: "city" "country" "crmActionType" "crmCreateEmail" "crmCreatePsw" "crmEmail" "crmOrigin" "crmPsw" "dropCity" "dropCountry" "dropLocation" "dropLocationName" "email" "lang" "langCurrencyActionType" "location" "locationName" "prefcurrency"
 "preflang" "tmp_email" "tmp_ref" ].
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:
```



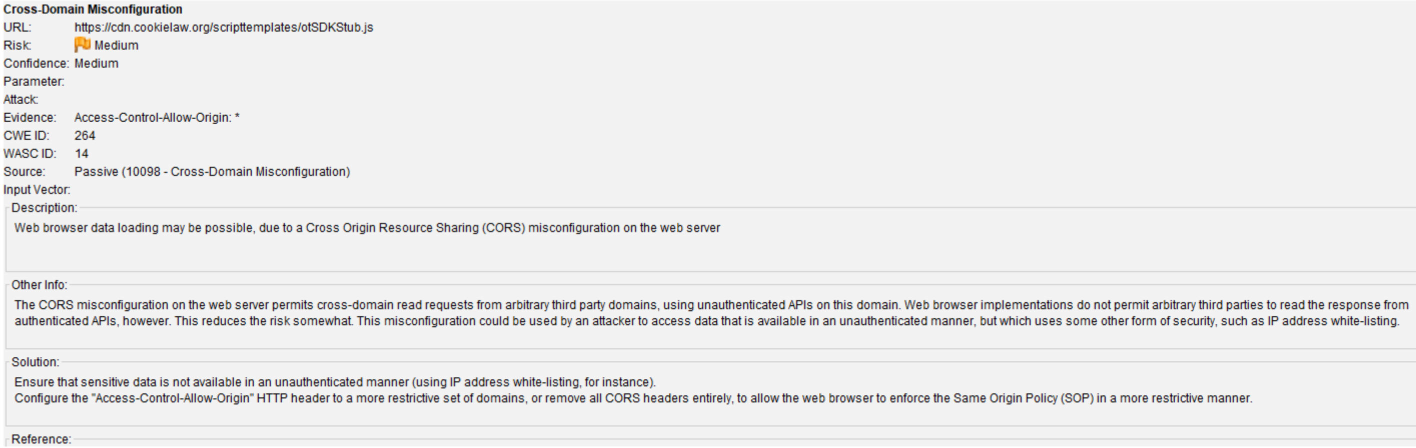
```
Absence of Anti-CSRF Tokens
URL:          https://widget.rentalcars.com/AboutUs.do
Risk:         Medium
Confidence:   Low
Parameter:
Attack:
Evidence:     <form name="ViewMyBookingListForm" method="POST" action="/MyReservation.do" id="subscribeForm" accept-charset="UTF-8">
CWE ID:       352
WASC 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 user has for a web site. Like XSS, CSRF attacks are not necessarily
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 2: "affiliateCode" "booking.contact.email" "booking.reference" "org.apache.struts.taglib.html.TOKEN" "serverName" ].
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:
```



```
Absence of Anti-CSRF Tokens
URL:          https://widget.rentalcars.com/AboutUs.do?cor=lk
Risk:         Medium
Confidence:   Low
Parameter:
Attack:
Evidence:     <form action="https://secure.rentalcars.com/AboutUs.do" method="POST" acceptCharset="UTF-8" id="langCurrencyForm" name="langCurrencyForm">
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 user has for a web site. Like XSS, CSRF attacks are not necessarily
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: "city" "cor" "country" "crmActionType" "crmCreateEmail" "crmCreatePsw" "crmEmail" "crmOrigin" "crmPsw" "dropCity" "dropCountry" "dropLocation" "dropLocationName" "email" "langCurrencyActionType" "location" "locationName" "prefcurrency"
 "preflang" "tmp_email" "tmp_ref" ].
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.
```



```
Content Security Policy (CSP) Header Not Set
URL:              https://widget.rentalcars.com/
Risk:             Medium
Confidence:       High
Parameter:
Attack:
Evidence:
CWE ID:           693
WASC ID:          15
Source:           Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference:  10038-1
Input Vector:
Description:
 Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from
 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 JavaScr
 and embeddable objects such as Java applets, ActiveX, audio and video files.
Other Info:
Solution:
 Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
```



**Cross-Domain Misconfiguration**

URL: https://cdn.cookielaw.org/scripttemplates/otSDKStub.js
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

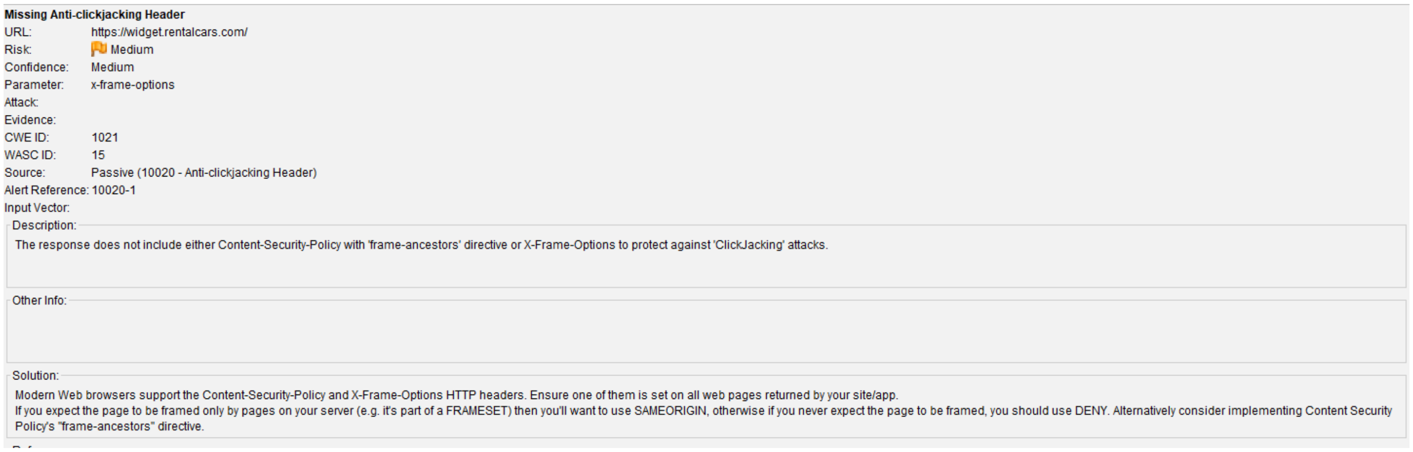
Other Info:

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:



**Missing Anti-clickjacking Header**

URL: https://widget.rentalcars.com/
Risk: Medium
Confidence: Medium
Parameter: x-frame-options
Attack:
Evidence:
CWE ID: 1021
WASC ID: 15
Source: Passive (10020 - Anti-clickjacking Header)
Alert Reference: 10020-1
Input Vector:

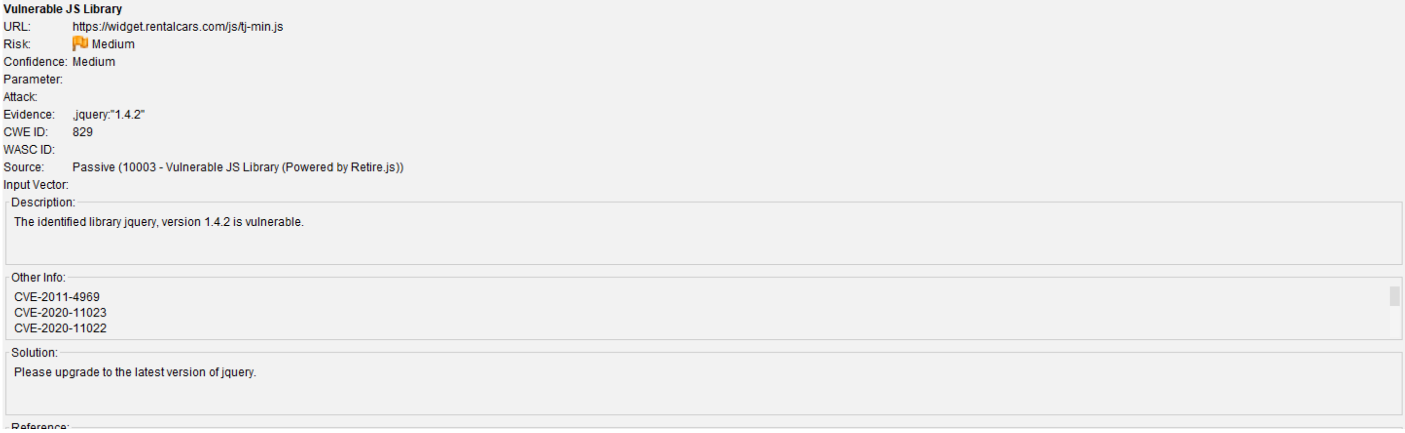
Description:

The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

Other Info:

Solution:

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.
If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.



**Vulnerable JS Library**

URL: https://widget.rentalcars.com/js/tj-min.js
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: jquery:"1.4.2"
CWE ID: 829
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:

Description:

The identified library jquery, version 1.4.2 is vulnerable.

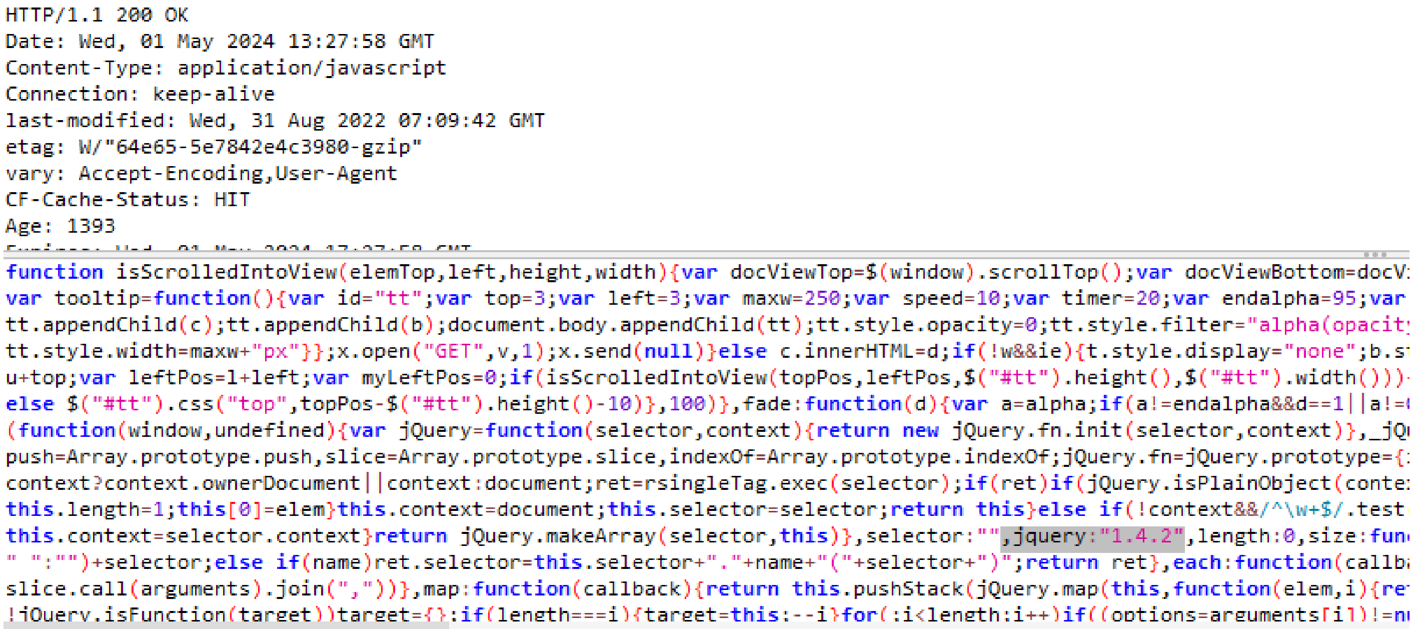
Other Info:

CVE-2011-4969
CVE-2020-11023
CVE-2020-11022

Solution:

Please upgrade to the latest version of jquery.

Reference:



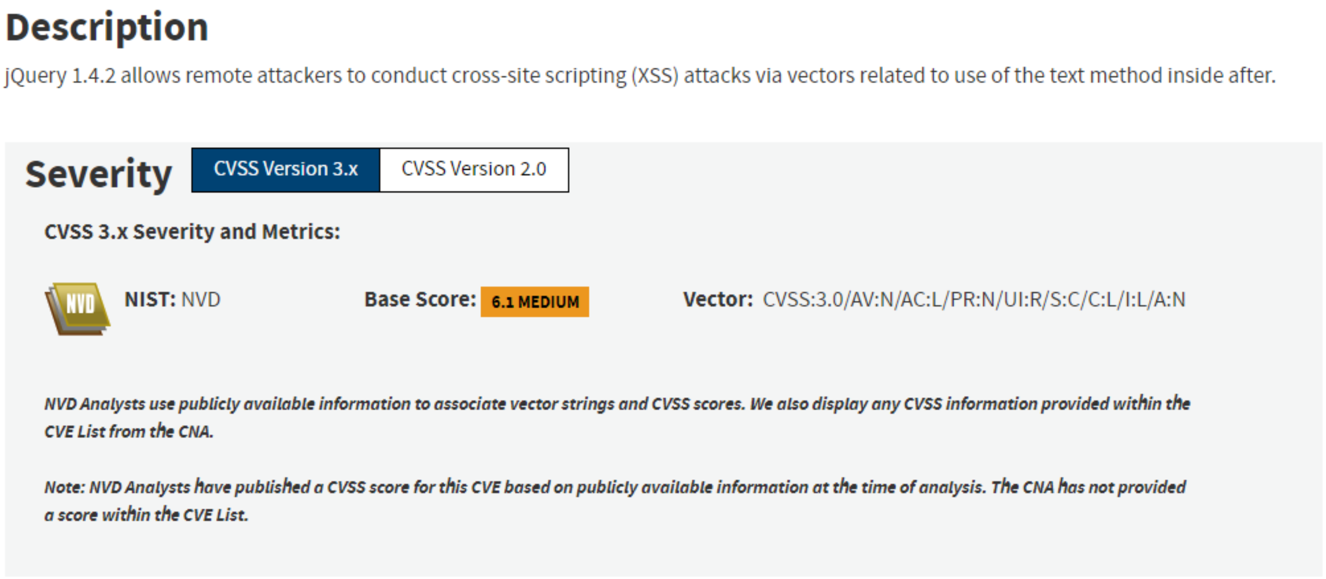
```
HTTP/1.1 200 OK
Date: Wed, 01 May 2024 13:27:58 GMT
Content-Type: application/javascript
Connection: keep-alive
last-modified: Wed, 31 Aug 2022 07:09:42 GMT
etag: W/"64e65-5e7842e4c3980-gzip"
vary: Accept-Encoding,User-Agent
CF-Cache-Status: HIT
Age: 1393
Expires: Wed, 01 May 2024 17:27:58 GMT
```

```
function isScrolledIntoView(elemTop,left,height,width){var docViewTop=$(window).scrollTop();var docViewBottom=docV
var tooltip=function(){var id="tt";var top=3;var left=3;var maxw=250;var speed=10;var timer=20;var endalpha=95;var
tt.appendChild(c);tt.appendChild(b);document.body.appendChild(tt);tt.style.opacity=0;tt.style.filter="alpha(opacit
tt.style.width=maxw+"px"}};x.open("GET",v,1);x.send(null)}else c.innerHTML=d;if(!w&&ie){t.style.display="none";b.s
u+top;var leftPos=l+left;var myLeftPos=0;if(isScrolledIntoView(topPos,leftPos,$("#tt").height(),$("#tt").width()))
else $("#tt").css("top",topPos-$("#tt").height()-10)},100)},fade:function(d){var a=alpha;if(a!=endalpha&&d==1||a!=
(function(window,undefined){var jQuery=function(selector,context){return new jQuery.fn.init(selector,context)},_jQ
push=Array.prototype.push,slice=Array.prototype.slice,indexOf=Array.prototype.indexOf;jQuery.fn=jQuery.prototype={
context?context.ownerDocument||context:document;ret=rsingleTag.exec(selector);if(ret)if(jQuery.isPlainObject(conte
this.length=1;this[0]=elem}this.context=document;this.selector=selector;return this}else if(!context&&/^\w+$/.test
this.context=selector.context}return jQuery.makeArray(selector,this)},selector:"",jquery:"1.4.2",length:0,size:fun
" ":"")+selector;else if(name)ret.selector=this.selector+"."+name+"("+selector+")";return ret},each:function(callb
slice.call(arguments).join(","))},map:function(callback){return this.pushStack(jQuery.map(this,function(elem,i){re
!jQuery.isFunction(target))target={};if(length===i){target=this;--i}for(;i<length;i++)if((options=arguments[i])!=n
```

The js library they are using is jquery 1.4.2

jQuery 1.4.2 allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to use of the text method inside after.

## CVE-2014-6071 Detail



### Description

jQuery 1.4.2 allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to use of the text method inside after.

### Severity

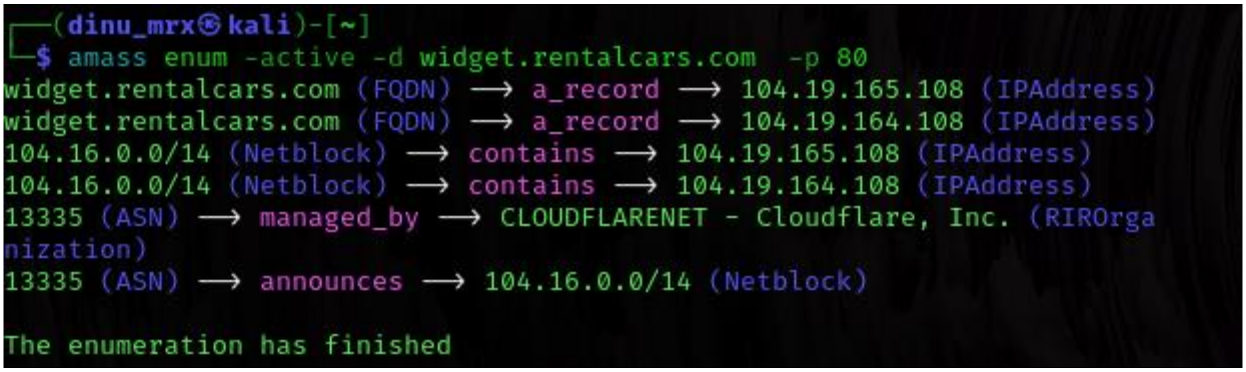
**CVSS 3.x Severity and Metrics:**

**NIST:** NVD **Base Score:** 6.1 MEDIUM **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.*

*Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.*

The results given from amass enum scan



```
┌──(dinu_mrx㉿kali)-[~]
└─$ amass enum -active -d widget.rentalcars.com  -p 80
widget.rentalcars.com (FQDN) ⟶ a_record ⟶ 104.19.165.108 (IPAddress)
widget.rentalcars.com (FQDN) ⟶ a_record ⟶ 104.19.164.108 (IPAddress)
104.16.0.0/14 (Netblock) ⟶ contains ⟶ 104.19.165.108 (IPAddress)
104.16.0.0/14 (Netblock) ⟶ contains ⟶ 104.19.164.108 (IPAddress)
13335 (ASN) ⟶ managed_by ⟶ CLOUDFLARENET - Cloudflare, Inc. (RIROrga
nization)
13335 (ASN) ⟶ announces ⟶ 104.16.0.0/14 (Netblock)

The enumeration has finished
```

From the above amass **enum** command output for **widget.rentalcars.com**, here's what we can derive:

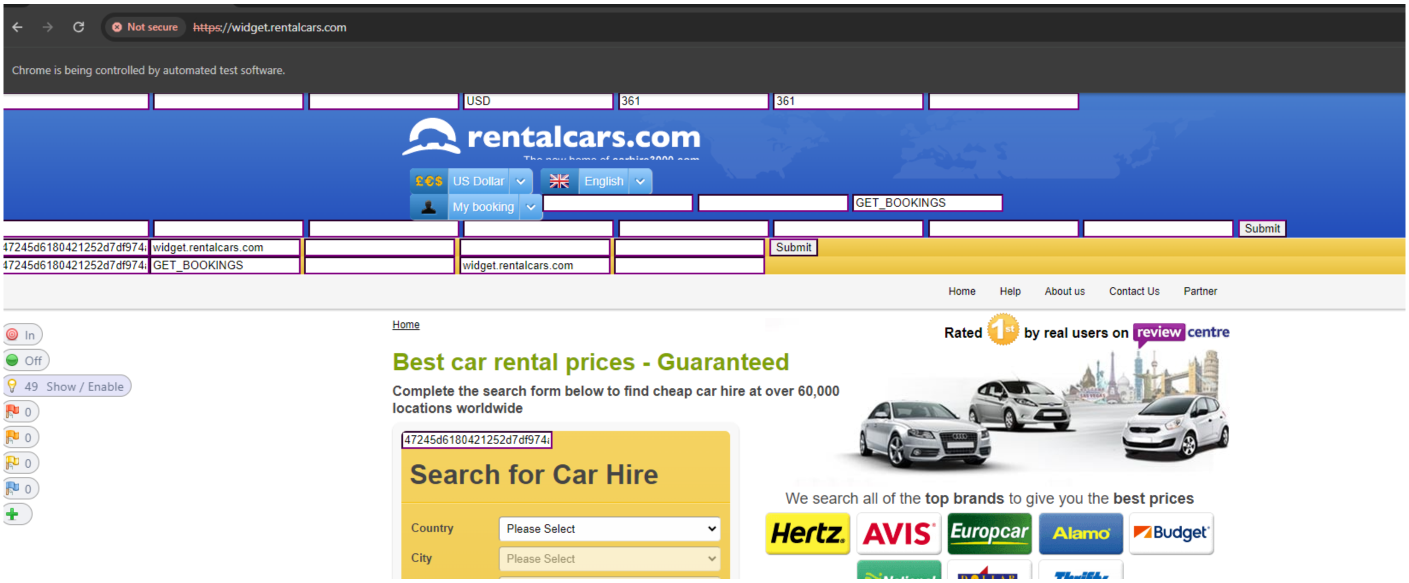
1. **Domain Name and IP Addresses**:
   - The domain **widget.rentalcars.com** resolves to two IP addresses:
     - **104.19.165.108**
     - **104.19.164.108**
2. **Netblock Information**:
   - Both IP addresses (**104.19.165.108** and **104.19.164.108**) belong to the netblock **104.16.0.0/14**, which is managed by Cloudflare (**13335 ASN**).
3. **Autonomous System Number (ASN)**:
   - The Autonomous System Number (**13335**) is managed by Cloudflare (**CLOUDFLARENET - Cloudflare, Inc.**).
   - Cloudflare announces the IP range **104.16.0.0/14**.
4. **Interpretation**:

- The domain **widget.rentalcars.com** is hosted on Cloudflare's infrastructure (**104.16.0.0/14** netblock).
- Cloudflare manages the DNS resolution and serves as a proxy for incoming traffic to the domain.

5. **Additional Context**:
   - The presence of multiple IP addresses (**104.19.165.108** and **104.19.164.108**) might indicate load balancing or redundancy for the domain.
   - Cloudflare's management of the domain suggests that security features like DDoS protection, SSL termination, and content caching are likely employed.

Results which were obtain by manual exploration of the site.

This has 49 hidden fields they have been shown in the screenshot



Not secure ~~https~~://widget.rentalcars.com

Chrome is being controlled by automated test software.

USD | 361 | 361

GET_BOOKINGS

47245d6180421252d7df974ǀ | widget.rentalcars.com

47245d6180421252d7df974ǀ | GET_BOOKINGS | widget.rentalcars.com

Best car rental prices - Guaranteed

Complete the search form below to find cheap car hire at over 60,000 locations worldwide

47245d6180421252d7df974ǀ

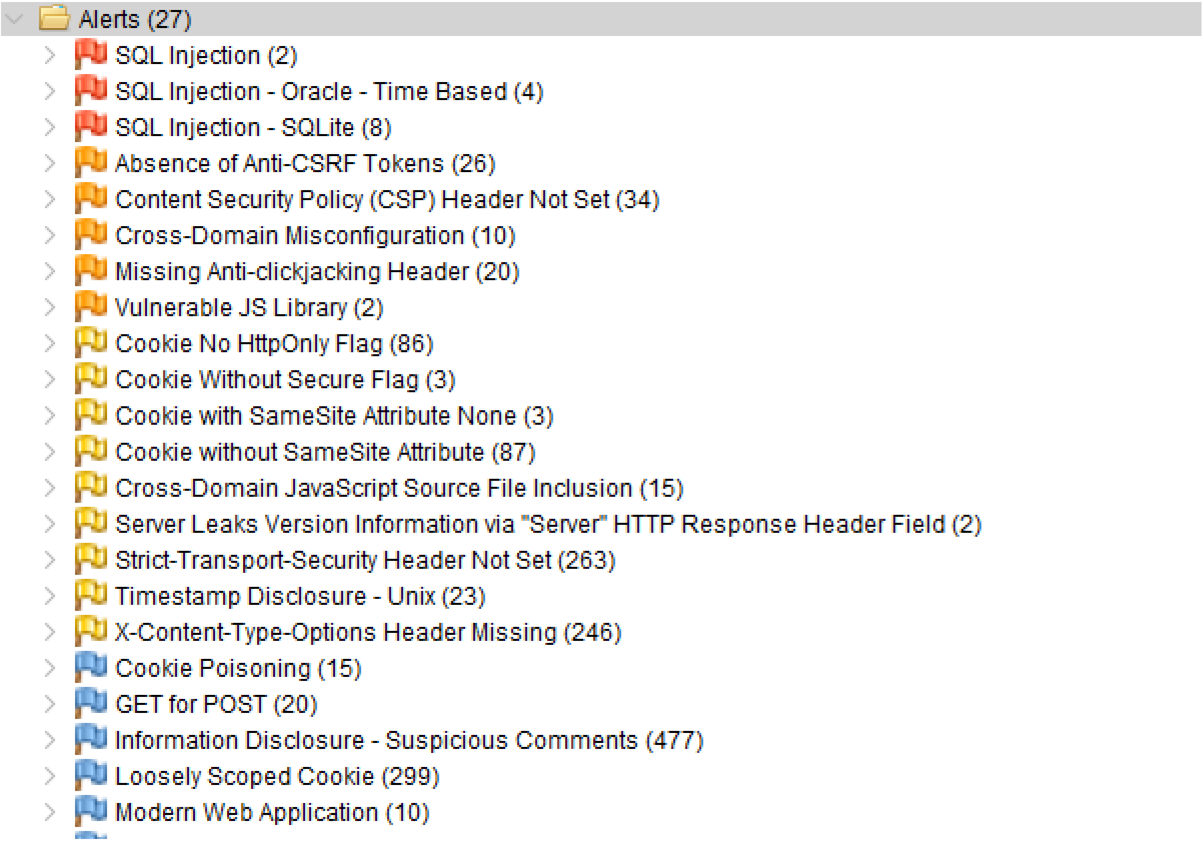
Search for Car Hire

Country: Please Select

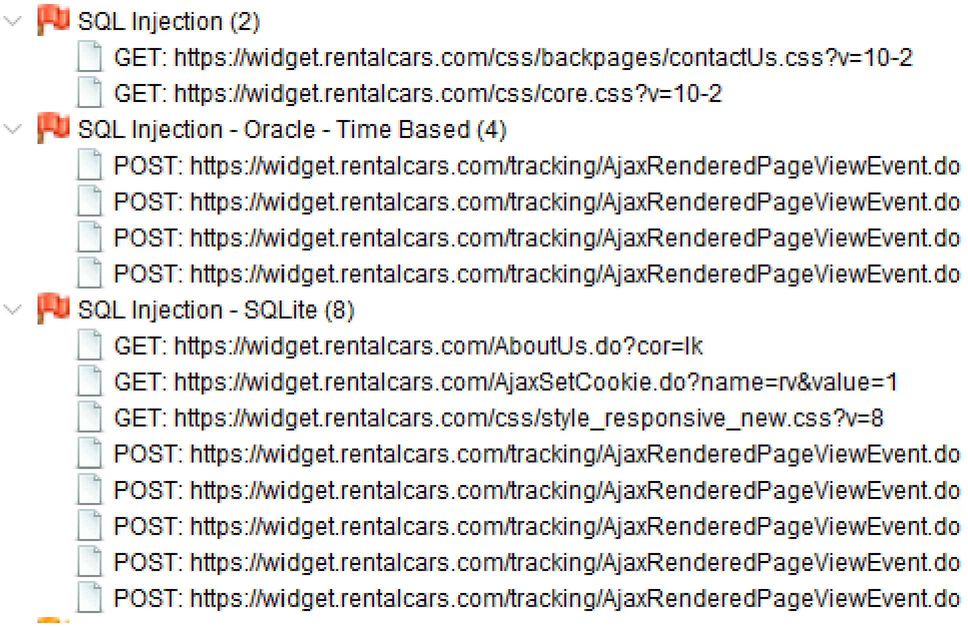
City: Please Select

Rated 1st by real users on review centre

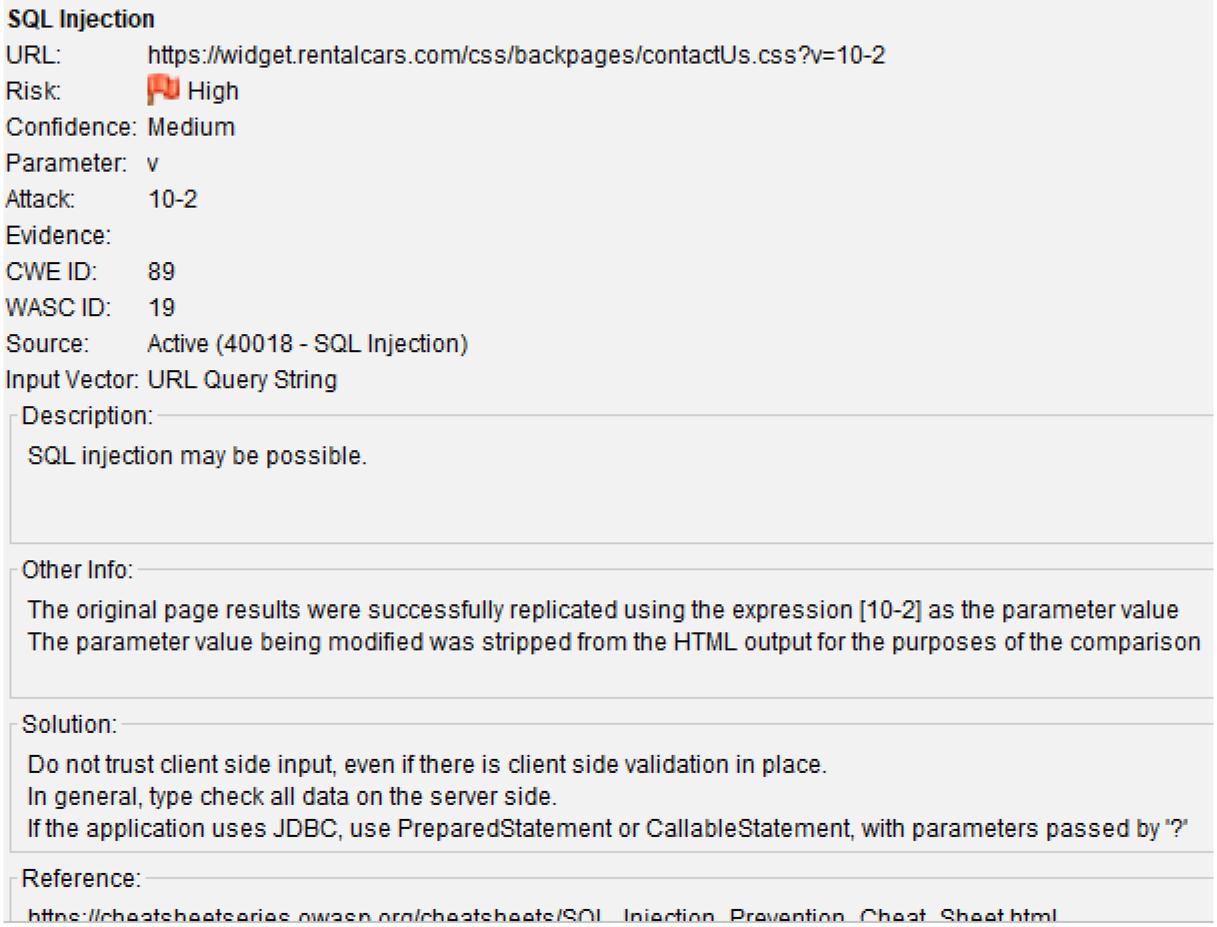
We search all of the **top brands** to give you the **best prices**



- Alerts (27)
  - SQL Injection (2)
  - SQL Injection - Oracle - Time Based (4)
  - SQL Injection - SQLite (8)
  - Absence of Anti-CSRF Tokens (26)
  - Content Security Policy (CSP) Header Not Set (34)
  - Cross-Domain Misconfiguration (10)
  - Missing Anti-clickjacking Header (20)
  - Vulnerable JS Library (2)
  - Cookie No HttpOnly Flag (86)
  - Cookie Without Secure Flag (3)
  - Cookie with SameSite Attribute None (3)
  - Cookie without SameSite Attribute (87)
  - Cross-Domain JavaScript Source File Inclusion (15)
  - Server Leaks Version Information via "Server" HTTP Response Header Field (2)
  - Strict-Transport-Security Header Not Set (263)
  - Timestamp Disclosure - Unix (23)
  - X-Content-Type-Options Header Missing (246)
  - Cookie Poisoning (15)
  - GET for POST (20)
  - Information Disclosure - Suspicious Comments (477)
  - Loosely Scoped Cookie (299)
  - Modern Web Application (10)



- SQL Injection (2)
  - GET: https://widget.rentalcars.com/css/backpages/contactUs.css?v=10-2
  - GET: https://widget.rentalcars.com/css/core.css?v=10-2
- SQL Injection - Oracle - Time Based (4)
  - POST: https://widget.rentalcars.com/tracking/AjaxRenderedPageViewEvent.do
  - POST: https://widget.rentalcars.com/tracking/AjaxRenderedPageViewEvent.do
  - POST: https://widget.rentalcars.com/tracking/AjaxRenderedPageViewEvent.do
  - POST: https://widget.rentalcars.com/tracking/AjaxRenderedPageViewEvent.do
- SQL Injection - SQLite (8)
  - GET: https://widget.rentalcars.com/AboutUs.do?cor=lk
  - GET: https://widget.rentalcars.com/AjaxSetCookie.do?name=rv&value=1
  - GET: https://widget.rentalcars.com/css/style_responsive_new.css?v=8
  - POST: https://widget.rentalcars.com/tracking/AjaxRenderedPageViewEvent.do
  - POST: https://widget.rentalcars.com/tracking/AjaxRenderedPageViewEvent.do
  - POST: https://widget.rentalcars.com/tracking/AjaxRenderedPageViewEvent.do
  - POST: https://widget.rentalcars.com/tracking/AjaxRenderedPageViewEvent.do
  - POST: https://widget.rentalcars.com/tracking/AjaxRenderedPageViewEvent.do



**SQL Injection**

URL: https://widget.rentalcars.com/css/backpages/contactUs.css?v=10-2
Risk: 🚩 High
Confidence: Medium
Parameter: v
Attack: 10-2
Evidence:
CWE ID: 89
WASC ID: 19
Source: Active (40018 - SQL Injection)
Input Vector: URL Query String

Description:

SQL injection may be possible.

Other Info:

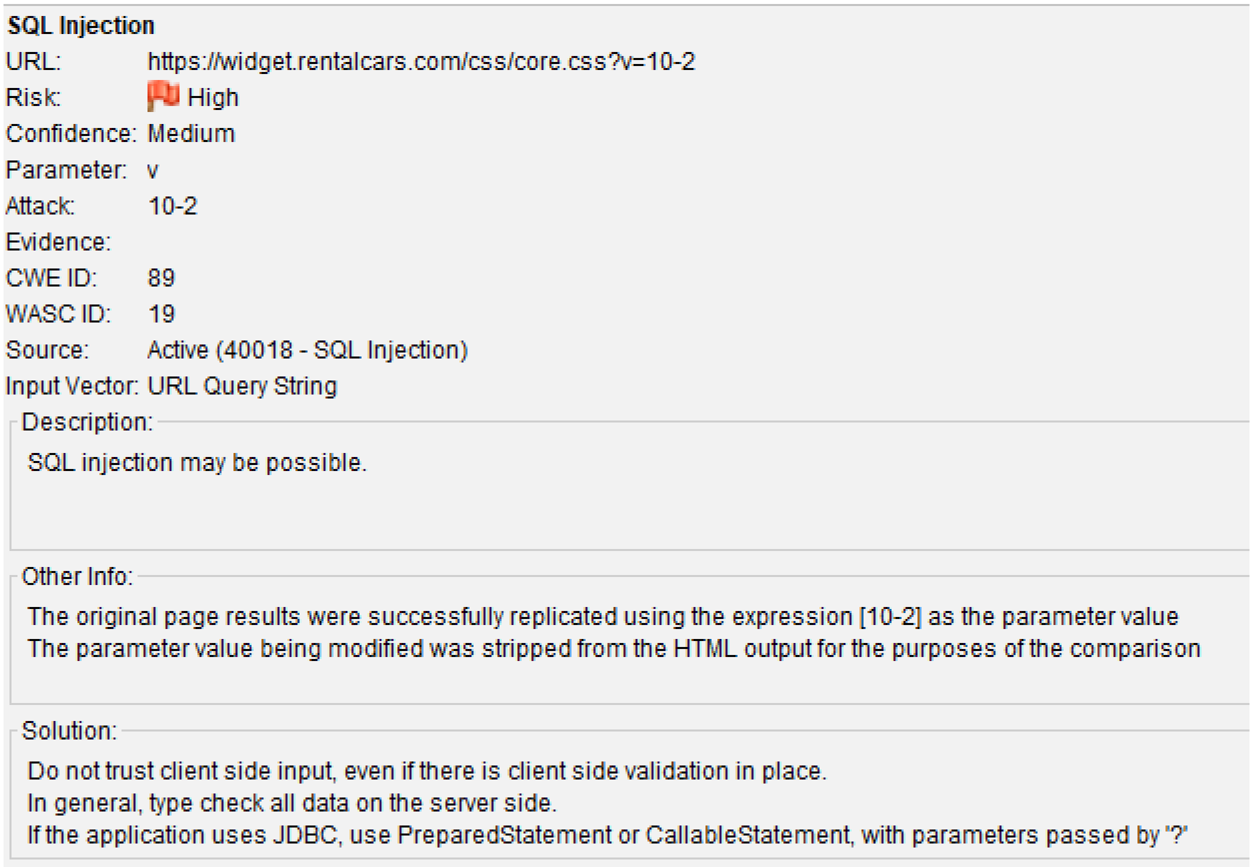
The original page results were successfully replicated using the expression [10-2] as the parameter value
The parameter value being modified was stripped from the HTML output for the purposes of the comparison

Solution:

Do not trust client side input, even if there is client side validation in place.
In general, type check all data on the server side.
If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'

Reference:

https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html



**SQL Injection**

URL: https://widget.rentalcars.com/css/core.css?v=10-2
Risk: 🚩 High
Confidence: Medium
Parameter: v
Attack: 10-2
Evidence:
CWE ID: 89
WASC ID: 19
Source: Active (40018 - SQL Injection)
Input Vector: URL Query String

Description:

SQL injection may be possible.

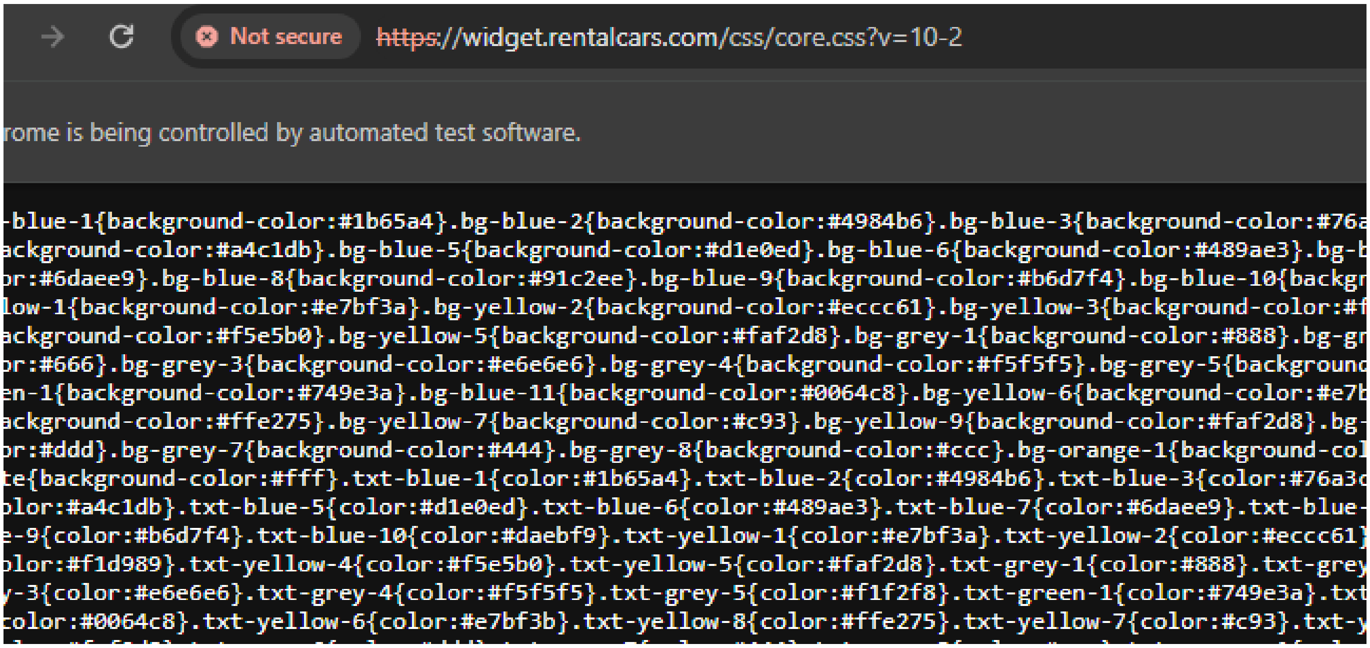
Other Info:

The original page results were successfully replicated using the expression [10-2] as the parameter value
The parameter value being modified was stripped from the HTML output for the purposes of the comparison

Solution:

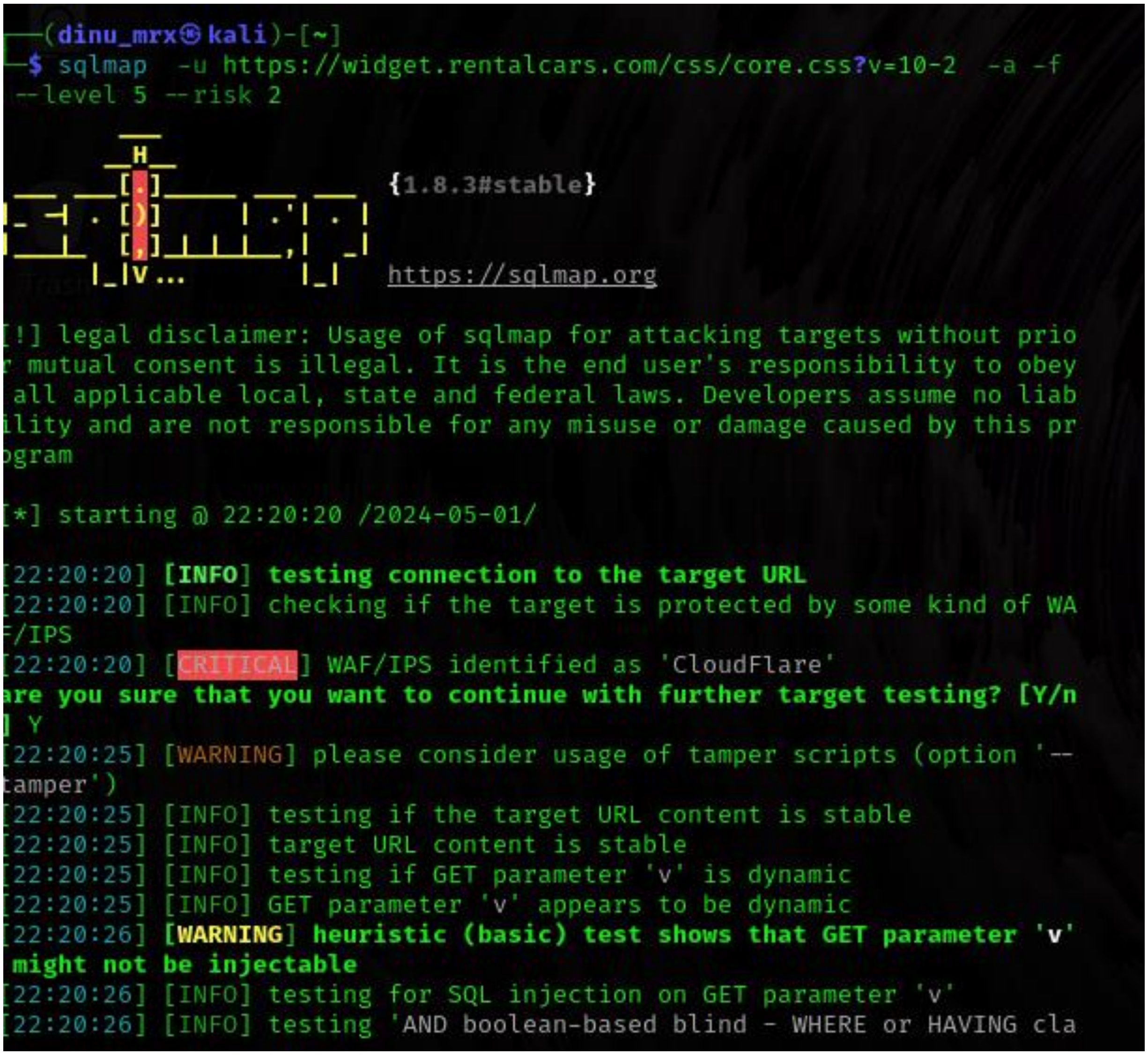
Do not trust client side input, even if there is client side validation in place.
In general, type check all data on the server side.
If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'

https://widget.rentalcars.com/css/core.css?v=10-2

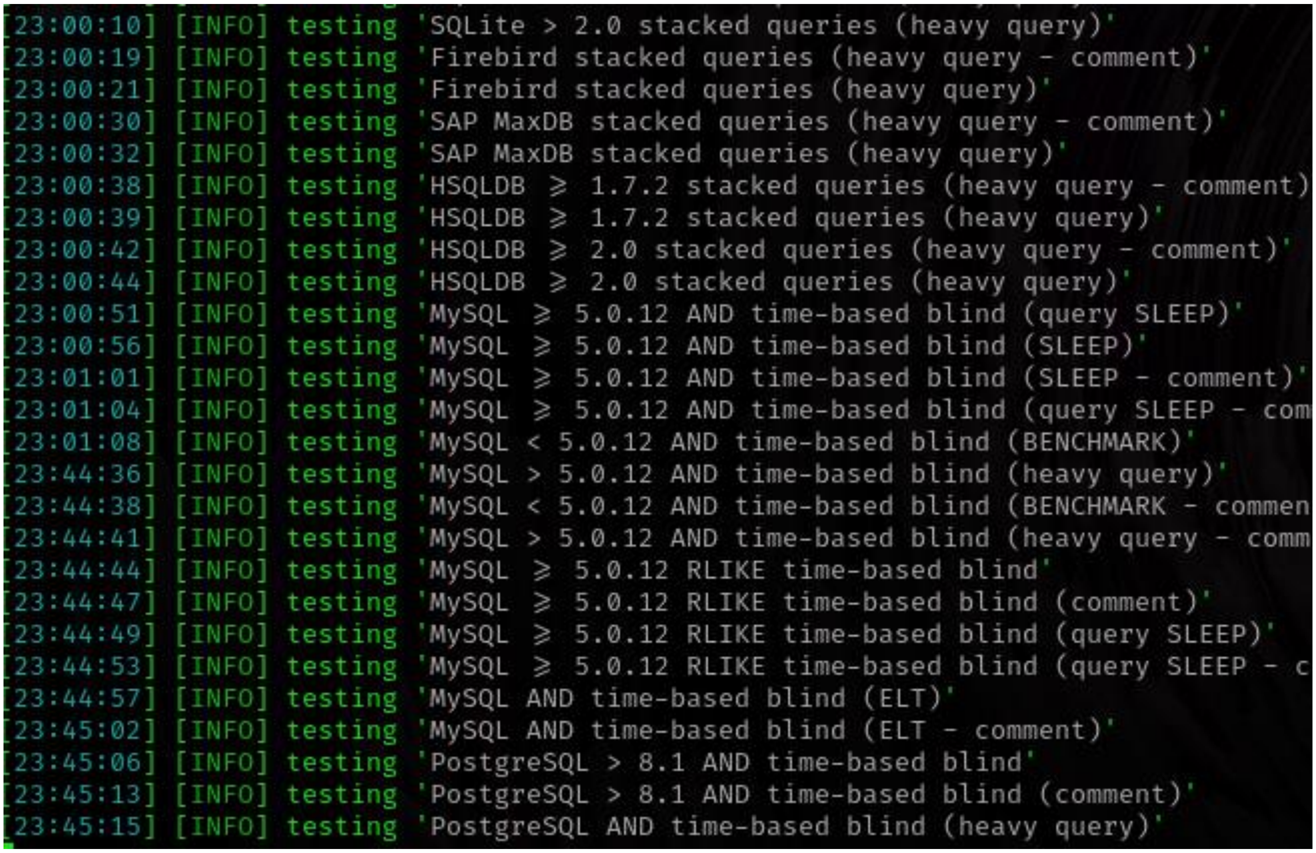


rome is being controlled by automated test software.

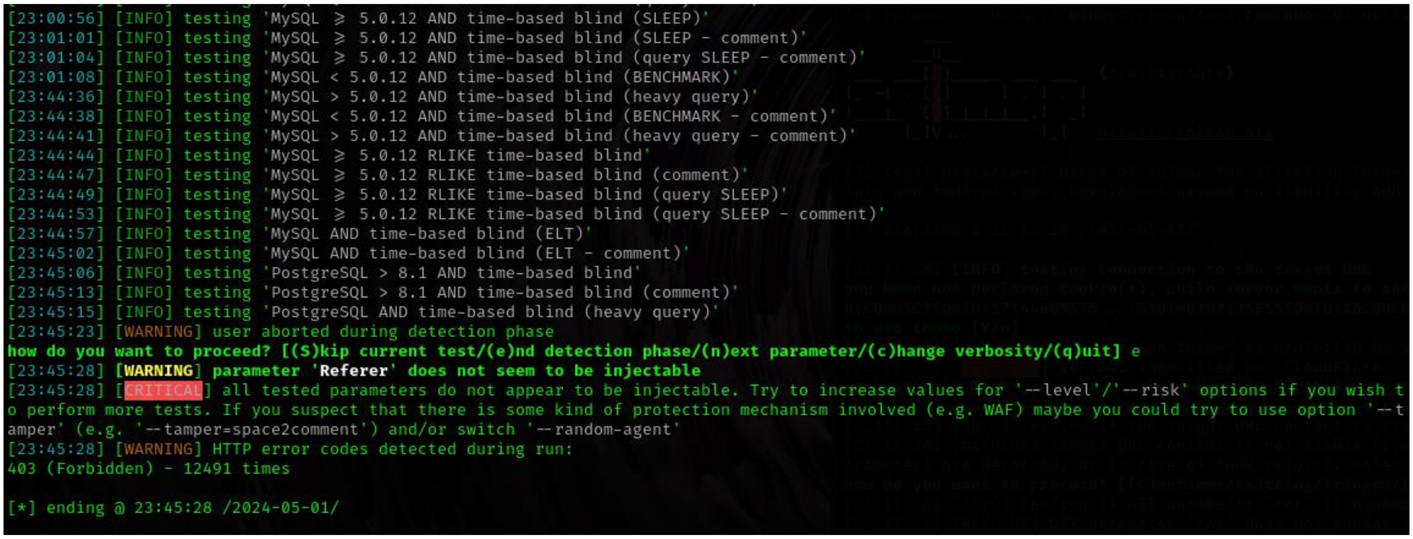
```
-blue-1{background-color:#1b65a4}.bg-blue-2{background-color:#4984b6}.bg-blue-3{background-color:#76a
ackground-color:#a4c1db}.bg-blue-5{background-color:#d1e0ed}.bg-blue-6{background-color:#489ae3}.bg-b
or:#6daee9}.bg-blue-8{background-color:#91c2ee}.bg-blue-9{background-color:#b6d7f4}.bg-blue-10{backgr
low-1{background-color:#e7bf3a}.bg-yellow-2{background-color:#eccc61}.bg-yellow-3{background-color:#f
ackground-color:#f5e5b0}.bg-yellow-5{background-color:#faf2d8}.bg-grey-1{background-color:#888}.bg-gr
or:#666}.bg-grey-3{background-color:#e6e6e6}.bg-grey-4{background-color:#f5f5f5}.bg-grey-5{backgroun
en-1{background-color:#749e3a}.bg-blue-11{background-color:#0064c8}.bg-yellow-6{background-color:#e7b
ackground-color:#ffe275}.bg-yellow-7{background-color:#c93}.bg-yellow-9{background-color:#faf2d8}.bg-
or:#ddd}.bg-grey-7{background-color:#444}.bg-grey-8{background-color:#ccc}.bg-orange-1{background-col
te{background-color:#fff}.txt-blue-1{color:#1b65a4}.txt-blue-2{color:#4984b6}.txt-blue-3{color:#76a3c
olor:#a4c1db}.txt-blue-5{color:#d1e0ed}.txt-blue-6{color:#489ae3}.txt-blue-7{color:#6daee9}.txt-blue-
e-9{color:#b6d7f4}.txt-blue-10{color:#daebf9}.txt-yellow-1{color:#e7bf3a}.txt-yellow-2{color:#eccc61}
olor:#f1d989}.txt-yellow-4{color:#f5e5b0}.txt-yellow-5{color:#faf2d8}.txt-grey-1{color:#888}.txt-grey
y-3{color:#e6e6e6}.txt-grey-4{color:#f5f5f5}.txt-grey-5{color:#f1f2f8}.txt-green-1{color:#749e3a}.txt
color:#0064c8}.txt-yellow-6{color:#e7bf3b}.txt-yellow-8{color:#ffe275}.txt-yellow-7{color:#c93}.txt-y
```



```
─(dinu_mrx㉿kali)-[~]
─$ sqlmap  -u https://widget.rentalcars.com/css/core.css?v=10-2  -a -f
 --level 5 --risk 2
        ___
       __H__
 ___ ___[.]_____ ___ ___      {1.8.3#stable}
|_ -| . [)]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|      https://sqlmap.org

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

[*] starting @ 22:20:20 /2024-05-01/

[22:20:20] [INFO] testing connection to the target URL
[22:20:20] [INFO] checking if the target is protected by some kind of WA
F/IPS
[22:20:20] [CRITICAL] WAF/IPS identified as 'CloudFlare'
are you sure that you want to continue with further target testing? [Y/n
] Y
[22:20:25] [WARNING] please consider usage of tamper scripts (option '--
tamper')
[22:20:25] [INFO] testing if the target URL content is stable
[22:20:25] [INFO] target URL content is stable
[22:20:25] [INFO] testing if GET parameter 'v' is dynamic
[22:20:25] [INFO] GET parameter 'v' appears to be dynamic
[22:20:26] [WARNING] heuristic (basic) test shows that GET parameter 'v'
 might not be injectable
[22:20:26] [INFO] testing for SQL injection on GET parameter 'v'
[22:20:26] [INFO] testing 'AND boolean-based blind - WHERE or HAVING cla
```

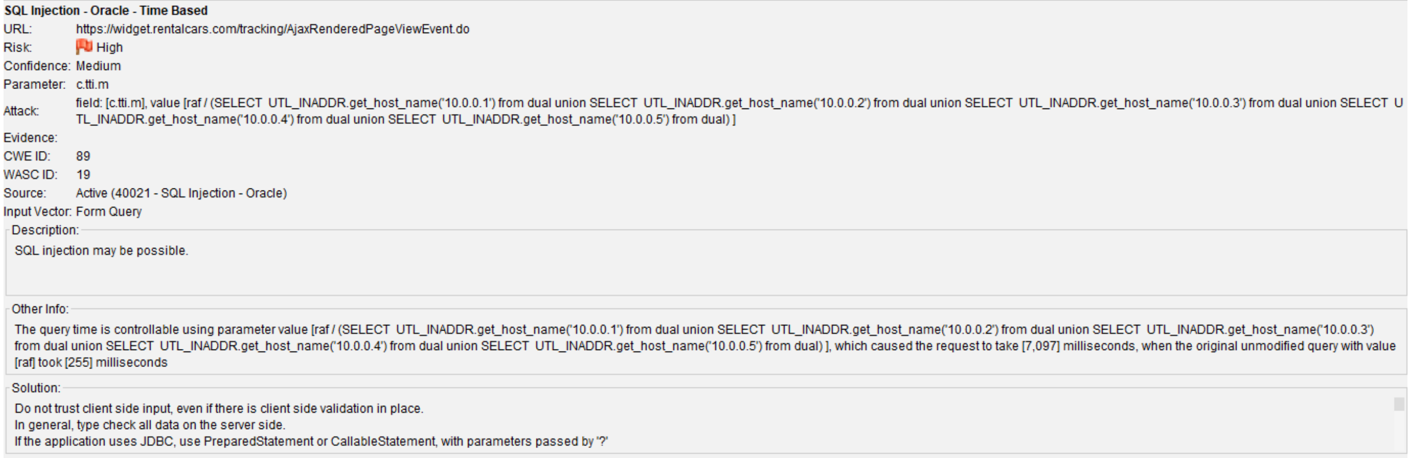


```
[23:00:10] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query)'
[23:00:19] [INFO] testing 'Firebird stacked queries (heavy query - comment)'
[23:00:21] [INFO] testing 'Firebird stacked queries (heavy query)'
[23:00:30] [INFO] testing 'SAP MaxDB stacked queries (heavy query - comment)'
[23:00:32] [INFO] testing 'SAP MaxDB stacked queries (heavy query)'
[23:00:38] [INFO] testing 'HSQLDB ≥ 1.7.2 stacked queries (heavy query - comment)
[23:00:39] [INFO] testing 'HSQLDB ≥ 1.7.2 stacked queries (heavy query)'
[23:00:42] [INFO] testing 'HSQLDB ≥ 2.0 stacked queries (heavy query - comment)'
[23:00:44] [INFO] testing 'HSQLDB ≥ 2.0 stacked queries (heavy query)'
[23:00:51] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[23:00:56] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (SLEEP)'
[23:01:01] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (SLEEP - comment)'
[23:01:04] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP - com
[23:01:08] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK)'
[23:44:36] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query)'
[23:44:38] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK - commen
[23:44:41] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query - comm
[23:44:44] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind'
[23:44:47] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (comment)'
[23:44:49] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (query SLEEP)'
[23:44:53] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (query SLEEP - c
[23:44:57] [INFO] testing 'MySQL AND time-based blind (ELT)'
[23:45:02] [INFO] testing 'MySQL AND time-based blind (ELT - comment)'
[23:45:06] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:45:13] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind (comment)'
[23:45:15] [INFO] testing 'PostgreSQL AND time-based blind (heavy query)'
```



```
[23:00:56] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (SLEEP)'
[23:01:01] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (SLEEP - comment)'
[23:01:04] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP - comment)'
[23:01:08] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK)'
[23:44:36] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query)'
[23:44:38] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK - comment)'
[23:44:41] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query - comment)'
[23:44:44] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind'
[23:44:47] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (comment)'
[23:44:49] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (query SLEEP)'
[23:44:53] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (query SLEEP - comment)'
[23:44:57] [INFO] testing 'MySQL AND time-based blind (ELT)'
[23:45:02] [INFO] testing 'MySQL AND time-based blind (ELT - comment)'
[23:45:06] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:45:13] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind (comment)'
[23:45:15] [INFO] testing 'PostgreSQL AND time-based blind (heavy query)'
[23:45:23] [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hange verbosity/(q)uit] e
[23:45:28] [WARNING] parameter 'Referer' does not seem to be injectable
[23:45:28] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish t
o perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--t
amper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[23:45:28] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 12491 times

[*] ending @ 23:45:28 /2024-05-01/
```

There no any positive result on the vulnerability when scanned with sqlmap.



**SQL Injection - Oracle - Time Based**

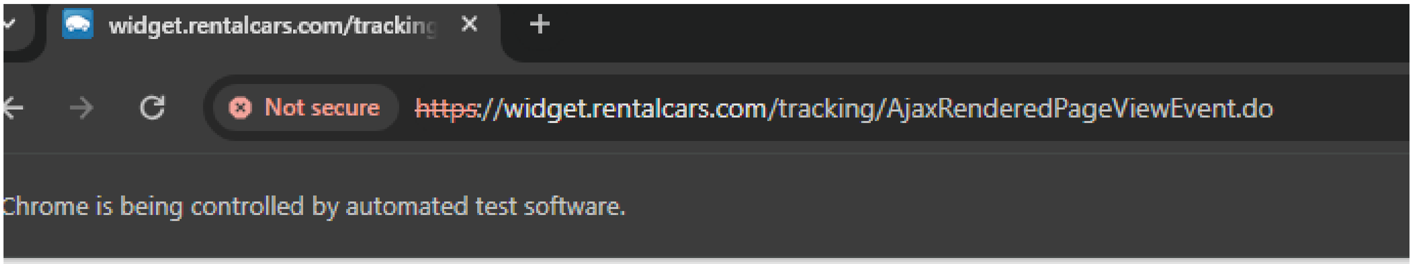
URL: https://widget.rentalcars.com/tracking/AjaxRenderedPageViewEvent.do
Risk: 🚩 High
Confidence: Medium
Parameter: c.tti.m
Attack: field: [c.tti.m], value [raf / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) ]
Evidence:
CWE ID: 89
WASC ID: 19
Source: Active (40021 - SQL Injection - Oracle)
Input Vector: Form Query

Description:
SQL injection may be possible.

Other Info:
The query time is controllable using parameter value [raf / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) ], which caused the request to take [7,097] milliseconds, when the original unmodified query with value [raf] took [255] milliseconds

Solution:
Do not trust client side input, even if there is client side validation in place.
In general, type check all data on the server side.
If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'

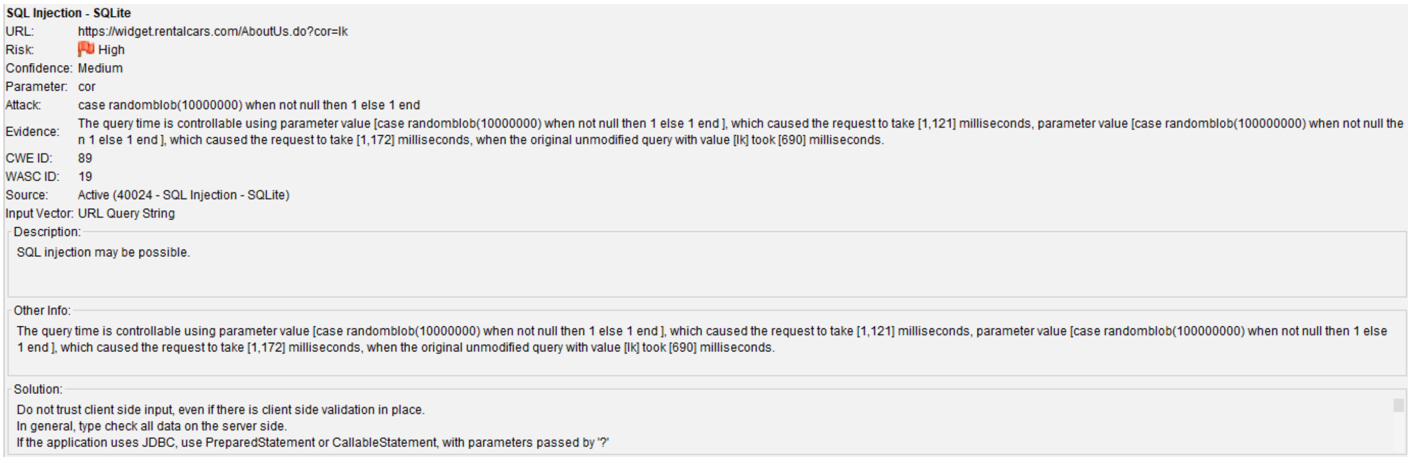
The above page is in inaccessible the below screenshot gives appearance of the above site https://widget.rentalcars.com/tracking/AjaxRenderedPageViewEvent.do



~~https~~://widget.rentalcars.com/tracking/AjaxRenderedPageViewEvent.do

Chrome is being controlled by automated test software.

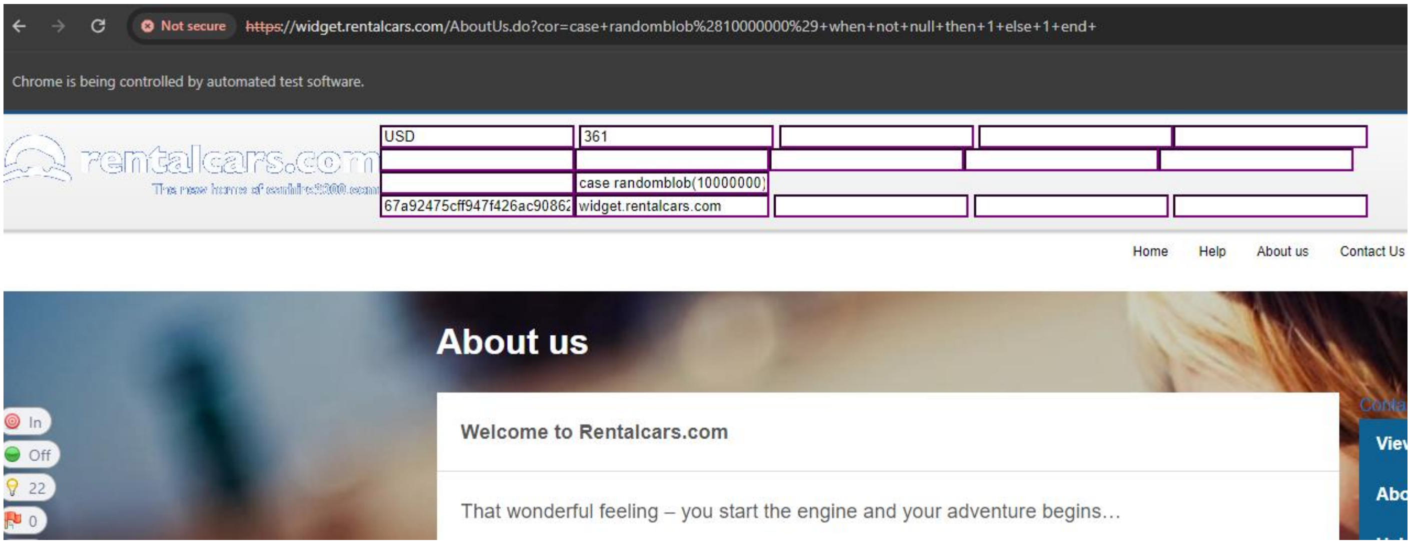
Above site was just a blank site.



```
SQL Injection - SQLite
URL:          https://widget.rentalcars.com/AboutUs.do?cor=lk
Risk:         High
Confidence:   Medium
Parameter:    cor
Attack:       case randomblob(10000000) when not null then 1 else 1 end
Evidence:     The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end ], which caused the request to take [1,121] milliseconds, parameter value [case randomblob(100000000) when not null the
              n 1 else 1 end ], which caused the request to take [1,172] milliseconds, when the original unmodified query with value [lk] took [690] milliseconds.
CWE ID:       89
WASC ID:      19
Source:       Active (40024 - SQL Injection - SQLite)
Input Vector: URL Query String
Description:
 SQL injection may be possible.
Other Info:
 The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end ], which caused the request to take [1,121] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else
 1 end ], which caused the request to take [1,172] milliseconds, when the original unmodified query with value [lk] took [690] milliseconds.
Solution:
 Do not trust client side input, even if there is client side validation in place.
 In general, type check all data on the server side.
 If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'
```

https://widget.rentalcars.com/AboutUs.do?cor=lk

The above site contain 22 hidden fields is shown in the below screenshot

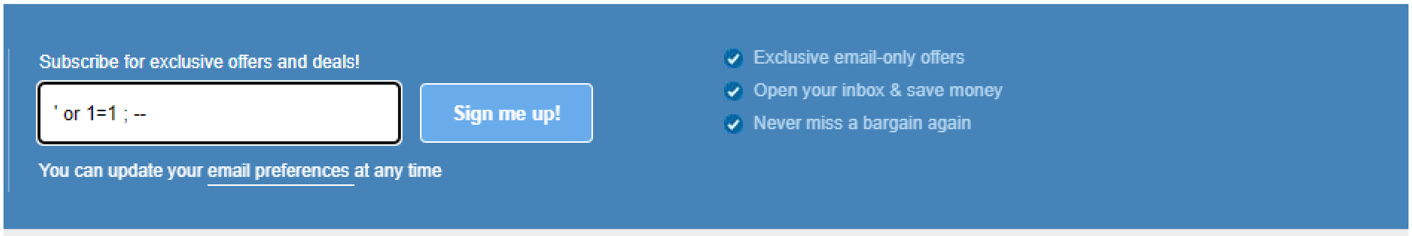


Not secure https://widget.rentalcars.com/AboutUs.do?cor=case+randomblob%2810000000%29+when+not+null+then+1+else+1+end+

Chrome is being controlled by automated test software.

USD | 361 | case randomblob(10000000) | 67a92475cff947f426ac90862 | widget.rentalcars.com

rentalcars.com
The new home of carhire3000.com
Home
Help
About us
Contact Us
About us
Welcome to Rentalcars.com
That wonderful feeling – you start the engine and your adventure begins…
In
Off
22
0

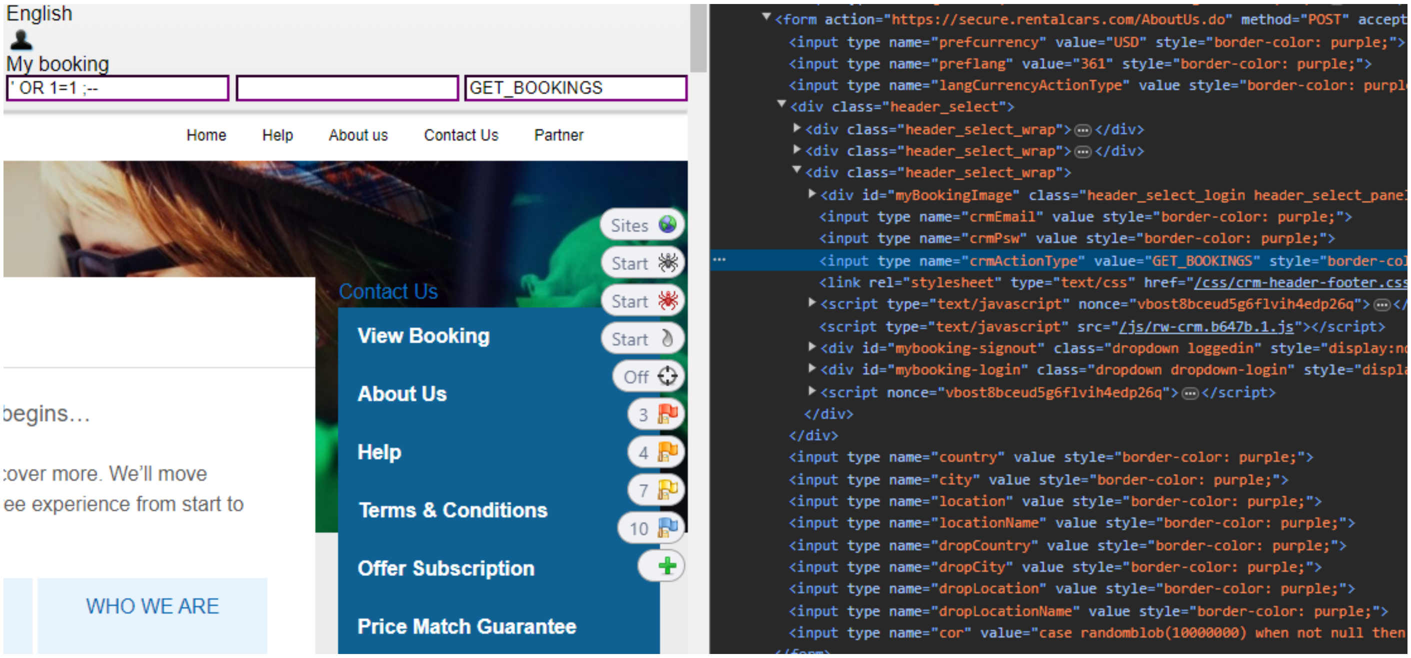


Subscribe for exclusive offers and deals!

' or 1=1 ; --

Sign me up!
Exclusive email-only offers
Open your inbox & save money
Never miss a bargain again
You can update your email preferences at any time

We can’t inject here, there the data is properly sanitized.

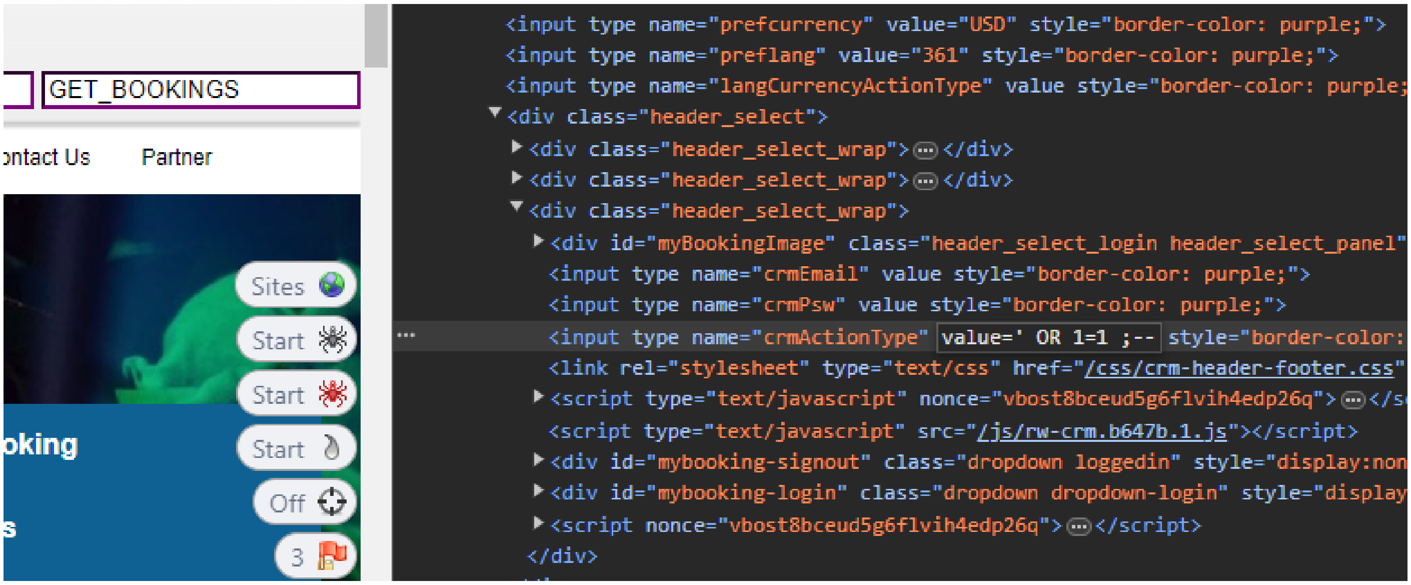


' OR 1=1 ;--

GET_BOOKINGS

```
▼<form action="https://secure.rentalcars.com/AboutUs.do" method="POST" accept
   <input type name="prefcurrency" value="USD" style="border-color: purple;">
   <input type name="preflang" value="361" style="border-color: purple;">
   <input type name="langCurrencyActionType" value style="border-color: purpl
  ▼<div class="header_select">
    ▶<div class="header_select_wrap">⋯</div>
    ▶<div class="header_select_wrap">⋯</div>
    ▼<div class="header_select_wrap">
      ▶<div id="myBookingImage" class="header_select_login header_select_panel
       <input type name="crmEmail" value style="border-color: purple;">
       <input type name="crmPsw" value style="border-color: purple;">
…      <input type name="crmActionType" value="GET_BOOKINGS" style="border-col
       <link rel="stylesheet" type="text/css" href="/css/crm-header-footer.css
      ▶<script type="text/javascript" nonce="vbost8bceud5g6flvih4edp26q">⋯</
       <script type="text/javascript" src="/js/rw-crm.b647b.1.js"></script>
      ▶<div id="mybooking-signout" class="dropdown loggedin" style="display:no
      ▶<div id="mybooking-login" class="dropdown dropdown-login" style="displa
      ▶<script nonce="vbost8bceud5g6flvih4edp26q">⋯</script>
     </div>
   </div>
   <input type name="country" value style="border-color: purple;">
   <input type name="city" value style="border-color: purple;">
   <input type name="location" value style="border-color: purple;">
   <input type name="locationName" value style="border-color: purple;">
   <input type name="dropCountry" value style="border-color: purple;">
   <input type name="dropCity" value style="border-color: purple;">
   <input type name="dropLocation" value style="border-color: purple;">
   <input type name="dropLocationName" value style="border-color: purple;">
   <input type name="cor" value="case randomblob(10000000) when not null then
```

Following inject also didn't work and I tried to change GET_BOOKINGS in the hidden field to the payload but we can't change it once the enter button is pressed it automatically changes.



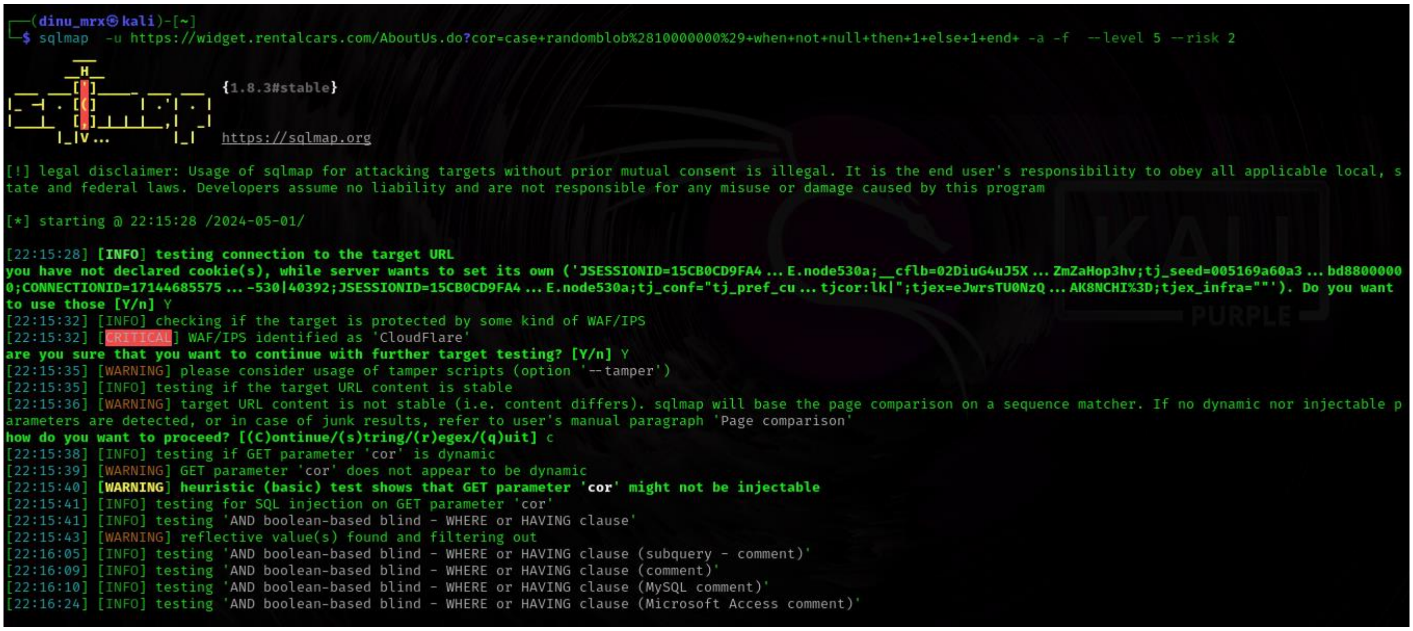
GET_BOOKINGS

```
   <input type name="prefcurrency" value="USD" style="border-color: purple;">
   <input type name="preflang" value="361" style="border-color: purple;">
   <input type name="langCurrencyActionType" value style="border-color: purple;
  ▼<div class="header_select">
    ▶<div class="header_select_wrap">⋯</div>
    ▶<div class="header_select_wrap">⋯</div>
    ▼<div class="header_select_wrap">
      ▶<div id="myBookingImage" class="header_select_login header_select_panel"
       <input type name="crmEmail" value style="border-color: purple;">
       <input type name="crmPsw" value style="border-color: purple;">
…      <input type name="crmActionType" value=' OR 1=1 ;-- style="border-color:
       <link rel="stylesheet" type="text/css" href="/css/crm-header-footer.css"
      ▶<script type="text/javascript" nonce="vbost8bceud5g6flvih4edp26q">⋯</s
       <script type="text/javascript" src="/js/rw-crm.b647b.1.js"></script>
      ▶<div id="mybooking-signout" class="dropdown loggedin" style="display:non
      ▶<div id="mybooking-login" class="dropdown dropdown-login" style="display
      ▶<script nonce="vbost8bceud5g6flvih4edp26q">⋯</script>
     </div>
```

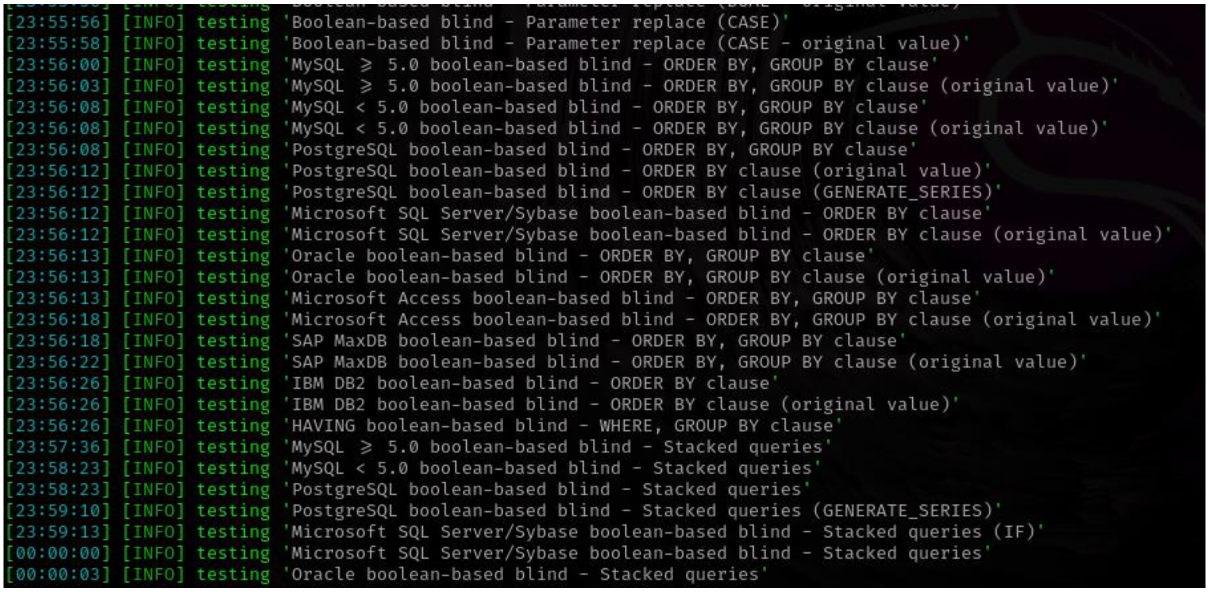
Checking with sqlmap for this particular site

[https://widget.rentalcars.com/AboutUs.do?cor=case+randomblob%2810000000%29+when+not+null+then+1+else+1+end](https://widget.rentalcars.com/AboutUs.do?cor=case+randomblob%2810000000%29+when+not+null+then+1+else+1+end)+

results are as follows.

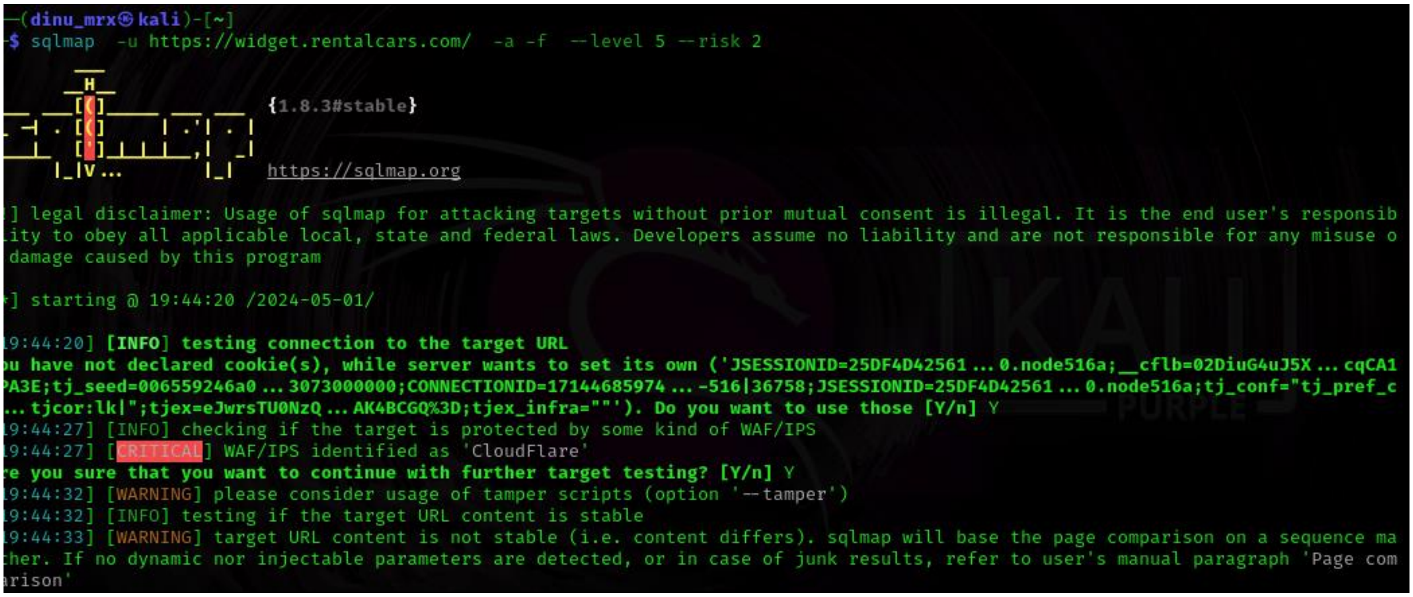


```
┌──(dinu_mrx㉿kali)-[~]
└─$ sqlmap  -u https://widget.rentalcars.com/AboutUs.do?cor=case+randomblob%2810000000%29+when+not+null+then+1+else+1+end+ -a -f  --level 5 --risk 2
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.3#stable}
|_ -| . [(]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 22:15:28 /2024-05-01/

[22:15:28] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('JSESSIONID=15CB0CD9FA4 ... E.node530a;__cflb=02DiuG4uJ5X ... ZmZaHop3hv;tj_seed=005169a60a3 ... bd8800000
0;CONNECTIONID=17144685575 ... -530|40392;JSESSIONID=15CB0CD9FA4 ... E.node530a;tj_conf="tj_pref_cu ... tjcor:lk|";tjex=eJwrsTU0NzQ ... AK8NCHI%3D;tjex_infra=""'). Do you want
to use those [Y/n] Y
[22:15:32] [INFO] checking if the target is protected by some kind of WAF/IPS
[22:15:32] [CRITICAL] WAF/IPS identified as 'CloudFlare'
are you sure that you want to continue with further target testing? [Y/n] Y
[22:15:35] [WARNING] please consider usage of tamper scripts (option '--tamper')
[22:15:35] [INFO] testing if the target URL content is stable
[22:15:36] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable p
arameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[22:15:38] [INFO] testing if GET parameter 'cor' is dynamic
[22:15:39] [WARNING] GET parameter 'cor' does not appear to be dynamic
[22:15:40] [WARNING] heuristic (basic) test shows that GET parameter 'cor' might not be injectable
[22:15:41] [INFO] testing for SQL injection on GET parameter 'cor'
[22:15:41] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:15:43] [WARNING] reflective value(s) found and filtering out
[22:16:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[22:16:09] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[22:16:10] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[22:16:24] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
```

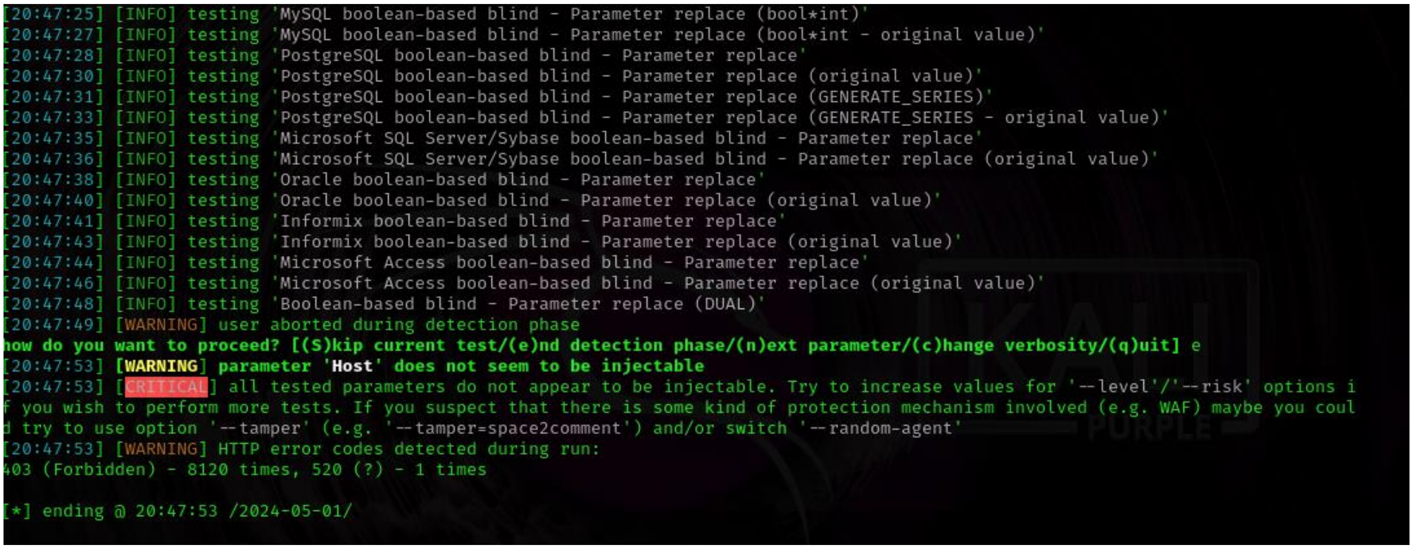


```
[23:55:56] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[23:55:58] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[23:56:00] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[23:56:03] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[23:56:08] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[23:56:08] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[23:56:08] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'
[23:56:12] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (original value)'
[23:56:12] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (GENERATE_SERIES)'
[23:56:12] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[23:56:12] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause (original value)'
[23:56:13] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'
[23:56:13] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[23:56:13] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause'
[23:56:18] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[23:56:18] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause'
[23:56:22] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[23:56:26] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause'
[23:56:26] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause (original value)'
[23:56:26] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[23:57:36] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - Stacked queries'
[23:58:23] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[23:58:23] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[23:59:10] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries (GENERATE_SERIES)'
[23:59:13] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'
[00:00:00] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries'
[00:00:03] [INFO] testing 'Oracle boolean-based blind - Stacked queries'
```

Results given by SQLmap for [https://widget.rentalcars.com/](https://widget.rentalcars.com/)

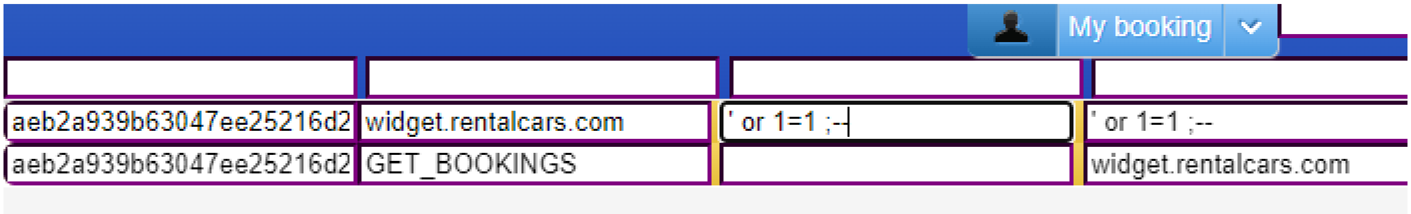


```
─(dinu_mrx㉿kali)-[~]
$ sqlmap  -u https://widget.rentalcars.com/  -a -f  --level 5 --risk 2
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.3#stable}
|_ -| . [(]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

*] starting @ 19:44:20 /2024-05-01/

19:44:20] [INFO] testing connection to the target URL
ou have not declared cookie(s), while server wants to set its own ('JSESSIONID=25DF4D42561...0.node516a;__cflb=02DiuG4uJ5X...cqCA1
PA3E;tj_seed=006559246a0...3073000000;CONNECTIONID=17144685974...-516|36758;JSESSIONID=25DF4D42561...0.node516a;tj_conf="tj_pref_c
...tjcor:lk|";tjex=eJwrsTU0NzQ...AK4BCGQ%3D;tjex_infra=""'). Do you want to use those [Y/n] Y
19:44:27] [INFO] checking if the target is protected by some kind of WAF/IPS
19:44:27] [CRITICAL] WAF/IPS identified as 'CloudFlare'
re you sure that you want to continue with further target testing? [Y/n] Y
19:44:32] [WARNING] please consider usage of tamper scripts (option '--tamper')
19:44:32] [INFO] testing if the target URL content is stable
19:44:33] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence ma
ther. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page com
arison'
```

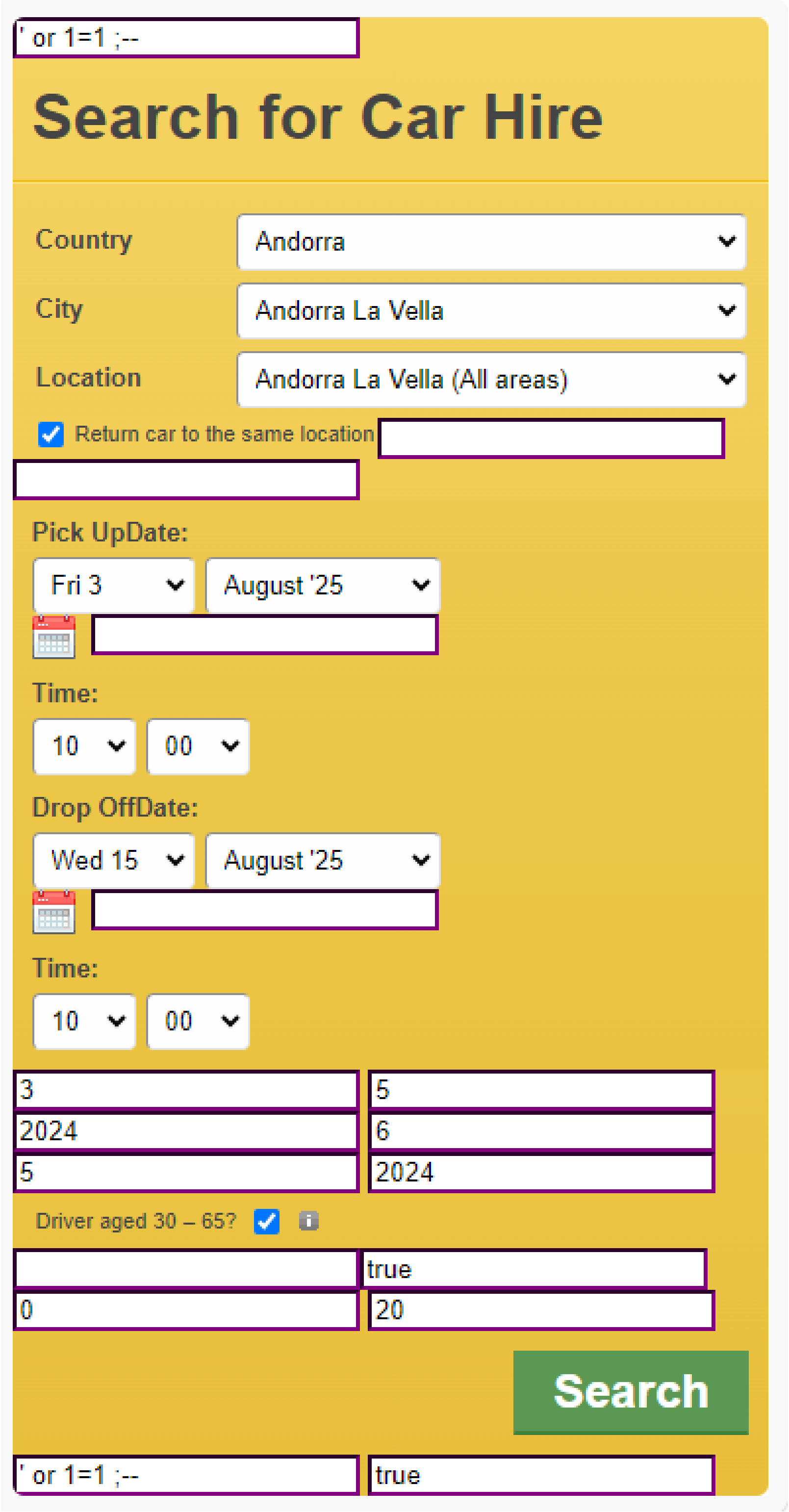


```
[20:47:25] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int)'
[20:47:27] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int - original value)'
[20:47:28] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[20:47:30] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (original value)'
[20:47:31] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES)'
[20:47:33] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES - original value)'
[20:47:35] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'
[20:47:36] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)'
[20:47:38] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[20:47:40] [INFO] testing 'Oracle boolean-based blind - Parameter replace (original value)'
[20:47:41] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[20:47:43] [INFO] testing 'Informix boolean-based blind - Parameter replace (original value)'
[20:47:44] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[20:47:46] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace (original value)'
[20:47:48] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[20:47:49] [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)hange verbosity/(q)uit] e
[20:47:53] [WARNING] parameter 'Host' does not seem to be injectable
[20:47:53] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options i
f you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you coul
d try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[20:47:53] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 8120 times, 520 (?) - 1 times

[*] ending @ 20:47:53 /2024-05-01/
```

This domain is invulnerable to SQL injection. I tested this manually also here are the results.



| | | | |
|---|---|---|---|
| | | | |
| aeb2a939b63047ee25216d2 | widget.rentalcars.com | ' or 1=1 ;-- | ' or 1=1 ;-- |
| aeb2a939b63047ee25216d2 | GET_BOOKINGS | | widget.rentalcars.com |



' or 1=1 ;--

## Search for Car Hire

Country: Andorra

City: Andorra La Vella

Location: Andorra La Vella (All areas)

☑ Return car to the same location

Pick UpDate: Fri 3 | August '25

Time: 10 | 00

Drop OffDate: Wed 15 | August '25

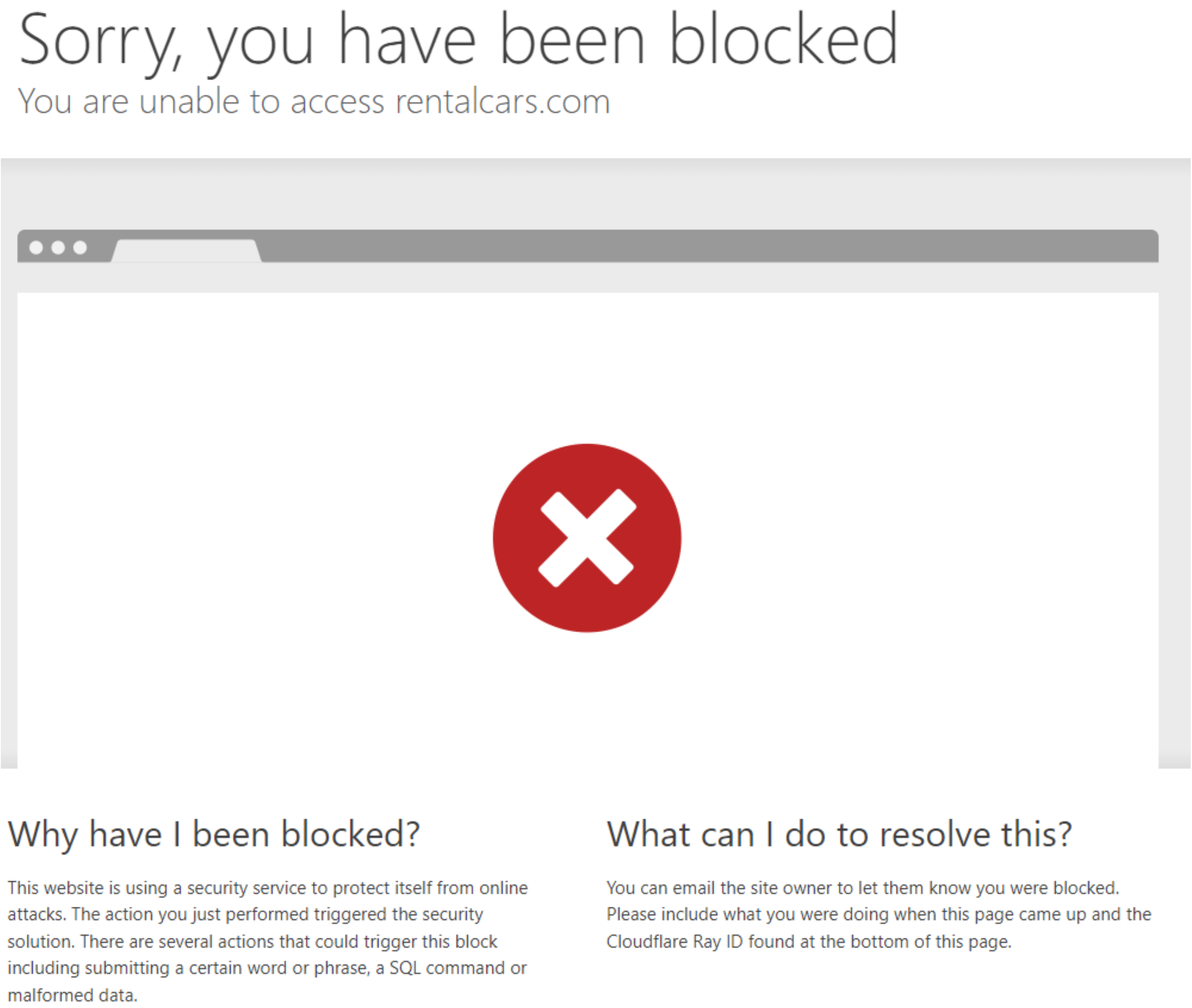
Time: 10 | 00

| | |
|---|---|
| 3 | 5 |
| 2024 | 6 |
| 5 | 2024 |

Driver aged 30 – 65? ☑

| | |
|---|---|
| | true |
| 0 | 20 |

| | |
|---|---|
| ' or 1=1 ;-- | true |



Sorry, you have been blocked

You are unable to access rentalcars.com

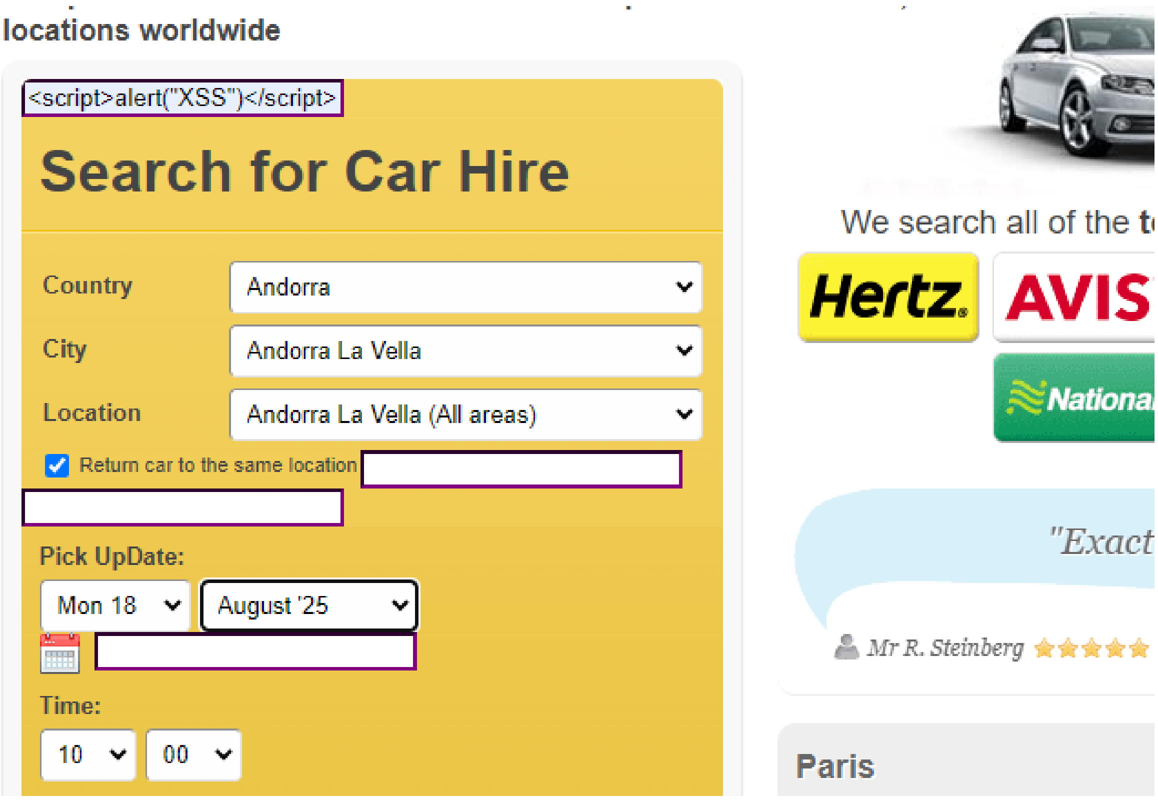
Why have I been blocked?

This website is using a security service to protect itself from online attacks. The action you just performed triggered the security solution. There are several actions that could trigger this block including submitting a certain word or phrase, a SQL command or malformed data.

What can I do to resolve this?

You can email the site owner to let them know you were blocked. Please include what you were doing when this page came up and the Cloudflare Ray ID found at the bottom of this page.

This domain is invulnerable to XSS injection. I test this manually also here are the results.



locations worldwide

<script>alert("XSS")</script>

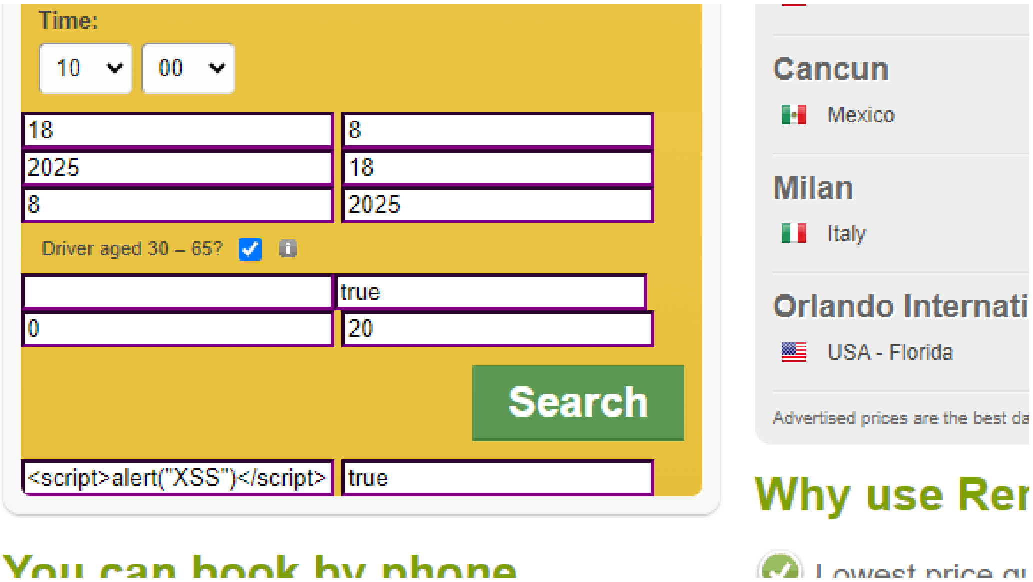
Search for Car Hire

| | |
|---|---|
| Country | Andorra |
| City | Andorra La Vella |
| Location | Andorra La Vella (All areas) |

☑ Return car to the same location

Pick UpDate: Mon 18 August '25

Time: 10 00



Time:

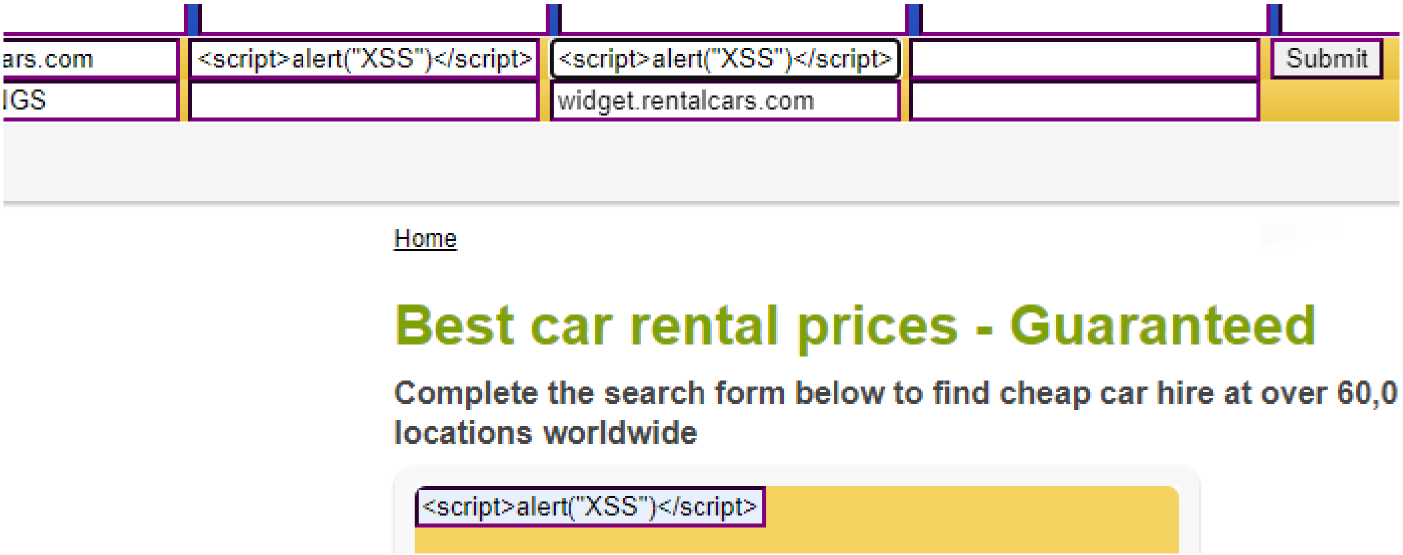
10 00

| | |
|---|---|
| 18 | 8 |
| 2025 | 18 |
| 8 | 2025 |

Driver aged 30 – 65? ☑

| | |
|---|---|
| | true |
| 0 | 20 |

| | |
|---|---|
| <script>alert("XSS")</script> | true |



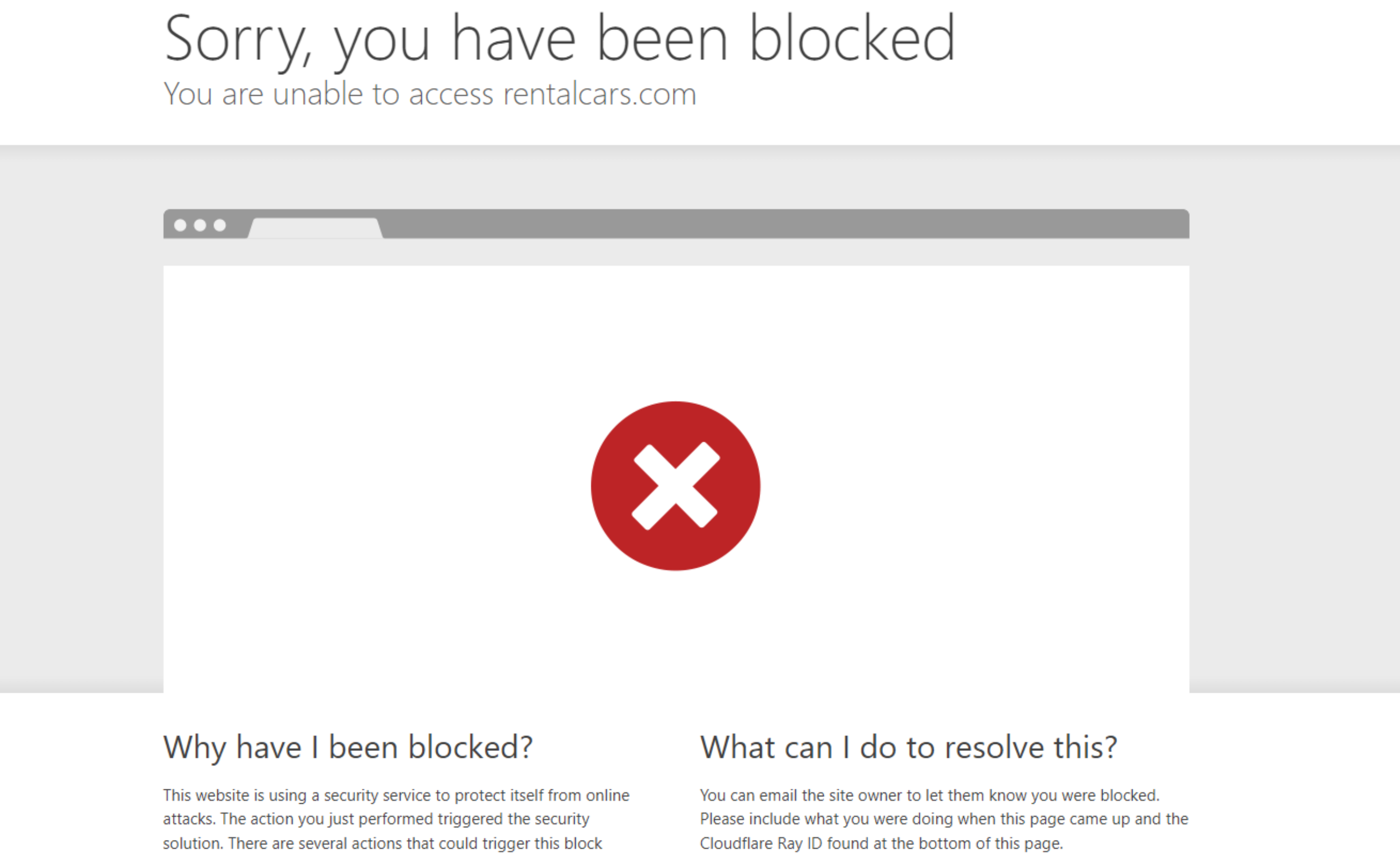
| | | | | |
|---|---|---|---|---|
| ars.com | <script>alert("XSS")</script> | <script>alert("XSS")</script> | | Submit |
| IGS | | widget.rentalcars.com | | |

Best car rental prices - Guaranteed

Complete the search form below to find cheap car hire at over 60,0 locations worldwide

<script>alert("XSS")</script>

I enter basic XSS attack to almost all the hidden fields they are also properly sanitized



# Sorry, you have been blocked

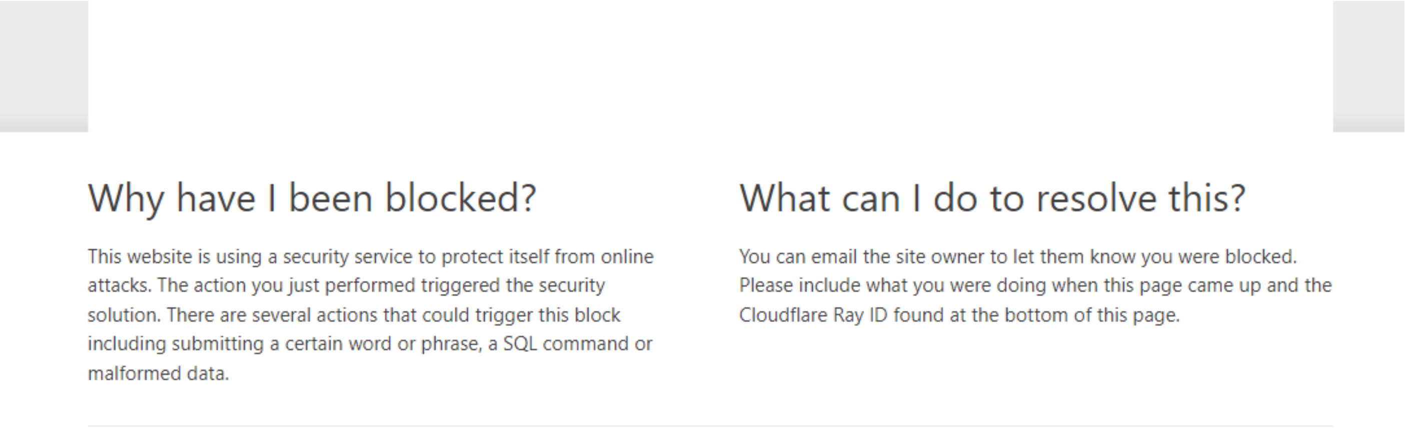
You are unable to access rentalcars.com

## Why have I been blocked?

This website is using a security service to protect itself from online attacks. The action you just performed triggered the security solution. There are several actions that could trigger this block

## What can I do to resolve this?

You can email the site owner to let them know you were blocked. Please include what you were doing when this page came up and the Cloudflare Ray ID found at the bottom of this page.



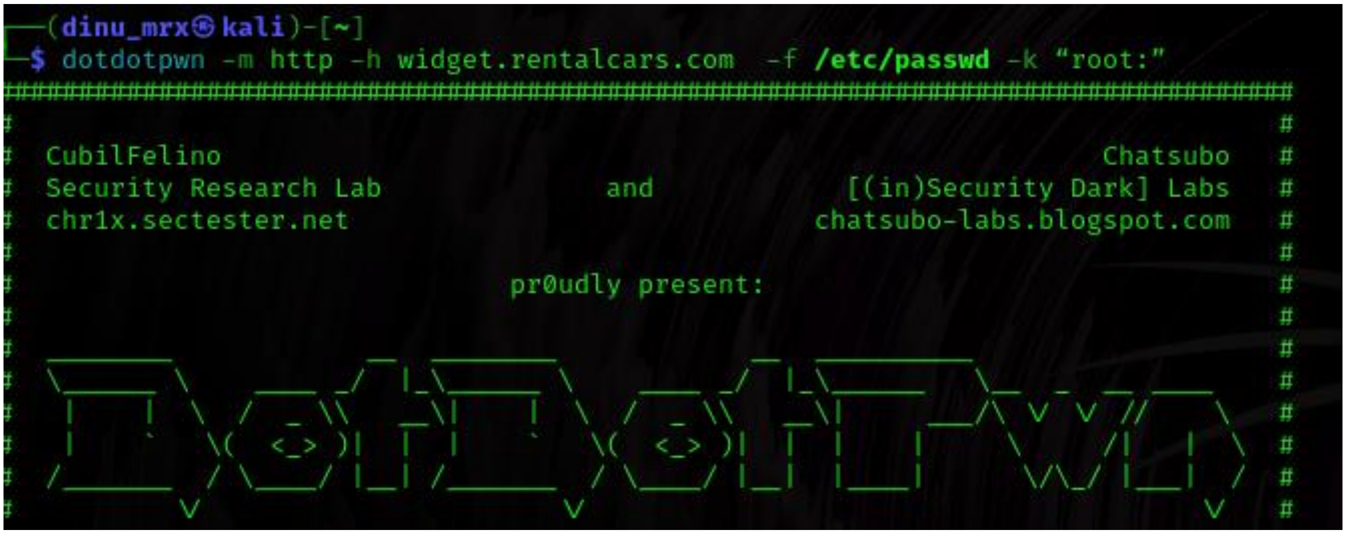
## Why have I been blocked?

This website is using a security service to protect itself from online attacks. The action you just performed triggered the security solution. There are several actions that could trigger this block including submitting a certain word or phrase, a SQL command or malformed data.

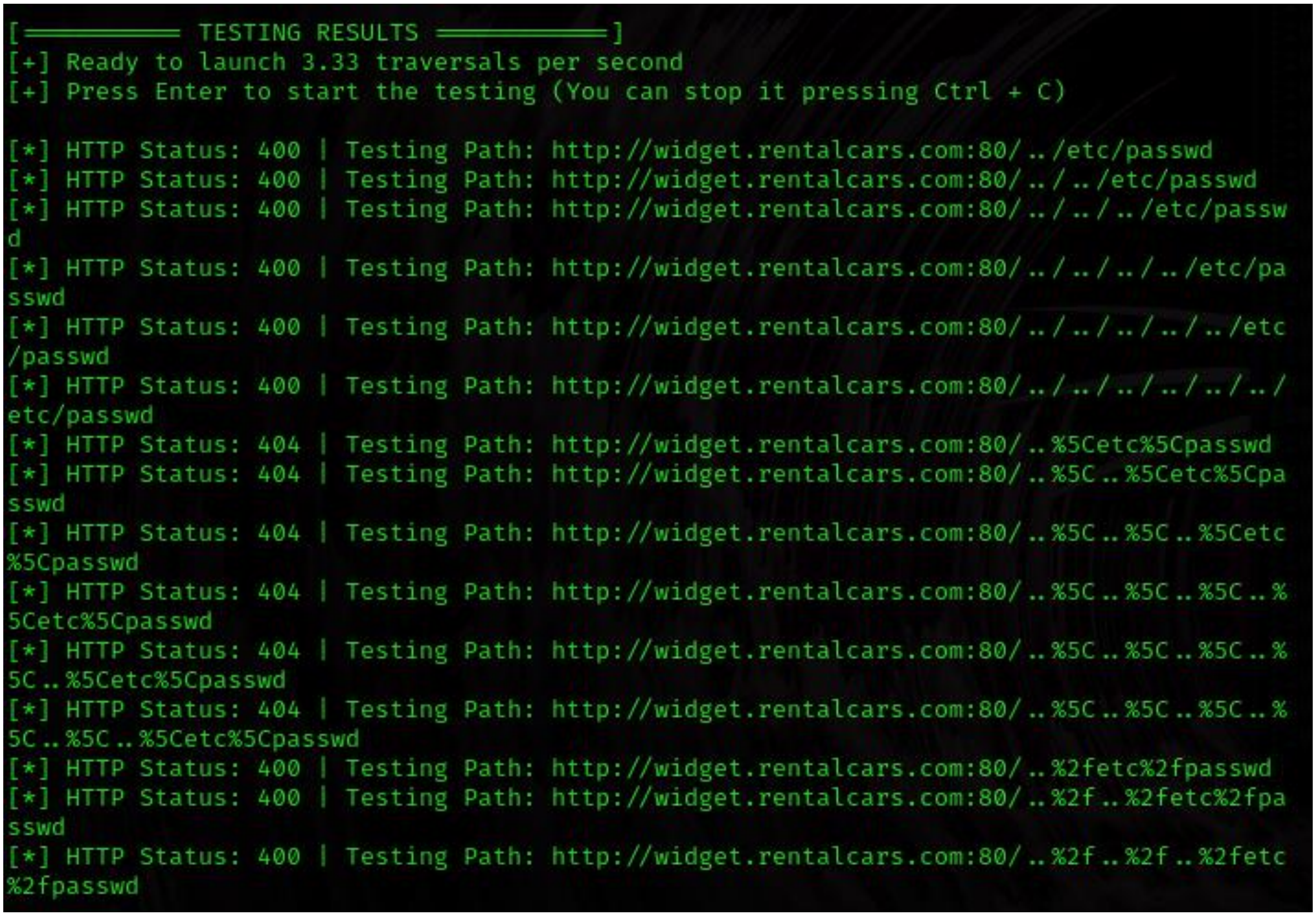
## What can I do to resolve this?

You can email the site owner to let them know you were blocked. Please include what you were doing when this page came up and the Cloudflare Ray ID found at the bottom of this page.

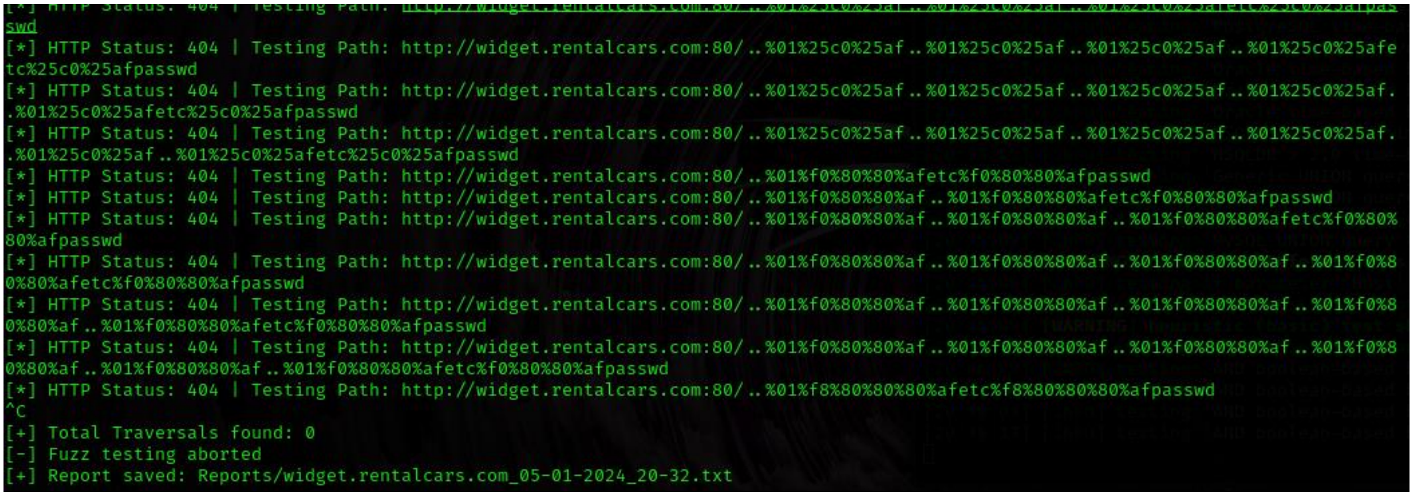
The site is invulnerable to directory traversal.



```
┌──(dinu_mrx㉿kali)-[~]
└─$ dotdotpwn -m http -h widget.rentalcars.com  -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 RESULTS ===========]
[+] Ready to launch 3.33 traversals per second
[+] Press Enter to start the testing (You can stop it pressing Ctrl + C)

[*] HTTP Status: 400 | Testing Path: http://widget.rentalcars.com:80/../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://widget.rentalcars.com:80/../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://widget.rentalcars.com:80/../../../etc/passw
d
[*] HTTP Status: 400 | Testing Path: http://widget.rentalcars.com:80/../../../../etc/pa
sswd
[*] HTTP Status: 400 | Testing Path: http://widget.rentalcars.com:80/../../../../../etc
/passwd
[*] HTTP Status: 400 | Testing Path: http://widget.rentalcars.com:80/../../../../../../
etc/passwd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%5Cetc%5Cpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%5C..%5Cetc%5Cpa
sswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%5C..%5C..%5Cetc
%5Cpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%5C..%5C..%5C..%
5Cetc%5Cpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%5C..%5C..%5C..%
5C..%5Cetc%5Cpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%5C..%5C..%5C..%
5C..%5C..%5Cetc%5Cpasswd
[*] HTTP Status: 400 | Testing Path: http://widget.rentalcars.com:80/..%2fetc%2fpasswd
[*] HTTP Status: 400 | Testing Path: http://widget.rentalcars.com:80/..%2f..%2fetc%2fpa
sswd
[*] HTTP Status: 400 | Testing Path: http://widget.rentalcars.com:80/..%2f..%2f..%2fetc
%2fpasswd
```



```
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%01%25c0%25af..%01%25c0%25af..%01%25c0%25afetc%25c0%25afpas
swd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%01%25c0%25af..%01%25c0%25af..%01%25c0%25af..%01%25c0%25afe
tc%25c0%25afpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%01%25c0%25af..%01%25c0%25af..%01%25c0%25af..%01%25c0%25af.
.%01%25c0%25afetc%25c0%25afpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%01%25c0%25af..%01%25c0%25af..%01%25c0%25af..%01%25c0%25af.
.%01%25c0%25af..%01%25c0%25afetc%25c0%25afpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%01%f0%80%80%afetc%f0%80%80%afpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%01%f0%80%80%af..%01%f0%80%80%afetc%f0%80%80%afpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%01%f0%80%80%af..%01%f0%80%80%af..%01%f0%80%80%afetc%f0%80%
80%afpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%01%f0%80%80%af..%01%f0%80%80%af..%01%f0%80%80%af..%01%f0%8
0%80%afetc%f0%80%80%afpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%01%f0%80%80%af..%01%f0%80%80%af..%01%f0%80%80%af..%01%f0%8
0%80%af..%01%f0%80%80%afetc%f0%80%80%afpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%01%f0%80%80%af..%01%f0%80%80%af..%01%f0%80%80%af..%01%f0%8
0%80%af..%01%f0%80%80%af..%01%f0%80%80%afetc%f0%80%80%afpasswd
[*] HTTP Status: 404 | Testing Path: http://widget.rentalcars.com:80/..%01%f8%80%80%80%afetc%f8%80%80%80%afpasswd
^C
[+] Total Traversals found: 0
[-] Fuzz testing aborted
[+] Report saved: Reports/widget.rentalcars.com_05-01-2024_20-32.txt
```