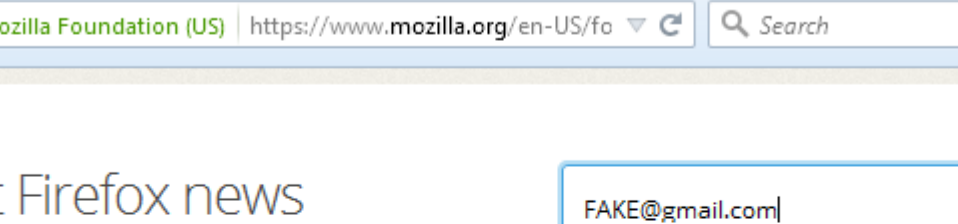


Web Server flood attack and email Flood attack is possible as *CAPTCHA* is not Implemented.

1. Go to <https://www.mozilla.org/en-US/foundation/licensing/website-content/>
2. Just above footer section, go to "Get Firefox news" section.



Get Firefox news

FAKE@gmail.com

India

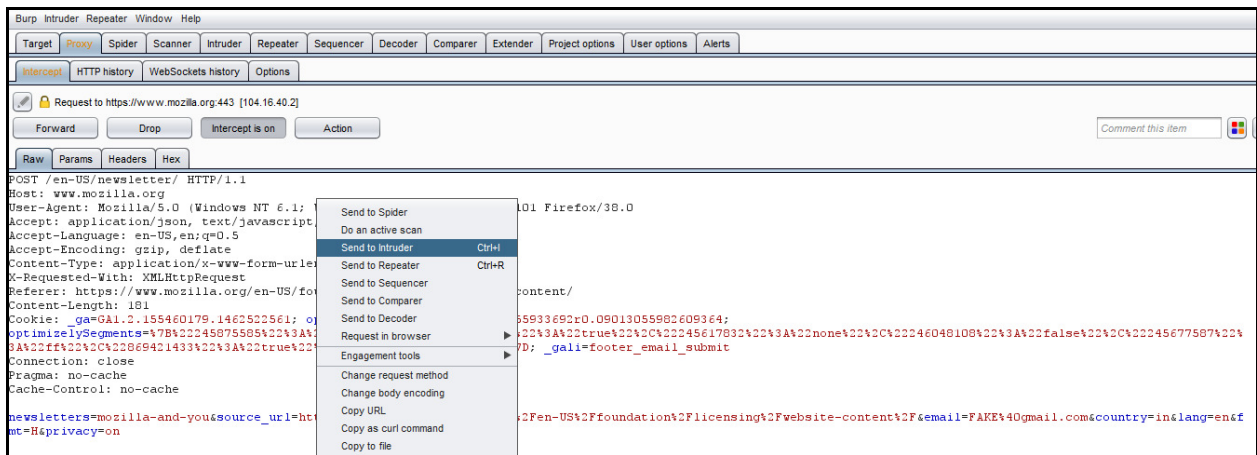
English

☒ HTML

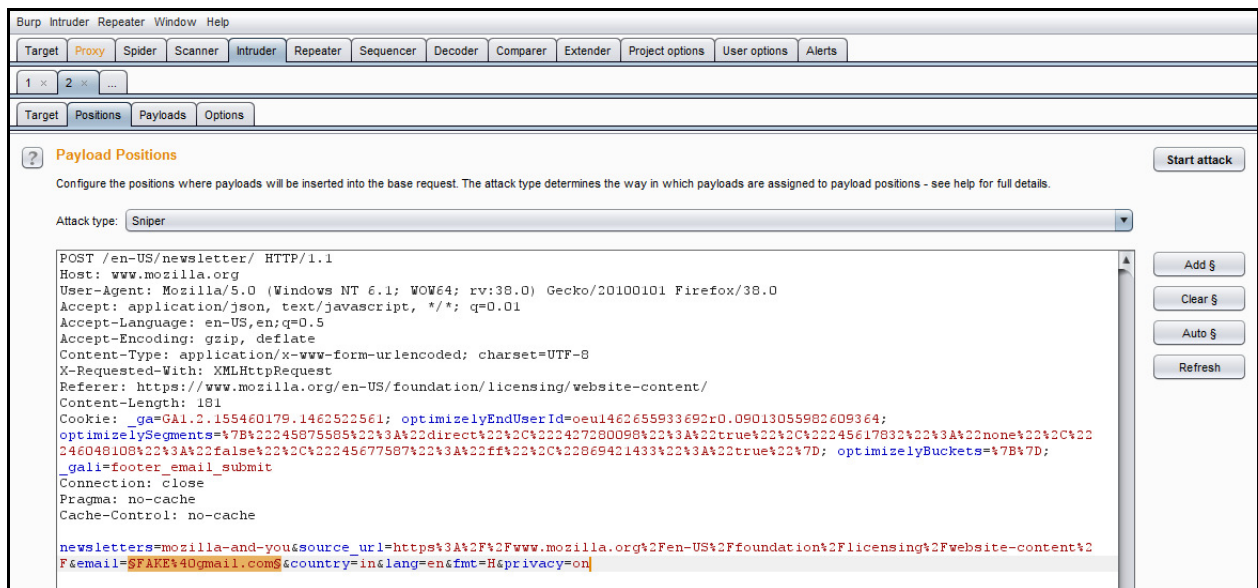
☐ Text

☒ I'm okay with Mozilla handling my info as explained in [this Privacy Notice](#)

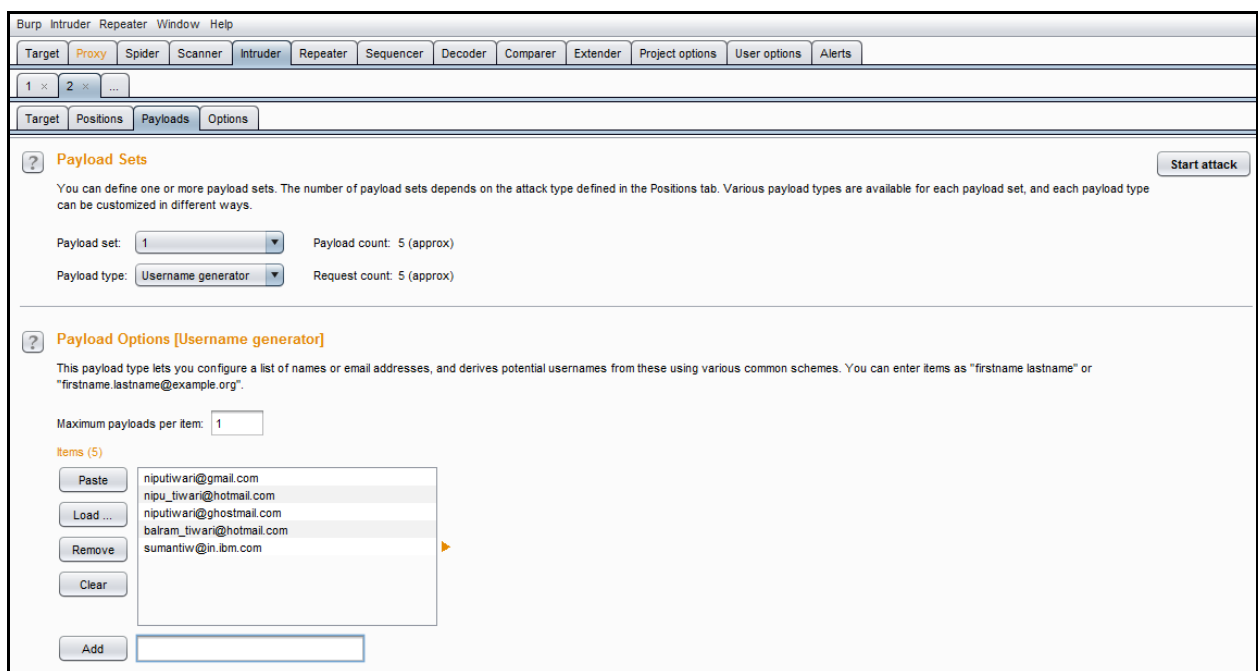
3. Use Proxy editing tool like Burpsuite to intercept the traffic. Enter email ID and click "Sign Up Now" button and intercept the traffic in Burp.
4. Send the request to Intruder.



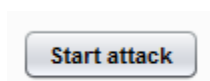
5. In intruder's "Positions" tab select attack type as "**Sniper**" and click "**Clear \$**" and Then click "**ADD \$**" and add entered email ID. Here I have added/entered FAKE@gmail.com



- Go to Intruder's **"Payloads"** tab and select Payload set as "1" and Payload Type as **"Username generator"**. Here, I have used maximum payload per item as 1 and have used only 5 items. **Attack can load a huge list.**



- Click on "Start attack" button.



- Observe that attacker is able to automate the request and may flood the email and web server. My email id was at position 3rd and I too received an email from Mozila.

Intruder attack 1

Attack Save Columns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			370	
1	niputiwari@gmail.com	200			370	
2	niputiwari@hotmail.com	200			370	
3	niputiwari@ghostmail.com	200			370	
4	balramtiwari@hotmail.com	200			370	
5	sumantiw@in.ibm.com	200			370	

RequestResponse

RawParamsHeadersHex

Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://www.mozilla.org/en-US/foundation/licensing/website-content/
Content-Length: 191
Cookie: _ga=GA1.2.155460179.1462522561; optimizelyEndUserId=oeul462655933692r0.09013055982609364;
optimizelySegments=%7B%22245875585%22%3A%22direct%22%2C%222427280098%22%3A%22true%22%2C%22245617832%22%3A%22none%22%2C%22246048108%22%3A%22false%22%2C%22245677587%22%3A%22ff%22%2C%22869421433%22%3A%22true%22%7D; optimizelyBuckets=%7B%7D;
_gali=footer_email_submit
Connection: close
Pragma: no-cache
Cache-Control: no-cache

newsletters=mozilla-and-you&source_url=https%3A%2F%2Fwww.mozilla.org%2Fen-US%2Ffoundation%2Flicensing%2Fwebsite-content%2F
&email=niputiwari@ghostmail%2ecom&country=in&lang=en&fmt=H&privacy=on

Intruder attack 1

Attack Save Columns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

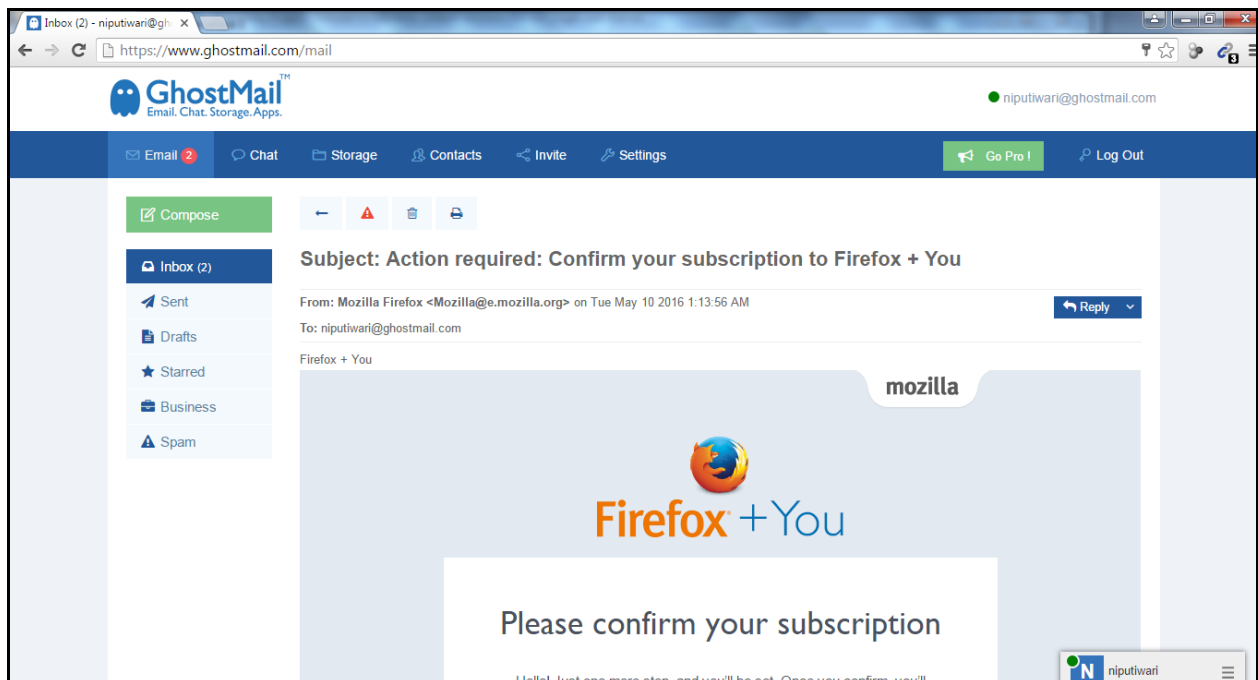
Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	370	
1	niputiwari@gmail.com	200	<input type="checkbox"/>	<input type="checkbox"/>	370	
2	niputiwari@hotmail.com	200	<input type="checkbox"/>	<input type="checkbox"/>	370	
3	niputiwari@ghostmail.com	200	<input type="checkbox"/>	<input type="checkbox"/>	370	
4	balramtiwari@hotmail.com	200	<input type="checkbox"/>	<input type="checkbox"/>	370	
5	sumantiw@in.ibm.com	200	<input type="checkbox"/>	<input type="checkbox"/>	370	

RequestResponse

RawHeadersHex

HTTP/1.1 200 OK
Date: Mon, 09 May 2016 19:43:24 GMT
Content-Type: application/json
Content-Length: 17
Connection: close
Vary: Accept-Encoding
X-Backend-Server: 6fcd4ab62063.bedrock-prod.eu-west.moz.works
X-Clacks-Overhead: GNU Terry Pratchett
X-Frame-Options: DENY
X-Robots-Tag: noodp
Server: cloudflare-nginx
CF-RAY: 2a07a3df86742da9-BOM

{"success": true}



Impact/Threat:

1. Reputation:

Let's take a scenario in which attacker is sending/automating 50,000+ emails per hour. Recipients may mark these email from Mozilla as SPAM. Now, based on user's responses, even genuine email will go into spam folder. Based on user responses, Yahoo, gmail, outlook etc will start treating email from Mozilla as a SPAM.

2. Web and email server Flood as CAPTCHA is not used

Thank You