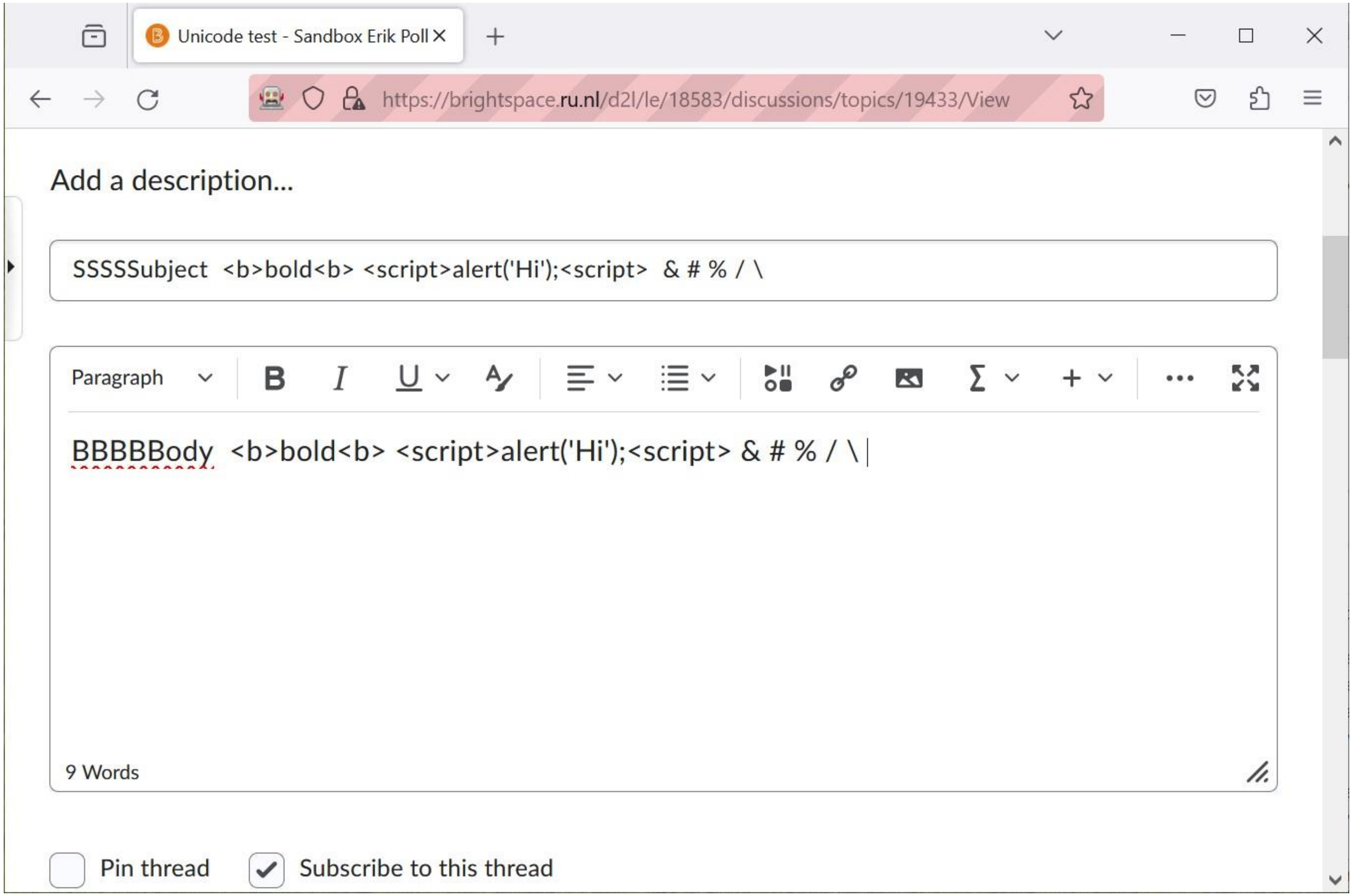
Web Security

Güneş Acar & Erik Poll

Digital Security group
Radboud University Nijmegen

Post with special characters & keyword in subject & body


Unicode test - Sandbox Erik Poll
https://brightspace.ru.nl/d2l/le/18583/discussions/topics/19433/View
Paragraph
B
I
U

Add a description...

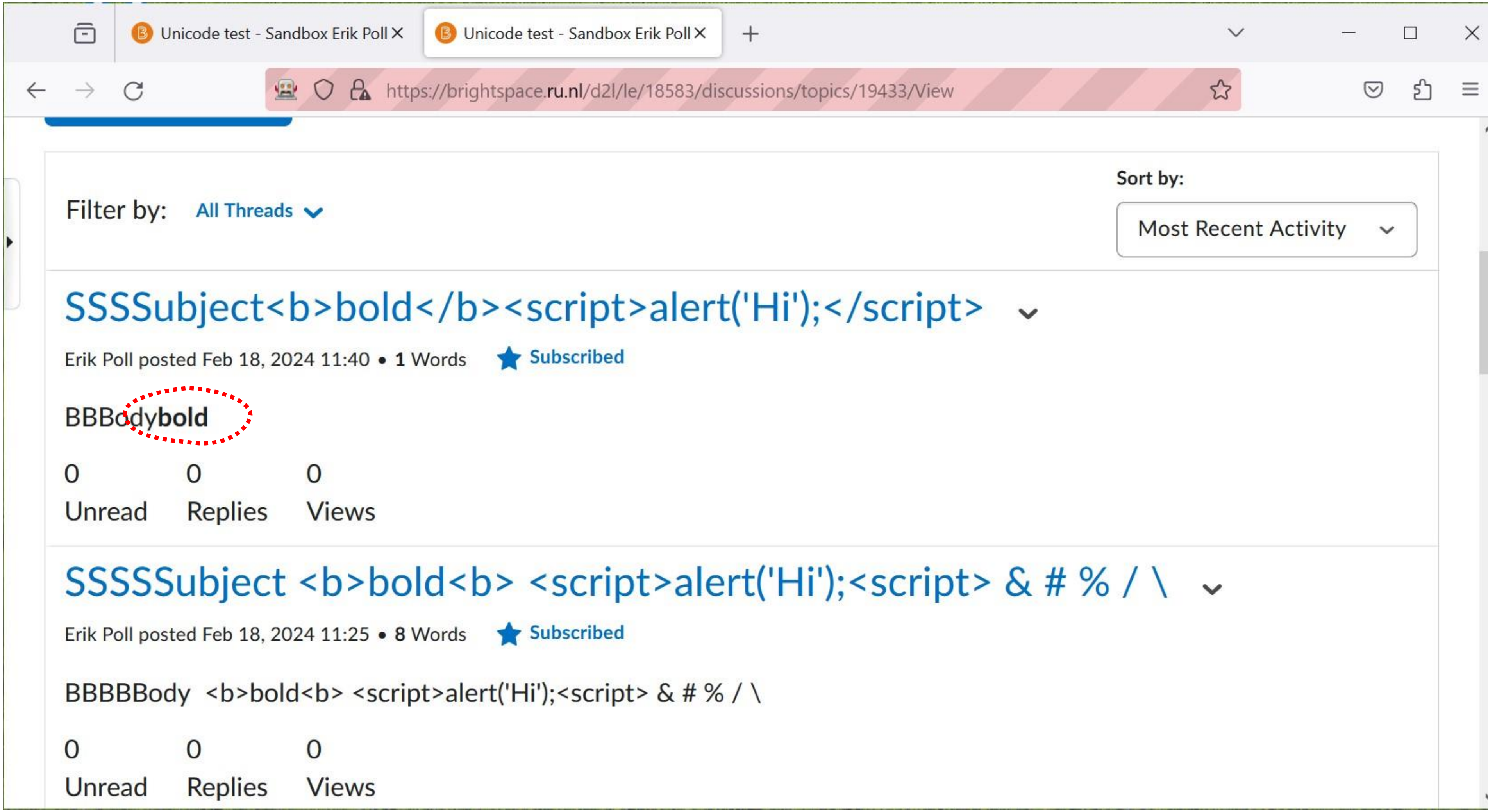
SSSSSubject <b>bold<b> <script>alert('Hi');<script> & # % / \

BBBBBody <b>bold<b> <script>alert('Hi');<script> & # % / \

9 Words

□ Pin thread ☑ Subscribe to this thread

Result


Unicode test - Sandbox Erik Poll
Unicode test - Sandbox Erik Poll
https://brightspace.ru.nl/d2l/le/18583/discussions/topics/19433/View

Filter by: All Threads

Sort by: Most Recent Activity

SSSubject<b>bold</b><script>alert('Hi');</script>

Erik Poll posted Feb 18, 2024 11:40 • **1** Words ★ Subscribed

BBBody**bold**

0 Unread 0 Replies 0 Views

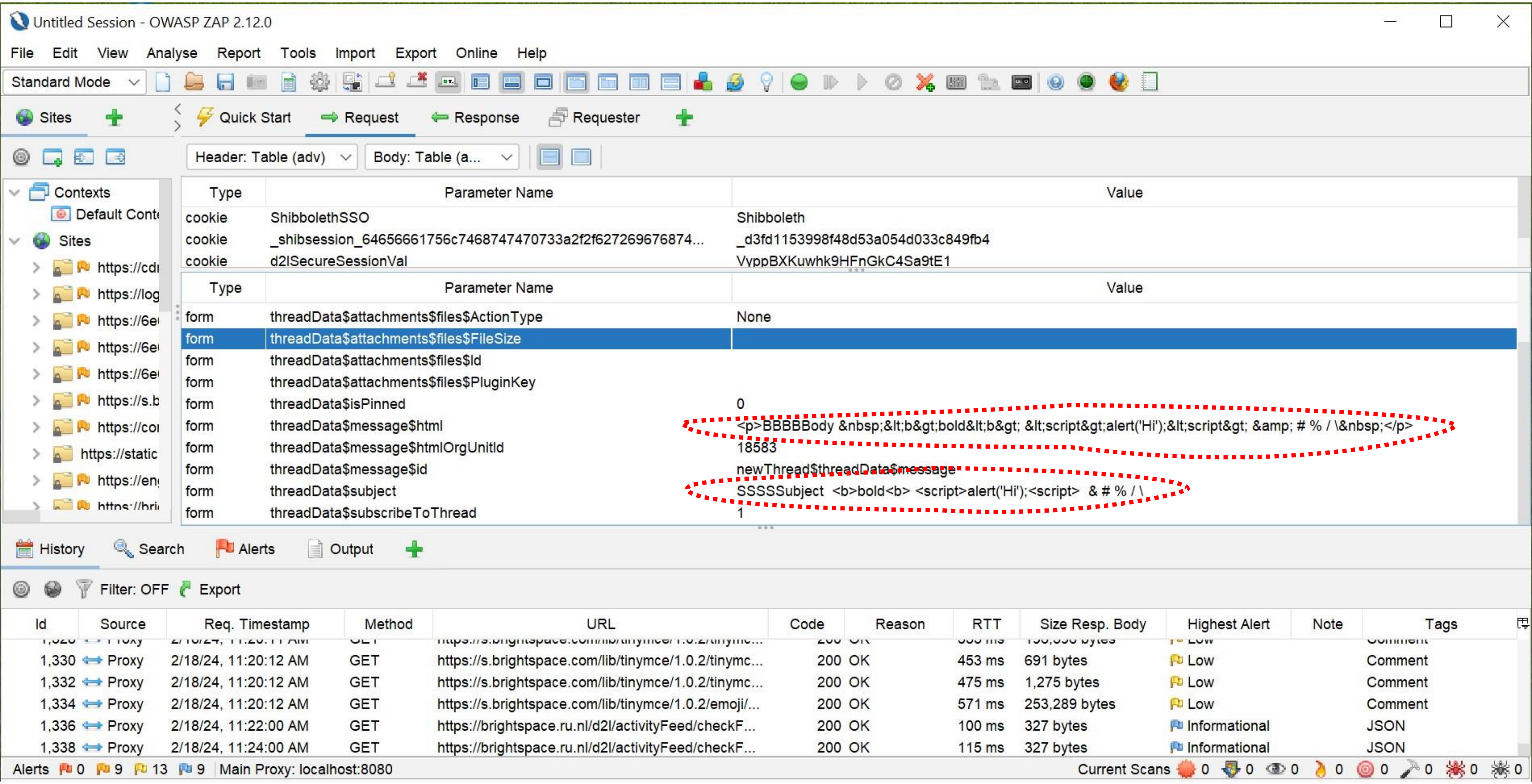
SSSSubject <b>bold<b> <script>alert('Hi');<script> & # % / \

Erik Poll posted Feb 18, 2024 11:25 • **8** Words ★ Subscribed

BBBBBody <b>bold<b> <script>alert('Hi');<script> & # % / \

0 Unread 0 Replies 0 Views

Resulting HTTP request in ZAP



Type	Parameter Name	Value
cookie	ShibbolethSSO	Shibboleth
cookie	_shibsession_64656661756c7468747470733a2f2f627269676874...	_d3fd1153998f48d53a054d033c849fb4
cookie	d2lSecureSessionVal	VyppBXKuwhk9HFnGkC4Sa9tE1

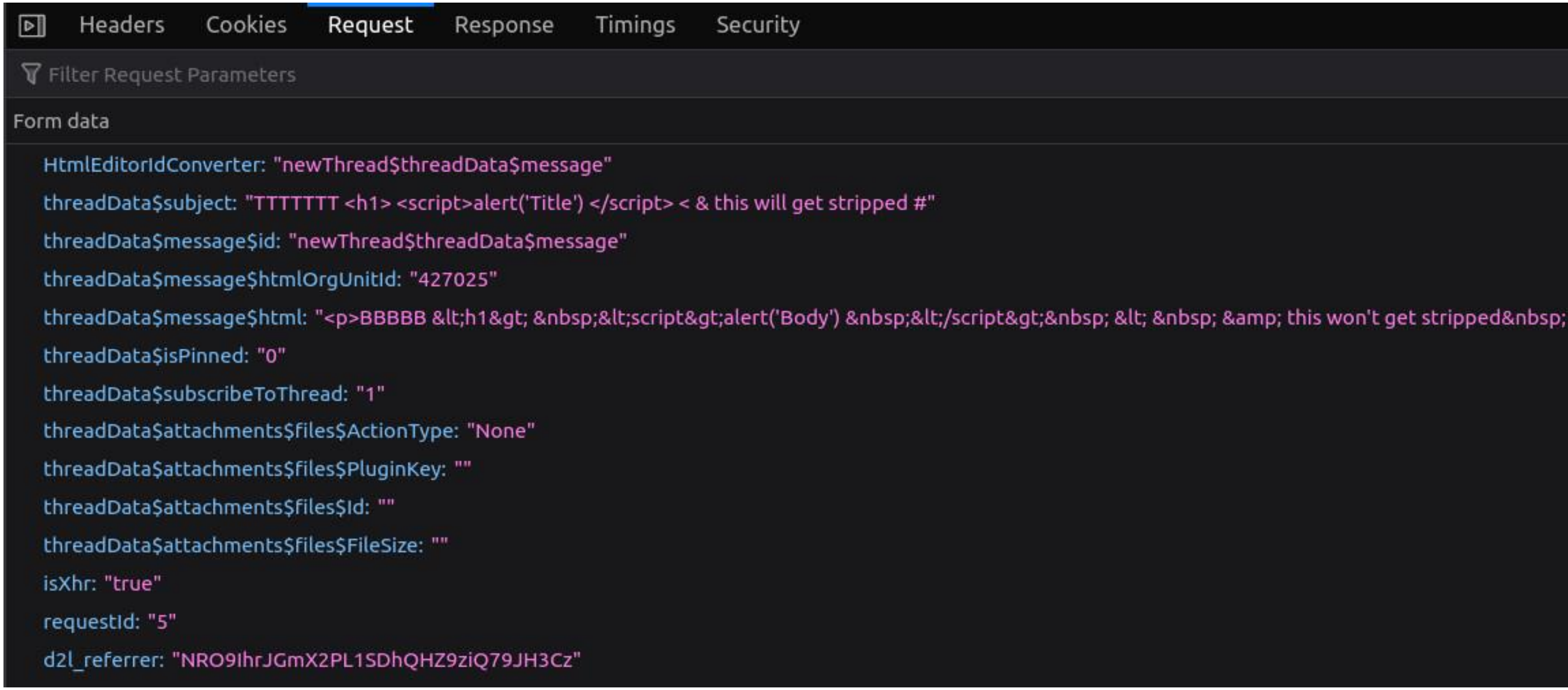
Type	Parameter Name	Value
form	threadData$attachments$files$ActionType	None
form	threadData$attachments$files$FileSize	
form	threadData$attachments$files$Id	
form	threadData$attachments$files$PluginKey	
form	threadData$isPinned	0
form	threadData$message$html	<p>BBBBBody &lt;b&gt;bold&lt;b&gt; &lt;script&gt;alert('Hi');&lt;script&gt; &amp; # % / \&nbsp;</p>
form	threadData$message$htmlOrgUnitId	18583
form	threadData$message$id	newThread$threadData$message
form	threadData$subject	SSSSSubject <b>bold<b> <script>alert('Hi');<script> & # % / \
form	threadData$subscribeToThread	1

Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1,330	⟷ Proxy	2/18/24, 11:20:12 AM	GET	https://s.brightspace.com/lib/tinymce/1.0.2/tinymc...	200	OK	453 ms	691 bytes	Low		Comment
1,332	⟷ Proxy	2/18/24, 11:20:12 AM	GET	https://s.brightspace.com/lib/tinymce/1.0.2/tinymc...	200	OK	475 ms	1,275 bytes	Low		Comment
1,334	⟷ Proxy	2/18/24, 11:20:12 AM	GET	https://s.brightspace.com/lib/tinymce/1.0.2/emoji/...	200	OK	571 ms	253,289 bytes	Low		Comment
1,336	⟷ Proxy	2/18/24, 11:22:00 AM	GET	https://brightspace.ru.nl/d2l/activityFeed/checkF...	200	OK	100 ms	327 bytes	Informational		JSON
1,338	⟷ Proxy	2/18/24, 11:24:00 AM	GET	https://brightspace.ru.nl/d2l/activityFeed/checkF...	200	OK	115 ms	327 bytes	Informational		JSON

Alerts 0 9 13 9 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

Resulting HTTP request in Firefox

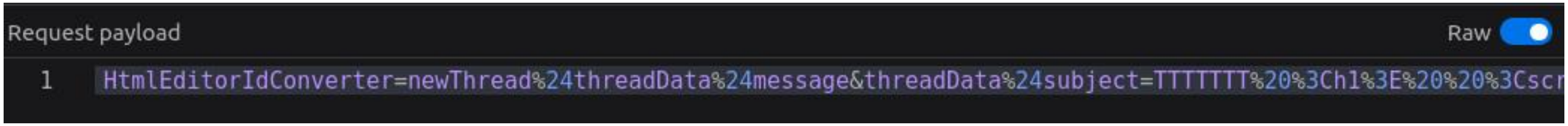
You can look at HTTP request nicely formatted



Form data

```
HtmlEditorIdConverter: "newThread$threadData$message"
threadData$subject: "TTTTTTT <h1> <script>alert('Title') </script> < & this will get stripped #"
threadData$message$id: "newThread$threadData$message"
threadData$message$htmlOrgUnitId: "427025"
threadData$message$html: "<p>BBBBB &lt;h1&gt; &nbsp;&lt;script&gt;alert('Body') &nbsp;&lt;/script&gt;&nbsp; &lt; &nbsp; &amp; this won't get stripped&nbsp;
threadData$isPinned: "0"
threadData$subscribeToThread: "1"
threadData$attachments$files$ActionType: "None"
threadData$attachments$files$PluginKey: ""
threadData$attachments$files$Id: ""
threadData$attachments$files$FileSize: ""
isXhr: "true"
requestId: "5"
d2l_referrer: "NRO9lhrJGmX2PL1SDhQHZ9ziQ79JH3Cz"
```

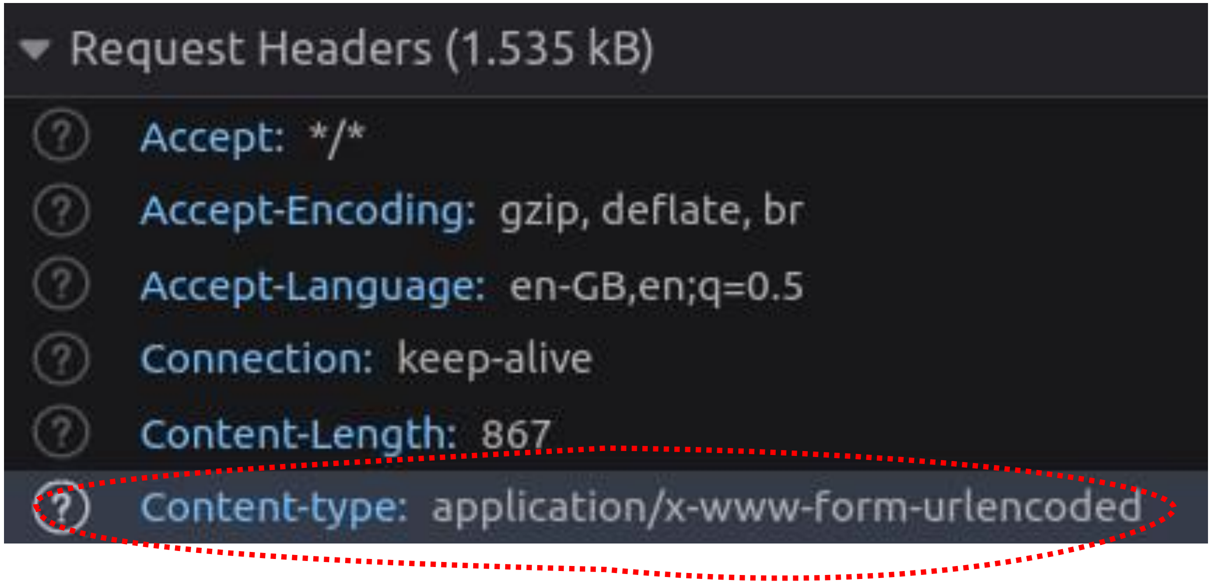
or at the raw request



Request payload

```
HtmlEditorIdConverter=newThread%24threadData%24message&threadData%24subject=TTTTTTT%20%3Ch1%3E%20%20%3Cscr
```

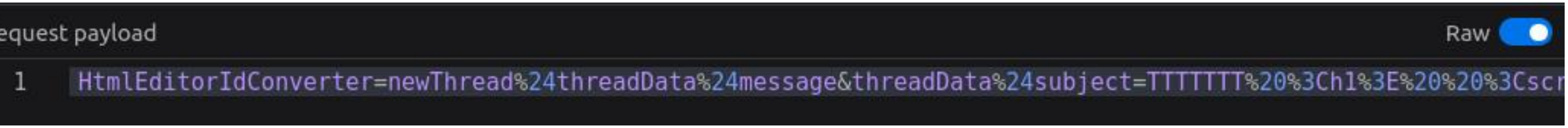
Headers in resulting HTTP request



```
Request Headers (1.535 kB)
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en;q=0.5
Connection: keep-alive
Content-Length: 867
Content-type: application/x-www-form-urlencoded
```

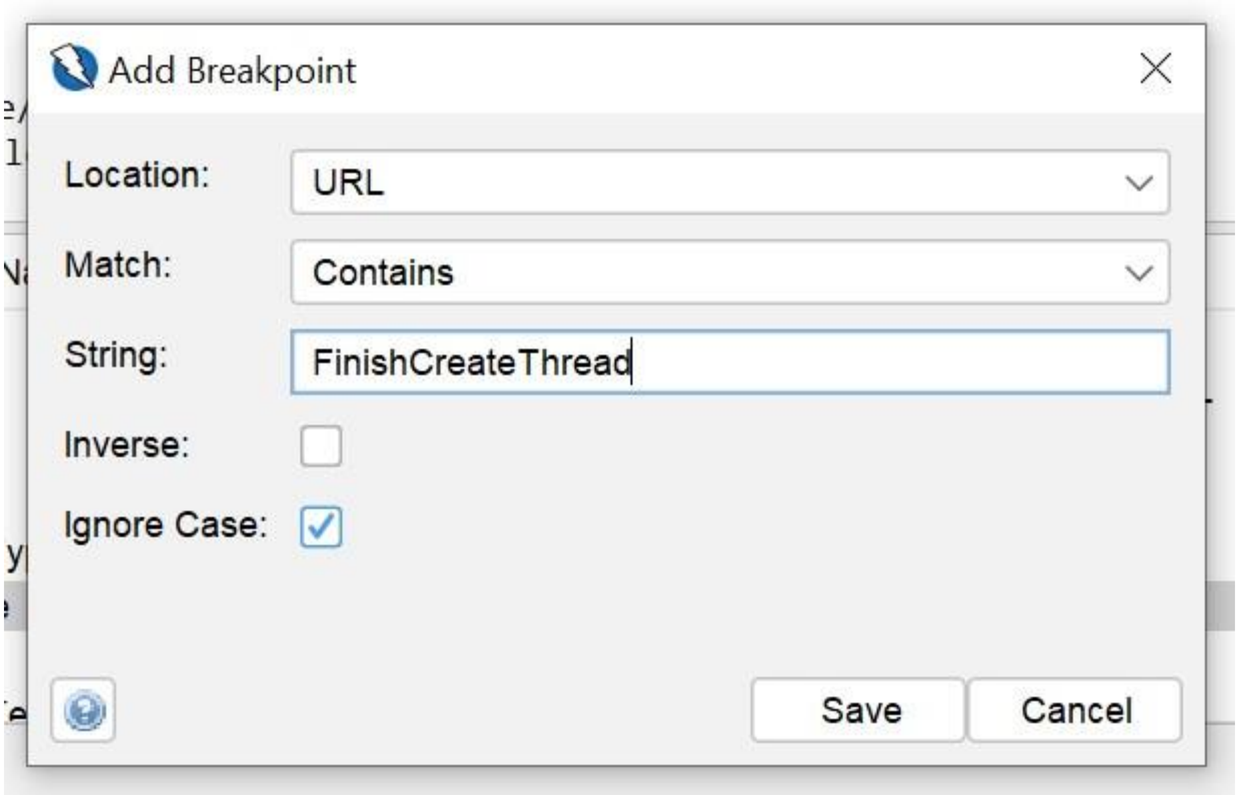
So content is URL encoded

Resulting HTTP request in Firefox – Raw



```
HtmlEditorIdConverter=newThread%24threadData%24message&threadData%24subject=TTTTTTT%20%3Ch1%3E%20%20%3Cscr
```

Setting breakpoint



Location: URL

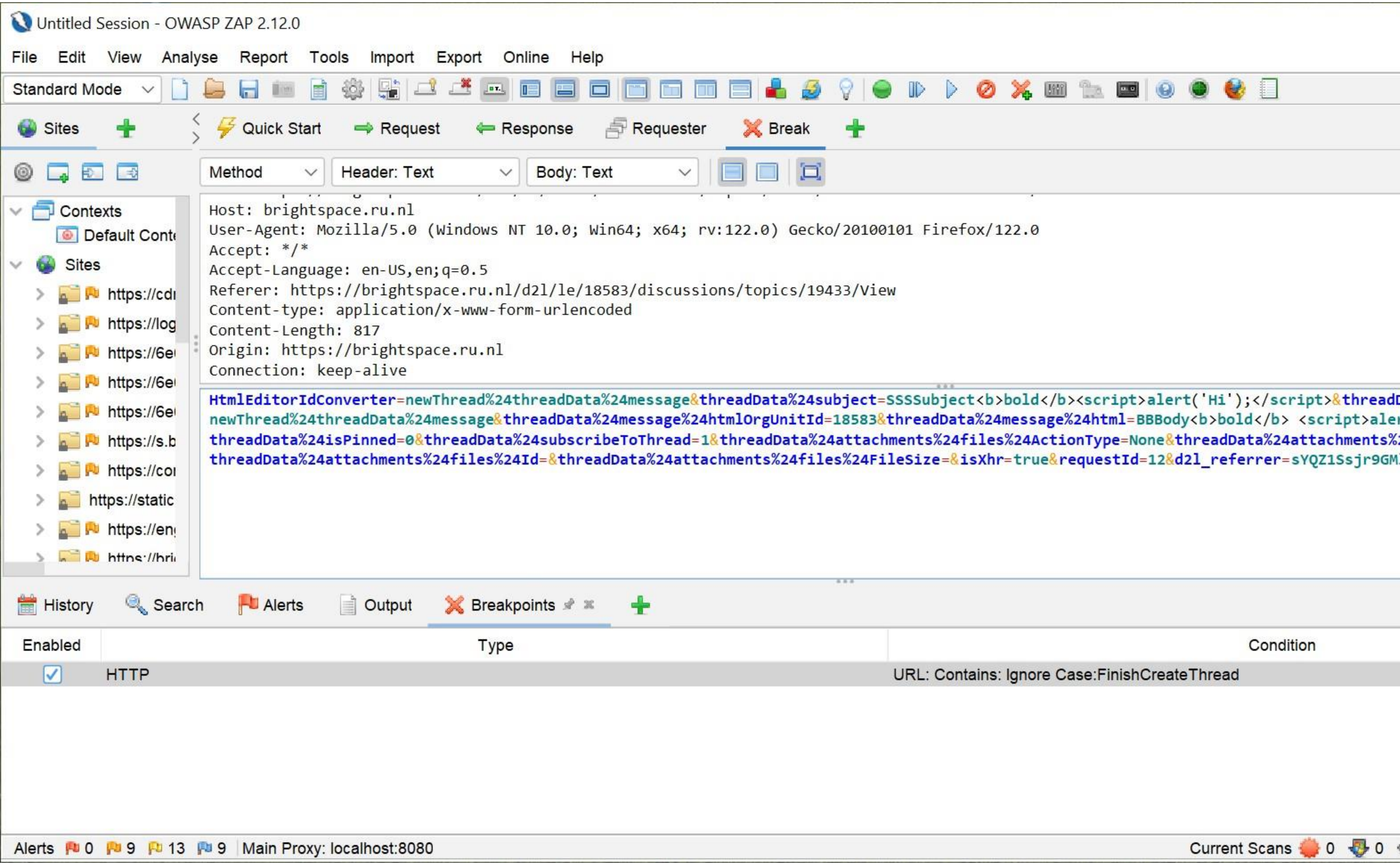
Match: Contains

String: FinishCreateThread

Inverse: □

Ignore Case: ☑

Intercepting at breakpoint to edit



```
Host: brightspace.ru.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: https://brightspace.ru.nl/d2l/le/18583/discussions/topics/19433/View
Content-type: application/x-www-form-urlencoded
Content-Length: 817
Origin: https://brightspace.ru.nl
Connection: keep-alive
```

```
HtmlEditorIdConverter=newThread%24threadData%24message&threadData%24subject=SSSSubject<b>bold</b><script>alert('Hi');</script>&threadD
newThread%24threadData%24message&threadData%24message%24htmlOrgUnitId=18583&threadData%24message%24html=BBBody<b>bold</b> <script>aler
threadData%24isPinned=0&threadData%24subscribeToThread=1&threadData%24attachments%24files%24ActionType=None&threadData%24attachments%
threadData%24attachments%24files%24Id=&threadData%24attachments%24files%24FileSize=&isXhr=true&requestId=12&d2l_referrer=sYQZ1Ssjr9GM
```

Enabled	Type	Condition
☑	HTTP	URL: Contains: Ignore Case:FinishCreateThread