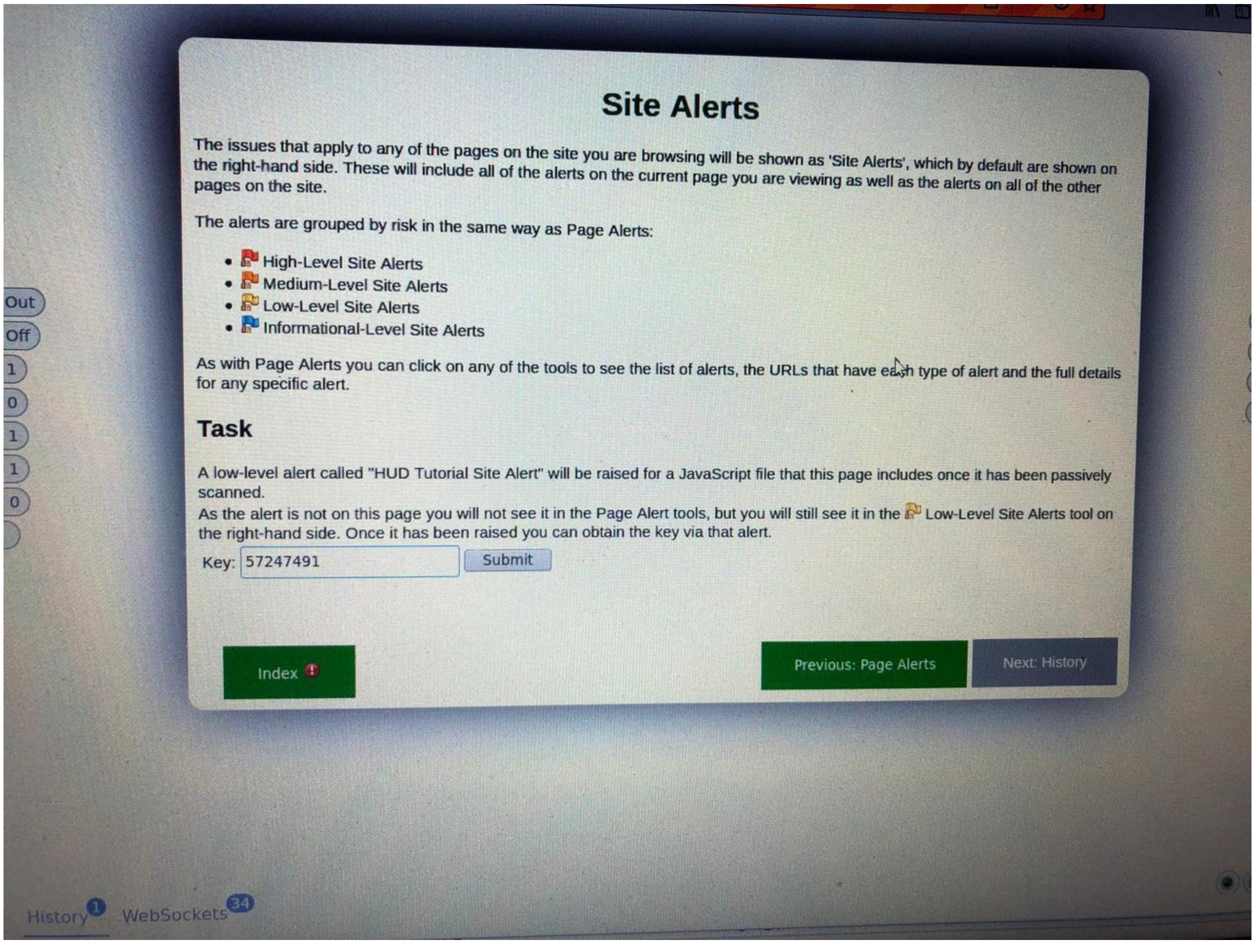
2.3 OWASP ZAP tutorial



Site Alerts

The issues that apply to any of the pages on the site you are browsing will be shown as 'Site Alerts', which by default are shown on the right-hand side. These will include all of the alerts on the current page you are viewing as well as the alerts on all of the other pages on the site.

The alerts are grouped by risk in the same way as Page Alerts:

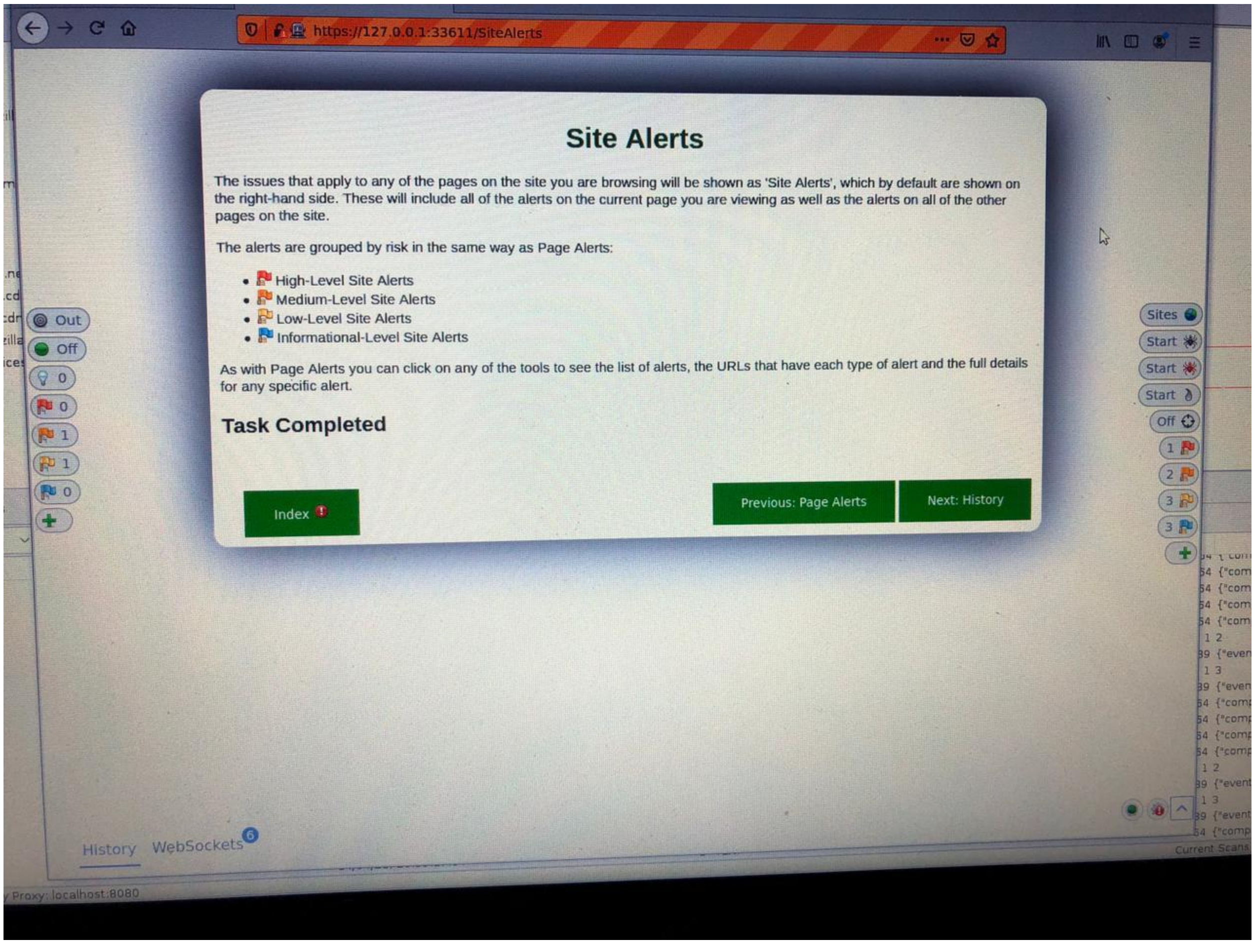
- ⚑ High-Level Site Alerts
- ⚑ Medium-Level Site Alerts
- ⚑ Low-Level Site Alerts
- ⚑ Informational-Level Site Alerts

As with Page Alerts you can click on any of the tools to see the list of alerts, the URLs that have each type of alert and the full details for any specific alert.

Task

A low-level alert called "HUD Tutorial Site Alert" will be raised for a JavaScript file that this page includes once it has been passively scanned.
As the alert is not on this page you will not see it in the Page Alert tools, but you will still see it in the ⚑ Low-Level Site Alerts tool on the right-hand side. Once it has been raised you can obtain the key via that alert.

Key: 57247491



Site Alerts

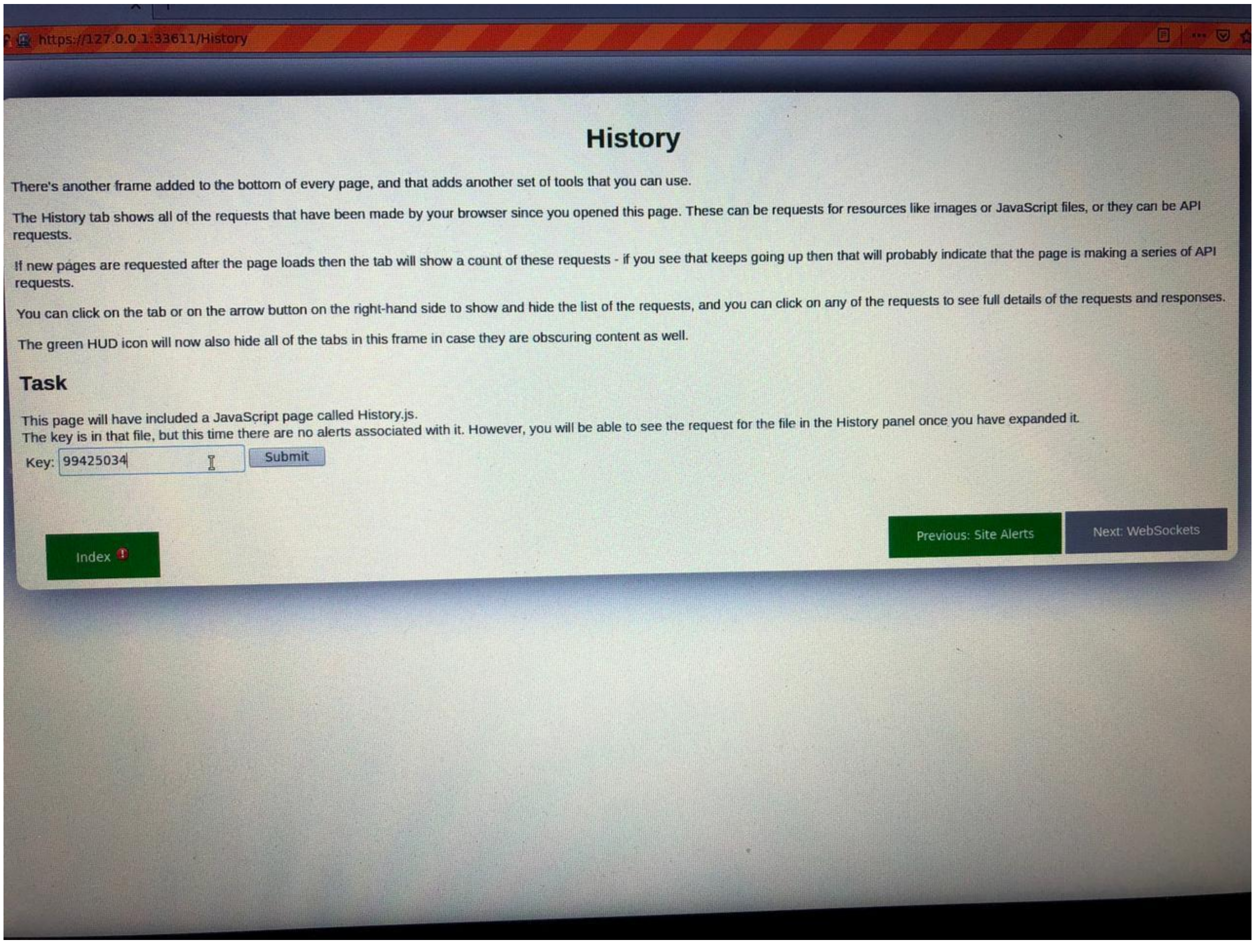
The issues that apply to any of the pages on the site you are browsing will be shown as 'Site Alerts', which by default are shown on the right-hand side. These will include all of the alerts on the current page you are viewing as well as the alerts on all of the other pages on the site.

The alerts are grouped by risk in the same way as Page Alerts:

- High-Level Site Alerts
- Medium-Level Site Alerts
- Low-Level Site Alerts
- Informational-Level Site Alerts

As with Page Alerts you can click on any of the tools to see the list of alerts, the URLs that have each type of alert and the full details for any specific alert.

Task Completed



History

There's another frame added to the bottom of every page, and that adds another set of tools that you can use.

The History tab shows all of the requests that have been made by your browser since you opened this page. These can be requests for resources like images or JavaScript files, or they can be API requests.

If new pages are requested after the page loads then the tab will show a count of these requests - if you see that keeps going up then that will probably indicate that the page is making a series of API requests.

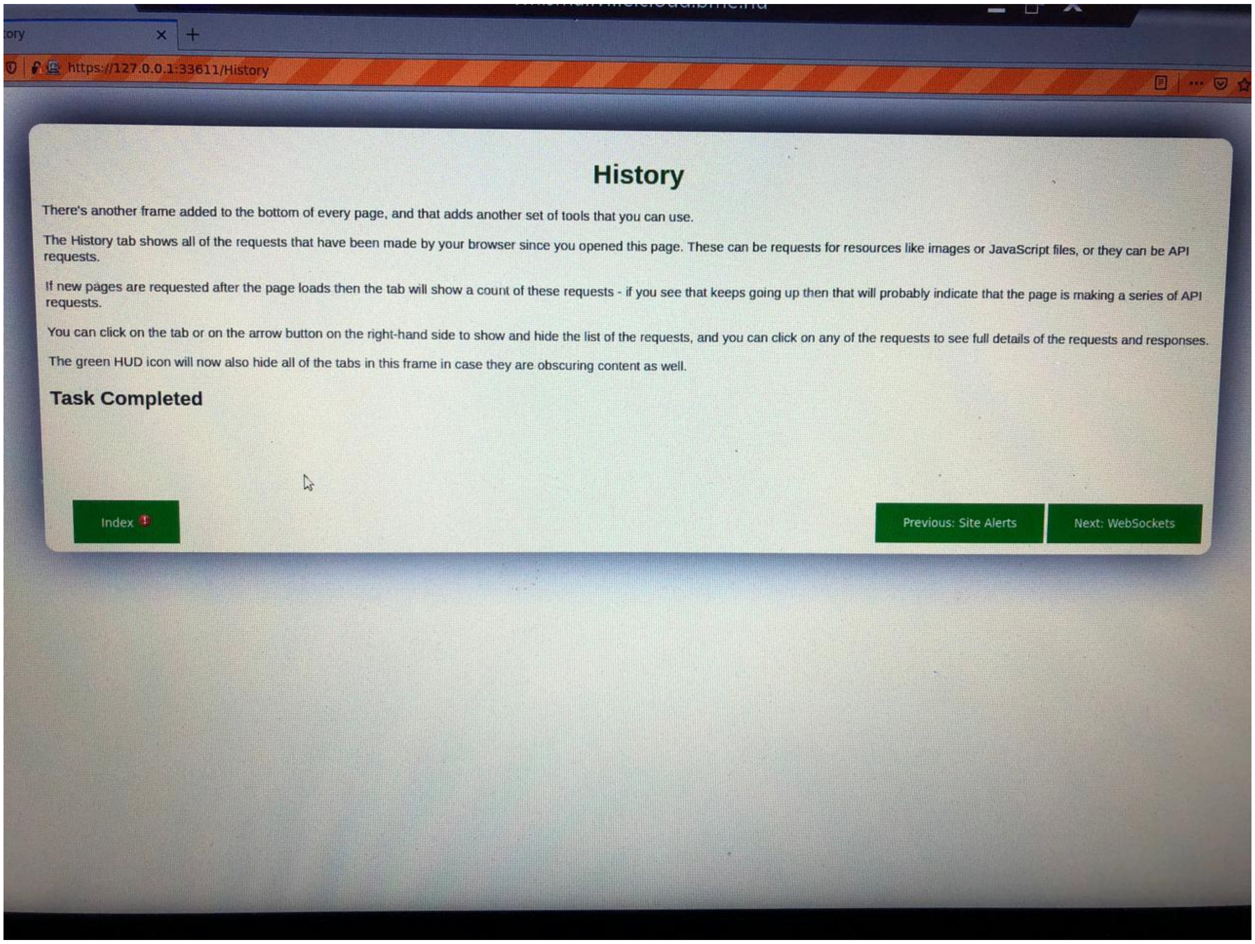
You can click on the tab or on the arrow button on the right-hand side to show and hide the list of the requests, and you can click on any of the requests to see full details of the requests and responses.

The green HUD icon will now also hide all of the tabs in this frame in case they are obscuring content as well.

Task

This page will have included a JavaScript page called History.js.
The key is in that file, but this time there are no alerts associated with it. However, you will be able to see the request for the file in the History panel once you have expanded it.

Key: 99425034



History

There's another frame added to the bottom of every page, and that adds another set of tools that you can use.

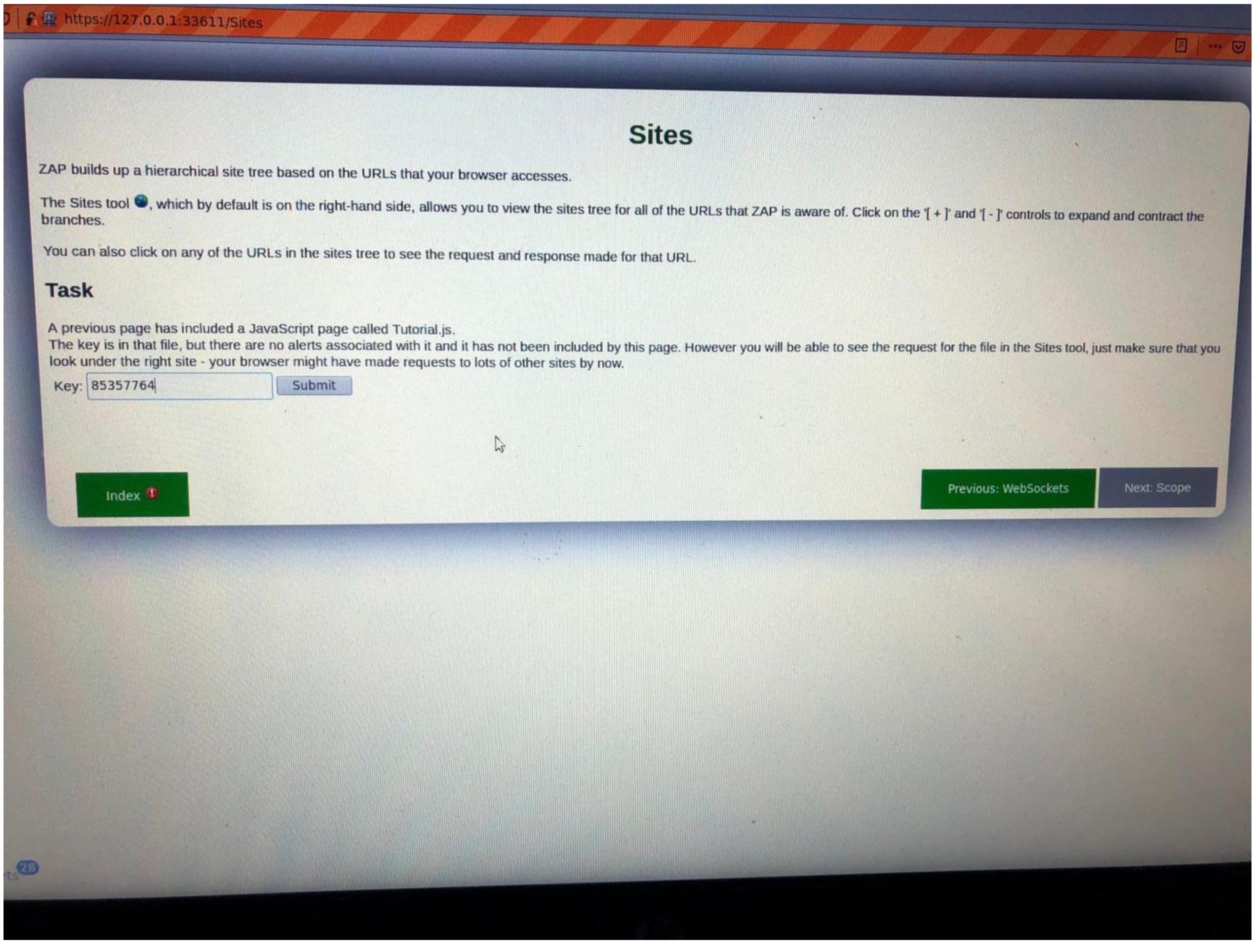
The History tab shows all of the requests that have been made by your browser since you opened this page. These can be requests for resources like images or JavaScript files, or they can be API requests.

If new pages are requested after the page loads then the tab will show a count of these requests - if you see that keeps going up then that will probably indicate that the page is making a series of API requests.

You can click on the tab or on the arrow button on the right-hand side to show and hide the list of the requests, and you can click on any of the requests to see full details of the requests and responses.

The green HUD icon will now also hide all of the tabs in this frame in case they are obscuring content as well.

Task Completed



Sites

ZAP builds up a hierarchical site tree based on the URLs that your browser accesses.

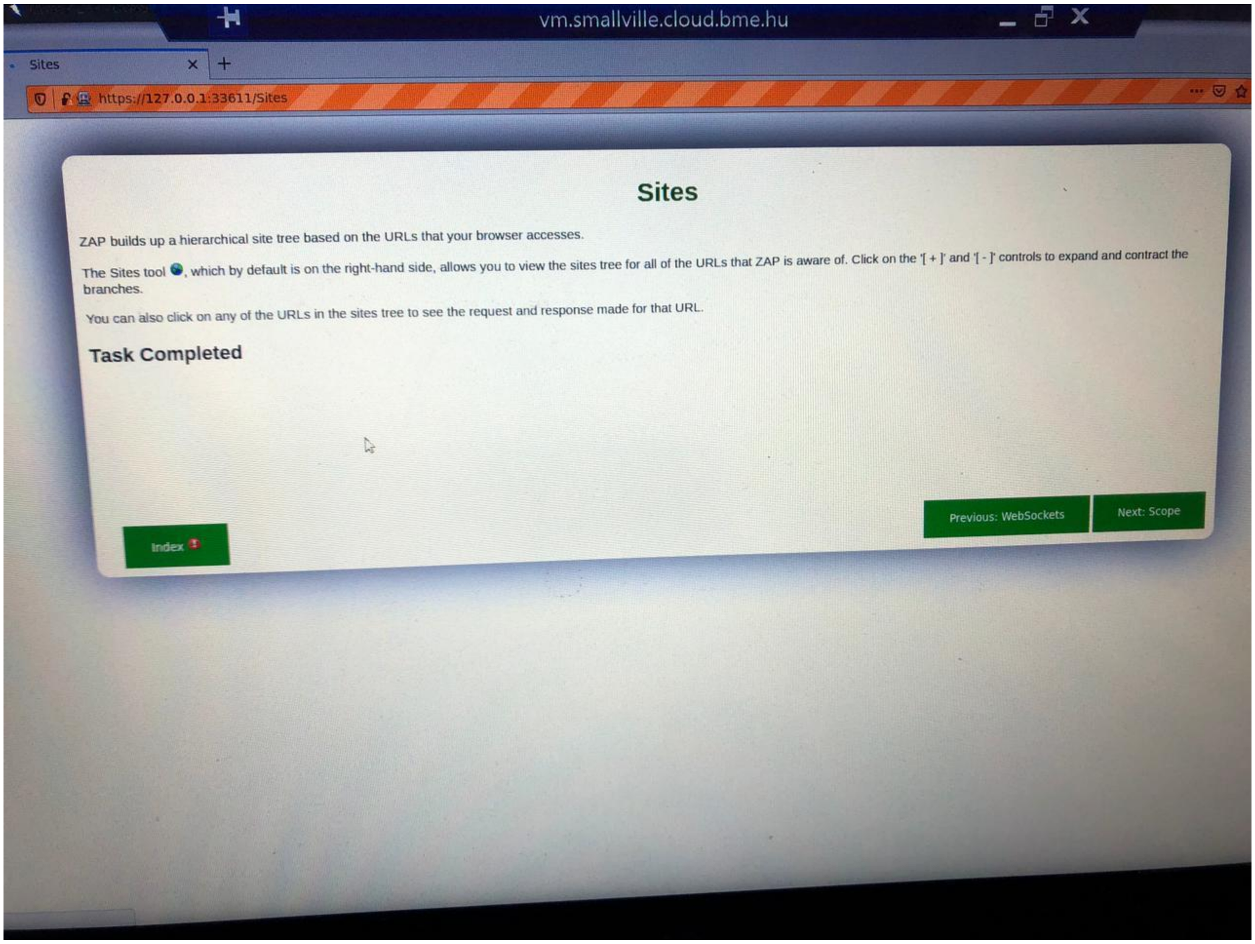
The Sites tool 🌍, which by default is on the right-hand side, allows you to view the sites tree for all of the URLs that ZAP is aware of. Click on the '[+]' and '[-]' controls to expand and contract the branches.

You can also click on any of the URLs in the sites tree to see the request and response made for that URL.

Task

A previous page has included a JavaScript page called Tutorial.js.
The key is in that file, but there are no alerts associated with it and it has not been included by this page. However you will be able to see the request for the file in the Sites tool, just make sure that you look under the right site - your browser might have made requests to lots of other sites by now.

Key: 85357764



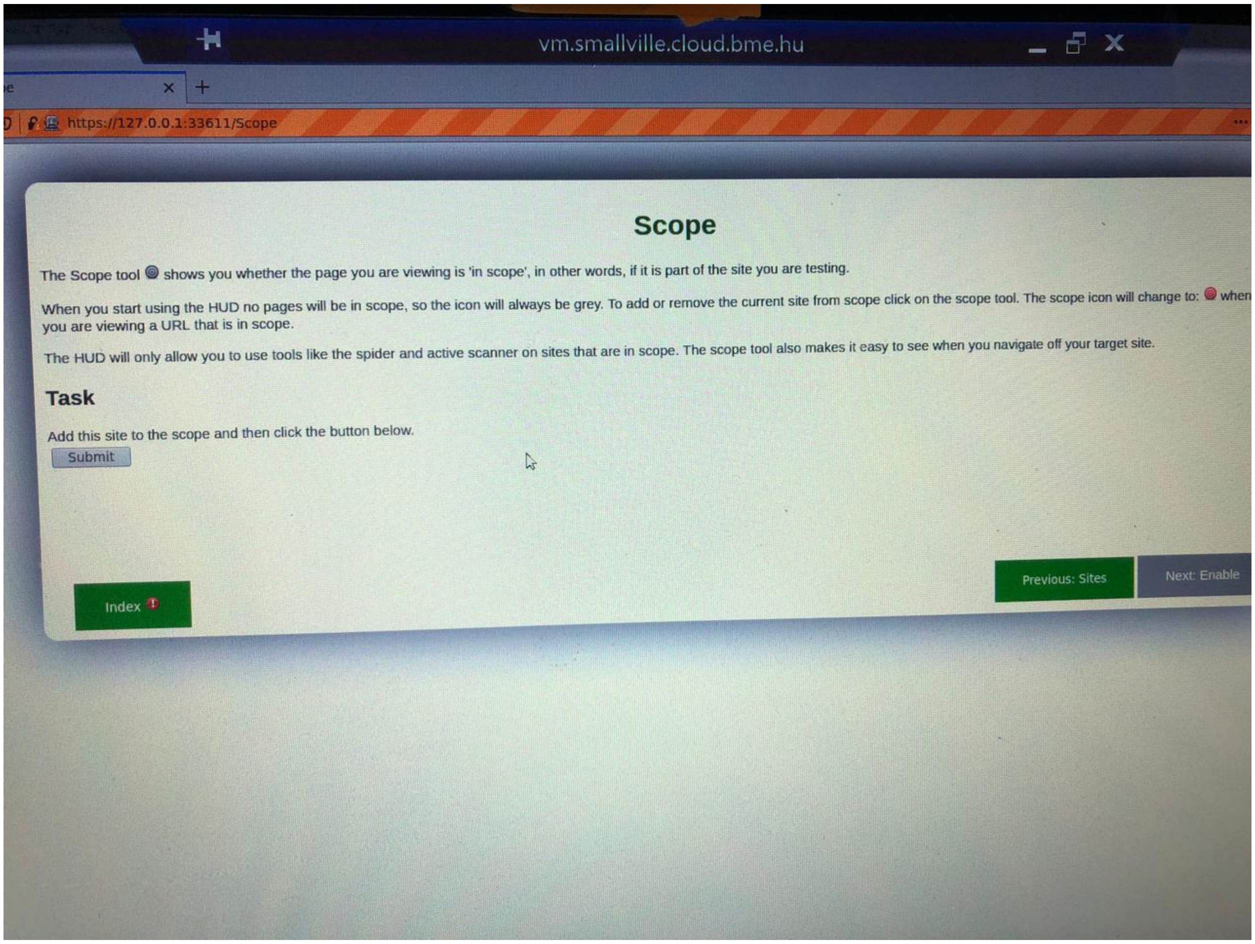
Sites

ZAP builds up a hierarchical site tree based on the URLs that your browser accesses.

The Sites tool 🌐, which by default is on the right-hand side, allows you to view the sites tree for all of the URLs that ZAP is aware of. Click on the '[+]' and '[-]' controls to expand and contract the branches.

You can also click on any of the URLs in the sites tree to see the request and response made for that URL.

Task Completed



Scope

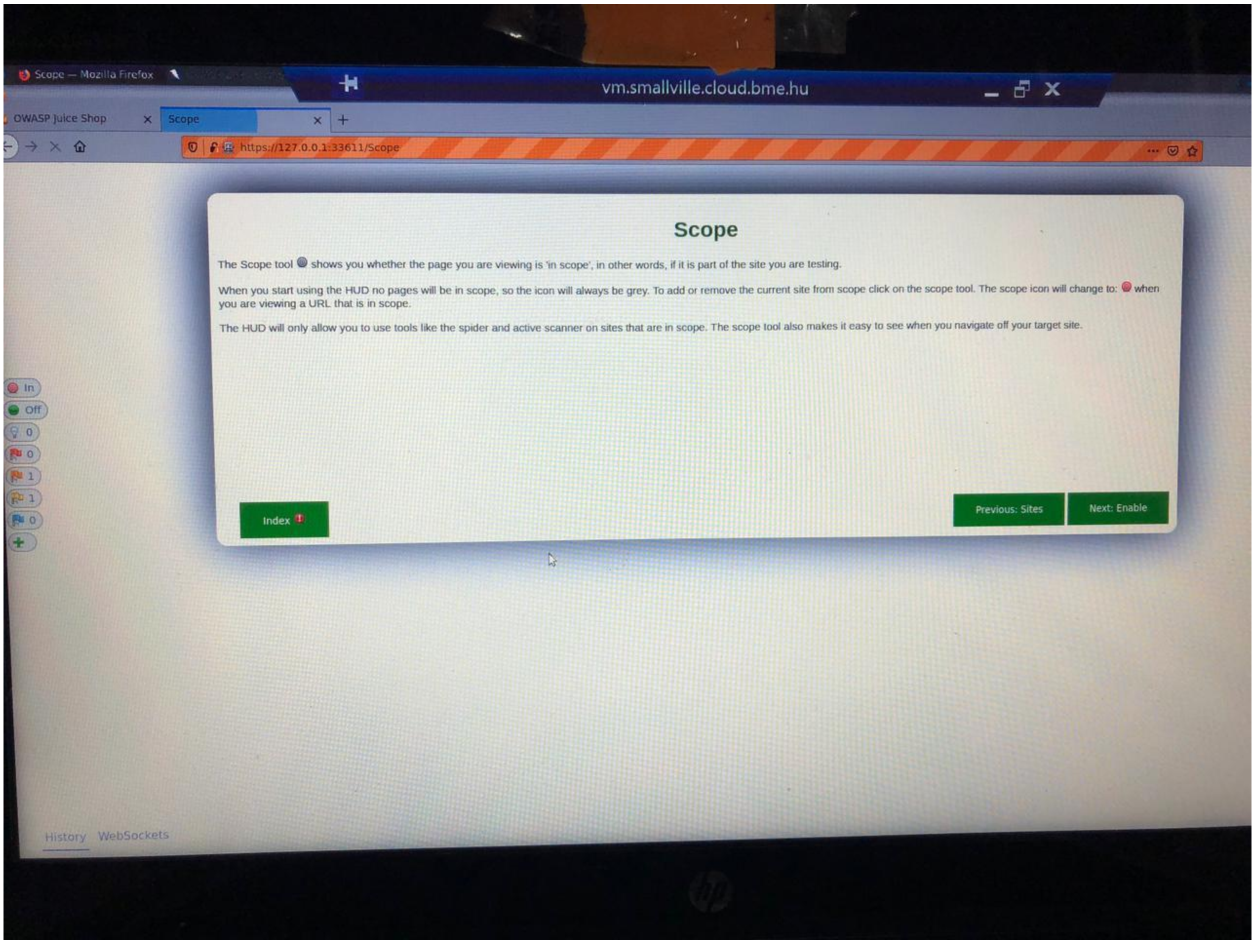
The Scope tool ● shows you whether the page you are viewing is 'in scope', in other words, if it is part of the site you are testing.

When you start using the HUD no pages will be in scope, so the icon will always be grey. To add or remove the current site from scope click on the scope tool. The scope icon will change to: ● when you are viewing a URL that is in scope.

The HUD will only allow you to use tools like the spider and active scanner on sites that are in scope. The scope tool also makes it easy to see when you navigate off your target site.

Task

Add this site to the scope and then click the button below.

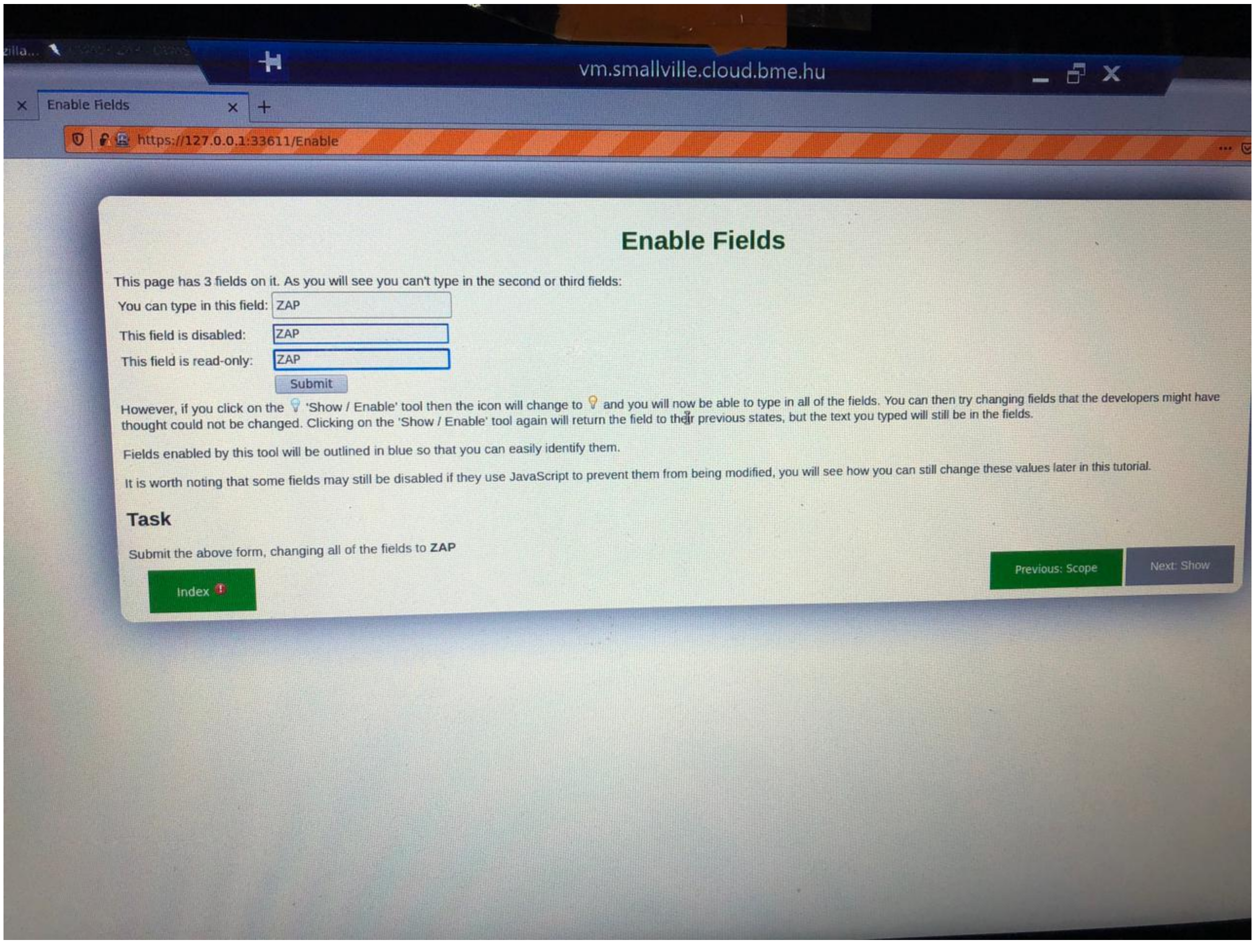


Scope

The Scope tool ● shows you whether the page you are viewing is 'in scope', in other words, if it is part of the site you are testing.

When you start using the HUD no pages will be in scope, so the icon will always be grey. To add or remove the current site from scope click on the scope tool. The scope icon will change to: ● when you are viewing a URL that is in scope.

The HUD will only allow you to use tools like the spider and active scanner on sites that are in scope. The scope tool also makes it easy to see when you navigate off your target site.



Enable Fields

This page has 3 fields on it. As you will see you can't type in the second or third fields:

You can type in this field:	ZAP
This field is disabled:	ZAP
This field is read-only:	ZAP

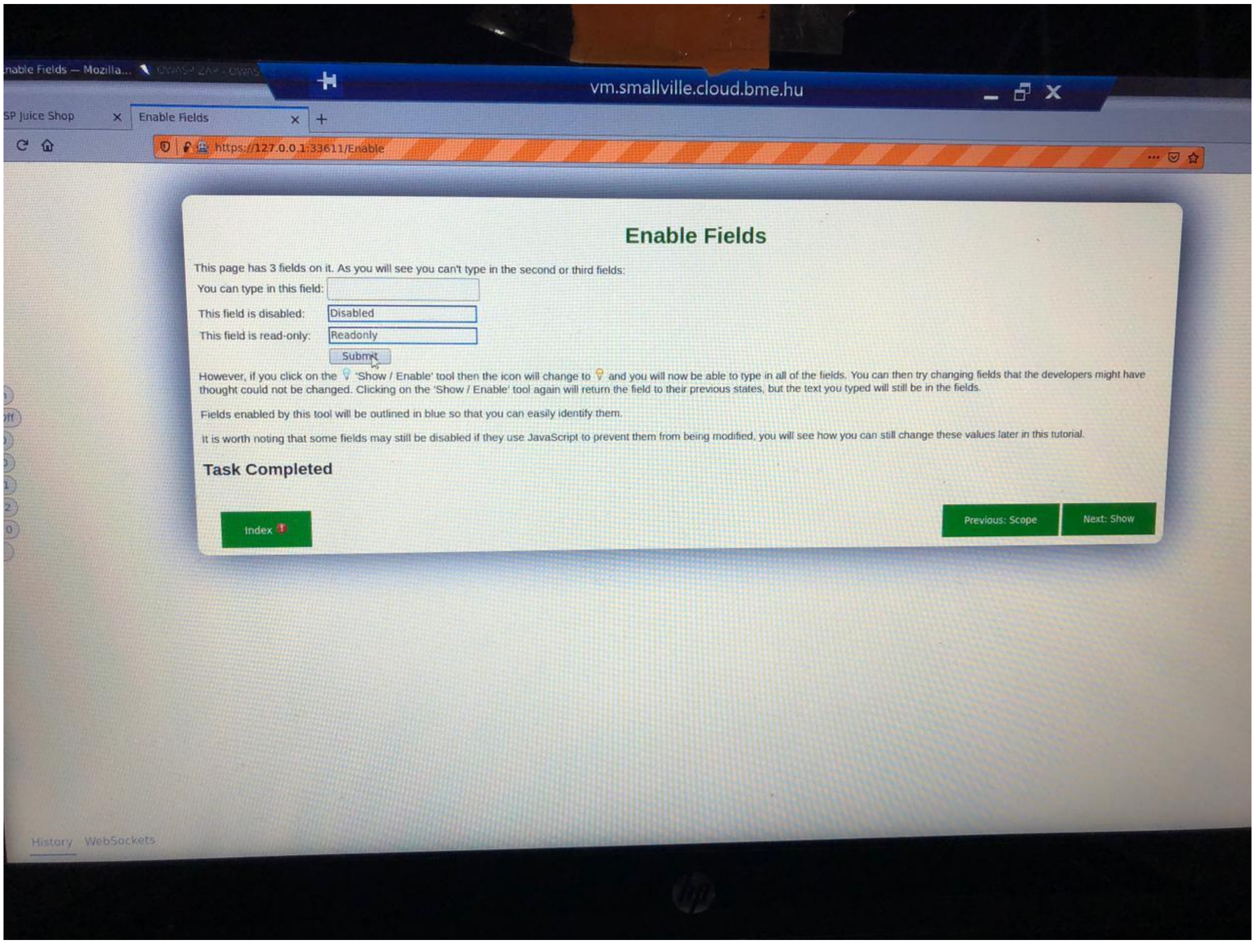
However, if you click on the 'Show / Enable' tool then the icon will change to and you will now be able to type in all of the fields. You can then try changing fields that the developers might have thought could not be changed. Clicking on the 'Show / Enable' tool again will return the field to their previous states, but the text you typed will still be in the fields.

Fields enabled by this tool will be outlined in blue so that you can easily identify them.

It is worth noting that some fields may still be disabled if they use JavaScript to prevent them from being modified, you will see how you can still change these values later in this tutorial.

Task

Submit the above form, changing all of the fields to **ZAP**


nable Fields — Mozilla...
OWASP ZAP - OWAS
vm.smallville.cloud.bme.hu
SP Juice Shop
Enable Fields
https://127.0.0.1:33611/Enable
History
WebSockets

Enable Fields

This page has 3 fields on it. As you will see you can't type in the second or third fields:

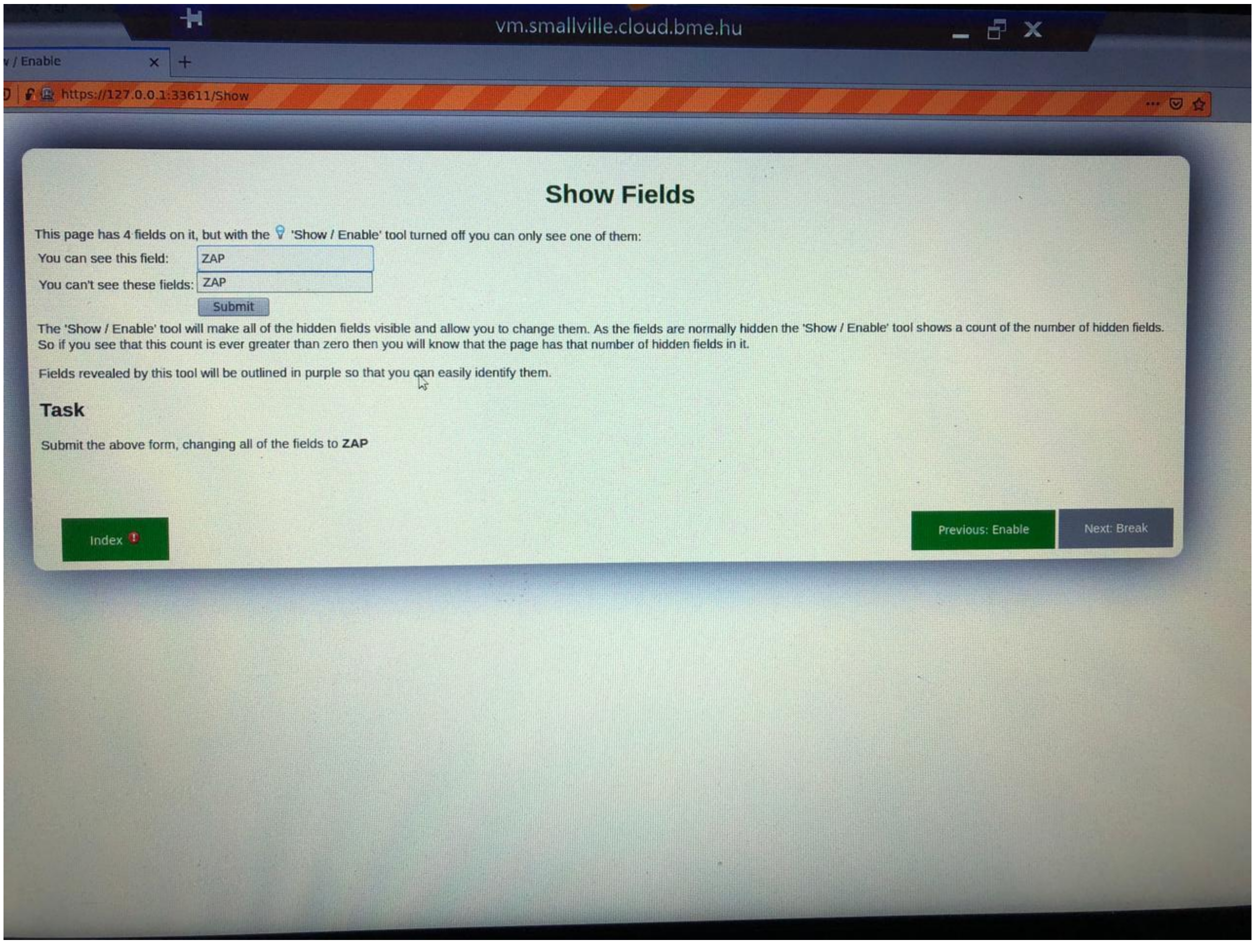
You can type in this field:	
This field is disabled:	Disabled
This field is read-only:	Readonly

However, if you click on the 'Show / Enable' tool then the icon will change to and you will now be able to type in all of the fields. You can then try changing fields that the developers might have thought could not be changed. Clicking on the 'Show / Enable' tool again will return the field to their previous states, but the text you typed will still be in the fields.

Fields enabled by this tool will be outlined in blue so that you can easily identify them.

It is worth noting that some fields may still be disabled if they use JavaScript to prevent them from being modified, you will see how you can still change these values later in this tutorial.

Task Completed



Show Fields

This page has 4 fields on it, but with the 'Show / Enable' tool turned off you can only see one of them:

You can see this field:	ZAP
You can't see these fields:	ZAP

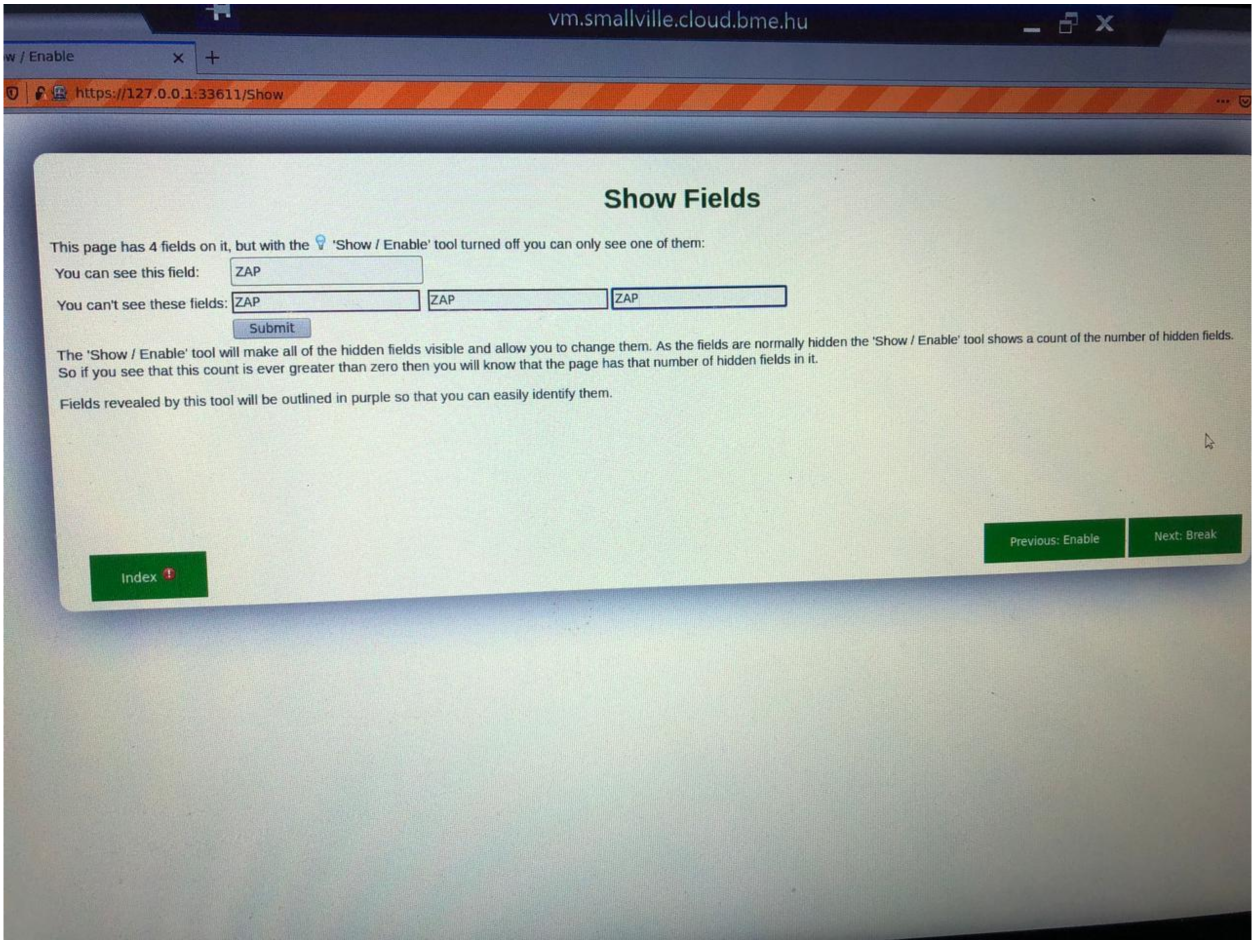
Submit

The 'Show / Enable' tool will make all of the hidden fields visible and allow you to change them. As the fields are normally hidden the 'Show / Enable' tool shows a count of the number of hidden fields. So if you see that this count is ever greater than zero then you will know that the page has that number of hidden fields in it.

Fields revealed by this tool will be outlined in purple so that you can easily identify them.

Task

Submit the above form, changing all of the fields to **ZAP**



Show Fields

This page has 4 fields on it, but with the 'Show / Enable' tool turned off you can only see one of them:

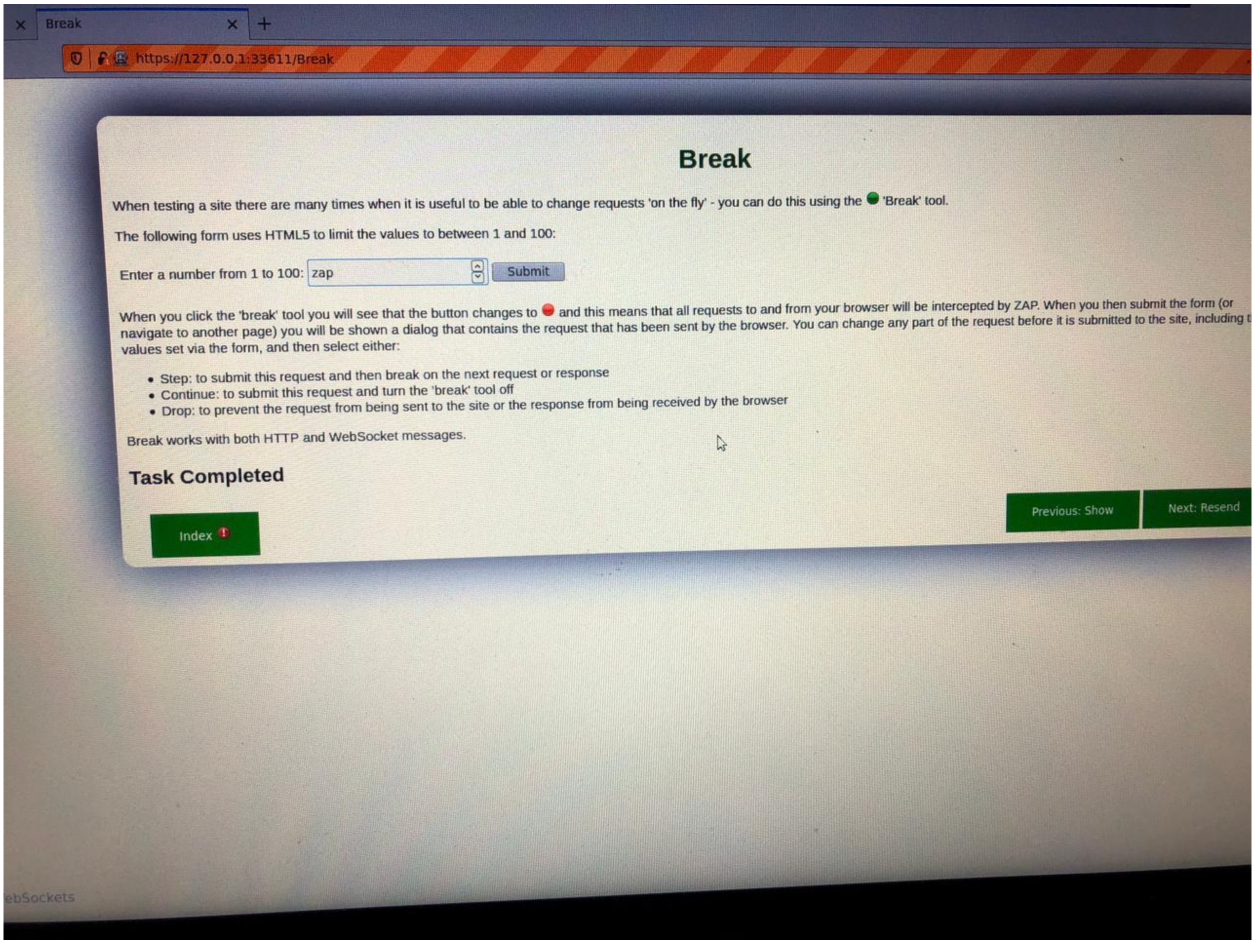
You can see this field: ZAP

You can't see these fields: ZAP ZAP ZAP

Submit

The 'Show / Enable' tool will make all of the hidden fields visible and allow you to change them. As the fields are normally hidden the 'Show / Enable' tool shows a count of the number of hidden fields. So if you see that this count is ever greater than zero then you will know that the page has that number of hidden fields in it.

Fields revealed by this tool will be outlined in purple so that you can easily identify them.



Break

When testing a site there are many times when it is useful to be able to change requests 'on the fly' - you can do this using the ● 'Break' tool.

The following form uses HTML5 to limit the values to between 1 and 100:

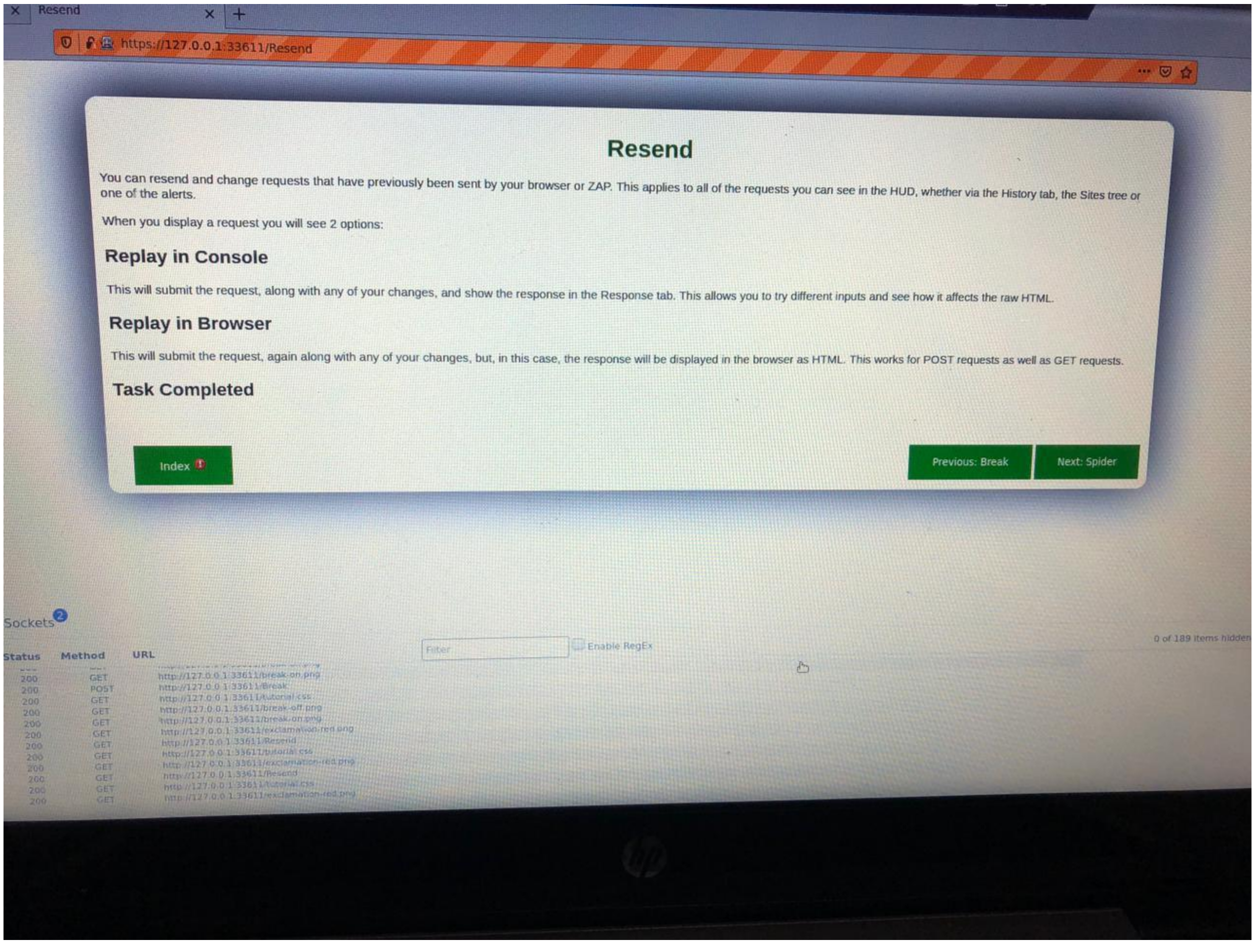
Enter a number from 1 to 100: zap

When you click the 'break' tool you will see that the button changes to ● and this means that all requests to and from your browser will be intercepted by ZAP. When you then submit the form (or navigate to another page) you will be shown a dialog that contains the request that has been sent by the browser. You can change any part of the request before it is submitted to the site, including t values set via the form, and then select either:

- Step: to submit this request and then break on the next request or response
- Continue: to submit this request and turn the 'break' tool off
- Drop: to prevent the request from being sent to the site or the response from being received by the browser

Break works with both HTTP and WebSocket messages.

Task Completed



Resend

You can resend and change requests that have previously been sent by your browser or ZAP. This applies to all of the requests you can see in the HUD, whether via the History tab, the Sites tree or one of the alerts.

When you display a request you will see 2 options:

Replay in Console

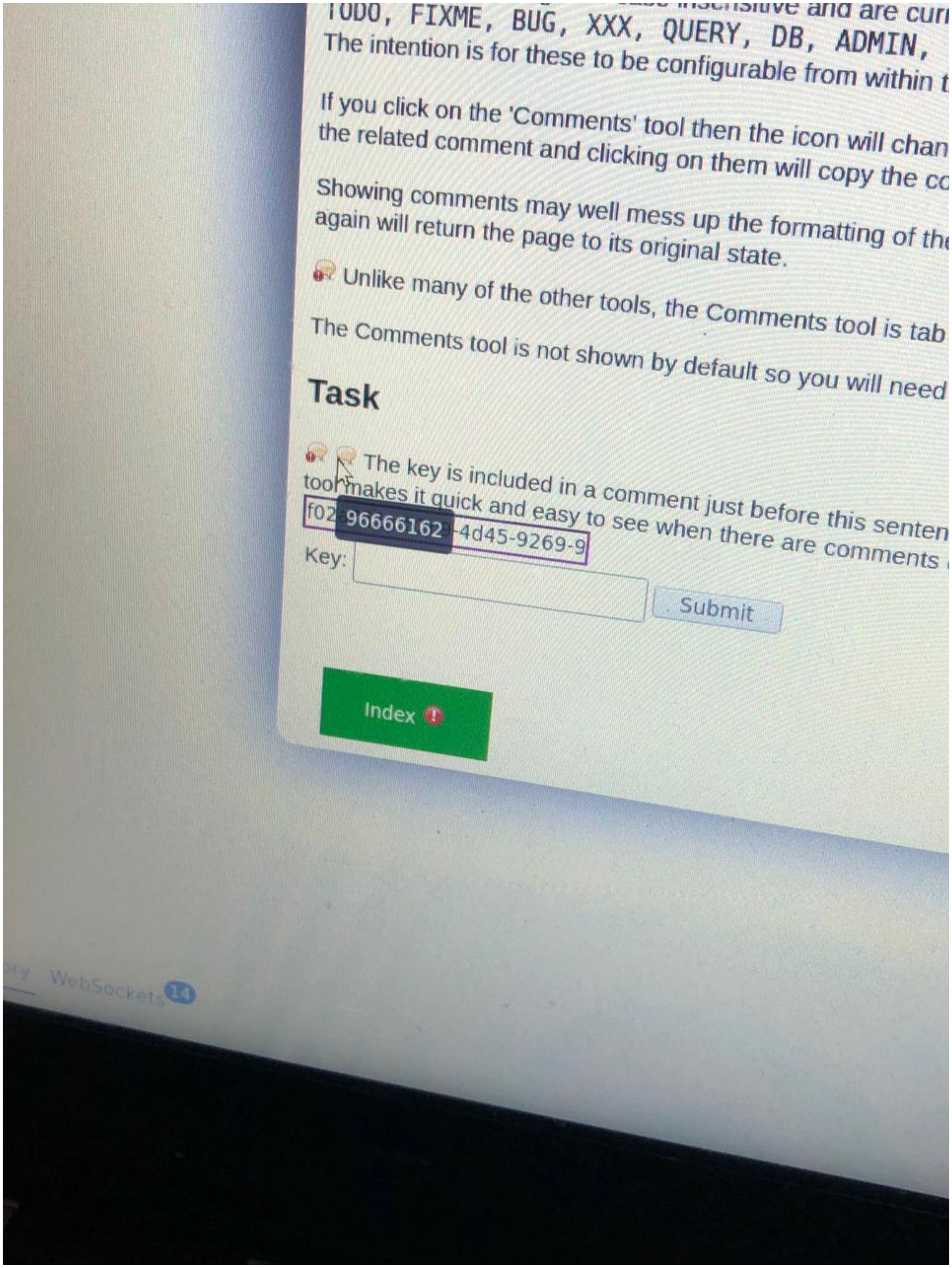
This will submit the request, along with any of your changes, and show the response in the Response tab. This allows you to try different inputs and see how it affects the raw HTML.

Replay in Browser

This will submit the request, again along with any of your changes, but, in this case, the response will be displayed in the browser as HTML. This works for POST requests as well as GET requests.

Task Completed

Status	Method	URL
200	GET	http://127.0.0.1:33611/break-on.png
200	POST	http://127.0.0.1:33611/Break
200	GET	http://127.0.0.1:33611/tutorial.css
200	GET	http://127.0.0.1:33611/break-off.png
200	GET	http://127.0.0.1:33611/break-on.png
200	GET	http://127.0.0.1:33611/exclamation-red.png
200	GET	http://127.0.0.1:33611/Resend
200	GET	http://127.0.0.1:33611/tutorial.css
200	GET	http://127.0.0.1:33611/exclamation-red.png
200	GET	http://127.0.0.1:33611/Resend
200	GET	http://127.0.0.1:33611/tutorial.css
200	GET	http://127.0.0.1:33611/exclamation-red.png



insensitive and are curr

TODO, FIXME, BUG, XXX, QUERY, DB, ADMIN,

The intention is for these to be configurable from within t

If you click on the 'Comments' tool then the icon will chan
the related comment and clicking on them will copy the co

Showing comments may well mess up the formatting of the
again will return the page to its original state.

Unlike many of the other tools, the Comments tool is tab

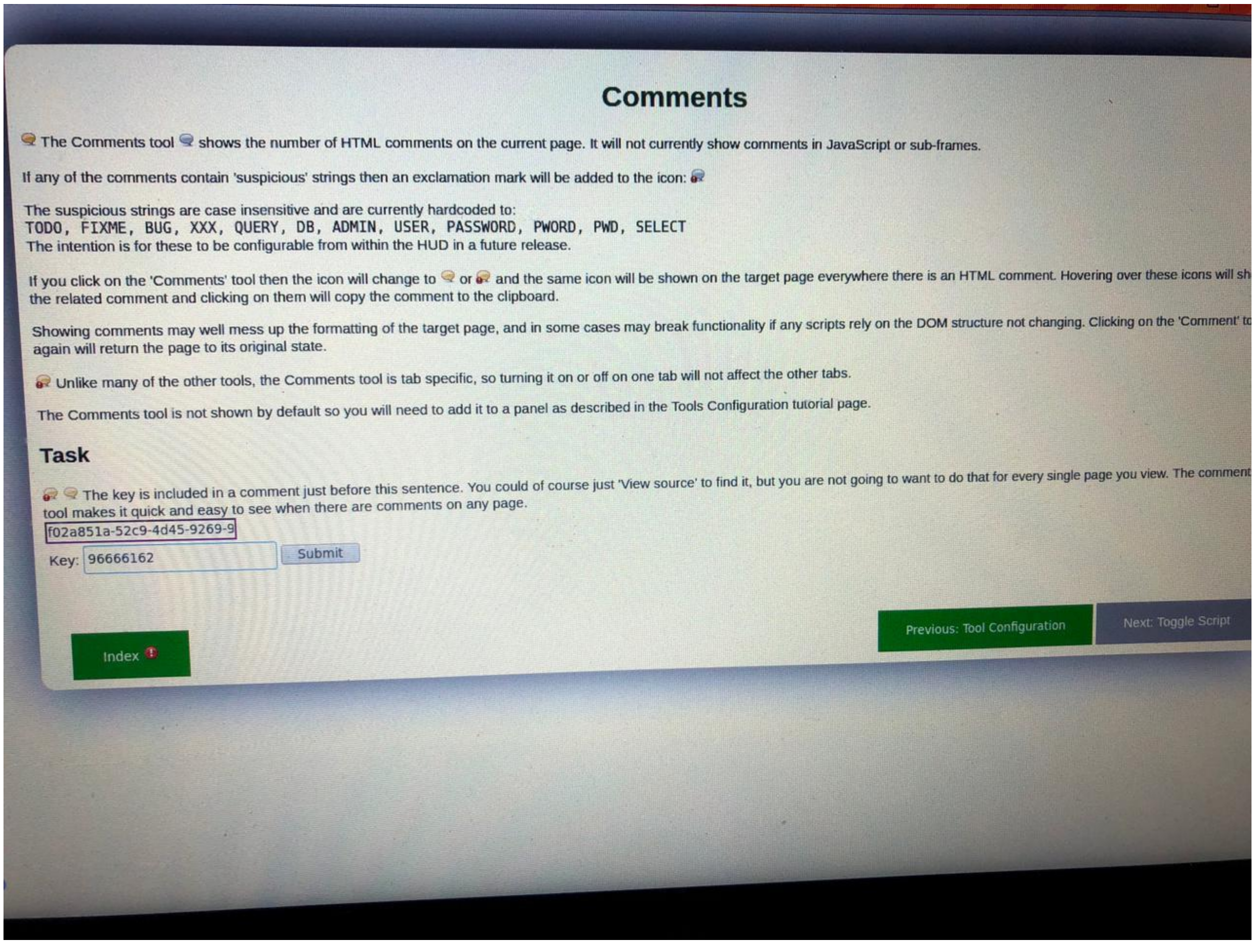
The Comments tool is not shown by default so you will need

Task

The key is included in a comment just before this senten
tool makes it quick and easy to see when there are comments

f02 96666162 -4d45-9269-9

Key:



Comments

💬 The Comments tool 💬 shows the number of HTML comments on the current page. It will not currently show comments in JavaScript or sub-frames.

If any of the comments contain 'suspicious' strings then an exclamation mark will be added to the icon: 💬

The suspicious strings are case insensitive and are currently hardcoded to:
`TODO, FIXME, BUG, XXX, QUERY, DB, ADMIN, USER, PASSWORD, PWORD, PWD, SELECT`
The intention is for these to be configurable from within the HUD in a future release.

If you click on the 'Comments' tool then the icon will change to 💬 or 💬 and the same icon will be shown on the target page everywhere there is an HTML comment. Hovering over these icons will sh the related comment and clicking on them will copy the comment to the clipboard.

Showing comments may well mess up the formatting of the target page, and in some cases may break functionality if any scripts rely on the DOM structure not changing. Clicking on the 'Comment' to again will return the page to its original state.

💬 Unlike many of the other tools, the Comments tool is tab specific, so turning it on or off on one tab will not affect the other tabs.

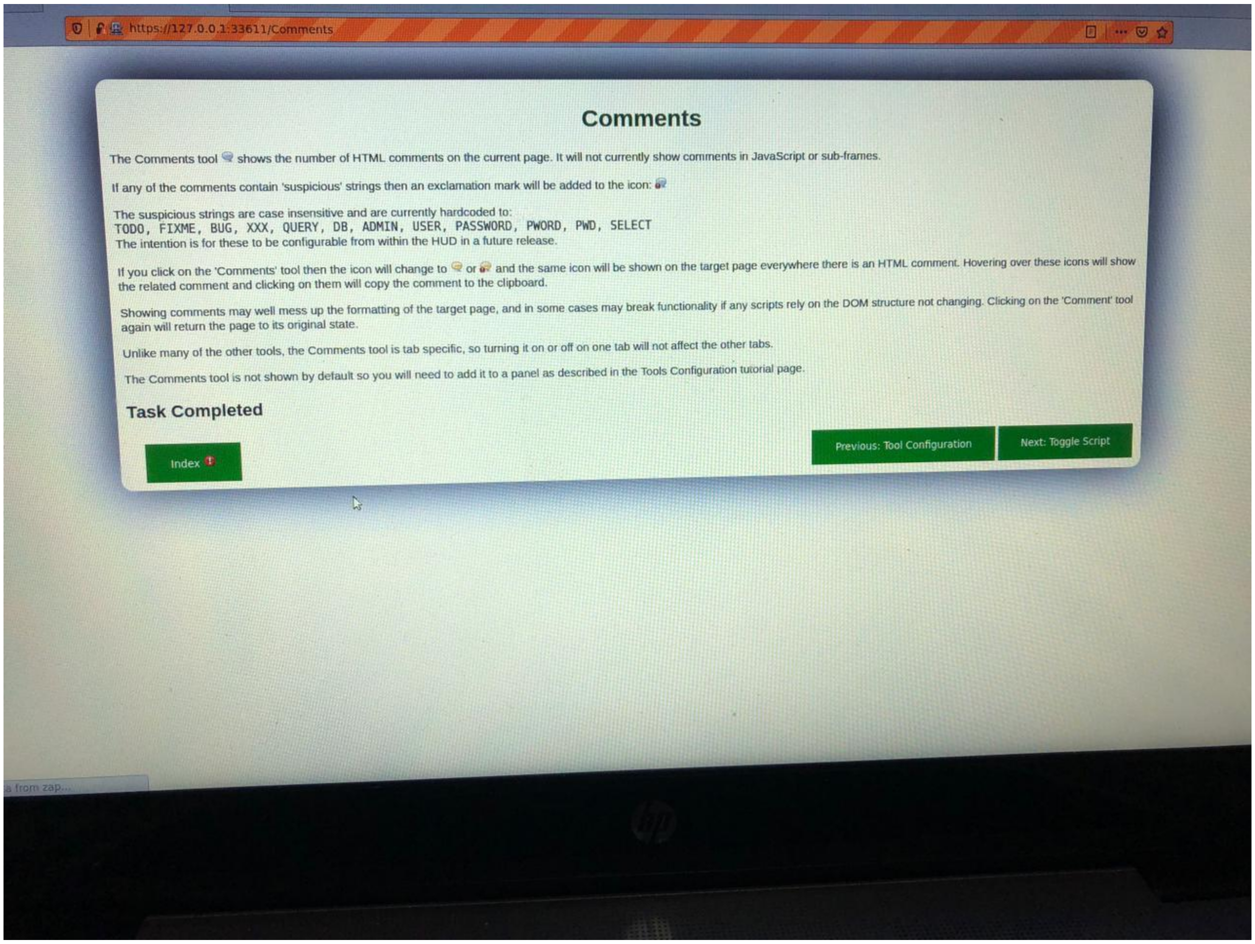
The Comments tool is not shown by default so you will need to add it to a panel as described in the Tools Configuration tutorial page.

Task

💬 💬 The key is included in a comment just before this sentence. You could of course just 'View source' to find it, but you are not going to want to do that for every single page you view. The comment tool makes it quick and easy to see when there are comments on any page.

f02a851a-52c9-4d45-9269-9

Key: 96666162



Comments

The Comments tool shows the number of HTML comments on the current page. It will not currently show comments in JavaScript or sub-frames.

If any of the comments contain 'suspicious' strings then an exclamation mark will be added to the icon:

The suspicious strings are case insensitive and are currently hardcoded to:
`TODO, FIXME, BUG, XXX, QUERY, DB, ADMIN, USER, PASSWORD, PWORD, PWD, SELECT`
The intention is for these to be configurable from within the HUD in a future release.

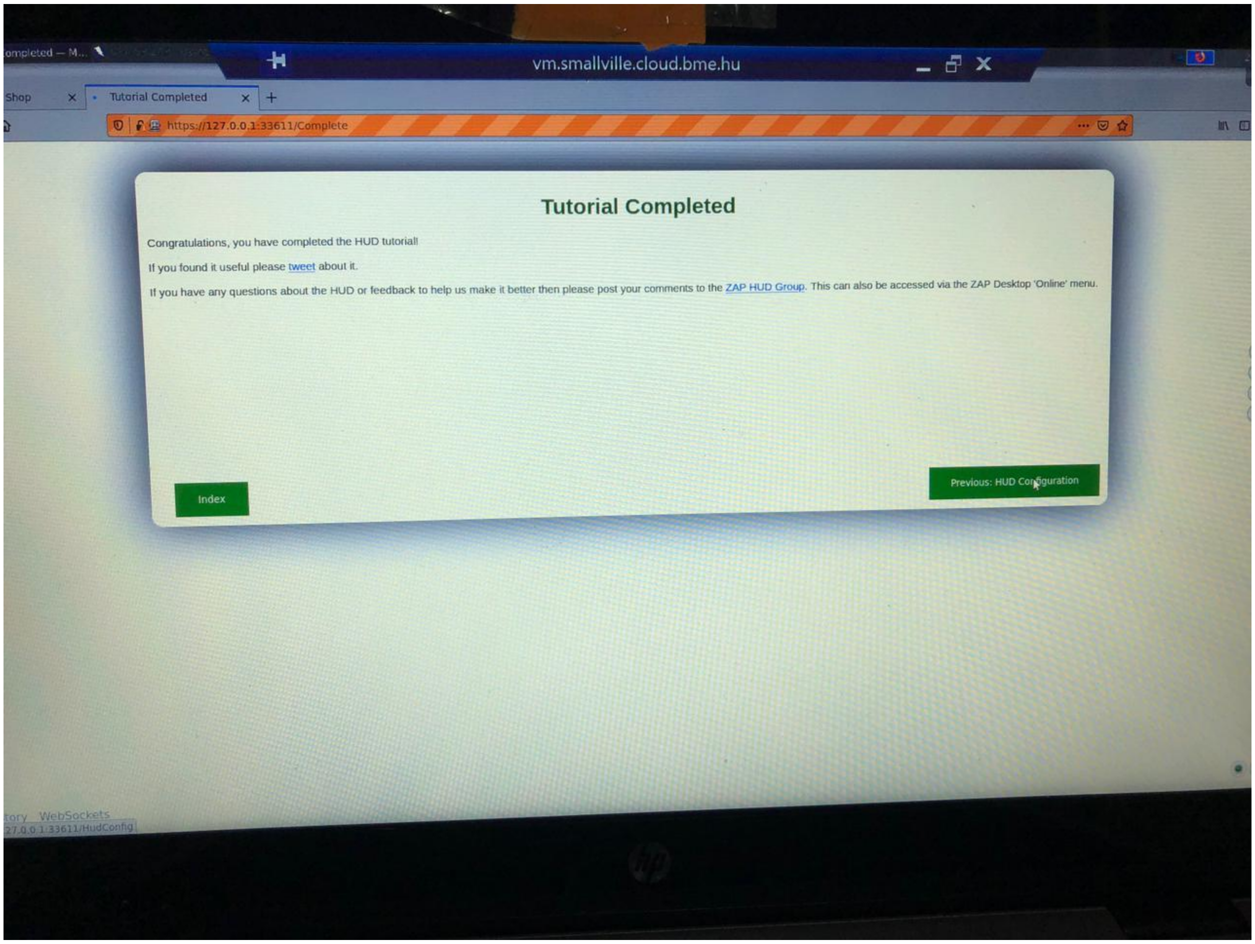
If you click on the 'Comments' tool then the icon will change to or and the same icon will be shown on the target page everywhere there is an HTML comment. Hovering over these icons will show the related comment and clicking on them will copy the comment to the clipboard.

Showing comments may well mess up the formatting of the target page, and in some cases may break functionality if any scripts rely on the DOM structure not changing. Clicking on the 'Comment' tool again will return the page to its original state.

Unlike many of the other tools, the Comments tool is tab specific, so turning it on or off on one tab will not affect the other tabs.

The Comments tool is not shown by default so you will need to add it to a panel as described in the Tools Configuration tutorial page.

Task Completed


vm.smallville.cloud.bme.hu
ompleted — M...
Shop
Tutorial Completed
https://127.0.0.1:33611/Complete
tory WebSockets
127.0.0.1:33611/HudConfig

Tutorial Completed

Congratulations, you have completed the HUD tutorial!

If you found it useful please tweet about it.

If you have any questions about the HUD or feedback to help us make it better then please post your comments to the ZAP HUD Group. This can also be accessed via the ZAP Desktop 'Online' menu.

Index
Previous: HUD Configuration