Hacking with a Heads Up Display

Creating Usable Security with ZAP
accessible, intuitive, flexible
Usable software leads to a more effective organization.
Usable security software leads to a more secure organization.
Enabling developers to use security tools will improve the security of your organization.
Is your new feature vulnerable to XSS?
Zed Attack Proxy (ZAP)
GET juiceshop.org

<html>
<body>
...
</body>
</html>

GET juiceshop.org

<html>
<body>
...
</body>
</html>
All Products

<table>
<thead>
<tr>
<th>Image</th>
<th>Product</th>
<th>Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Apple Juice" /></td>
<td>Apple Juice (1000ml)</td>
<td>The all-time classic.</td>
<td>1.99</td>
</tr>
<tr>
<td><img src="image" alt="Apple Pomace" /></td>
<td>Apple Pomace (1000ml)</td>
<td>Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling.</td>
<td>0.89</td>
</tr>
<tr>
<td><img src="image" alt="Banana Juice" /></td>
<td>Banana Juice (1000ml)</td>
<td>Monkeys love it the most.</td>
<td>1.99</td>
</tr>
<tr>
<td><img src="image" alt="Carrot Juice" /></td>
<td>Carrot Juice (1000ml)</td>
<td>As the old German saying goes: “Carrots are good for the eyes. Or has anyone ever seen a rabbit with glasses?”</td>
<td>2.99</td>
</tr>
<tr>
<td><img src="image" alt="Eggfruit Juice" /></td>
<td>Eggfruit Juice (500ml)</td>
<td>Now with even more exotic flavour.</td>
<td>8.99</td>
</tr>
<tr>
<td><img src="image" alt="Fruit Press" /></td>
<td>Fruit Press</td>
<td>Fruits go in. Juice comes out. Pomace you can send back to us for recycling purposes.</td>
<td>89.99</td>
</tr>
</tbody>
</table>
Zed Attack Proxy (ZAP)

- Intercept requests
- Replay requests
- Spider sites
- Fuzz requests
- Passive Scanning
- Active Scanning
  - Command Injection
  - SQLi
  - Remote File Inclusion
  - XSS
  - Redirects
- Encoding/Decoding
- Automation & API
- Scripting
- Robust Add-On Ecosystem
- Automated Authentication & Sessions
DEV SHOT SHOWCASING COLORBLIND SUPPORT ON CONSOLE
ZAP Heads Up Display (HUD)
Demo
Demo
Demo
So how does it work?
GET juiceshop.org

<html>
<body>
...<br/>
</body>
</html>

GET juiceshop.org

<html>
<body>
<script src="zap://inject.js">
</script>
</body>
</html>
injected script

```html
"content": { "message": "This website uses fruit cookies to ensure you get the juiciest tracking experience.", "dismiss"
  }});
</script>
<script src="dist/juice-shop.min.js"></script>
</head>
<body ng-cloak translate-cloak>
<nav class="navbar navbar-default" role="navigation">
  <div class="container-fluid" ng-controller="NavController"
  <div class="navbar-header">
```
javascript closure

(function () {
    // ... all vars and functions are in this scope only
    // still maintains access to all globals
})();

http://www.adequatelygood.com/JavaScript-Module-Pattern-In-Depth.html
iframes
<table>
<thead>
<tr>
<th>Image</th>
<th>Product</th>
<th>Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="apple-juice.png" alt="Image" /></td>
<td>Apple Juice (1000ml)</td>
<td>The all-time classic.</td>
<td>1.99</td>
</tr>
<tr>
<td><img src="apple-pomace.png" alt="Image" /></td>
<td>Apple Pomace</td>
<td>Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling.</td>
<td>0.89</td>
</tr>
<tr>
<td><img src="banana-juice.png" alt="Image" /></td>
<td>Banana Juice (1000ml)</td>
<td>Monkeys love it the most.</td>
<td>1.99</td>
</tr>
<tr>
<td><img src="carrot-juice.png" alt="Image" /></td>
<td>Carrot Juice (1000ml)</td>
<td>As the old German saying goes: “Carrots are good for the eyes. Or has anyone ever seen a rabbit with glasses?”</td>
<td>2.99</td>
</tr>
<tr>
<td><img src="eggnog.png" alt="Image" /></td>
<td>Eggfruit Juice (500ml)</td>
<td>Now with even more exotic flavour.</td>
<td>8.99</td>
</tr>
<tr>
<td>Image</td>
<td>Product</td>
<td>Description</td>
<td>Price</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td><img src="image" alt="Apple Juice" /></td>
<td>Apple Juice (1000ml)</td>
<td>The all-time classic.</td>
<td>1.99</td>
</tr>
<tr>
<td><img src="image" alt="Apple Juice" /></td>
<td>Apple Pomace</td>
<td>Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling.</td>
<td>0.89</td>
</tr>
<tr>
<td><img src="image" alt="Banana Juice" /></td>
<td>Banana Juice (1000ml)</td>
<td>Monkeys love it the most.</td>
<td>1.99</td>
</tr>
<tr>
<td><img src="image" alt="Carrot Juice" /></td>
<td>Carrot Juice (1000ml)</td>
<td>As the old German saying goes: “Carrots are good for the eyes. Or has anyone ever seen a rabbit with glasses?”</td>
<td>2.99</td>
</tr>
<tr>
<td><img src="image" alt="Eggfruit Juice" /></td>
<td>Eggfruit Juice (500ml)</td>
<td>Now with even more exotic flavour.</td>
<td>8.99</td>
</tr>
</tbody>
</table>
## Our Best Deals!

<table>
<thead>
<tr>
<th>Product</th>
<th>Type</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>GZ XT4</td>
<td>Gizmos</td>
<td>£4.45</td>
</tr>
<tr>
<td>GZ K77</td>
<td>Gizmos</td>
<td>£3.05</td>
</tr>
<tr>
<td>Bonzo dog doo dah</td>
<td>Doodahs</td>
<td>£2.45</td>
</tr>
<tr>
<td>Thingies 2</td>
<td>Thingies</td>
<td>£3.20</td>
</tr>
<tr>
<td>Whatst called</td>
<td>Whatsits</td>
<td>£4.10</td>
</tr>
<tr>
<td>GZ FZ8</td>
<td>Gizmos</td>
<td>£1.00</td>
</tr>
<tr>
<td>Whatst weigh</td>
<td>Whatsits</td>
<td>£2.50</td>
</tr>
<tr>
<td>Mindblank</td>
<td>Whatchamacallits</td>
<td>£1.00</td>
</tr>
<tr>
<td>GZ XT4</td>
<td>Gizmos</td>
<td>£4.45</td>
</tr>
</tbody>
</table>
### The Bodgelt Store

**We bodge it, so you don't have to!**

*Guest user*

**Our Best Deals!**

<table>
<thead>
<tr>
<th>Product</th>
<th>Type</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>GZ XT4</td>
<td>Gizmos</td>
<td>$4.45</td>
</tr>
<tr>
<td>GZ K77</td>
<td>Gizmos</td>
<td>$3.05</td>
</tr>
<tr>
<td>Bonzo dog doo dah</td>
<td>Doodahs</td>
<td>$2.45</td>
</tr>
<tr>
<td>Thingies 2</td>
<td>Things</td>
<td>$3.20</td>
</tr>
<tr>
<td>Whatsit called</td>
<td>Whatstis</td>
<td>$4.10</td>
</tr>
<tr>
<td>Whatchamacallits</td>
<td>GZ FZ8</td>
<td>$1.00</td>
</tr>
<tr>
<td>Mindblank</td>
<td>Whatchamacallits</td>
<td>$1.00</td>
</tr>
<tr>
<td>Whatstis weigh</td>
<td>GZ FZ8</td>
<td>$2.50</td>
</tr>
<tr>
<td>Mindblank</td>
<td>Whatchamacallits</td>
<td>$1.00</td>
</tr>
<tr>
<td>GZ XT4</td>
<td>Gizmos</td>
<td>$4.45</td>
</tr>
</tbody>
</table>
postMessage

Service Worker

inject.js
Service Worker

postMessage

inject.js
ZAP API
Web Sockets
postMessage
Service Worker
Is your new feature vulnerable to XSS?
So now what?

Want to help build the HUD?
Reach out!

Want to support the HUD?
Share!
Want to play with the HUD?

Alpha release (*hopefully*)
Monday
Available in Weekly Release
Or
AddOn Marketplace
Keep up with the HUD
@david_scrobonia
@zaproxy

Questions?