Pizza Roulette

Catherine McIlvride and Fiona Sasse
## Starting Point

<table>
<thead>
<tr>
<th>Pizza Place</th>
<th>Website</th>
<th>Android App</th>
<th>iOS App</th>
<th>Online Ordering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pizza place A</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Pizza place B</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Pizza place C</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Pizza place D</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Pizza place E</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Pizza place F</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Pizza place G</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Pizza place H</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
Too Easy.
POODLE (TLS)
Heartbeat [hɑːtˈbɛt]  
The cycle of contraction of the heart, normal PACEMAKER for the heart.

Heartbeat (UK TV series)  
From Wikipedia, the free encyclopedia

Heartbeat is a British police procedural television series (formerly Yorkshire Television evenings). The 372nd and final episode aired on 17 November 2018, after the series moved to Sunday evenings. It came sixth in the UK TV ratings list with a peak audience of 6 million people.

Ex-policeman DI Jack Carling (played by James Whale) and his colleagues DCI Charlie Barlow (played by Mark Stephenson) and PC Nigel Millett (played by Mark Moraghan) investigate a number of crimes in the fictional Yorkshire town of Holmsford. During each episode, Carling actively works with Barlow and Millett to solve a crime and demonstrates his Yorkshire values.

This article is about the television series. For the English verb, see Heartbeat (verb).

Written by ex-policeman Peter N Walker, under the pseudonym Tony Clark, the series was produced by ITV Studios. It moved to Sunday evenings. The 372nd and final episode aired on 17 November 2018, after the series moved to Sunday evenings.

Heartbeat proved popular from the outset and has had a long run on British television: 24.9 million people tuned in to watch the first episode when it aired on Yorkshire Television on 14 September 1992.

The series was nominated for the BAFTA for Best Drama Series in 1997 and 2008, winning in 2008, and was also nominated for the British Academy Television Award for Best Drama Series in 2008 for its last episode.

The series was an international success, with around 1000 countries around the world broadcasting the show. It has been licensed in over 100 countries and has been adapted into several languages.

The show is often remembered for its catchphrase, ‘Time for a Heartbeat’.
Pretending to know what we are doing
Just a little frustrated
We tried!!!
Risk Profiles

- Low-Moderate
- High
- Very High
- Severe
- Extreme
- Catastrophic
<!DOCTYPE html>
<html>
  <head>
    <title>Example</title>
    <link rel="stylesheet" href="style.css" />
  </head>
  <body>
    <h1><a href="/">Header</a></h1>
    <nav>
      <a href="one/">One</a>
      <a href="two/">Two</a>
      <a href="three/">Three</a>
    </nav>
    <article>
      <h2>Cross-site scripting (reflected)</h2>
      <p><strong>Issue:</strong> Cross-site scripting (reflected)</p>
      <p><strong>Severity:</strong> High</p>
      <p><strong>Confidence:</strong> Certain</p>
      <p><strong>Host:</strong> http://0b7bd624bab7.mdseclabs.net</p>
      <p><strong>Path:</strong> /search/11/Default.aspx</p>
      <p><strong>Issue detail</strong></p>
      <p>The value of the SearchTerm request parameter is copied into the HTML document as plain text between tags. The payload `1d329c<script>alert('x');</script>` was submitted in the SearchTerm parameter. This input was echoed unmodified in the application’s response.</p>
    </article>
  </body>
</html>
Hack Yourself First: How to go on the Cyber-Offense

"Hack Yourself First" is all about developers building up cyber-offense skills and proactively seeking out security vulnerabilities in their own websites before an attacker does.

Start FREE course

Course Info

<table>
<thead>
<tr>
<th>Retina</th>
<th>Level</th>
<th>Updated</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5/5</td>
<td>Intermediate</td>
<td>August 30, 2013</td>
<td>9h 25m</td>
</tr>
</tbody>
</table>

Description

The prevalence of online attacks against websites has accelerated quickly in recent years and the same risks continue to be readily exploited. However, these are very often easily identified directly within the browser; it's just a matter of understanding the vulnerable patterns to look for. This course comes at security from the view of the attacker in that their entry point is typically the browser. They have a website they want to probe for security risks and this is how they go about it. This approach is more reflective of the real online threat than reviewing source code and it empowers developers to begin immediately assessing their applications even when they're running in a live environment without access to the source. After all, that's what online attackers are doing.
The following is a depiction of the events that occurred on the night of 4th October 2017
fiona  2:38 PM
Shit
I may have stuffed up
I have accidentally accessed someone’s information

kevinnz  2:40 PM
Well it’s kind of cool, but it’s an issue with the site
Now we need to confirm that you have found a bug

kevinnz  2:42 PM
If it’s a problem we might be stepping into a gray area

fiona  2:43 PM
But i have access to a name, a phone number an address and an email

kevinnz  2:44 PM
Cool. I have to go to a meeting. Don’t get arrested until I get back
250 Damaging or interfering with computer system

(1) Every one is liable to imprisonment for a term not exceeding 10 years who intentionally or recklessly destroys, damages, or alters any computer system if he or she knows or ought to know that danger to life is likely to result.

(2) Every one is liable to imprisonment for a term not exceeding 7 years who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised,—

(a) damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system; or

(b) causes any data or software in any computer system to be damaged, deleted, modified, or otherwise interfered with or impaired; or

(c) causes any computer system to—

(i) fail, or

(ii) deny service to any authorised users.

## OWASP Top 10

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Injection</td>
</tr>
<tr>
<td>A2</td>
<td>Broken Authentication and Session Management</td>
</tr>
<tr>
<td>A3</td>
<td>Sensitive Data Exposure</td>
</tr>
<tr>
<td>A4</td>
<td>XML External Entity (XXE)</td>
</tr>
<tr>
<td>A5</td>
<td>Broken Access Control</td>
</tr>
<tr>
<td>A6</td>
<td>Security Misconfiguration</td>
</tr>
<tr>
<td>A7</td>
<td>Cross Site Scripting</td>
</tr>
<tr>
<td>A8</td>
<td>Insecure Deserialization</td>
</tr>
<tr>
<td>A9</td>
<td>Using Components with Known Vulnerabilities</td>
</tr>
<tr>
<td>A10</td>
<td>Insufficient Logging &amp; Monitoring</td>
</tr>
</tbody>
</table>
HTTP vs HTTPS
ARMADILLO CHEESY GARLIC BREAD

I'm having issues even writing about cheese because it's so
obvious and yet all. Every single person on this
planet, there are five billion, has reached for a piece and this is
happening all over the table. We all go to the rush and
ash over each bite. It is the best way to eat cheese. A loaf
just perfectly pillows itself on your tongue and you just
keep eating it. Never enough. Never enough.

Preheat the oven to 400°F.

In a bowl, combine the mozzarella, butter, mayonnaise, garlic,
cheese, pepper flakes, salt, and black pepper. Using a
serrated knife, cut the bread in a crosshatch pattern, making
cuts 2 inches apart and taking care not to cut through the
bottom of the bread.

Place the bread on a large sheet of foil on a baking sheet. Stuff
most of the cheese mixture into all of the cracks in the bread.
Slather the remainder over the top of the bread. Coat another
sheet of foil with cooking spray and lay spray-side down on the
top of the loaf. Crimp the two pieces together to seal the bread in
foil.

Bake for 20 minutes, then reduce the oven temperature to 350°F.
Remove the top sheet of foil and bake until the top gets golden
and the cheese is super melty, 15 to 20 minutes longer.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A2</td>
<td>Broken Authentication and Session Management</td>
</tr>
<tr>
<td>A10</td>
<td>Insufficient Logging &amp; Monitoring</td>
</tr>
</tbody>
</table>
A7 Cross Site Scripting

<script>alert('hello');</script>

hello

OK
Using order numbers to bring up other people's details
# OWASP Top 10

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Injection</td>
</tr>
<tr>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>A2</td>
<td>Broken Authentication and Session Management</td>
</tr>
<tr>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>A3</td>
<td>Sensitive Data Exposure</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>A4</td>
<td>XML External Entity (XXE)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>A5</td>
<td>Broken Access Control</td>
</tr>
<tr>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>A6</td>
<td>Security Misconfiguration</td>
</tr>
<tr>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>A7</td>
<td>Cross Site Scripting</td>
</tr>
<tr>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>A8</td>
<td>Insecure Deserialization</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>A9</td>
<td>Using Components with Known Vulnerabilities</td>
</tr>
<tr>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>A10</td>
<td>Insufficient Logging &amp; Monitoring</td>
</tr>
</tbody>
</table>
Things we learnt!!
Time!!!
Mentorship is a must
So what now.....
Massive Thanks To Kevin!
That's all Folks!