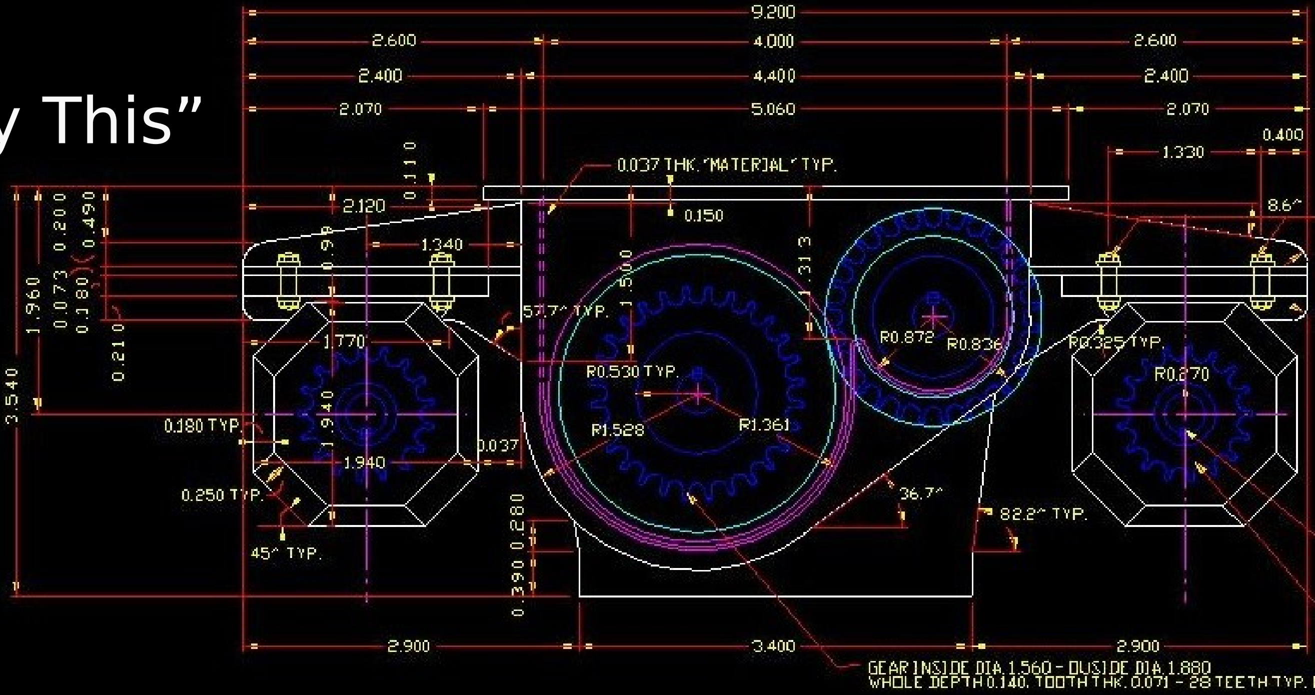
OOPS: That’s Not Supposed to Happen

Bypassing IE’s XSS Filter

Carlos
@RTWaysea

About Me

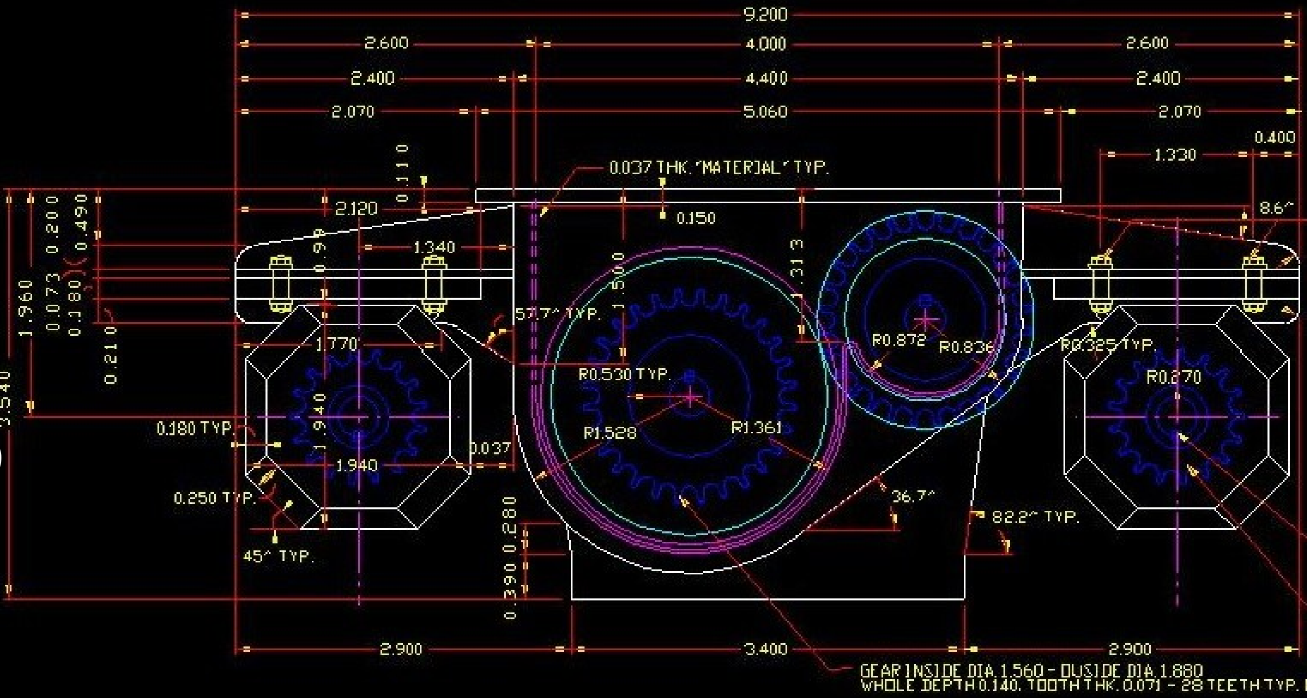
- Mechanical Drafting Background
- Friend Said “Try This”
- Three Years at WhiteHatSec



Agenda

- Bypass: IE Anti-Reflective XSS Filter
- Explanation: Do Not Rely On Browsers
- Process: Security Test Tooling

BYPASS


9.200
2.600
4.000
2.600
2.400
4.400
2.400
2.070
5.060
2.070
0.400
1.330
0.110
0.037 THK. 'MATERIAL' TYP.
2.120
0.150
8.6^
1.340
1.313
1.500
1.960
0.073
0.200
0.180
0.490
0.210
3.540
57.7^ TYP.
1.770
R0.872
R0.836
R0.325 TYP.
R0.530 TYP.
R0.270
0.180 TYP.
1.940
1.940
R1.528
R1.361
0.037
0.250 TYP.
36.7^
82.2^ TYP.
45^ TYP.
0.280
0.390
2.900
3.400
2.900
GEAR INSIDE DIA 1.560 - OUSIDE DIA 1.880
WHOLE DEPTH 0.140, TOOTH THK. 0.071 - 28 TEETH TYP.

Bypass

Almost One Year Ago…

- Late Friday, August 23rd, 2013
- Finishing Webapp Assessment
- Visiting Site in Different Browsers
  - Already Tried: Firefox, Chrome, Opera, & Safari
  - On Deck: Internet Explorer

Bypass

Earlier I Had Found A Reflective XSS Vulnerability

- Page Reflects Injection
- JavaScript Block Before Execute
- Check page rendered within iframe from specific page (“self” != “parent”)

Bypass

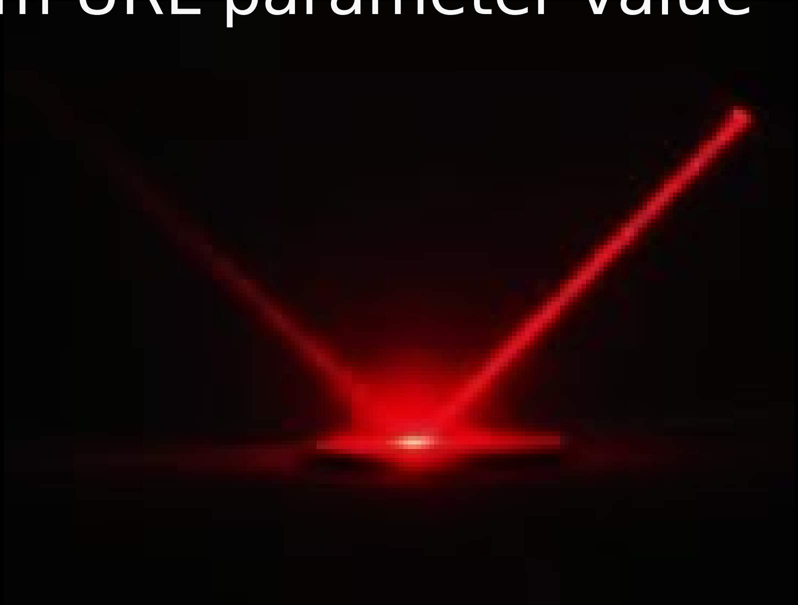
Earlier I Had Found A Reflective XSS Vulnerability

- If:
  - Page not rendered within context of parent page
- Then:
  - JavaScript redirect user to that page
  - Vulnerable page reloaded in iframe without injection

Bypass

Earlier I Had Found A Reflective XSS Vulnerability

Page in iframe defined from URL parameter value



Reflective XSS

1. Attacker sends URL
2. Victim visits URL
3. URL camouflages malicious site within trusted one
4. Attacker gathers input (e.g. victim credentials)

Bypass

Tools From Training

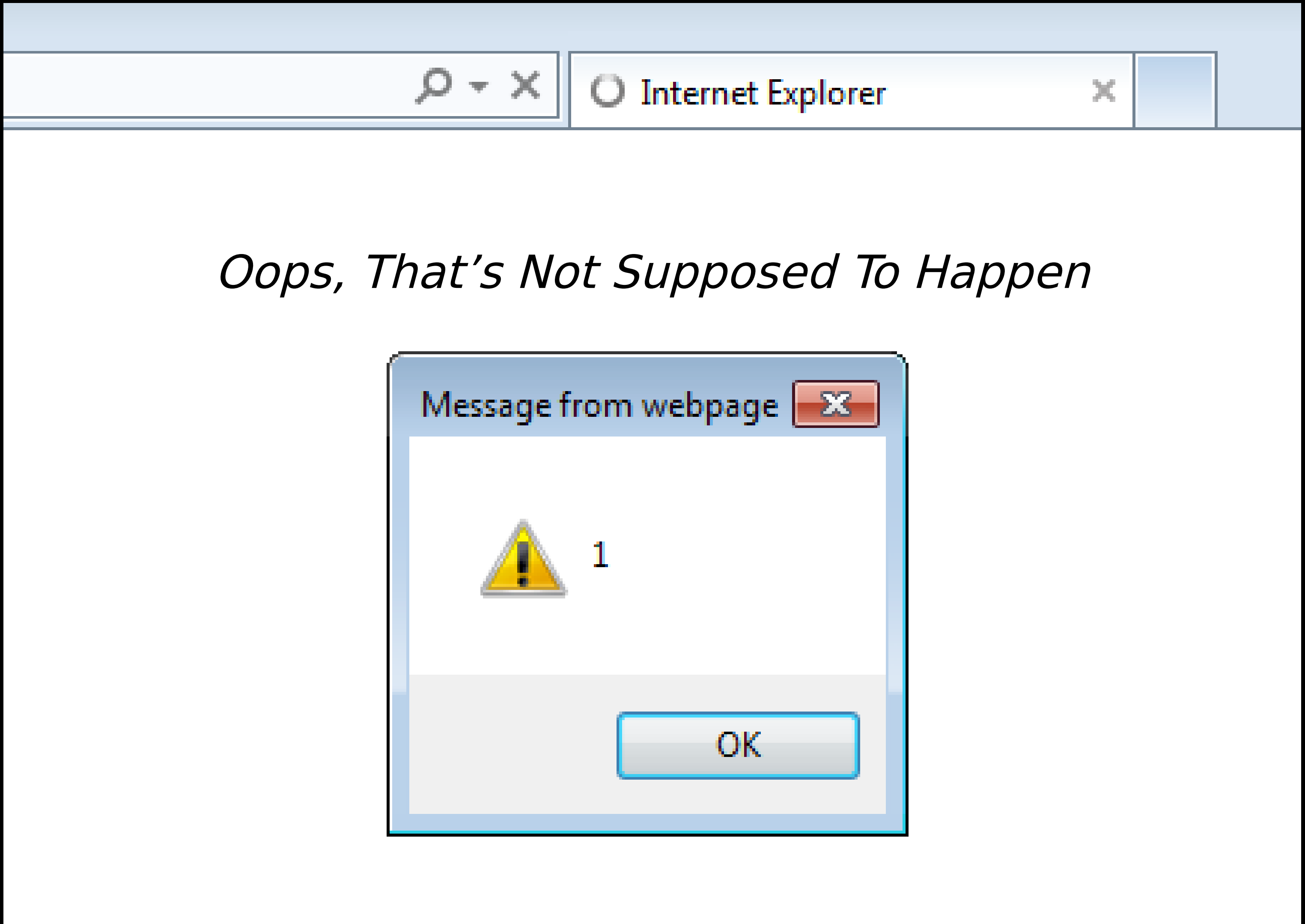
- Vuln initially found with Firefox
- Looked for other browser-specific functionality
- Tested Internet Explorer last
- Decided to poke vuln that looked interesting

Bypass

Tools From Training

- Standard XSS training
  - Hex entities decoded in attribute space
  - ‘param=“value”’ part of html tag
- Try an injection that doesn’t look like <script>alert(1)</script>
- Encode characters, enter injection into IE

Bypass



Oops, That’s Not Supposed To Happen

Message from webpage

1

Bypass

Confirmation & Repeatability

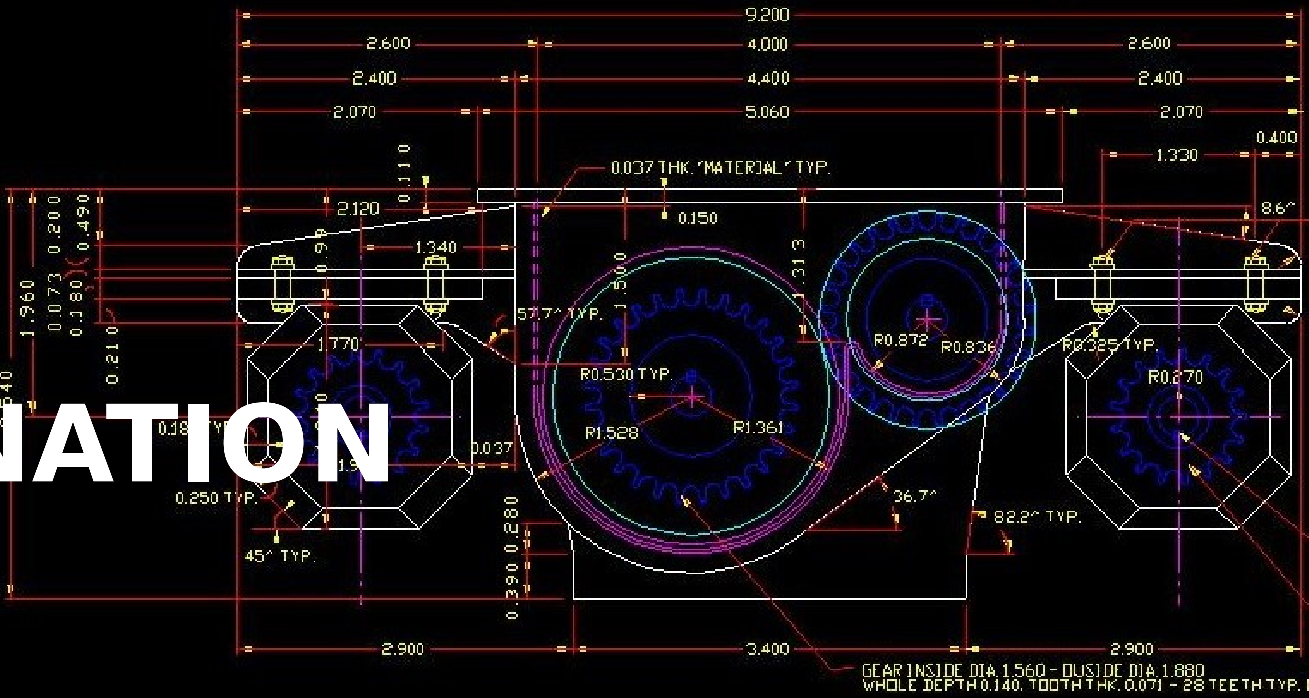
- User Error Was First Thought
  (Setting turned off?)
- Restarted VM, Restarted Computer
- Showed to Coworker
- Sent Report to Management
- Went Home for Weekend

Bypass

Confirmation & Repeatability

- Weekend
  - Built Deliberately Vulnerable PHP
  - Clearly Recreated Bypass
  - Reported to Microsoft: Aug 26, 2013 (Case #15412)
- Response from Microsoft “No Fix”: Oct 4, 2013

EXPLANATION



Explanation

Browser-Defined Trust

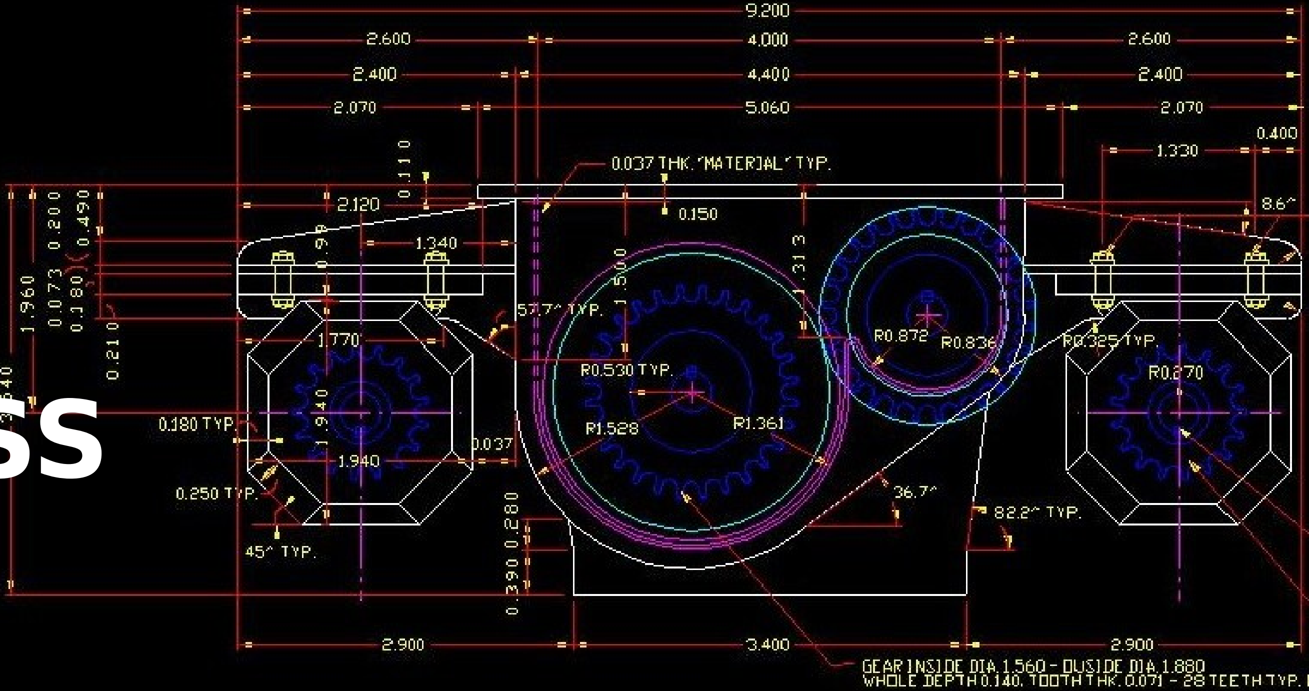
- Abuse Trust, Bypass Filter
- Internet Explorer Trust Decision
  - Filtered Requests
  - Unfiltered Requests

Explanation

How To Abuse The Browser-Defined Trust

- Primary request with injection is made
- Doesn’t cause IMMEDIATE JavaScript code execution
- Secondary request *within the same domain* induced with data from Primary injection
- Secondary request Trusted and Not filtered
- Does cause JavaScript code execution

PROCESS


9.200
2.600
4.000
2.600
2.400
4.400
2.400
2.070
5.060
2.070
0.400
1.330
0.037 THK. 'MATERIAL' TYP.
0.110
2.120
0.150
8.6^
1.340
1.313
1.500
0.99
1.960
0.073
0.200
0.180
0.490
0.210
57.7^ TYP.
1.770
R0.872
R0.836
R0.325 TYP.
R0.530 TYP.
R0.270
3.540
1.940
0.180 TYP.
R1.528
R1.361
0.037
1.940
0.250 TYP.
36.7^
82.2^ TYP.
45^ TYP.
0.280
0.390
2.900
3.400
2.900
GEAR INSIDE DIA 1.560 - OUSIDE DIA 1.880
WHOLE DEPTH 0.140, TOOTH THK. 0.071 - 28 TEETH TYP.

Process

Your Toolkit: Look For

- Iframes, Frames
- Form submissions
- href attributes
- JavaScript Redirects
- Places where both <a> and </a> can be injected

Process

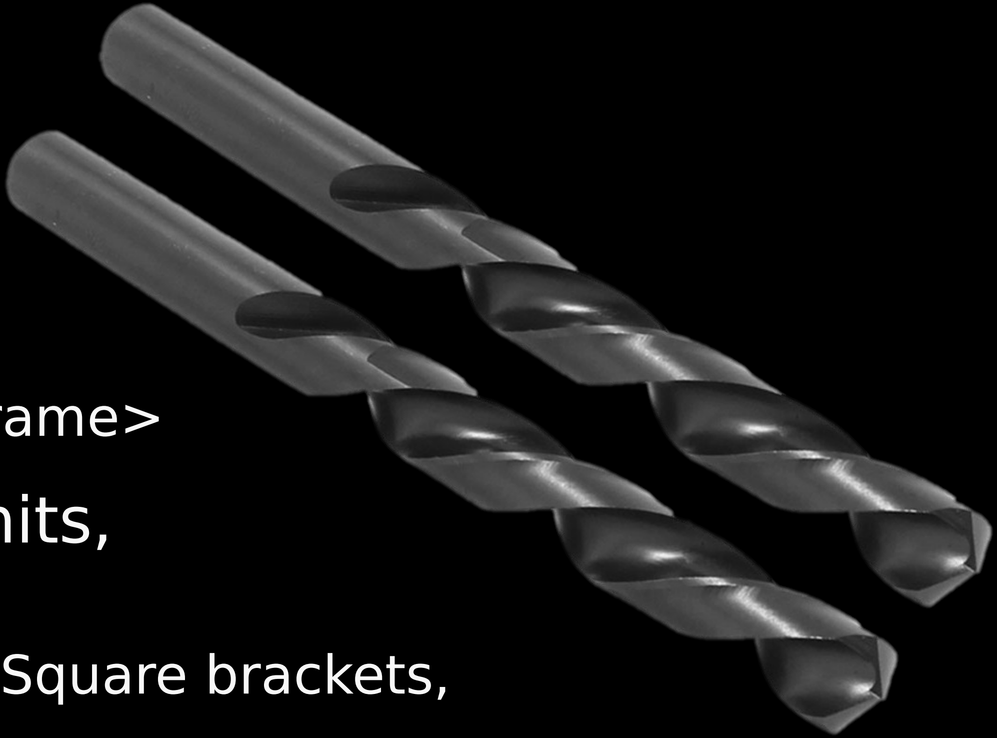
Your Toolkit: Try Using

“This is Not a Drill”

- Hexadecimal: &#xYY;
    - HTML 4.0 Standard- 1998
- Decimal: &#ZZ;
    - HTML 2.0 Standard- 1995
- Named Entity: &ww;
    - HTML 2.0 Standard- 1995
- URL/URI: %VV
    - RFC 1630 - 1994

Process

Your Toolkit: Add This



- Filter doesn’t like
  - . Periods
  - <form> <frame> <iframe>
- Filter sometimes permits, sometimes doesn’t:
  - ( ) [ ] { } Parenthesis, Square brackets, Curly brackets
  - The word “style”

DEMOs

Turning Parts Into An Assembly

end Notes

Microsoft’s “No Fix” Response

- Initially: “Requires special functionality”
  - Category 3 on http://blogs.msdn.com/b/dross/archive/2008/07/03/ie8-xss-filter-design-philosopy-in-depth.aspx
- Later: “Requires user interaction”
  - –Partial Truth
  - –Exceptions

End Notes

Pulling It All Together

- Website up for at least the next week
  - Please don’t break (unless you tell me first)
- PHP code can be downloaded from GitHub
  - https://github.com/RTWaysea/ie-xss-filter-bypass

Questions?

Thank You BSides Las Vegas