TRACE:

What is it good for?

This Talk is Really a Story

Code, Laughs, Tears, and Lessons Learned

NIKTO

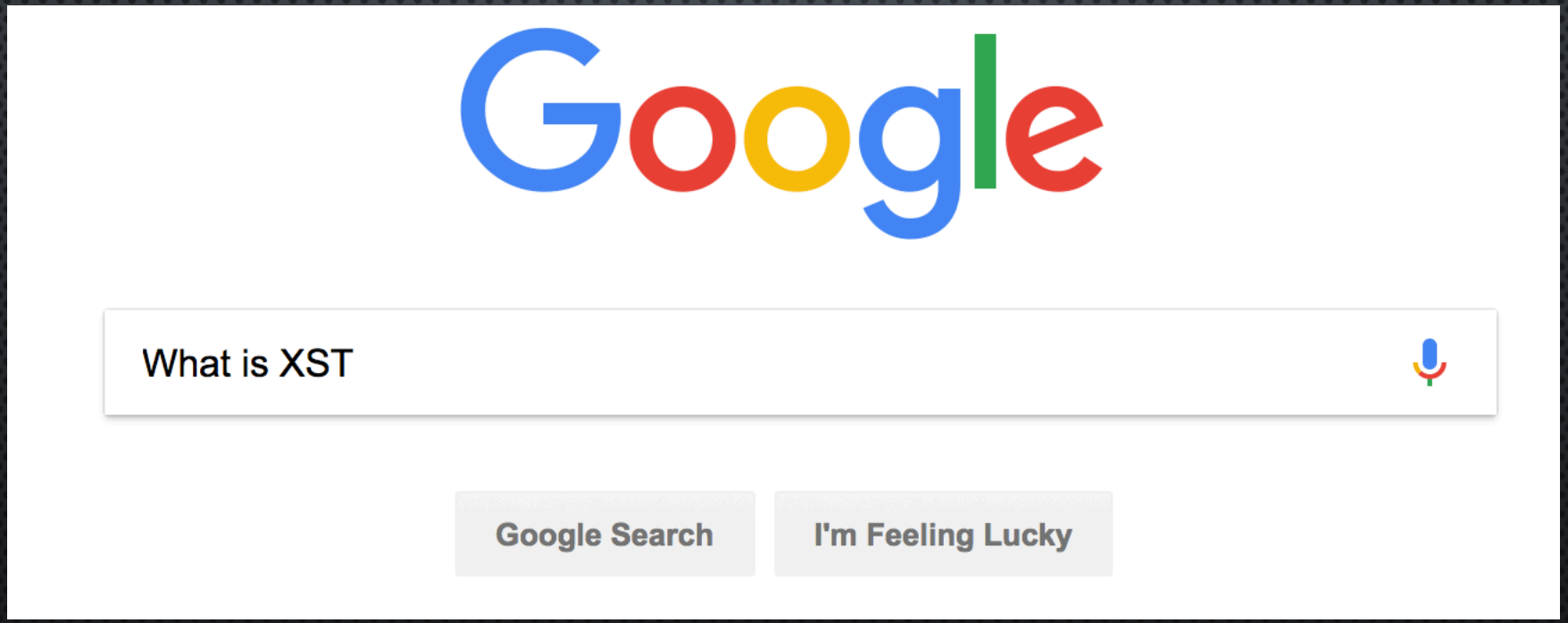
+ Server: Apache/2.4.10 (Debian)
+ Retrieved x-powered-by header: PHP/7.0.24
+ The anti-clickjacking X-Frame-Options header is not present.
+ Cookie PHPSESSID created without the httponly flag
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details. OSVDB-3093: /db.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ /login.php: Admin login page/section found.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

WHAT IS XST ???

Things I've heard of

- XSS – Cross-Site Scripting
- CSRF – Cross-Site Request Forgery
- Yep – That's it. No XST

LET THE LEARNING BEGIN



IT ALL STARTS WITH TRACE

- TRACE is an HTTP request method
- Was designed for Debugging
  - The start of all Tech Gone Wrong Talks
- Echoes the request exactly as received

THAT MAKES SENSE

Request

Raw | Params | Headers | Hex

```
TRACE / HTTP/1.1
Host: 192.168.21.130
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
10.13; rv:56.0) Gecko/20100101 Firefox/56.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=51a96c3d3f2183528878c97b28625745
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Mon, 06 Nov 2017 23:53:28 GMT
Server: Apache/2.4.10 (Debian)
Connection: close
Content-Type: message/http
Content-Length: 403

TRACE / HTTP/1.1
Host: 192.168.21.130
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
10.13; rv:56.0) Gecko/20100101 Firefox/56.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=51a96c3d3f2183528878c97b28625745
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

So what is XST ?

- XST – Cross-Site Tracing (or Tracking … more on that later)
- First outlined in white paper by Jeremiah Grossman
- OWASP – combination of XSS and TRACE
  - This seems silly
    - I have XSS what does XST give me

COOKIES

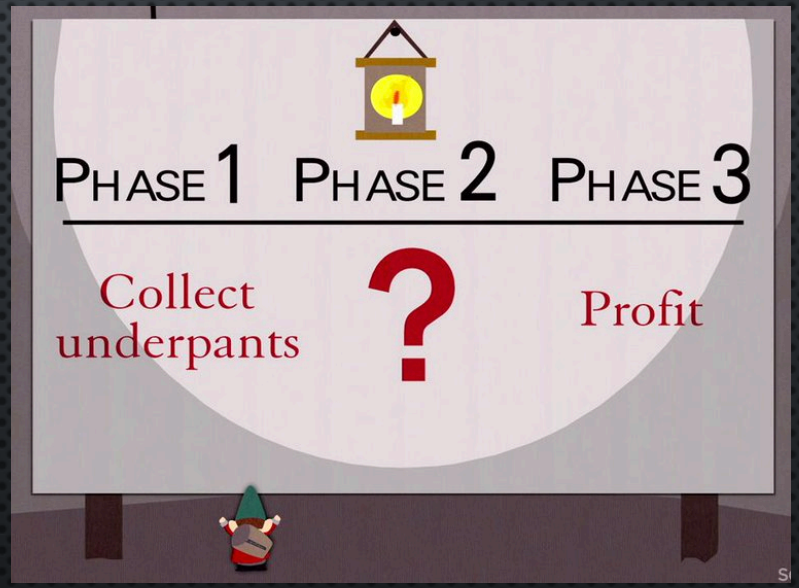
- HTTP is Stateless
- HTTP Header added to every request
  - Tracked and added by the browser
- Used to track state
  - And much more, but that's another talk

But document.cookie ?

- Ahh, but what about httponly flag
  - Introduced in 2002
  - Prevents JavaScript from accessing cookie value
  - Whole reason for XST

SESSION HIJACKING

- DETERMINE WHAT SITES USE COOKIES FOR SESSION TRACKING
- DETERMINE IF TARGET USER IS AUTHENTICATED TO THE SITE
- STEAL COOKIE
- ???
- PROFIT



COOKIE STEALING 101

```
var xhr = new XMLHttpRequest();
xhr.open("TRACE", "http://bank.com", false);
xhr.send();
alert(xhr.responseText);
```

I know this won't work, but it did at one time

Why no working?

- CORS – Cross Origin Resource Sharing
  - Prevents XHR requests to foreign URLs
- The async flag must be true
- But, we rely on the browser to enforce all this

DEMO TIME

But wait

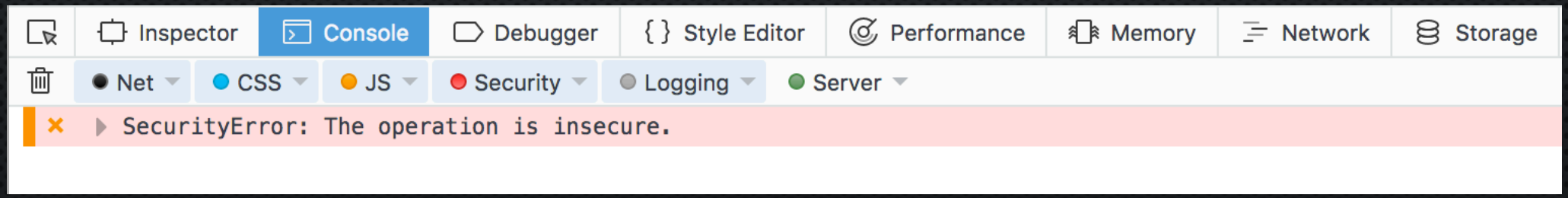
There's more

More than cookies?

- Yep
- Gives visibility to anything in the header
- What else is in header?
  - HTTP Basic Authentication
    - Surely you jest?
    - Nope, I still see this

AND THIS ALL STILL WORKS?

- NOPE
- CORS STOPS REQUESTS TO OTHER SITES
- BROWSERS BLOCK ALL TRACE REQUESTS AS INSECURE



So you wasted our time?

- Yep
- Thanks for playing

Really ???

- No, of course not
- Still very useful
  - Think on original purpose
  - What might be in between us and the APP?
    - WAF – Web App Firewall
    - Load Balancer

DEMO TIME

ANY QUESTIONS?

Cross-site tracking

- Exactly as discussed
- Microsoft likes to be different
- TRACK method is only for IIS servers

THANK YOU

Joshua Barone

@tygarsai

https://github.com/jbarone/xstlab

SANS SECURITY EAST 2018 (JAN 8 -13)

- https://www.sans.org/event/security-east-2018
- Lots of classes
  - Network Security
  - Pen Testing
  - DFIR
  - Dev
  - Management
- Netwars – Huge CTF game
  - Core
  - DFIR
- Community Night (Jan 10th)
  - Free networking event
  - Free @Night talks