Stanford Applied Cyber

Intro Security Workshop

Cooper de Nicola, Aditya Saligrama

The Language of the Web

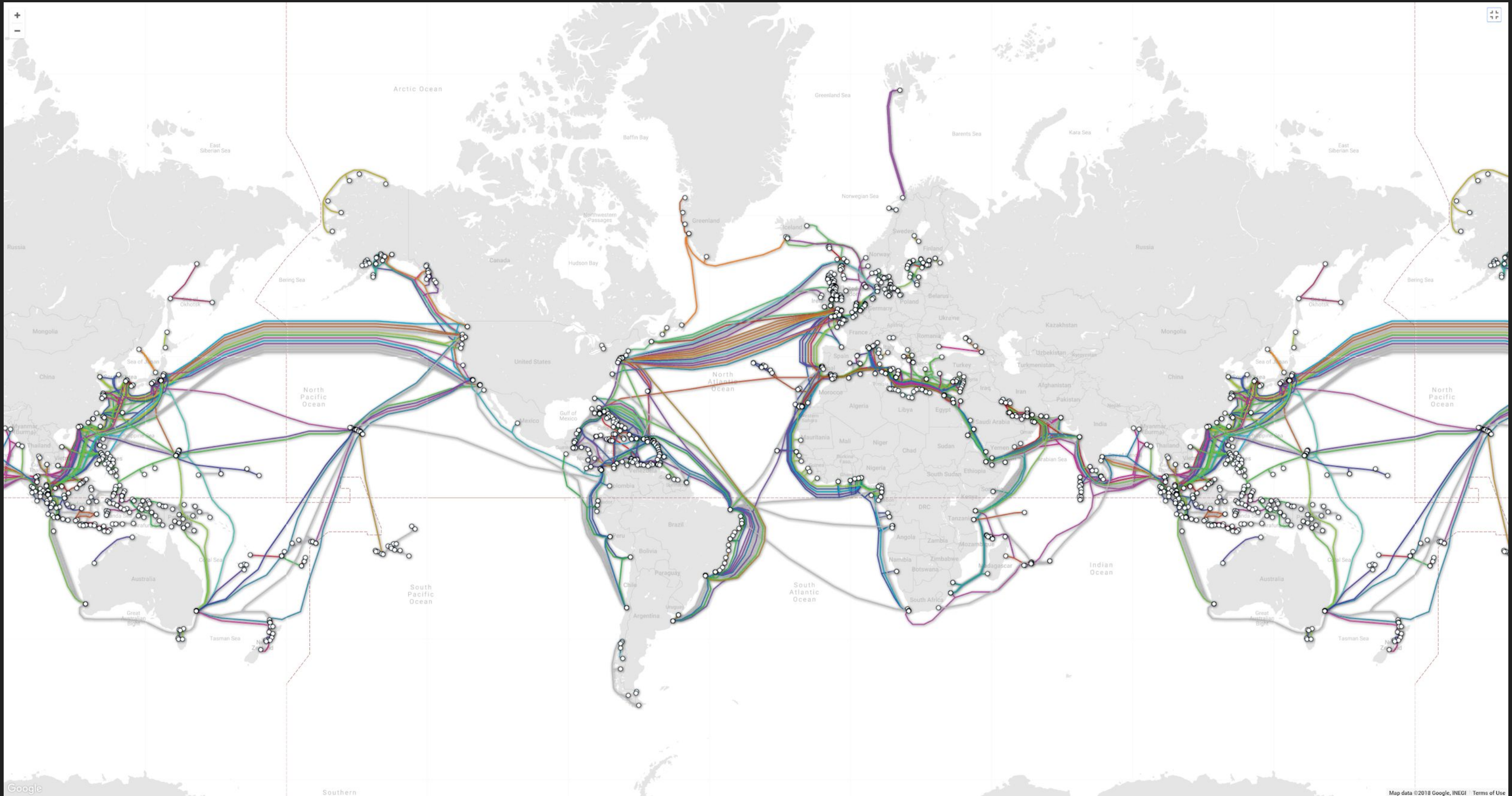
What language does the web speak?

```
<body style="margin: 0
<div i
<h
```

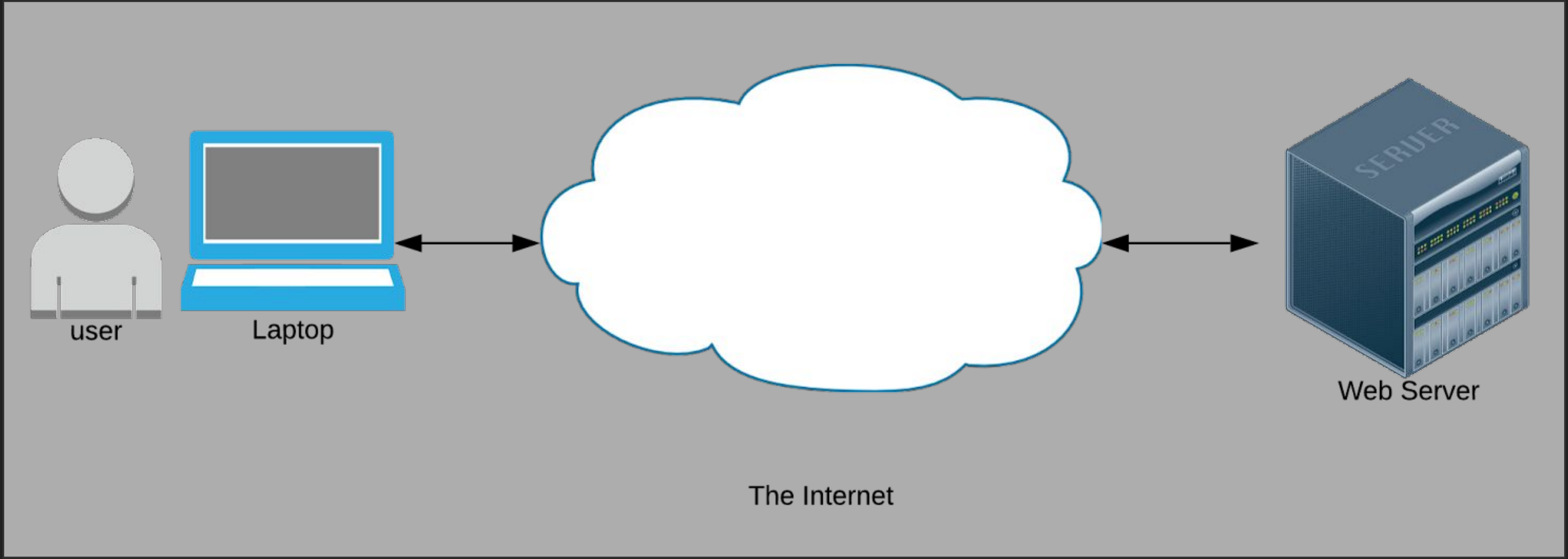
```
.screen-reader-text:hover,
.screen-reader-text:active,
.screen-reader-text:focus {
    background-color: #f1f1f1;
    border-radius: 3px;
    box-shadow: 0 0 2px 2px rgba(0, 0, 0, 0.6);
olbar. */
```

```
<link rel="stylesheet" href="http://localhost/css.css" type="text/css">
<script type="text/javascript" src="http://localhost/javascript.js"></script>
<script type="text/javascript">
(function(){
  onLoaded: function(request) {
    if (request.name == 'log_error') return;
    log.trace("Ajax.Request: " + (request.name || request.url.substr(0, 30
    )) + "...");

  },
  onComplete: function(request) {
    if (request.name == 'log_error') return;

  },
  onException: function(request, e) {
    if (request.name == 'log_error') return;
    log.fatal(request.url + ' : ' + e.name + ' | ' + e.message + ' | ' +
    .stack);
```

How does the Internet Work?



Our Internet Abstraction



How do websites work?

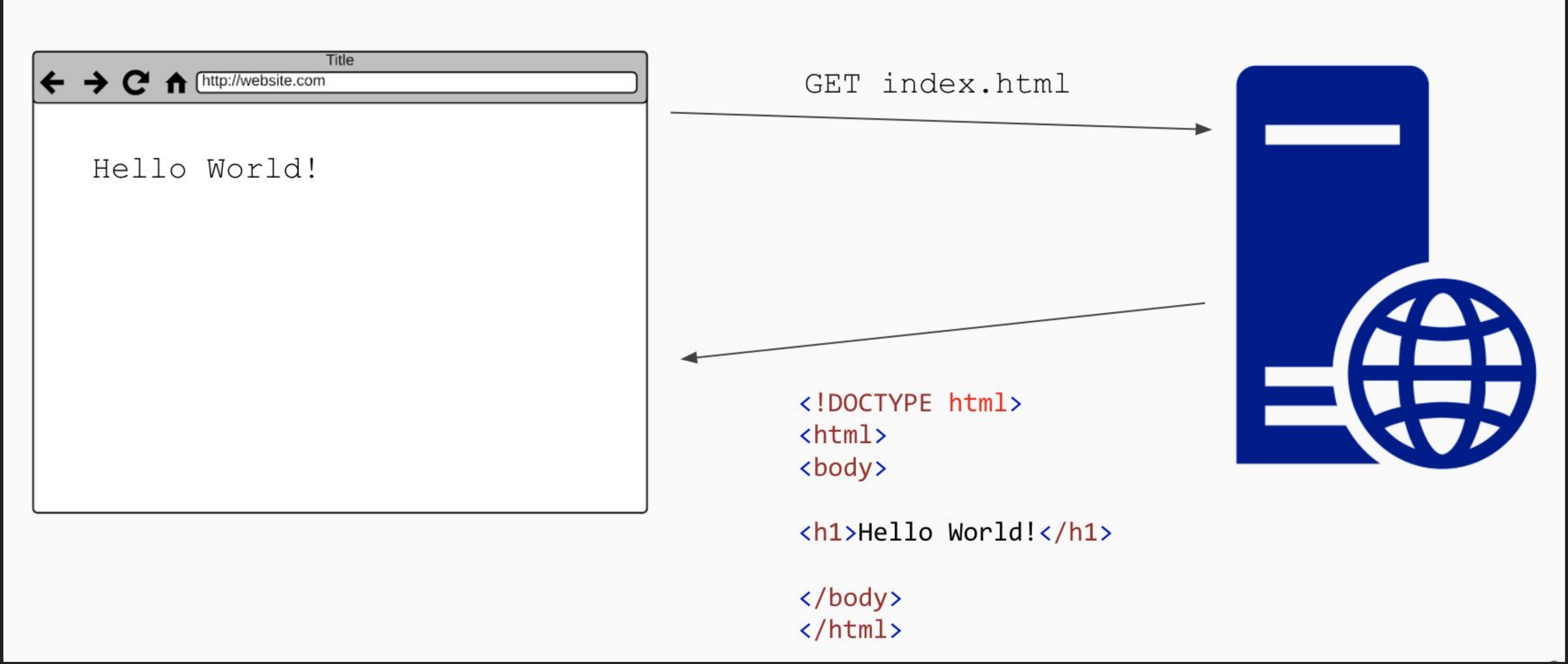
HACKERS BRIEFLY TOOK DOWN THE WEBSITE OF THE CIA YESTERDAY...
WHAT PEOPLE HEAR:
SOMEONE HACKED INTO THE COMPUTERS OF THE *CIA*!!
WHAT COMPUTER EXPERTS HEAR:
SOMEONE TORE DOWN A POSTER HUNG UP BY THE *CIA*!!

How do we communicate with a web server?

HTTP

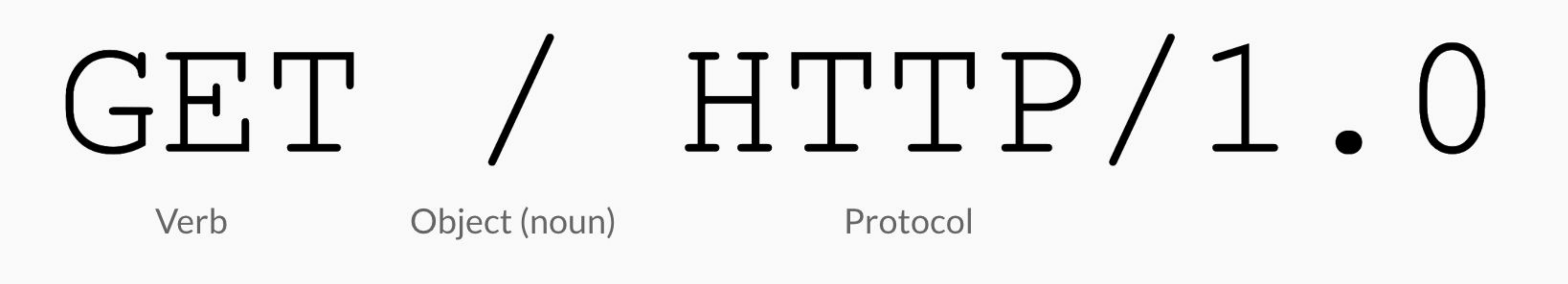
Hypertext Transport Protocol

HTTP: the missing language of the web



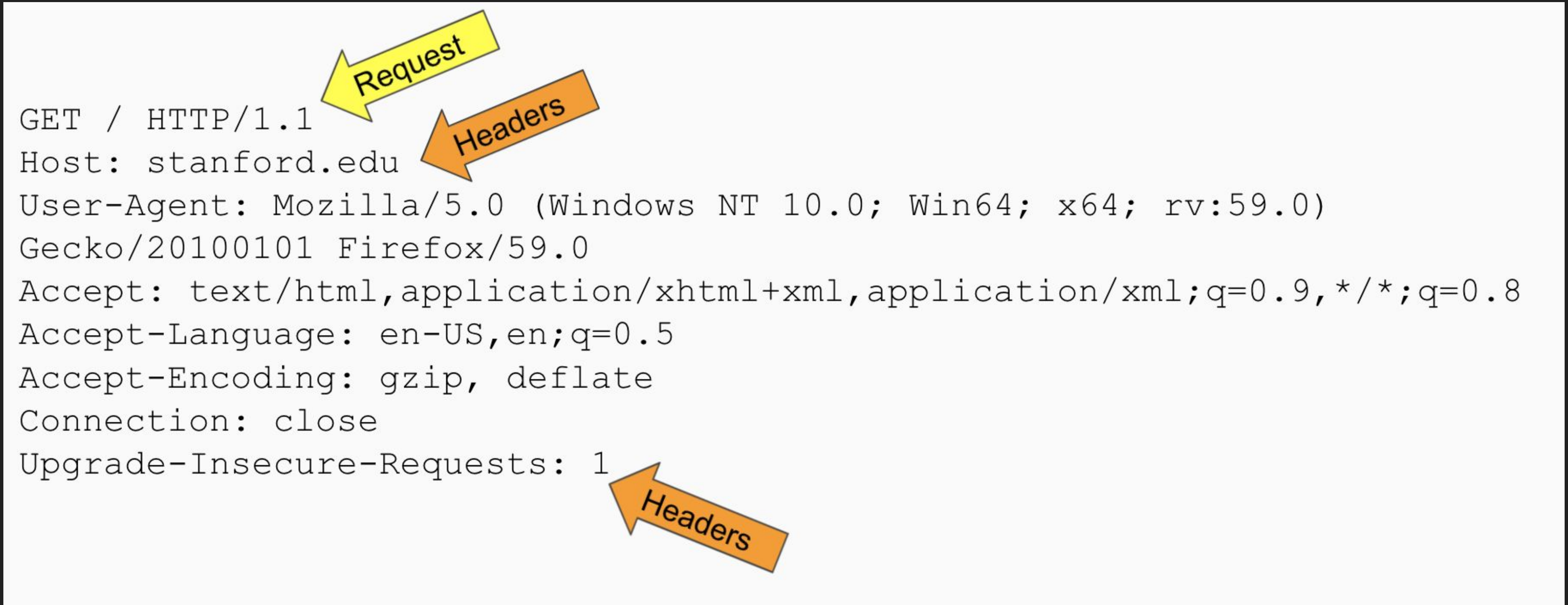
```
<!DOCTYPE html>
<html>
<body>

<h1>Hello World!</h1>

</body>
</html>
```

HTTP protocol



```
GET / HTTP/1.0
```

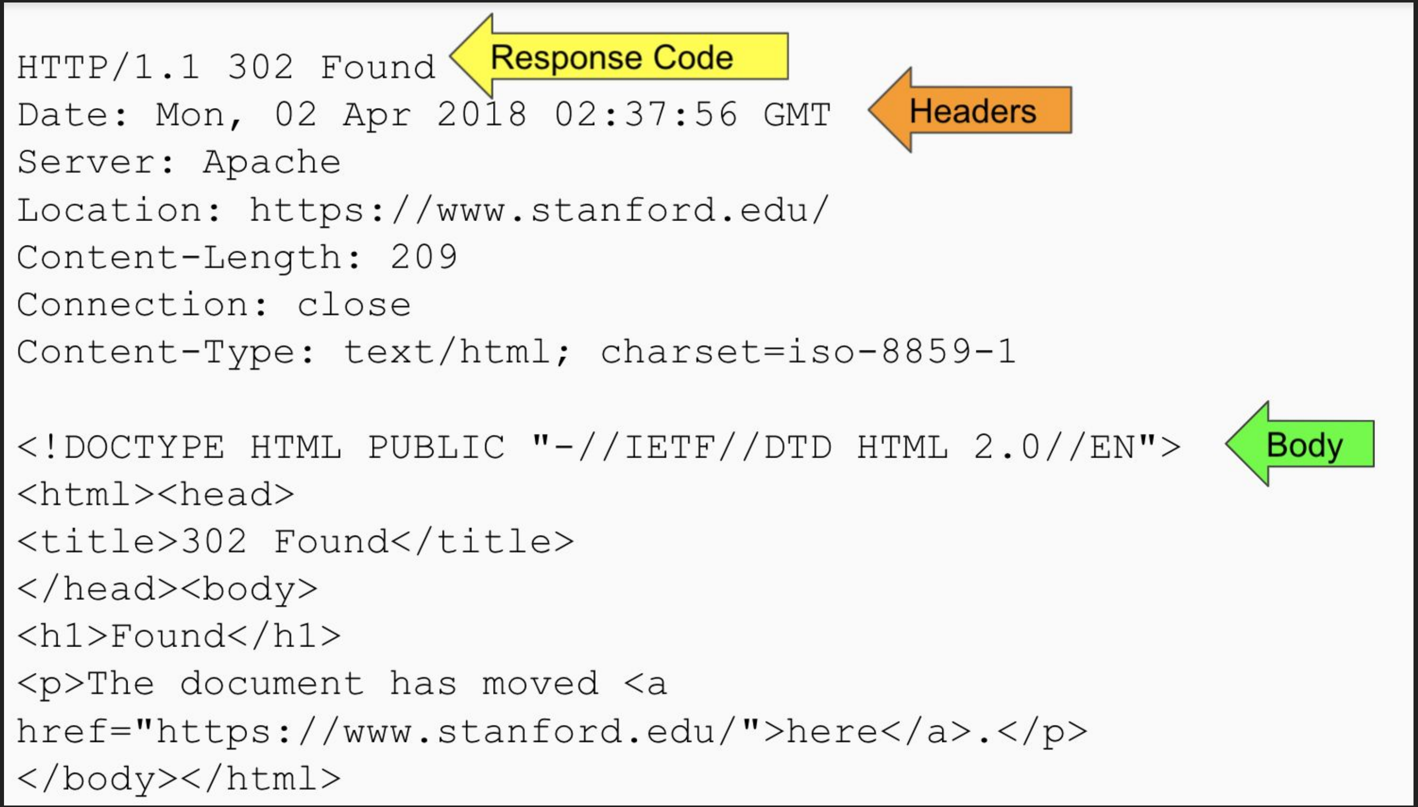
HTTP REQUEST



```
GET / HTTP/1.1
Host: stanford.edu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
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
Connection: close
Upgrade-Insecure-Requests: 1
```

Request
Headers
Headers

HTTP RESPONSE



```
HTTP/1.1 302 Found
Date: Mon, 02 Apr 2018 02:37:56 GMT
Server: Apache
Location: https://www.stanford.edu/
Content-Length: 209
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a
href="https://www.stanford.edu/">here</a>.</p>
</body></html>
```

Response Code
Headers
Body

HTTP Requests: GET and POST

GET — The GET method requests a specified resource.

Requests using GET should only retrieve data.

POST — The POST method is used to submit data to the specified resource.

This often causes changes in state or side effects on the server.

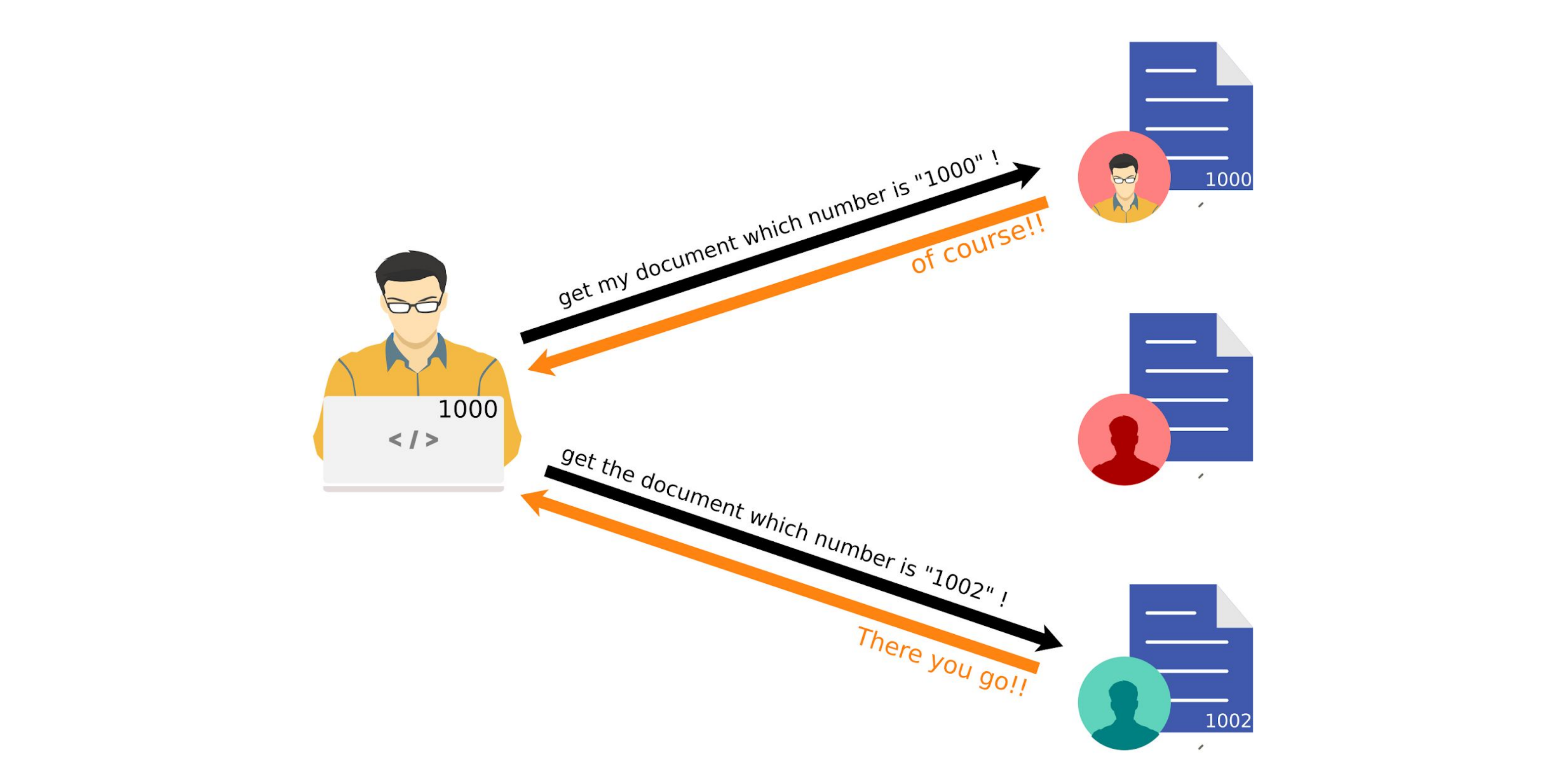
CatShare

We're a real startup!

Vulnerabilities

- IDOR
- XSS
- Improper Session Handling

Insecure Direct Object Reference (IDOR)


1000
< / >
get my document which number is "1000" !
of course!!
1000
get the document which number is "1002" !
There you go!!
1002

IDOR Case Study

70TB of user content leaked

IDOR

Why did this happen?

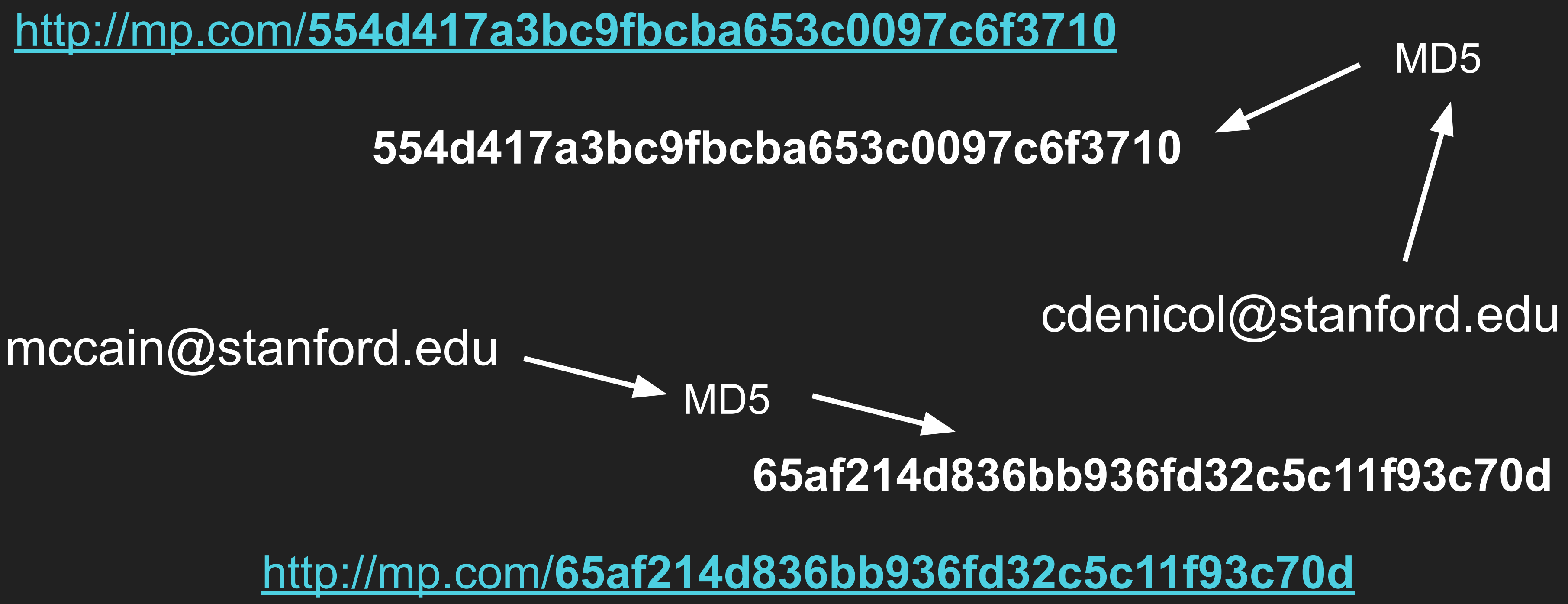
- Poor Engineering, Lack of Testing

Source: https://cybernews.com/news/70tb-of-parler-users-messages-videos-and-posts-leaked-by-security-researchers/

TRY IT!

- This AC team has a website http://catshare.saligrama.io/ that we want to store our personal information on
- We make a new endpoint http://catshare.saligrama.io/user to access this info
- Ex: http://catshare.saligrama.io/user?id=test
- We say that this is secure and only accessible to admins. Show us otherwise

Story Time with Cooper! Stanford Marriage Pact



http://mp.com/**554d417a3bc9fbcba653c0097c6f3710**

MD5

554d417a3bc9fbcba653c0097c6f3710

cdenicol@stanford.edu

mccain@stanford.edu

MD5

65af214d836bb936fd32c5c11f93c70d

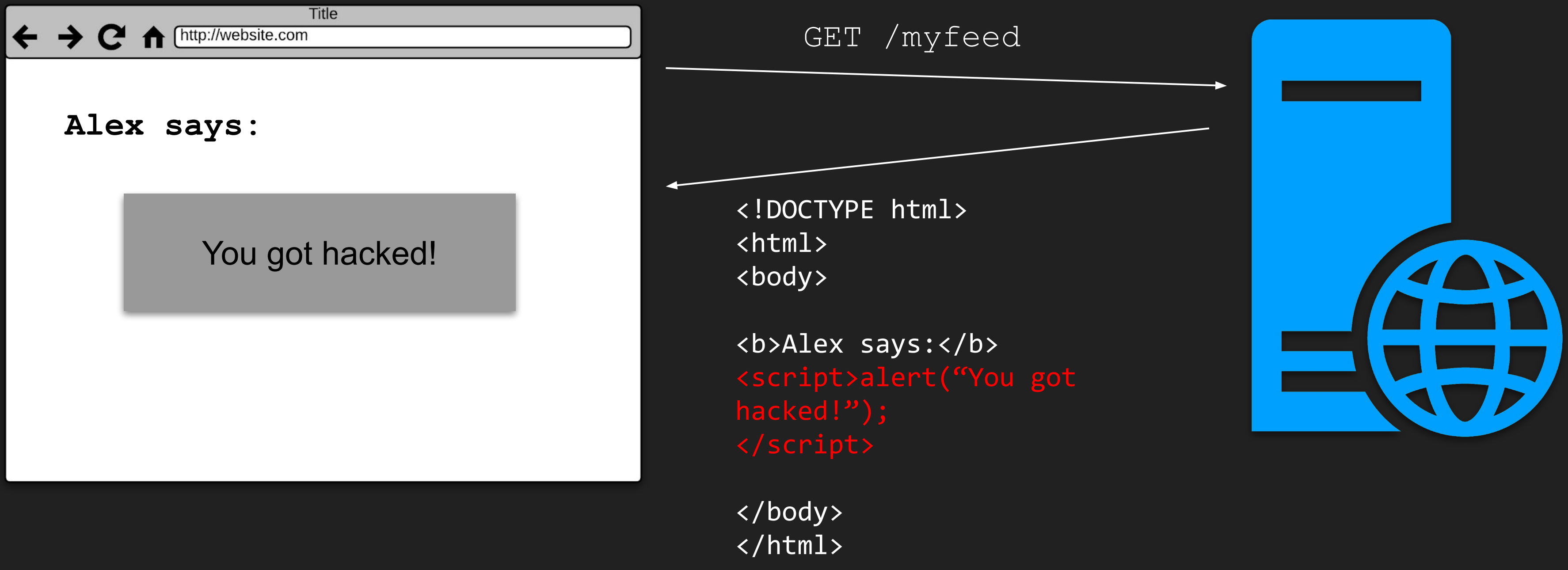
http://mp.com/**65af214d836bb936fd32c5c11f93c70d**

Cross Site Scripting (XSS)

XSS attacks enable attackers to **run JavaScript code** on your website for other users

They occur when **user input is not properly sanitized and displayed**, allowing it to execute as code

XSS



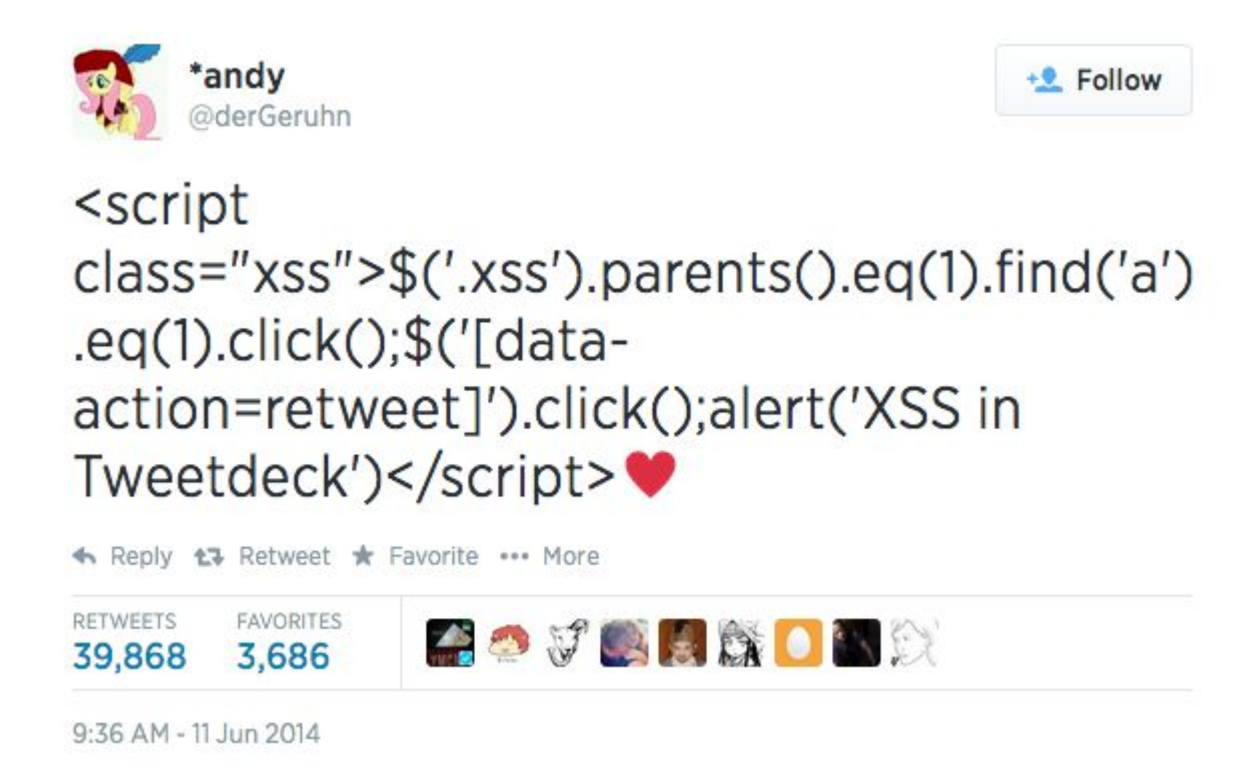
Alex says:

You got hacked!

GET /myfeed

```
<!DOCTYPE html>
<html>
<body>

<b>Alex says:</b>
<script>alert("You got
hacked!");
</script>

</body>
</html>
```

XSS on Tweetdeck



*andy
@derGeruhn

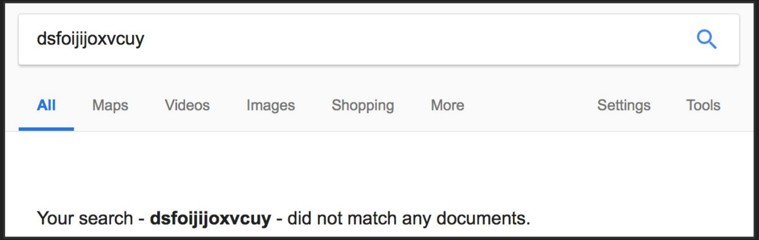
<script class="xss">$('.xss').parents().eq(1).find('a').eq(1).click();$('[data-action=retweet]').click();alert('XSS in Tweetdeck')</script>❤

RETWEETS 39,868

FAVORITES 3,686

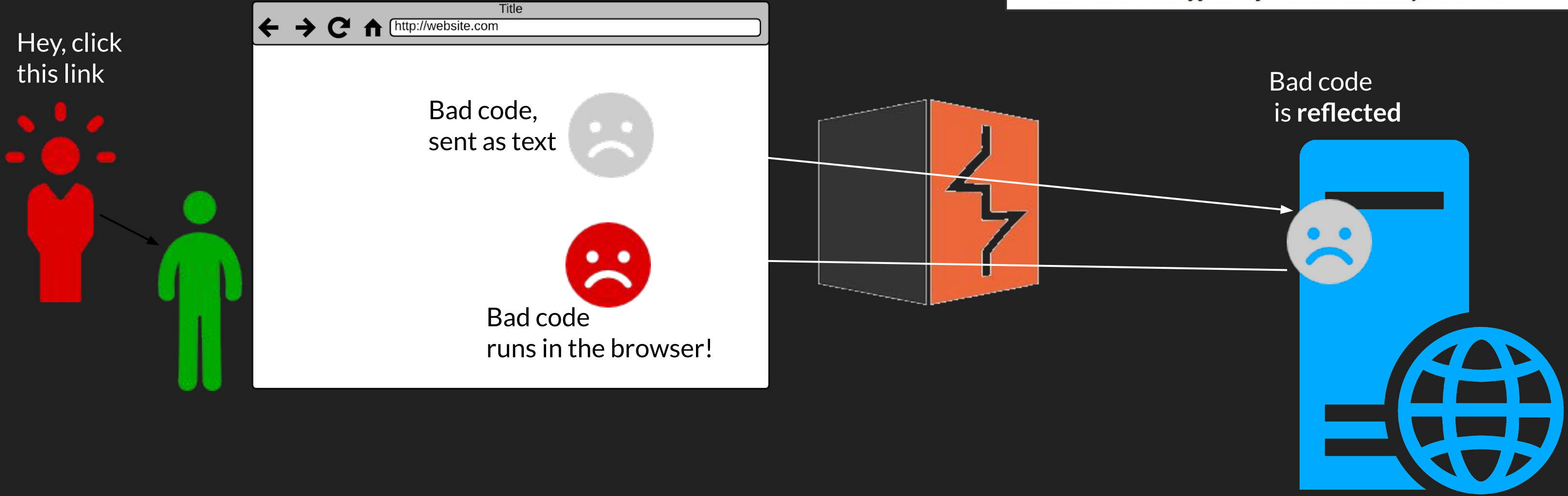
9:36 AM - 11 Jun 2014

Reflected XSS

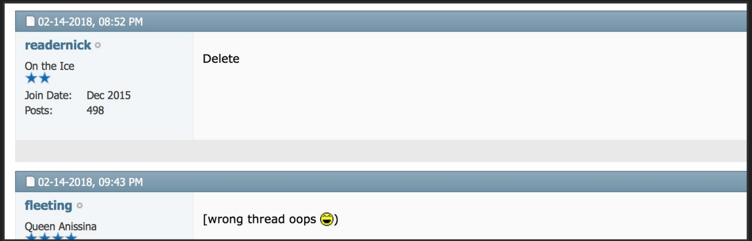


dsfoijijoxvcuy

Your search - **dsfoijijoxvcuy** - did not match any documents.



Stored XSS



02-14-2018, 08:52 PM

readernick

On the Ice

★★

Join Date: Dec 2015

Posts: 498

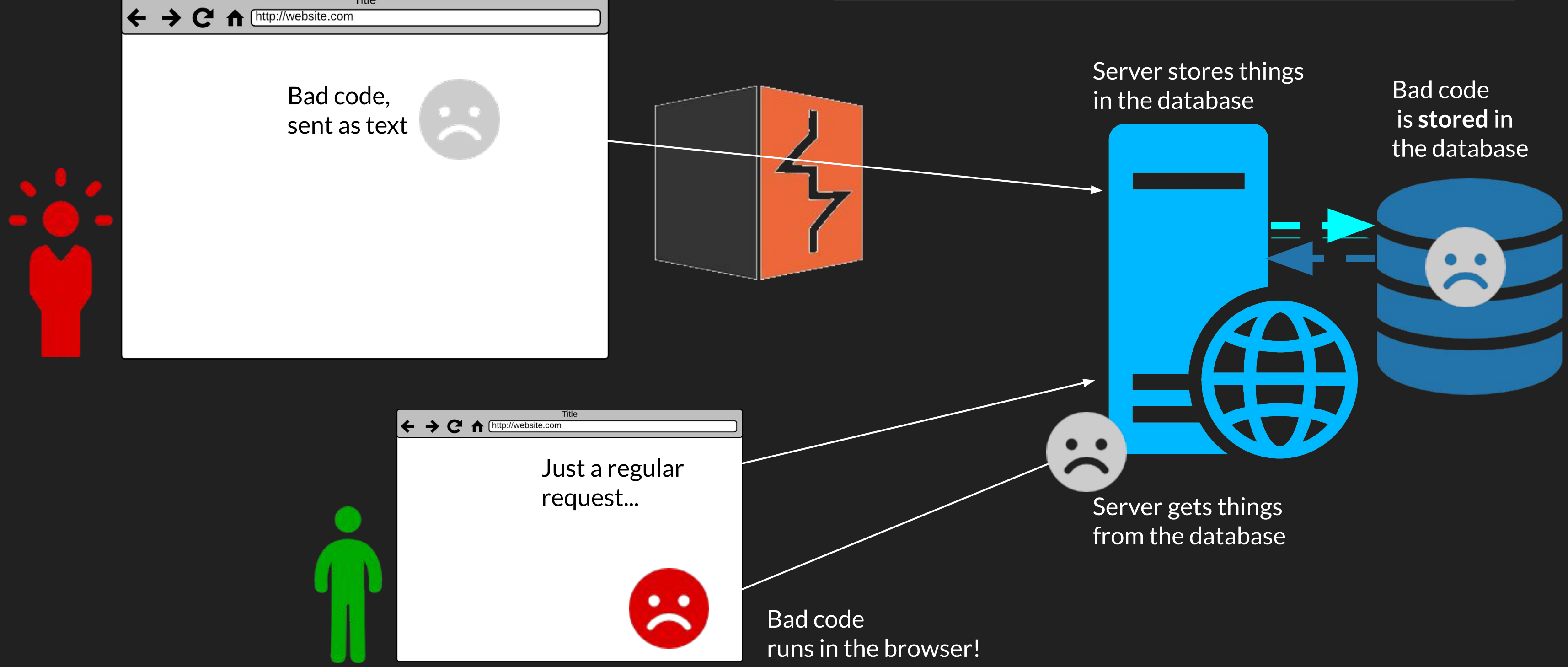
Delete

02-14-2018, 09:43 PM

fleeting

Queen Anissina

[wrong thread oops 😁)



Bad code,
sent as text

Server stores things
in the database

Bad code
is **stored** in
the database

Just a regular
request...

Server gets things
from the database

Bad code
runs in the browser!

www.yourwebsite.com/law/<?StealAllTheData.js>/supersecretdata

TRY IT!

- After our last data breach, us at http://catshare.saligrama.io/ want to make our customers feel like we care about them
- We added an endpoint http://catshare.saligrama.io/hello that takes a user’s name and greets them kindly. Ya’ know, to show we care
- Ex: http://catshare.saligrama.io/hello?name=User1
- We think this is harmless and will only build customer trust. Show us our mistake.

Improper Session Handling

- We have added an admin view to http://catshare.saligrama.io/login for admins to view user data
- One set of credentials is cooper:cooper
- Can you become admin and view the user data?

Mitigating Risk as a startup

Vulnerability Disclosure Policy

Let ethical hackers make your technology safer!

A vulnerability disclosure policy is intended to give ethical hackers clear guidelines for submitting potentially unknown and harmful security vulnerabilities to organizations.

Vulnerability Disclosure Policy Resources

DHS Template: https://cyber.dhs.gov/bod/20-01/vdp-template/

DoJ Framework: https://www.justice.gov/criminal-ccips/page/file/983996/download

HackerOne: https://www.hackerone.com/blog/What-Vulnerability-Disclosure-Policy-and-Why-You-Need-One

Example Safe Harbor: https://github.com/cybertransparency/vdp-terms

Credits

Source Code for Vulnerable Web App

https://github.com/cdenicola/CS106S-VulnerabilityExample

Sources

- Hack Lab INTLPOL 268 — (Alex Stamos, Jack Cable)
- Security Conference Presentation — (Maya Ziv, Cooper de Nicola)
- CatShare — (Cooper de Nicola, Aditya Saligrama, George Hosono)