how do I shot web

by @patil215

browsers have 4 exploitable parts

1. server-side code
2. client-side code
3. browser
4. user

CTFs focus on the first two

clients can be tricked into running things that shouldn't be run

servers can be manipulated into showing us things we shouldn't be able to see

PHP, Java, Python are server languages
HTML are basic blocks shown by browser
CSS makes things look pretty
Javascript makes browser do fancy things

how do we see these? (demo)

how do the client and server talk?

HTTP / HTTPS is the most common protocol

HTTP GET typically asks for information
HTTP POST typically sends information

what happens searching google.com?

1. browser does DNS lookup
2. browser sends GET to google.com
3. Google's servers process request
4. Google sends back webpage
5. browser renders webpage

what happens when logging in?

1. browser gets credentials entered into form
2. browser sends POST with credentials
3. server receives credentials and checks them
4. if good, server sends logged in page
5. if bad, server sends failure page

can I mess with PHP? not easily

can I mess with Javascript? yes (demo)

Never validate input on the client.
(demo)

how does Google remember I'm logged in?

Answer: cookies. (demo)

how does the server check my credentials?

often, using SQL

```
<?php
$user = $_POST['user'];
$pass = $_POST['password'];
$query  = "SELECT * FROM products
        WHERE username=$user and
     password=$pass;";
$result = pg_query($conn, $query);
?>
```

why is this bad? (demo)

how do I find hidden files on a server?

- Dirbuster (demo)
- robots.txt

cross-site scripting (XSS)

making someone else's client run code

Other attacks

- timing
- local file inclusion
- phishing
- OWASP top 10