OWASP
The Open Web Application Security Project

Security implications of the Cross-Origin Resource Sharing

Gergely Revay
http://gerionsecurity.com
@geri_revay

Disclaimer

OWASP
The Open Web Application Security Project

This presentation is purely my opinion and not related to SIEMENS.

https://c1.staticflickr.com/1/21/27423135_082e7b5983.jpg

The Game

Agenda

OWASP
The Open Web Application Security Project

- What is CORS ?
- Pre-C !S solutions
- Attac"er model
- What's the problem?
- Attac" Scenarios
- Solution
- Demo

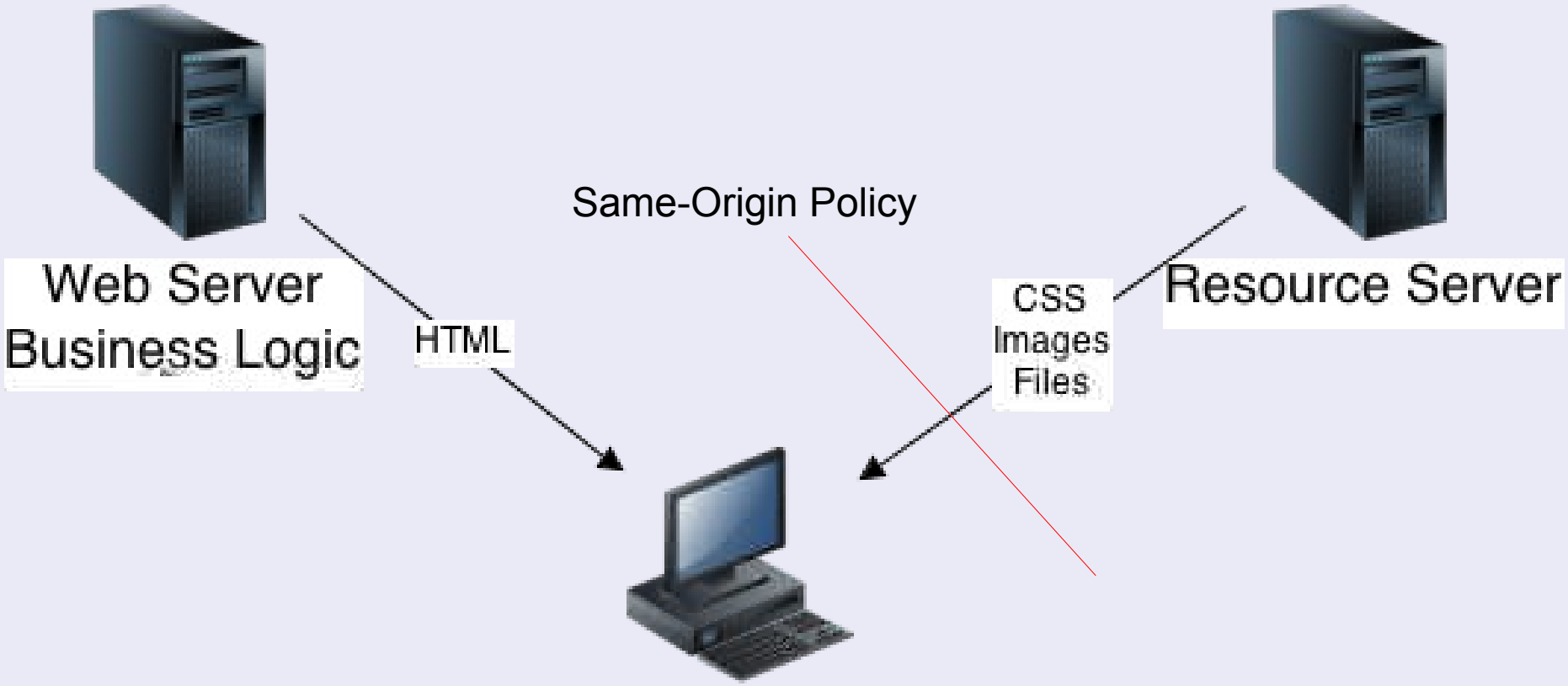
) hat is C !S

OWASP
The Open Web Application Security Project

- Cross- rigin !esource Sharing
- #TM$% &eature
- 'ml#TTP!e(uest
- $oad content &rom another domain on the client-side

) hat is C !S

OWASP
The Open Web Application Security Project



Pre-C !S

OWASP
The Open Web Application Security Project

- Many di&&erent hac"s
- Pro*y in same-origin
- +S N-P

HTML code:

Response Content:

#o , C !S , or"s-

OWASP
The Open Web Application Security Project

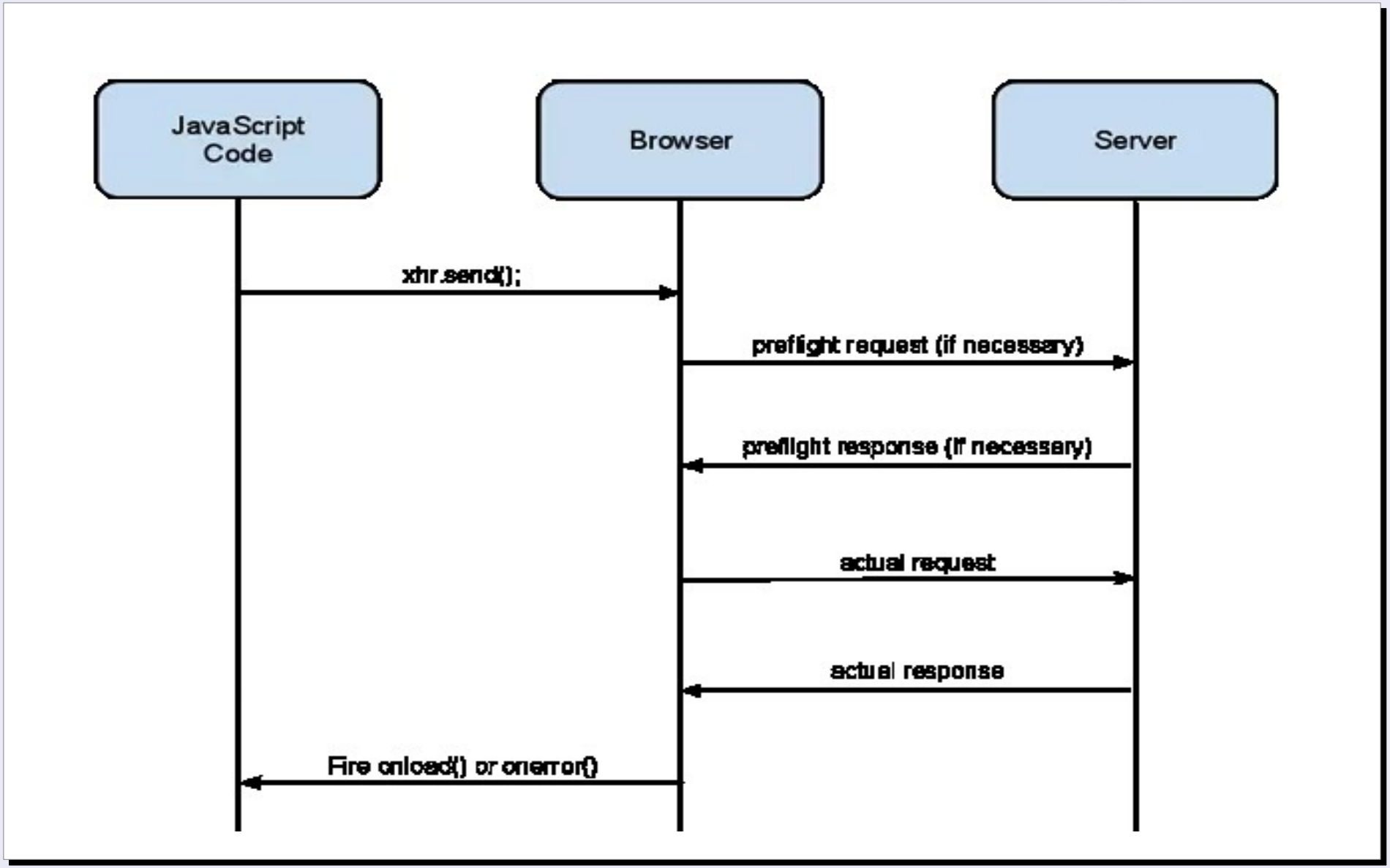
- . di&&erent re(uest types/
  - Simple re(uest
  - Not simple re(uest
- 0ro , ser ma"es the decision

The tric" 1 simple re(uest

OWASP
The Open Web Application Security Project

- #EAD2GET or P ST
- #eaders/
  - Accept
  - Accept-$anguage
  - Content-$anguage
  - $ast-E3ent-ID
  - Content-Type2 4ut only i& the 3alue is one o&/
    - application5*- , , , -&orm-urlencoded
    - multipart5&orm-data
    - te*t5plain

The tric" 1 N T simple re(



Pre&light e*ample

OWASP
The Open Web Application Security Project

Preflight request:

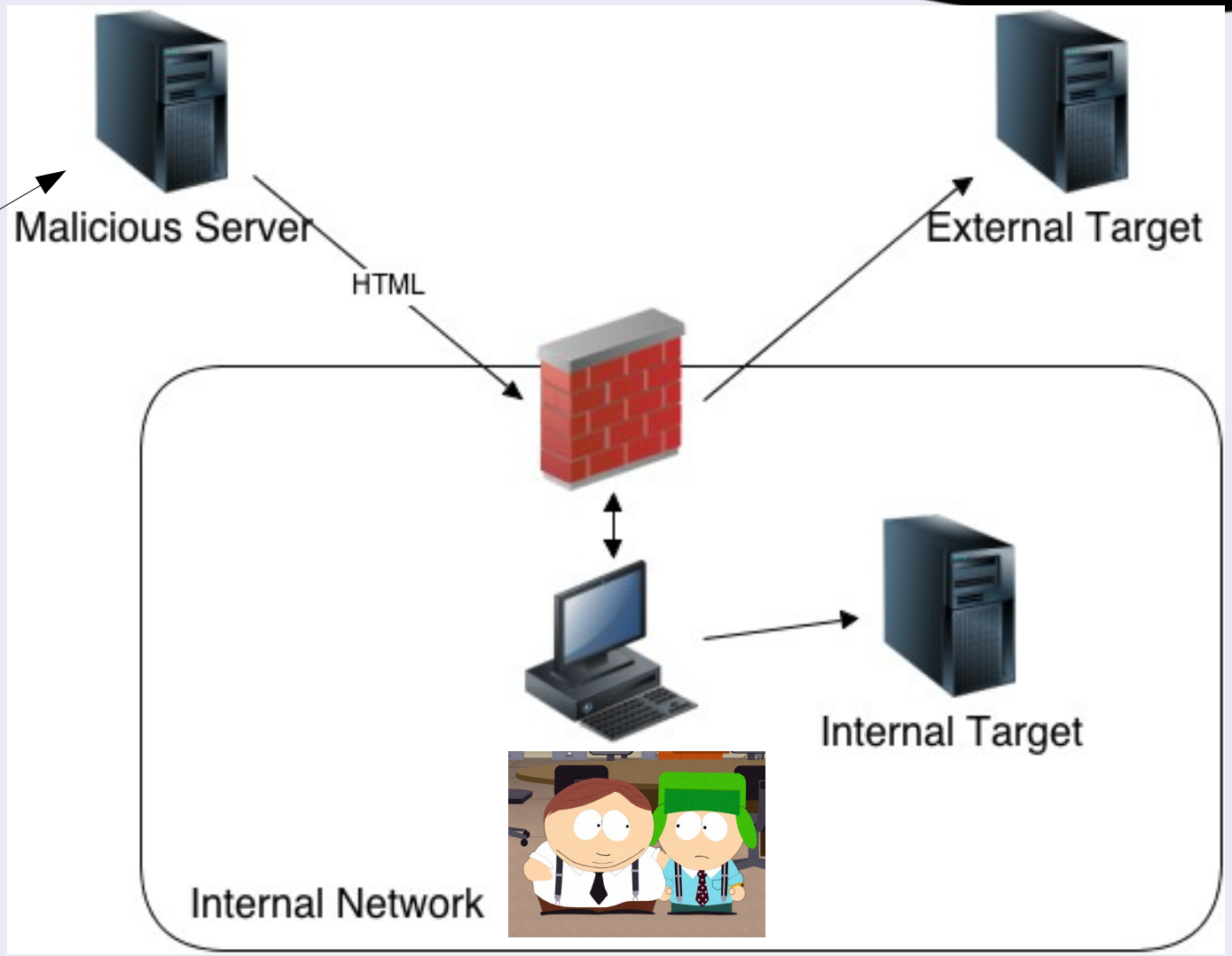
```
OPTIONS /cors HTTP/1.1
Origin: http://api.bob.com
Access-Control-Request-Method: PUT
Access-Control-Request-Headers: X-Custom-Header
Host: api.alice.com
Accept-Language: en-US
Connection: keep-alive
User-Agent: Mozilla/5.0
```

Preflight response:

```
Access-Control-Allow-Origin: http://api.bob.com
Access-Control-Allow-Methods: GET, POST, PUT
Access-Control-Allow-Headers: X-Custom-Header
Content-Type: text/html; charset=utf-8
```

Attac"er Model

Attac"er Model



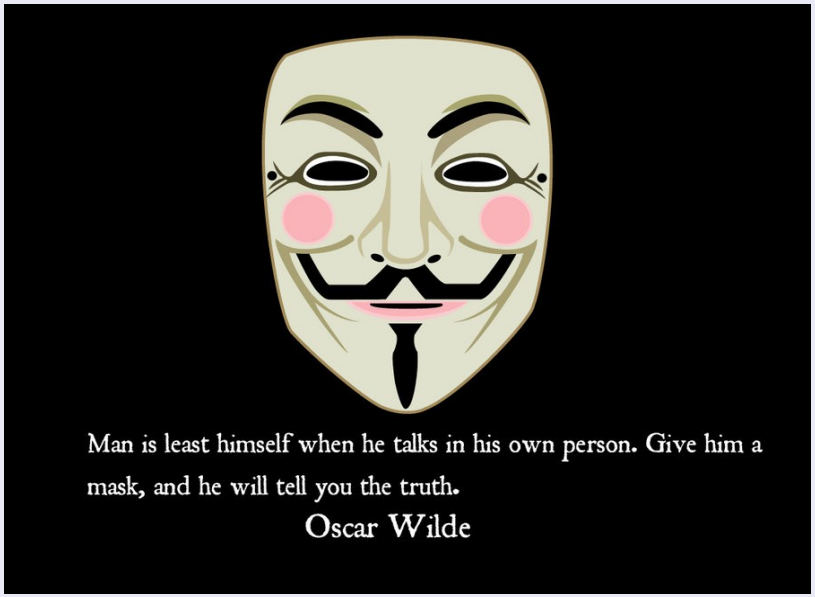
Attac"er Model/ 6no , ledge

OWASP
The Open Web Application Security Project

Does he ha3e internal "no , ledge -

Internal

E*ternal



Attac"er Model/ Goal

OWASP
The Open Web Application Security Project

- Get access to the internal net , or"
- Attac" internal ser3ices
- Steal data &rom the user.

Attac"er Model/ $ocation

OWASP
The Open Web Application Security Project

$ocal

!emote

) hat is the pro4lem-

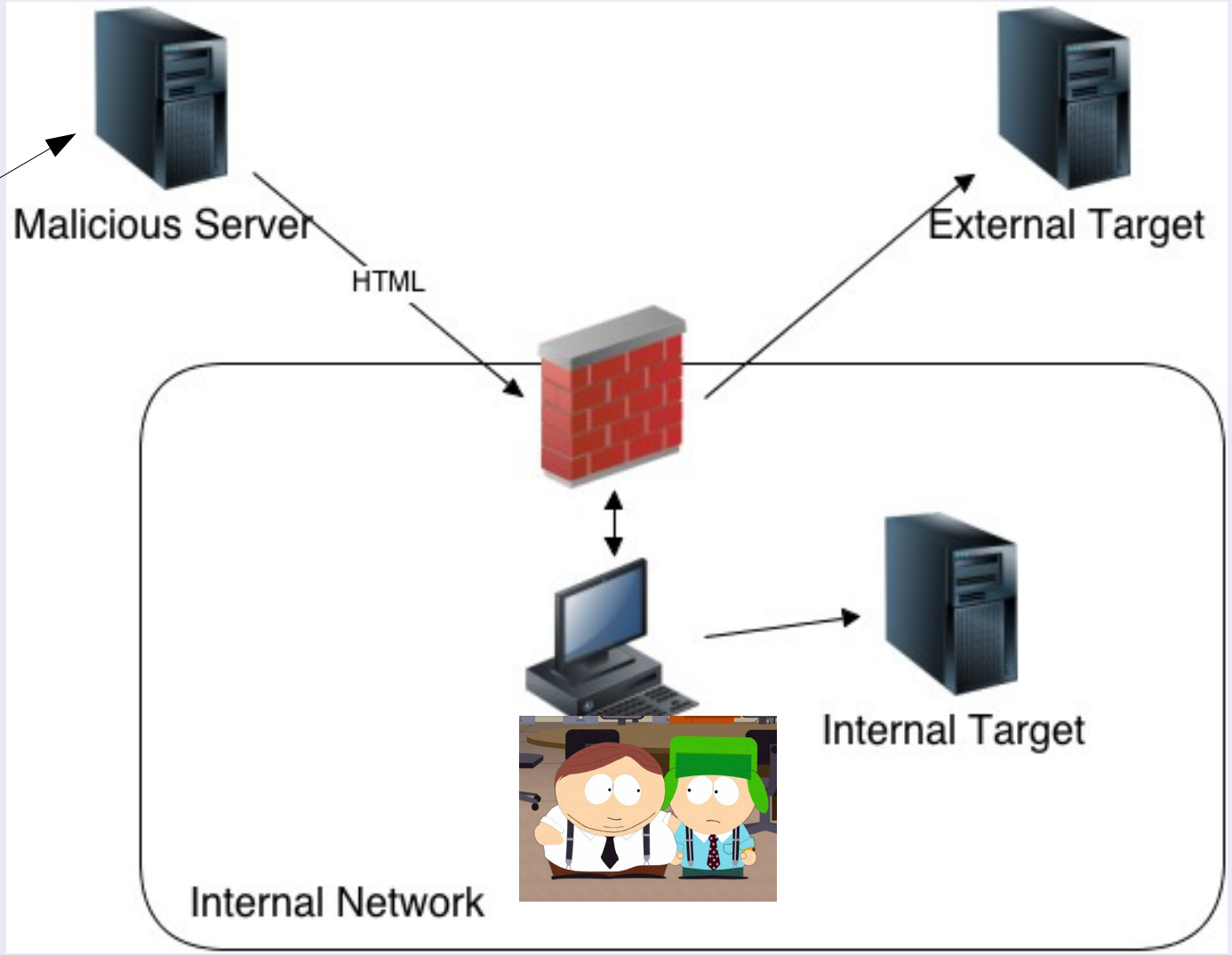
Attac" scenarios

OWASP
The Open Web Application Security Project

C !S is 7ust a tool2 not a 3ulnera4ility.

Attac" scenarios/ CS!8 recap

OWASP
The Open Web Application Security Project



Attac" Scenarios

OWASP
The Open Web Application Security Project

- Multistage CS!8
- Cross-domain data the&t
- Comple* +a3aScript attac" scenarios
- Pi3oting 9OeE8:
- Net , or" Enumeration
- 8ile upload CS!8

E*ample/ 8ile upload CS!8

OWASP
The Open Web Application Security Project

```
---------------------------256672629917035
Content-Disposition: form-data; name="file"; filename="test2.txt"
Content-Type: text/plain
test3
---------------------------256672629917035
```

```
<html>
 <body>
  <script>
   function submitRequest()
   {
    var xhr = new XMLHttpRequest();
    xhr.open("POST", "https://example.com/new_file.html", true);
    xhr.setRequestHeader("Accept", "text/html,application/xhtml+xml;q=0.9,*/*;q=0.8");
    xhr.setRequestHeader("Accept-Language", "de-de,de;q=0.8,en-us;q=0.5,en;q=0.3");
    xhr.setRequestHeader("Content-Type", "multipart/form-data;
 boundary=--------------------------25667262991703 5");
    xhr.withCredentials = "true";
    var body = "--------------------------25667262991703 5\r\n" +
     "Content-Disposition: form-data; name=\"file\"; filename=\"test2.txt\"\r\n" +
     "Content-Type: text/plain\r\n" +
     "\r\n" +
     "test3\r\n" +
     "--------------------------25667262991703 5--\r\n";
    var aBody = new Uint8Array(body.length);
    for (var i = 0; i < aBody.length; i++)
     aBody[i] = body.charCodeAt(i);
    xhr.send(new Blob([aBody]));
   }
  </script>
  <form action="#">
   <input type="submit" value="Submit request" onclick="submitRequest();" />
  </form>
 </body>
</html>
```

Pretty strong limitations

$imitations/) rite only re(uests

OWASP
The Open Web Application Security Project

XmlHttpResponse is not readable if:

- No Access-Control-Allo , - rigins header
- Source origin is not allo , ed in A-C-Allo , - rigins
-) ithCredentials is true 4ut A-C-A- ;<

0ear in mind/ the re(uests are still sent=

$imitations/ Pre&light !e(8ails

OWASP
The Open Web Application Security Project

I& one o& the re(uirements o& the pre-&light re(uest is not satis&ied2 the original re(uest , ill not 4e sent.

```
OPTIONS /cors HTTP/1.1
Origin: http://api.bob.com
Access-Control-Request-Method: PUT
Access-Control-Request-Headers: X-Custom-Header
Host: api.alice.com
Accept-Language: en-US
Connection: keep-alive
User-Agent: Mozilla/5.0
```

Solution

OWASP
The Open Web Application Security Project

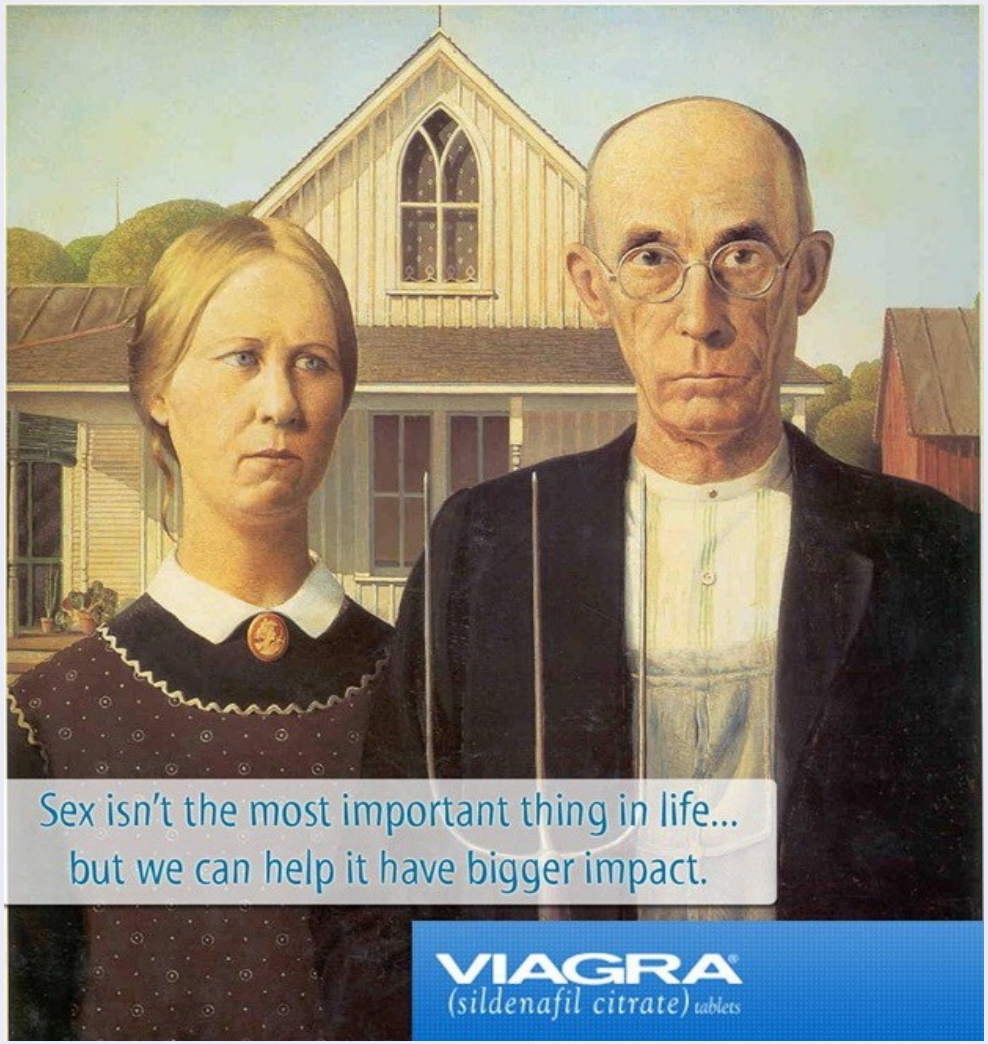
- More a , areness on the 4asics o& C !S
- Strict Allo , - rigin settings
- !e7ecting Allo , -Credential re(uests
- Change o& mindset/ de3elopment pro4lem

#ardening

OWASP
The Open Web Application Security Project

Can and need to 4e done on 3arious le3els/

-) e4ser3er
- Application



OWASP
The Open Web Application Security Project

- mod>headers
- In con&ig or .htaccess
- ?Directory@2 ?$ocation@2 ?8iles@ or ?Airtual#ost@

OWASP
The Open Web Application Security Project

Application logic should consider C !S and set the appropriate headers.

i.e./ ASP .NET/

DEM

OWASP
The Open Web Application Security Project

No animals , ere harmed in the ma''ing o& these demos.

OWASP
The Open Web Application Security Project

Than" you=

Gergely !e3ay
http/55gerionsecurity.com
Dgeri>re3ay

Resources:

- http://www.w3.org/TR/cors/
- http://www.html5rocks.com/en/tutorials/cors/
- https://code.google.com/p/html5security/wiki/CrossOriginRequestSecurity
- https://developer.mozilla.org/en-US/docs/HTTP/Access_control_CORS