

## 클래스카드 해킹 - 2023/9/24

클래스카드의 매칭게임을 한 후 /Match/save로 보내지는 페이로드의 일부를 가져왔다.

```
score 100
파일 편집 보기
arr_key[]: l
arr_key[]: k
arr_key[]: v
arr_key[]: g
arr_key[]: s
arr_key[]: n
arr_key[]: f
arr_key[]: h
arr_key[]: b
arr_key[]: e
arr_key[]: z
arr_key[]: y
arr_key[]: i
arr_key[]: d
arr_key[]: r
arr_key[]: t
arr_key[]: u
arr_key[]: o
arr_key[]: m
arr_key[]: j
arr_key[]: w
arr_key[]: q
arr_key[]: a
arr_key[]: p
arr_key[]: c
arr_key[]: x
arr_score[0][t]: kfennshbss.gge
arr_score[0][s]: 1
arr_score[0][m]: k
arr_score[1][t]: kfennshbnf.s
arr_score[1][s]: n1
arr_score[1][m]: 1
arr_score[2][t]: kfennshbfh.bhf
arr_score[2][s]: n1
arr_score[2][m]: k
arr_score[3][t]: kfennshbhh.hek
arr_score[3][s]: 1
arr_score[3][m]: k
arr_score[4][t]: kfennshbel.fhg
arr_score[4][s]: 1
arr_score[4][m]: k
arr_score[5][t]: kfennshelg.nsn
arr_score[5][s]: 1
arr_score[5][m]: k
arr_score[6][t]: kfennshesl.lvv
arr_score[6][s]: 1
arr_score[6][m]: k
arr_score[7][t]: kfennshenk.gbn
arr_score[7][s]: 1
arr_score[7][m]: k
arr_score[8][t]: kfennshefv.hge
arr_score[8][s]: 1
줄 5, 열 13
```

이 페이로드의 arr\_key와 arr\_score 부분이 아마 점수와 관련된 데이터라고 추측한다.  
 그래서 Match 폴더에 존재하는 스크립트에서 arr\_score가 어디에 정의되어있는지 확인했다.

```
function _0x402d01(_0x535f55) {
  var _0x431a98 = _0x5abd1f
    , _0x7ccfe1 = _0x2cfd8f;
  $data = {
    'set_idx': set_idx,
    'arr_key': ggk['a'](),
    'arr_score': _0x4adb0f,
    'activity': 0x4,
    'class_idx': class_idx,
    'user_name': _0x535f55,
    'tid': tid
  },
  jQuery[_0x7ccfe1(0x1d5)]({
    'url': _0x431a98(0x180),
    'global': ![],
  });
}
```

다음과 같이 'arr\_score' 부분을 어떤 데이터가 덮어쓰우는 구조로 되어있다.  
 이 데이터도 이 스크립트에서 검색을 해봤다.

```
- continue;
- case '2':
-   var _0x47a8a4 = ![]; _0x47a8a4 = true
-   continue;
- case '3':
-   _0x14eeeb += _0x346eec; _0x346eec = 100
-   continue;
- case '4':
-   _0x380501[_0x5d2370(0x492)](_0x346eec, 0x0) ? _0x4adb0f['push'](_0x380501[_0xe14a06(0x1eb, '7m8W')]) : _0x4adb0f['push'](ggk['d'](_0x346eec, 0x1));
-   continue;
- case '5':
-   var _0x346eec = 0x0;
-   continue;
- case '6':
-   _0x14eeeb == -0x1 && (_0x14eeeb = 0x64);
-   continue;
```

```
_0x380501[_0x5d2370(0x492)](_0x346eec, 0x0) ?
_0x4adb0f['push'](ggk['d'](_0x380501[_0xe14a06(0x1eb, '7m8W')]) : _0x4adb0f['push'](ggk['d'](_0x346eec, 0x1));
```

이때 어떤 조건에 의해서 arr\_score 배열에 ggk.d의 함수값을 추가하는 것으로 보이는데,  
 그럼 이 ggk 함수가 어떻게 구현되어있는지 확인해보자.

```
###AUDIO### <audio preload="auto" src="
###AUDIO### set playbackrate
> ggk
< ▶ {a: f, b: f, c: f, d: f}
> |
```

다음과 같이 ggk가 전역변수로 저장되어있다.  
 매칭 게임을 할때마다 ggk의 값이 변하는 것 같다.

```
var ggk = {
```

```

a: function () {
  return [
    "x",
    "b",
    "u",
    "q",
    "y",
    "g",
    "a",
    "t",
    "h",
    "s",
    "z",
    "j",
    "p",
    "r",
    "k",
    "c",
    "f",
    "l",
    "n",
    "w",
    "m",
    "d",
    "o",
    "e",
    "l",
    "v",
  ];
},
b: function () {
  return "basgggbxqy.buug";
},
c: function (a) {
  var r = "";
  var a =String(a);
  var k =this.a();
  for (var i =0; i < a.length; i++) {
    var ii = a.charAt(i);
    if (ii == ".") {
      r += ".";
      continue;
    }
    ii =eval(ii);
    if (ii < k.length) {
      r += k[ii];
    }
  }
  return r;
},
d: function (a, b) {
  return { t: ggk.c(new Date().getTime() /1000), s: ggk.c(a), m: ggk.c(b) };
},
};

```

ggk 코드를 가져왔다. ggk.a에는 arr\_key가, ggk.d는 t: ggk.c에 현재 초를 넣은 함수값, s에는 첫 번째 파라미터를 ggk.c에 넣은 함수값, m는 두 번째 파라미터를 ggk.c에 넣은 것이다.

ggk.c를 살펴보자면, 받은 파라미터를 각 자리의 문자를 ggk.a의 문자로 치환하는 것으로 볼 수 있다.

그럼 ggk.d가 어떻게 이용되는지 한번 알아보자.

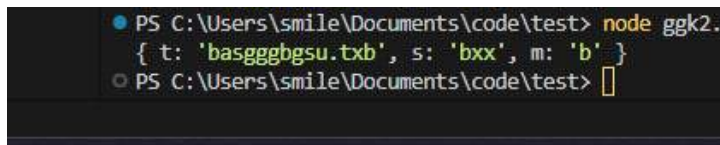


단어 한 개를 매칭에 성공한 후의 arr\_score의 값이다.

또한

```
console.log(ggk["d"])(100, 0x1));
```

를 실행한 결과는



s 값과 m값이 정확히 일치하는 것을 볼 수 있다.

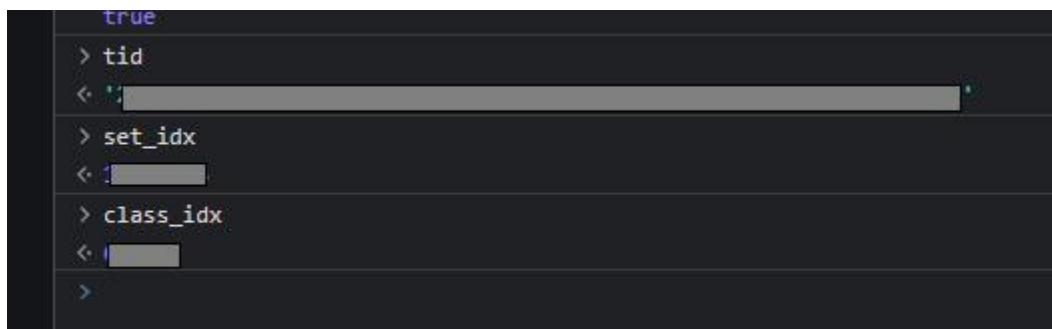
그러므로 ggk.d의 첫 번째 인자에는 이벤트로 인해서 얻게 된 점수가 들어가는 것을 확인할 수 있다.

그럼 우리는 ggk의 t를 조금 수정하고

```
ggk["d"](100, 0x1))
```

를 누적시켜, arr\_score 값을 생성해낼 수 있다.

그래서 arr\_score의 이차배열이 이벤트를 모두 모은 것, 이벤트는 t, s, m으로 구성되어있는 것임을 알 수 있다.




또한, 페이로드에 필요한 tid, set\_idx, class\_idx 모두 전역변수로 저장되어있는 것을 확인할 수 있다.

그리고, activity는 코드 상에서 0x4로 고정되어있는 것을 조금 전의 사진에서 확인할 수 있다.

그럼 한번 직접 해보자.

<https://www.instagram.com/reel/CxkzvgeM5PQ/>



매칭

780100점

최고기록