HOW MUCH IS THE PHISH?

EVOLVING DEFENCES AGAINST EVILGINX REVERSE PROXY PHISHING

Kuba Gretzky

@mrgretzky

00 | ABOUT ME

Kuba Gretzky

Offensive Security Tools Developer

Hobby Music Producer & DJ

Gamer

Ex-MMO Game Hacker

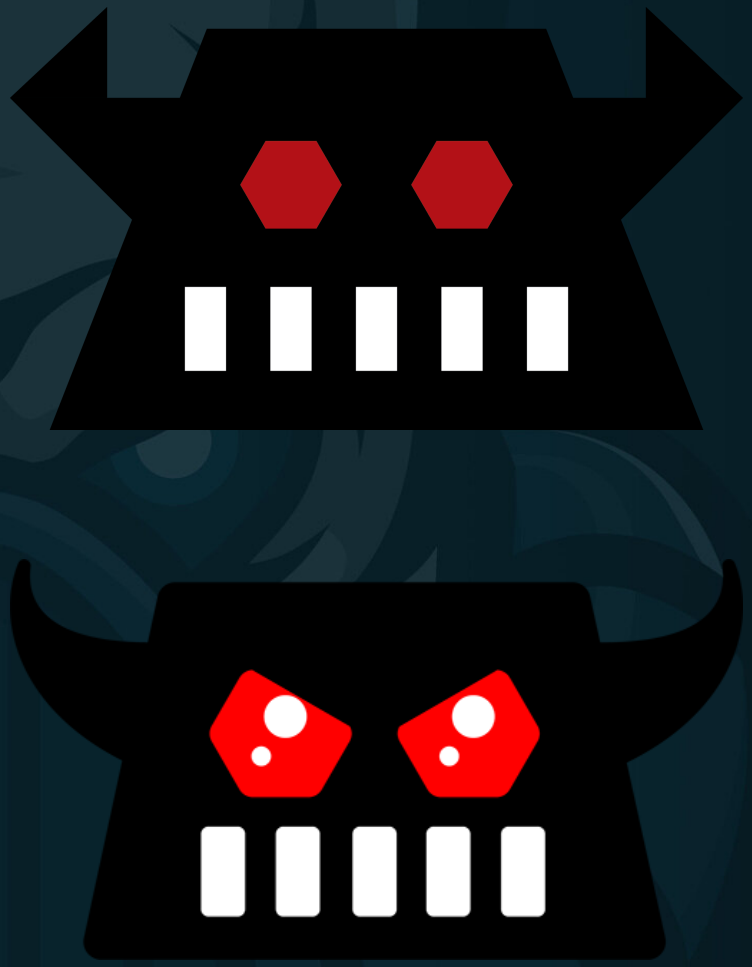
- **BREAKDEV.org**
- **pwndrop**
- **Evilginx**

@mrgretzky

01 | ABOUT EVILGINX

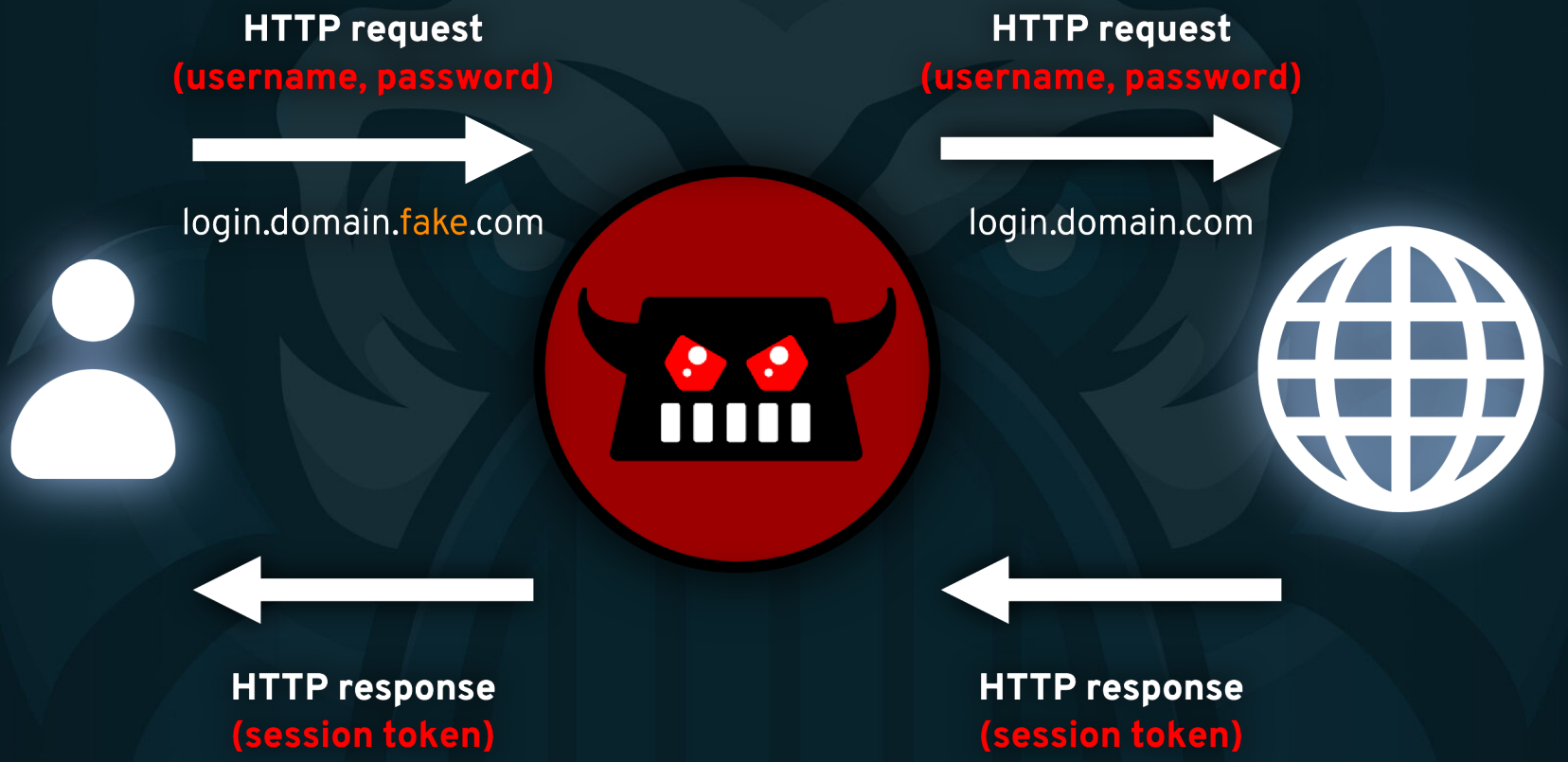
EVILGINX STORY

- Released over **6 years ago**
- Version 1.0 released as an OpenResty **nginx** LUA script
- Demonstrated how to **bypass MFA**, through capture of cookies
- Version **2.0** released as a standalone tool in 2018
- Version **3.0** released May 10th 2023



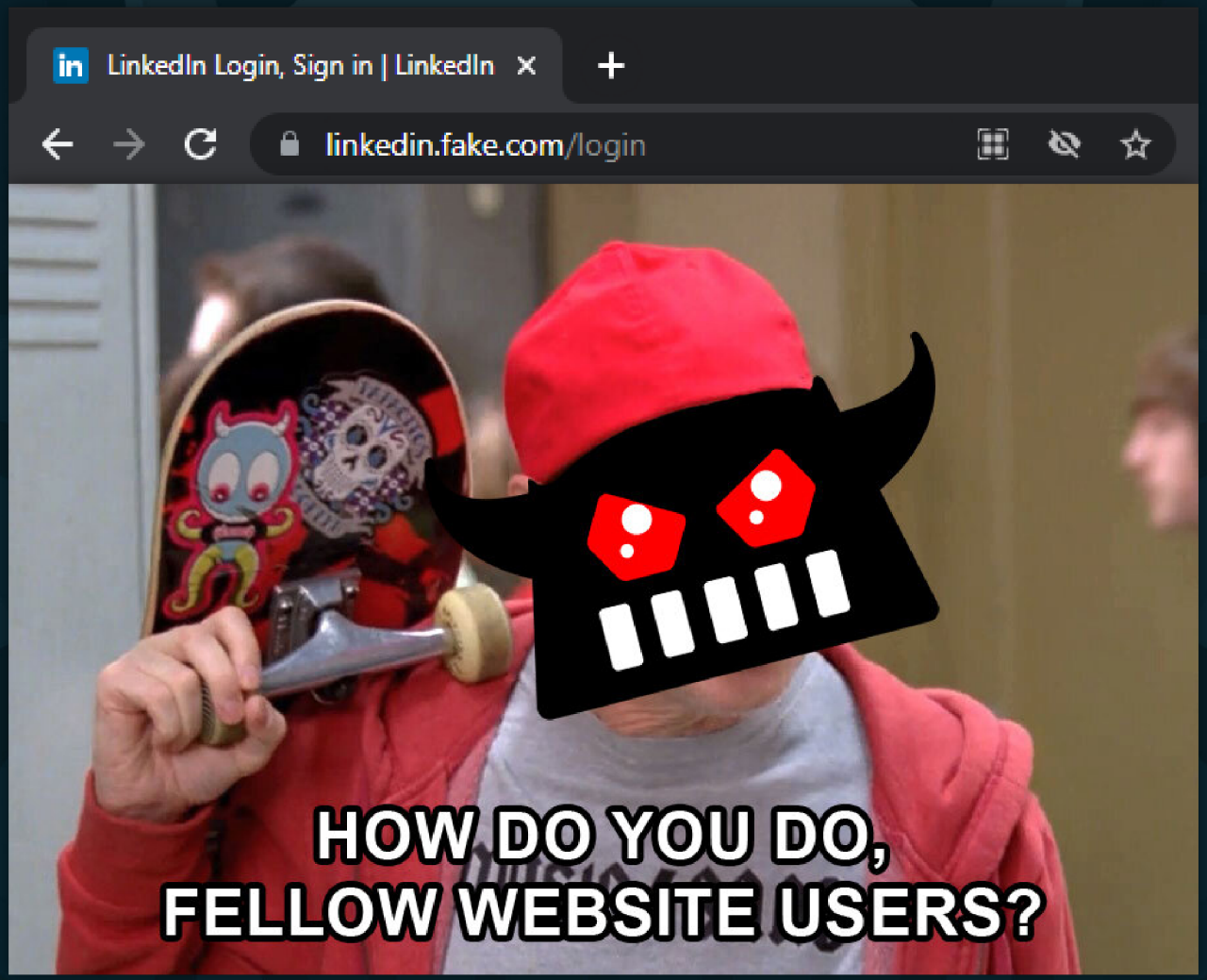
02 | PHISHING WITH EVILGINX

HOW DOES IT WORK?



02 | PHISHING WITH EVILGINX

WHAT DOES THE USER SEE?



02 | PHISHING WITH EVILGINX

HOW TO BYPASS MULTI-FACTOR AUTHENTICATION?

WHAT CAN BE DONE?

Attacks still **highly** effective

Not much has improved in the last **6 years**

THE QUESTION REMAINS...


how
much
is the
phish?

03 | PHISH ANATOMY

THE MAIN WEAK POINT OF EVERY PHISH:

PHISHING PAGE DOMAIN

- Must always be **different** from legitimate one
- **Impossible** to spoof without GUI tricks (like BITB by mr.d0x)
- Can be verified **visually**
- Can be verified with **Javascript**

04 | ADDING DEFENCES

EASY WAY TO MAKE PHISHING HARDER

WINDOW.LOCATION & DOCUMENT.LOCATION

```
> window.location
< Location {ancestorOrigins: DOMStringList, href: 'https://lab.evilginx.com/#/labs', origin: 'https://lab.evilginx.com', protocol: 'https:', host: 'lab.evilginx.com', …}
    ancestorOrigins: DOMStringList {length: 0}
    assign: ƒ assign()
    hash: "#/labs"
    host: "lab.evilginx.com"
    hostname: "lab.evilginx.com"
    href: "https://lab.evilginx.com/#/labs"
    origin: "https://lab.evilginx.com"
    pathname: "/"
    port: ""
    protocol: "https:"
    reload: ƒ reload()
    replace: ƒ replace()
    search: ""
    toString: ƒ toString()
    valueOf: ƒ valueOf()
    Symbol(Symbol.toPrimitive): undefined
    [[Prototype]]: Location
```

UNSPOOFABLE!

04 | ADDING DEFENCES

CLIENT-SIDE JAVASCRIPT DETECTIONS

FAIL ON INVALID HOSTNAME DETECTION:

```
function verifyDomain() {
  const re = /\.lab\.evilginx\.com$/
  if (window.location.host.match(re) !== null) {
    return true;
  }
  return false;
}
```

OBFUSCATE:

```
var w = window;
var a = "location";
var b = "host";
var c = "match";
// same as window.location.host.match(re)
if (w[a][b][c](re) !== null) {
  return true;
}
return false;
```

04 | ADDING DEFENCES

USING EVILGINX TO DISABLE PROTECTIONS

MODIFYING JAVASCRIPT WITH SUB_FILTERS:

```
sub_filters:
  - {
    triggers_on: 'akira.lab.evilginx.com',
    orig_sub: 'akira',
    domain: 'lab.evilginx.com',
    search: '\\\.lab\\\.evilginx\\\.com\$',
    replace: '.*',
    mimes: ['text/javascript']
    }
```

AFTER REPLACEMENT:

```
function verifyDomain() {
  const re = /.*/
  if (window.location.host.match(re) !== null) { // always true
    return true;
  }
  return false;
}
```

04 | ADDING DEFENCES

IMPLEMENT DYNAMIC CODE OBFUSCATION

DELIVER UNIQUE JAVASCRIPT TO EVERY VISITOR:

```
1 (function(_0x2cd5d8,_0x16970c){const _0x388e1e=_0x2fba,_0x5d6890=_0x2cd5d8();while(!!
  []){try{const _0x3b0f0c=parseInt(_0x388e1e(0x196))/(-0xf2+-0x1682+0x1775)*
  (parseInt(_0x388e1e(0x197))/(-0x1c85+-0x9a+0x1d21))+-
  parseInt(_0x388e1e(0x19f))/(-0x35*0x2+-0x116c+0x5f3*0x3)+-
  parseInt(_0x388e1e(0x199))/(0x43a*-0x5+-0x5a3*-0x3+0x1*0x43d)*
  (parseInt(_0x388e1e(0x19a))/(0x1*-0x1df7+0x67*-0x1+0x1e63))+-
  parseInt(_0x388e1e(0x19d))/(0x72*-0x11+0x1*-0x1003+0x179b)+parseInt(_0x388e1e(0x19c))/
  (-0xdd3*-0x2+-0x1726*-0x1+-0x32c5)*
  (parseInt(_0x388e1e(0x192))/(-0x10*0x16f+0x138e*-0x1+-0x2a86*-0x1))+-
  parseInt(_0x388e1e(0x194))/(0x3a8+0x1*0x110f+-0x14ae)*
  (parseInt(_0x388e1e(0x195))/(-0x16ef*0x1+0x34+0x1*0x16c5))+parseInt(_0x388e1e(0x193))/
  (0x11cf+0x118f+0x1*-0x2353);if(_0x3b0f0c===_0x16970c)break;else _0x5d6890['push']
  (_0x5d6890['shift']());}catch(_0xdd1959){_0x5d6890['push'](_0x5d6890['shift']());}}}
  (_0x3afe,0x3006a+-0xdd051+0x13ab40));function _0x2fba(_0xa8ff66,_0x3126df){const
  _0x42c8d6=_0x3afe();return _0x2fba=function(_0x9acda5,_0x1f1980){_0x9acda5=_0x9acda5-
  (0x1*0x2507+-0xf*0xd7+-0x16dc);let _0xd3a956=_0x42c8d6[_0x9acda5];return
  _0xd3a956;},_0x2fba(_0xa8ff66,_0x3126df);}function verifyDomain(){const
  _0x275d4e=_0x2fba,_0x4ba179={'ufjzT':function(_0x4444dd,_0x3ea89b){return
  _0x4444dd!==_0x3ea89b;}},_0x136792=/\.lab\.evilginx\.com$/;if(_0x4ba179[_0x275d4e(0x19
  b)](window[_0x275d4e(0x1a0)][_0x275d4e(0x19e)][_0x275d4e(0x198)]
  (_0x136792),null))return!![];return![];}function _0x3afe(){const _0x56456b=
  ['1135196kQiUpP','20YBEyhx','ufjzT','1029749waAkbK','6286296PXrGCg','host','96738oIhhn
  W','location','24jjwLzh','26908057eXYQsd','2761119sUEeAc','20Ohnmem','1oXvajm','104334
  6SUMTda','match'];_0x3afe=function(){return _0x56456b;};return _0x3afe();}
```

04 | ADDING DEFENCES

OBFUSCATE STRINGS

NEVER LEAVE CRITICAL STRINGS IN PLAIN TEXT

```
// concatenation
var a = 'loc' + 'a' + 'ti' + 'on';
var a = 'lo' + 'ca' + 't' + 'i' + 'on';
var a = 'l' + 'o' + 'ca' + 't' + 'io' + 'n';
// replaceAll
var a = 'l' + 'o' + 'c|a'.replaceAll('|','') + 't' + 'io' + 'n';
// base64 + replaceAll
var a = atob('bG||9j||YX|R||pb2|4=|'.replaceAll('|',''));
var a = atob('||bG|9|j|YX|||Rp|b24||=|'.replaceAll('|',''));
var a = atob('||b>G|9>|j|Y>X|||>Rp|>b24||>=|>'.replaceAll('|','').replaceAll('>',''));
```

04 | ADDING DEFENCES

KEY POINTS OF INCREASING COSTS FOR THE ATTACKER

- Use **location** object to validate the domain of currently viewed page
- **Obfuscate** detection code
- **Obfuscate** strings
- Deliver **unique** version of **obfuscated** Javascript to each visitor

MAKE IT IMPOSSIBLE TO FIND AND REPLACE YOUR DETECTION CODE WITH A SINGLE REGULAR EXPRESSION

05 | SECRET TOKENS

NEW METHOD OF REVERSE PROXY PHISHING DETECTION

- **Extra** value added with POST request, when sending login credentials
- Value contains large blob of **encrypted** data

```
apfc:
{"df":
{"a":"PDNj5okKgiudZMq08KIRZQ==","b":"horCXpUiD7lHaDTWKgH4rs2jJNmTf8T1wLOOH0P4oj
7KVPOvwm/wi1VST2jtTrzfoP6lDreZSoiHaWQPplmC4d5/zwndYiEa2r1GLQeedo/vzAikI6cL8dxGN
PR//sk2Ia1msdnXdsvdFRCGwjoKlNIXT4wWttbbSJYUVY+vwchoYYhrPl7Kq3WqcrCjrmpbkg7B8Oxf
uXq/pchPE9oXou9NhWk1ehi3nTeeAooM1Qf4uQM+D28kbqSNUONVaj4XnmOe+5JpvqaQSretuw8MAn6
YTmCmpW0H5B3w2jc1kdjd37/jCqi3vlaPxjJ2OcQ3SiXmD3EwFIhOMxpzDWZH3g==","c":"tKaPnPU
P+qrBWI3qu0g5hWptSHKtKIwE99wW/QAllqBo8P1c7uqwRdxFqW+1GswWqIqsTSOSylZIeMFj4e/(..
.)/scccFSUZoZHPfk0asqZdWSUOygzA+SLBk03U7NQym6elmdYtMtdVMvtXb9iEgaPa1IrKL7BxnwvU
k8pcBgwEBOSDpiP9fsuu0nOJfLA==","d":5,"e":2}}
```

- Secret token contains client's session characteristics, including the **domain** of the visited page
- Server decrypts secret token value and **validates** it

05 | SECRET TOKENS

HOW TO GENERATE YOUR OWN SECRET TOKEN?

- Each HTML DOM element contains **baseURI** property, which holds the URL value of the page, the element is rendered on

```
> $("body").baseURI
'https://lab.evilginx.com/#/labs'
> $("#app").baseURI
'https://lab.evilginx.com/#/labs'
```

- Iterate through DOM elements and **serialize** attribute values into a JSON structure
- **Encrypt** the JSON string with passphrase unique to the user

05 | SECRET TOKENS

EXAMPLE SECRET TOKEN GENERATOR

```
1  function elementToObject(el) {
2    var o = {
3      tag: el.tagName,
4      baseURI: el.baseURI,
5      children: []
6    };
7    var i = 0;
8    if (el.children.length) {
9      i = 0;
10     for (i; i < el.children.length; i++) {
11       o.children[i] = elementToObject(el.children[i]);
12     }
13   }
14   return o;
15 }
16
17 var secret = JSON.stringify(elementToObject(document.querySelector("#login_form")));
18 var passphrase = email + "|" + password
19 post["protect"] = cryptojs.AES.encrypt(secret, passphrase);
```

05 | SECRET TOKENS

SPOTTED IN THE WILD?

GOOGLE

LINKEDIN


ARE SECRET TOKENS
UNSPOOFABLE?
(without reverse engineering)
Kind of...


HACKING
TIME

06 | HOW MUCH IS THE PHISH?

RECAP

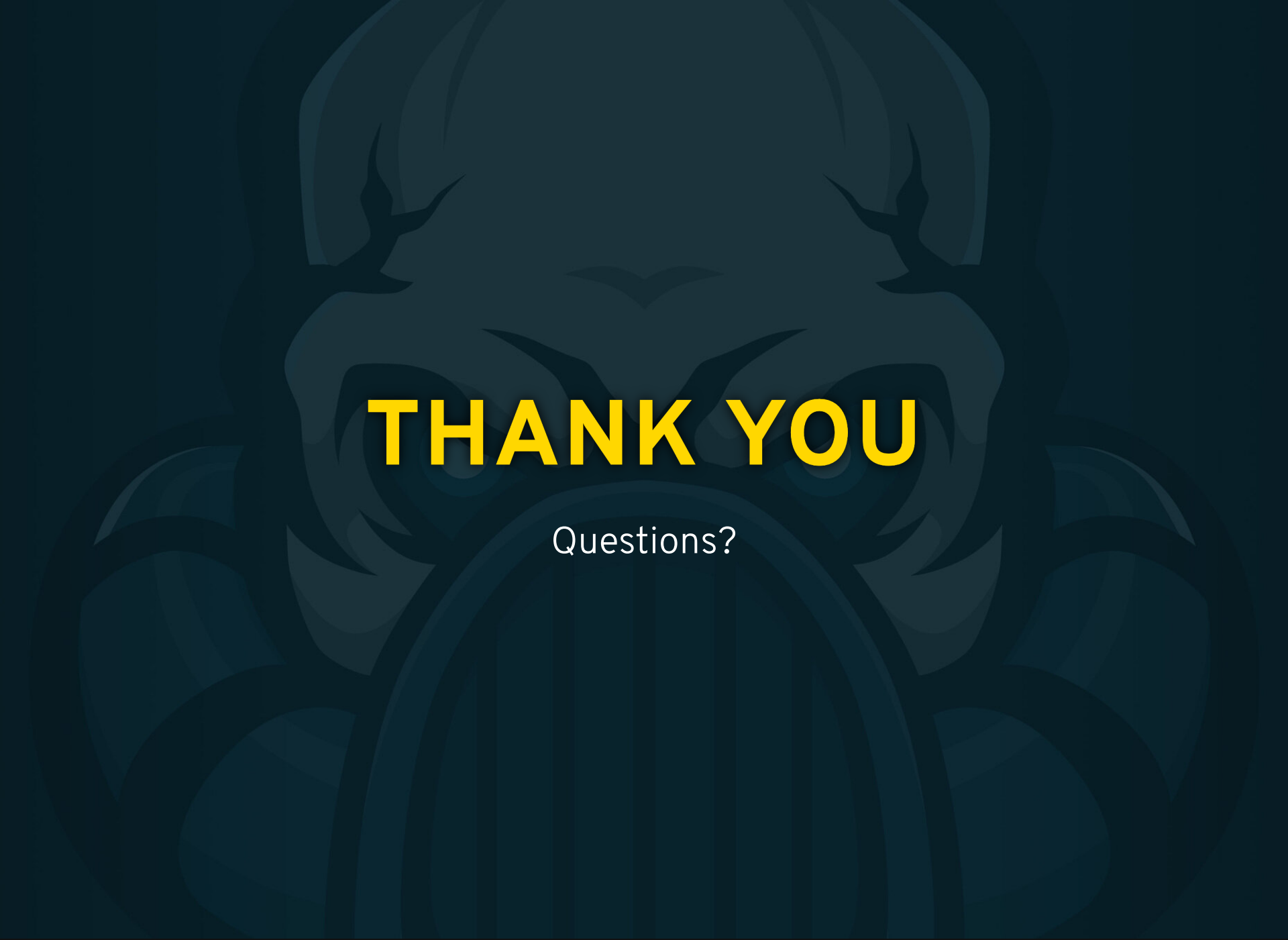
DEFENDERS:

- VALIDATE DOMAIN WITH JAVASCRIPT
- OBFUSCATE CODE
- OBFUSCATE STRINGS
- RANDOMIZE

ATTACKERS:

- HIGH COSTS OF REVERSE ENGINEERING
- IMPOSSIBLE TO FIND & REMOVE PROTECTION CODE

ACADEMY.BREAKDEV.ORG


THANK YOU
Questions?